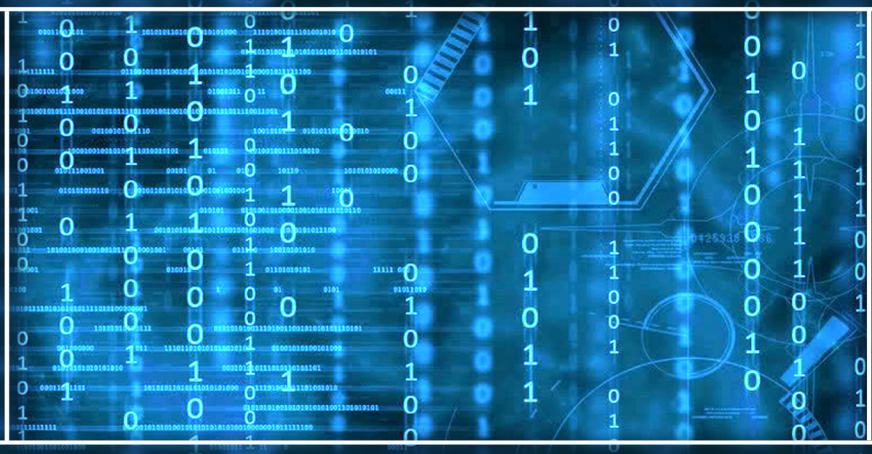
IJACSA
WHERE WISDOM SHARES
International Journal of Advanced Computer Science and Applications

Volume 15 Issue 11
November 2024



ISSN 2156-5570(Online)
ISSN 2158-107X(Print)

www.ijacsa.thesai.org

Editorial Preface

From the Desk of Managing Editor…

It may be difficult to imagine that almost half a century ago we used computers far less sophisticated than current home desktop computers to put a man on the moon. In that 50 year span, the field of computer science has exploded.

Computer science has opened new avenues for thought and experimentation. What began as a way to simplify the calculation process has given birth to technology once only imagined by the human mind. The ability to communicate and share ideas even though collaborators are half a world away and exploration of not just the stars above but the internal workings of the human genome are some of the ways that this field has moved at an exponential pace.

At the International Journal of Advanced Computer Science and Applications it is our mission to provide an outlet for quality research. We want to promote universal access and opportunities for the international scientific community to share and disseminate scientific and technical information.

We believe in spreading knowledge of computer science and its applications to all classes of audiences. That is why we deliver up-to-date, authoritative coverage and offer open access of all our articles. Our archives have served as a place to provoke philosophical, theoretical, and empirical ideas from some of the finest minds in the field.

We utilize the talents and experience of editor and reviewers working at Universities and Institutions from around the world. We would like to express our gratitude to all authors, whose research results have been published in our journal, as well as our referees for their in-depth evaluations. Our high standards are maintained through a double blind review process.

We hope that this edition of IJACSA inspires and entices you to submit your own contributions in upcoming issues. Thank you for sharing wisdom.

Thank you for Sharing Wisdom!

Kohei Arai
Editor-in-Chief
IJACSA
Volume 15 Issue 11 November 2024
ISSN 2156-5570 (Online)
ISSN 2158-107X (Print)

Editorial Board

CONTENTS

Predicting Cervical Cancer Based on Behavioral Risk Factors

Rakeshkumar Mahto[1], Kanika Sood[2]
Department of Electrical and Computer Engineering, California State University, Fullerton, California 92831, USA[1]
Department of Computer Science, California State University, Fullerton, California 92831, USA[2]

***Abstract*—Machine learning (ML) based predictive models are increasingly used in various fields due to their ability to find patterns and interpret complex relationships between variables in an extensive dataset. However, getting a comprehensive dataset is challenging in the field of medicine for rare or emerging infections. Therefore, developing a robust methodology and selecting ML classifiers that can still make compelling predictions even with smaller and imbalanced datasets is essential to defend against emerging threat or infections. This paper uses behavioral risk factors to predict cervical cancer risk. To create a robust technique, we intentionally selected a smaller imbalanced dataset and applied Adaptive Synthetic (ADASYN) sampling and hyperparameter tuning to enhance the predictive performance. In this work, hyperparameter tuning, evaluated through 3-fold cross-validation, is employed to optimize the performance of the Random Forest, XGBoost, and Voting Classifier models. The results demonstrated high classification performance, with all models achieving an accuracy of 97.12%. Confusion matrix analysis further revealed the models' robustness in identifying cervical cancer cases with minimal misclassification. A comparison with previous work confirmed the superiority of our approach, showcasing improved accuracy and precision. This study demonstrates the potential of ML models for early screening and risk assessment, even when working with limited datasets.**

***Keywords*—Cervical cancer; random forest; voting classifier; Adaptive Synthetic Sampling (ADASYN); predictive model**

I. Introduction

According to WHO, cervical cancer is the fourth most prevalent cancer in women across the globe [1]. The same report highlights that 94% of fatalities happening due to cervical cancer are in low and middle-income countries [1]. However, according to [2], globally, only 36% of women aged 30-49 have been screened for cervical cancer. This is due to a host of social determinants, including socioeconomic status, access to care, and behavioral risks, which make detecting and preventing these types of cancer earlier extremely challenging. Cervical cancer is primarily caused by prolonged infection with high-risk human papillomavirus (HPV) types, and it can be prevented through early-stage screening and vaccination. Various well-established screening methods exist, including Pap smears [3], [4], [5] and HPV DNA [6], [7], [8] testing. Unfortunately, due to the high cost of diagnosis, lack of infrastructure, and awareness in underdeveloped countries, these techniques failed to make an impact. With these limitations in mind, researchers and healthcare professionals are now examining the implementation of predictive models to help identify high-risk individuals for developing cervical cancer. This area of interest is particularly relevant when it comes to using behavioral and social risk factors known to be associated with cervical cancer occurrence (e.g., sexual activity, diet, and personal/intimate hygiene). Integrating these factors in prognostic models efficiently improves current screening techniques that lead to early detection and provide personalized care.

Several research studies have identified various factors that contribute to the development of cervical cancer. Kadir et al. in [9], found that sexual behaviors such as early sexual activity and multiple sexual partners, poor diet, inadequate personal hygiene, and lack of social support are key risk factors that result in cervical cancers. Additionally, a woman's behavioral and mental state can affect their ability to participate in regular screening, follow preventive measures that include HPV vaccination, and adhere to the treatment plan. Thus, having a predictive model equipped with such knowledge will enhance its ability to identify women at higher risk. These kinds of models can also contribute to better allocation of resources by prioritizing those individuals who might otherwise not seek care.

In recent times, machine learning (ML) has increasingly been integrated into the medical diagnostic arena due to its ability to analyze large amounts of data, identify trends, and make accurate predictions. ML models have been utilized to diagnose cervical cancer using behavioral, demographic, and clinical data [10]. In this research work [10], multiple ML models that include Random Forest, AdaBoost, Gradient Boost, MultiLayer Perceptron (MLP), eXtreme Gradient Boosting (XGB), Decision Tree, Logistic Regression, SVM, and Gaussian Naive Bayes (GNB) was trained on a dataset consisting of an individual's demographic data, medical history, sexual behavior, and reproductive health to predict early prediction of cervical cancer. Among all of them, XGB Classifier showed superior accuracy of 98% and ROC AUC of 99%. Similarly, in [11], various ML classifiers such as K-Nearest Neighbors (KNN), Linear Support Vector Machine (SVM), and Naive Bayes were trained using a dataset consisting of patients' demography, biopsy, and medical history. KNN outperformed in all metrics compared to the other two classifiers with an impressive accuracy of 97.59%.

Besides applying ML classifiers and getting trained on individuals' demography, biopsy, and medical history, Pap sear images, HPV DNA test results, and biopsy samples are also utilized for diagnosing Cervical cancer. For example, in the research work presented by Sholik et al., they applied a process that combines advanced methods from the neural network, convolutional neural network (CNN), and vision transformers to capture both detailed and overall patterns in images [12]. The dataset utilized for this work were Herlev [13], Mendeley LBC [14], and SIPaKMeD [15], which consists

of Pap smear images. They achieved an impressive accuracy of 100% with SVM, K-NN, MLP, and Logistic Regression (LR). Similarly, advanced deep learning models such as ResNet and GoogLeNet were employed to classify cervical cancer using Pap smear images [16]. Using fine-tuned ResNet18, a test accuracy of 98.51% was obtained. On the other hand, HPV viral load with bacterial vaginosis status was utilized to train an LR model for early diagnosis of cervical cancer [17]. The model achieved an impressive accuracy with AUC values ranging from 0.915 to 0.9614. However, the effectiveness and accuracy of these ML classifiers depend on the size and distribution of the dataset.

Class imbalance is one of the biggest problems while building predictive models for cervical cancer. The count of patients who are suffering from Cervical cancer is significantly less in real-world datasets as compared to the ones that do not suffer from this disease, which leads to an imbalanced dataset. This class imbalance of "cervical cancer" to "no cervical cancer" can significantly influence the performance of ML models, especially in terms of not being able to classify the minority group. In ML, specifically classification problems, the models tend to favor the majority class in case of imbalanced data, which results in higher overall accuracy but low sensitivity (i.e. the inability of the model to identify positive cases). In healthcare applications, this can be particularly problematic where the model fails to correctly identify individuals at risk of a fatal ailment like cervical cancer, which could lead to missed early intervention and prevention.

Besides class imbalance, the other issue in developing a robust ML model is the challenges in collecting comprehensive datasets, especially in resource-limited settings or the occurrence of rare and emerging infectious diseases. In this paper, we intentionally chose a smaller and imbalanced dataset [18] to demonstrate that advanced ML techniques can achieve high accuracy and precision. The success of the proposed model in achieving this goal will showcase the robustness and effectiveness of ML in predicting cervical cancer risk, even with a small and imbalanced dataset.

Additionally, in this paper, we analyze the impact of ML in the development of an efficient prediction model for cervical cancer using behavioral risk factors. In this work, we use Adaptive Synthetic Sampling (ADASYN) [19] to address the problem of class imbalance and smaller datasets to achieve better performance for distinguishing women who are at high risk of developing cervical cancer. The present study also intends to determine the potential of various behavioral risk factors significantly associated with cervical cancer by using feature importance analysis. This effort will lead to a greater understanding of the primary behavioral and social factors that may influence risk for cervical cancer, which ultimately results in further improvement in cervical cancer screening and prevention strategies. Additionally, the ML model developed in this work can be replicated and applied to rare diseases or those cases where getting a comprehensive dataset is challenging.

The remainder of this paper is organized as follows: Section II describes relevant work in cervical cancer prediction by applying ML techniques to behavior risk factors. This is followed by Section III, presenting the methodology utilized in this paper. This includes analyzing and describing the dataset used for training the various ML models, including Random Forest, XGBoost, and Voting Classifier. Results and discussion are presented in Sections IV and V, respectively, where the model's performance will be evaluated through various metrics like accuracy, precision, recall, and F1-score. Finally, Section VI concludes the paper where the implications of these findings are presented.

II. Relevant Work

ML models show great promise in diagnosing cervical cancer by leveraging behavioral risk factors. In cancer prediction, and especially for cervical cancer, behavioral risk factors play a more significant role compared to other datasets like clinical or genetic data. Behavioral information can be collected non-intrusively through surveys, interviews, or questionnaires, which makes it easier to collect, especially in resource-limited contexts where clinical tests such as Pap smears or genetic screening are scarce or too expensive for widespread use. Including behavioral information as input features for ML models can provide a more holistic view of all likely risk factors that may result in earlier detection and intervention. Various studies have been conducted to improve early detection using ML, which is significant for the treatment and increasing survival rates. For example, using the UCI machine learning repository with 32 features [20], Mehmood et al. achieved an accuracy of 93.6% with the Random Forest technique [21]. On the same dataset [20], Suman et al. attained an accuracy of 96.38% using BayeNet algorithm [22]. In another work on the same dataset [20], SMOTE and Random Forest were applied, yielding an accuracy of 85% [23]. Sun et al. developed a unique stacking-integrated machine learning (SIML) using the same dataset from UCI [20]. The SIML model combined multiple algorithms that included TreeBag, XGBoost, and MonMLP to achieve an AUC of 0.877, sensitivity of 81.8%, and specificity of 81.9%. Though various studies were conducted utilizing ML models to predict cervical cancer risk as presented in [20], [21], [22], [23], most have focused on demographic or clinical data, where behavioral factors were ignored entirely.

In another research work, Akter et al. applied the Decision Tree, Random Forest, and XGBoost on a different dataset at UCI machine learning repository dataset [18] with 19 attributes regarding behavior risk that can lead to cervical cancer [24]. Their ML model was able to achieve an accuracy of 93.33%. On the same dataset, various ML classifiers were applied that included Gaussian Naive Bayes (GNB), k Nearest Neighbor, and Decision Tree. Among all of them, GNB demonstrated a superior performance of 94% [25]. While the accuracy of ML models in predicting cervical cancer was impressive, most of these studies employ large datasets and balanced datasets, which do not reflect the real-world challenges of data scarcity and class imbalance, which are more prevalent in healthcare settings.

In most developing countries where the majority of the sufferers of cervical cancers reside, getting large and granular datasets is challenging due to inadequate health infrastructure, limitations of resources, and financial constraints. Additionally, cultural and logistical barriers become inhibiting factors for participant to share their information, making it challenging to create an extensive dataset. Given these constraints, it is vital to develop ML models that can perform well with a smaller

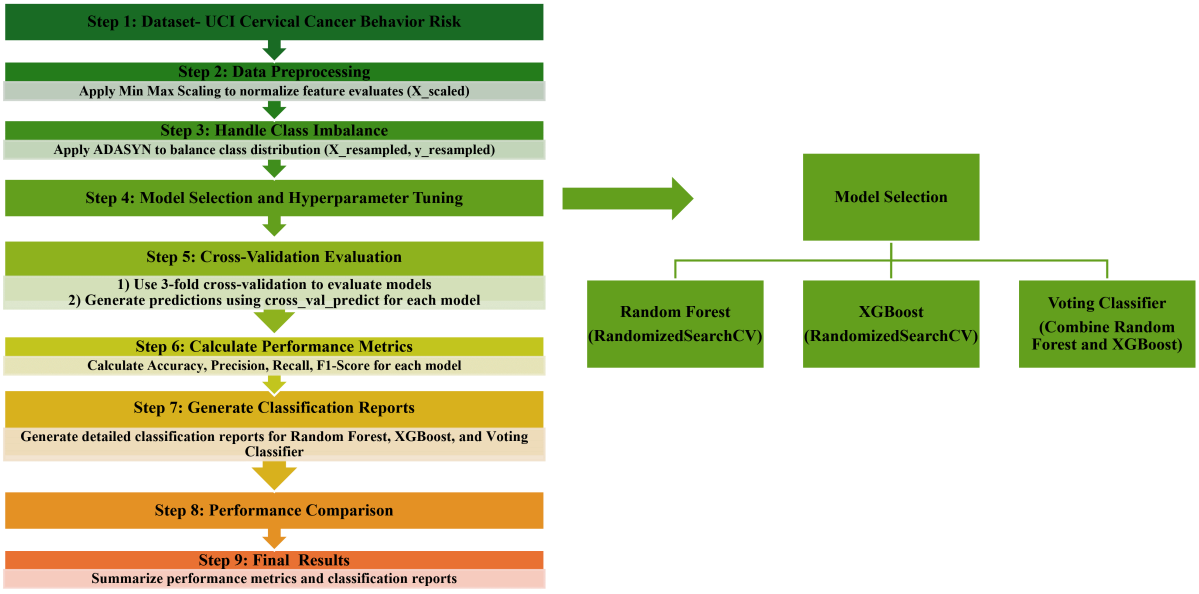


Fig. 1. Methodology flow diagram for developing an efficient prediction model for cervical cancer using behavioral risk factors.

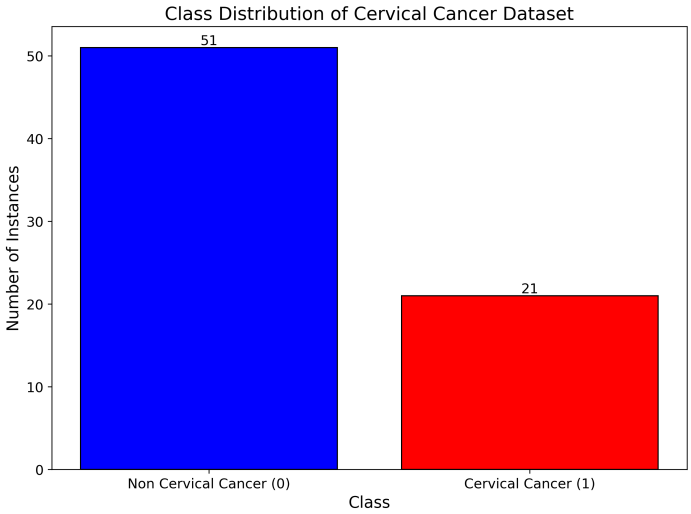


Fig. 2. Class distribution of the cervical cancer dataset.

number of data points and fewer attributes. Optimizing models to achieve high accuracy using few attributes will ensure that such models will remain useful when a comprehensive dataset is unavailable. These models are scalable, and their predictive performance can be further improved when trained on larger datasets.

III. Methodology

The methodology adopted for this work involves a comprehensive set of steps, including data preprocessing, handling class imbalance, hyperparameter tuning, model training, and evaluation using cross-validation techniques, as shown in Fig. 1.

A. Dataset Description

The dataset used in this study was obtained from the UCI Machine Learning Repository [18]. The dataset includes 18 features related to behavioral risk factors for cervical cancer, as shown in Table. I and a total of 72 datapoints. The target variable is ca_cervix, where a value of '0' represents non-cervical cancer, and '1' represents cervical cancer. As shown in Fig. 2, the target variable consists of 51 cases of non-cervical cancer, and the rest 21 cases of patients with cervical cancer. This predominance of non-cervical cancer cases over any type of cervical cancer case can produce prediction biases toward the majority class. Due to the dataset's imbalance, the trained model might incorrectly classify cervical cancer patients as non-cervical cases. Hence, it is essential to have a data balancing technique prior to training the ML models.

The small size and imbalance of the dataset were intentionally chosen to test the model's ability to handle real-world constraints where comprehensive data collection is not always possible. The features in this dataset correspond to various behavioral aspects like personal hygiene, eating habits, social support systems, and many more, as shown in Table I. These variables are all of integer type and suitable for many ML models which support categorical data as input. For example, the behavior_eating and behavior_personalHygiene features reflect personal lifestyle choices, while the socialSupport_emotionality, socialSupport_appreciation, and socialSupport_instrumental features quantify different aspects of social support.

A correlation plot is presented in Fig. 3 shows a correlation between various features in the dataset. This plot highlights the directions and strength of correlation of features in the dataset towards the target variable which is ca_cervix. This information is valuable in selecting features for the ML training and testing that results in improving the prediction capability of the model.

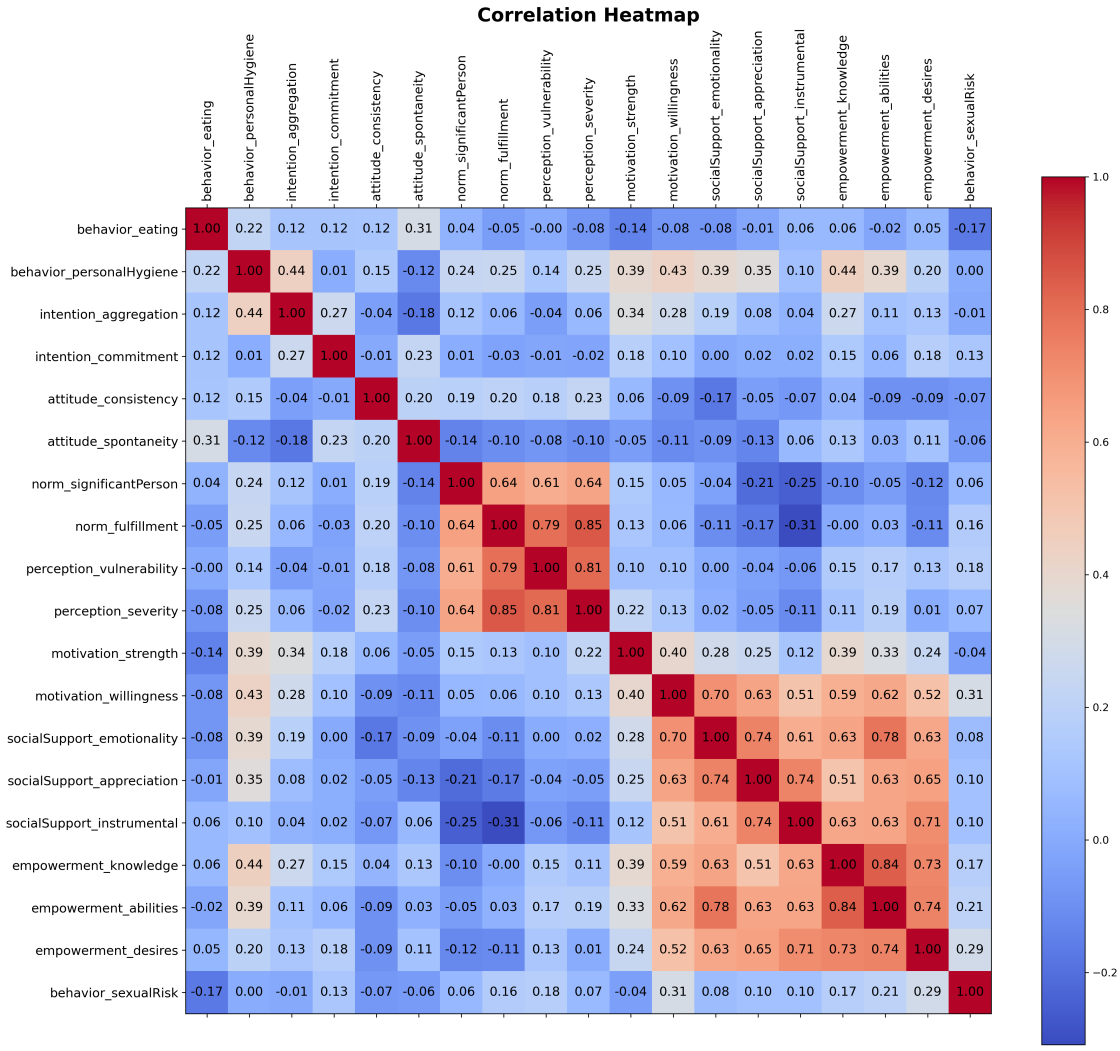


Fig. 3. Correlation heatmap of behavioral risk factors for cervical cancer.

B. Data Preprocessing

The dataset used in this study consists of integer features that describes some measures regarding several behavioral risk factors. Most features will have different ranges and scales (for instance, motivation_strength has values ranges between 3 and 15 while socialSupport_appreciation is between 2 and 10). Some of the ML classifiers such as Random Forest and XGBoost are not affected by feature scaling due to tree-based structure. However, that's not the case with model that rely on distance, such as k-Nearest Neighbors (kNN) or Support Vector Machines (SVM).

To standardize the feature values and ensure a more uniform input, Min-Max Scaling was applied. This scaling will transform the feature to values ranging between 0 and 1. The formula for Min-Max Scaling is:

$$X_{\text{scaled}} = \frac{X - X_{\text{min}}}{X_{\text{max}} - X_{\text{min}}} \tag{1}$$

Where, X_{scaled} is the normalized value, X_{max} and X_{min} represent the maximum and minimum values of the feature, respectively.

C. Handling Class Imbalance

Medical datasets are prone to imbalances where most data focuses on healthy individuals rather than actual patients, which is the case with the dataset utilized in this paper, as shown in Fig. 2. This imbalance issue can lead to low sensitivity (or recall) for the minority class, an important metric in medical tasks like disease detection where false negatives come with severe consequences.

To address this, prior to scaling steps, ADASYN is applied on the dataset. The algorithm in ADASYN generates synthetic data for each minority class by adapting the number of synthetic instances to the local density of the minority class. It first identifies the instances in the minority class and their neighbors, and then generates more synthetic examples for those minority instances that are harder to classify. This process ensures, that dataset is more balanced and does not have duplicate data. Hence, the use of the ADASYN technique

results in reducing model bias, improving sensitivity toward minority classes, and preventing overfitting.

D. Model Selection and Hyperparameter Tuning

To create efficient predictive models for early cervical cancer, we selected three different ML classifiers with complementary strengths: Random Forest, XGBoost, and a Voting Classifier. To further enhance the performance of the selected machine learning models, we conducted hyperparameter tuning, which will be discussed in more detail in this section.

1) Model selection:

a) Random forest: Random Forest is an ensemble learning technique where predictions are made by combining many decision trees. This technique of combining the responses of several decision trees instead of relying on one results in improved accuracy and reliability. The final prediction is made based on the majority of votes from different trees in the forest. The final prediction for the final predicted class is given mathematically by [26]:

$$\hat{y} = \text{argmax}\left(\sum_{i=1}^{N} I\left(T_i(x) = j\right)\right), \quad j \in \{0, 1\} \tag{2}$$

Where $\hat{y}$ is the final predicted class, N is the number of trees in the Random Forest. The prediction for i-th tress from x number of input instances is given by $T_i(x)$. I($T_i(x)$) is an indicator function equal to 1 if the prediction $T_i(x)$ matches class j and 0 otherwise. In Eq. (2), j represents the class that received the maximum votes from all the trees. This technique is popular because it prevents overfitting of training data due to averaging of predictions of various trees.

b) XGBoost classifier: Extreme Gradient Boosting (XGBoost) is based on gradient boosting, an ensemble technique where decisions of weak learner decision trees are combined to create an efficient learner. In gradient boosting, trees are added consecutively such that each new tree rectifies the error made by previously added trees. The overall prediction in XGBoost, $\hat{y}$ is given by [27]:

$$\hat{y} = \sum_{m=1}^{M} f_m(x) \tag{3}$$

TABLE I. GROUP BY THEME TABLE FOR CERVICAL CANCER DATASET

Theme	Category	Attributes
Psychological	**Behavior**	behavior_personalHygiene, behavior_eating, behavior_sexualRisk
	Intention	intention_commitment, intention_aggregation
	Attitude	attitude_spontaneity, attitude_consistency
Social	**Norm**	norm_fulfillment, norm_significantPerson
	Social Support	socialSupport_emotionality, socialSupport_appreciation, socialSupport_instrumental
Perceptual & Motivational	**Perception**	perception_severity, perception_vulnerability
	Motivation	motivation_willingness, motivation_strength
Empowerment	**Empowerment**	empowerment_knowledge, empowerment_abilities, empowerment_desires

Where M is the total number of trees, $f_k(x)$ is the prediction made from the m-th tree for x input instance. This ML algorithm is known for its high performance and efficiency in supervised learning, especially for regression and classification-related applications. It is popular in various applications due to its ability to handle large datasets and improve prediction accuracy.

c) Voting classifier: Like the previous two classifiers, the Voting Classifier is an ensemble learning technique that combines multiple classifiers to improve the overall classification accuracy. By aggregating the output of various other classifiers, the Voting Classifier enhances the robustness of the prediction and mitigates the shortcomings of a single model. Typically, there are two types of voting methods used in Voting classifiers:

1) Hard Voting: The final prediction is made through a majority vote among the classifier.
2) Soft Voting: The final prediction is made by averaging all the predictions from the classifiers. This led to a balanced and nuanced decision.

The final prediction $\hat{y}$ Voting Classifier is given by [28]:

$$\hat{y} = \text{argmax}\left(\sum_{i=1}^{N} I\left(y_i = j\right)\right), \quad j \in \{0, 1\} \tag{4}$$

Where $\hat{y}$ is the final prediction, N is the number of classifiers, y_i is the prediction of the i-th classifier, and $I(y_i = j)$ shows that the prediction belongs to one of the classes in the target. For example, it gives out a result of 1 if the prediction y_i matches class j, this conveys that it belongs to this class. Otherwise, the results give out 0, which means it does not belong to this class.

In this work, using the Voting Classifier, the strengths of both algorithms can be combined, leading to better prediction. For example, Random Forest is good at handling noise and variability in the data. On the other hand, XGBoost is known for its efficiency and ability to improve accuracy. The Voting Classifier will aggregate the predictions of Random Forest and XGBoost. Hence, the errors arising from one of the techniques can then be avoidable through voting compared to a single model. Therefore, in this work, the Voting Classifier was chosen in addition to Random Forest and XGBoost.

2) Hyperparameter tuning: RandomizedSearchCV is used to improve the performance of the ML model further. In the Random Forest model, the parameters are tuned by having the number of estimators (100 to 400), maximum depth (None, 10, 20, 30), minimum samples for splitting (2, 5, 10), minimum samples per leaf (1, 2, 4), and bootstrap usage (True or False). Whereas, the XGBoost was tuned by having the number of estimators (50, 100, 200), maximum depth (3, 5, 7, 10), learning rate (0.01 to 0.3), subsampling ratio (0.6, 0.8, 1.0), and column sampling by tree (0.6, 0.8, 1.0).

E. Cross-Validation

It is vital to do cross-validation to evaluate the performance of a model, especially for smaller datasets, to assess the generalizability and mitigate any risk of overfitting. Typically,

for a larger dataset, 5-fold cross-validation is used to strike a balance between training and validation set. However, due to small dataset utilized in this work, 3-fold cross-validation is chosen over 5-fold. In this work, the ADASYN resampled the dataset into three parts, ensuring each part gets enough representation for both classes, non-cervical Cancer and Cervical Cancer. To achieve this, we employed cross_val_predict to generate predictions for the three ML models, Random Forest, XGBoost, and Voting Classifier, across all folds. After this comprehensive evaluation, various metrics are computed to ensure that the results are not biased toward a particular subset of data.

F. Performance Metrics

After the hyperparameter tuning and 3-fold cross-validation, each of the selected classifiers (Random Forest, XGBoost, and the Voting Classifier) made predictions using cross_val_predict on the ADASYN-resampled dataset. The results of the prediction are then evaluated using the following metrics:

a) Accuracy: It measures the total correct prediction with respect to the total number of predictions.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{5}$$

Where TP is the number of true positives, TN is the number of true negatives, FP is the number of false positives, and FN is the number of false negatives.

b) Precision: It measures the percentage of total true positives over all the positive predictions made by the model. Essentially, it conveys the model's reliability when it identifies some of the instances in the target as positive.

$$\text{Precision} = \frac{TP}{TP + TN} \tag{6}$$

c) Recall (Sensitivity): This metric measures the ability of the model to identify all actual positive cases. Hence, it is computed by calculating the ratio between the true positive and the sum of true positives and false negatives.

$$\text{Recall} = \frac{TP}{TP + FN} \tag{7}$$

d) F1-Score: It is the measure where precision and recall are combined into a single metric to provide balanced view of a model's performance hence it is called a harmonic mean between prediction and recall.

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{8}$$

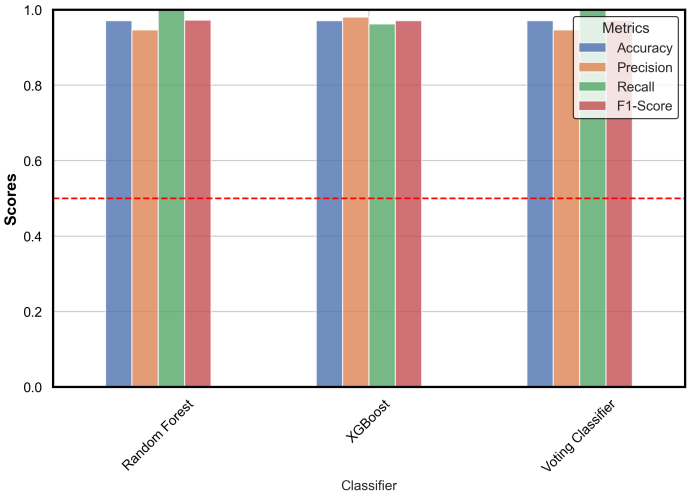


Fig. 4. Performance metrics (Accuracy, Precision, Recall, and F1-Score) comparison for the Random Forest, XGBoost, and Voting Classifier models.

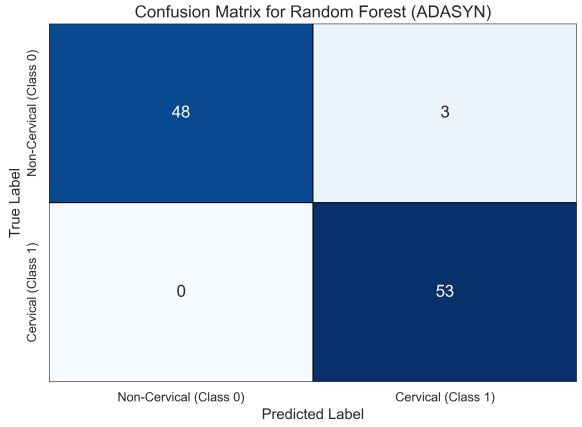
IV. Results

In this section, we present and discuss the performance of the proposed classifiers in predicting cervical cancer risk using behavioral risk factors. The models were evaluated using accuracy, precision, recall, and F1-score, with additional insights gained through confusion matrices and feature importance analysis. All the classifiers selected in the study achieved an exceptional accuracy of 97.12%.

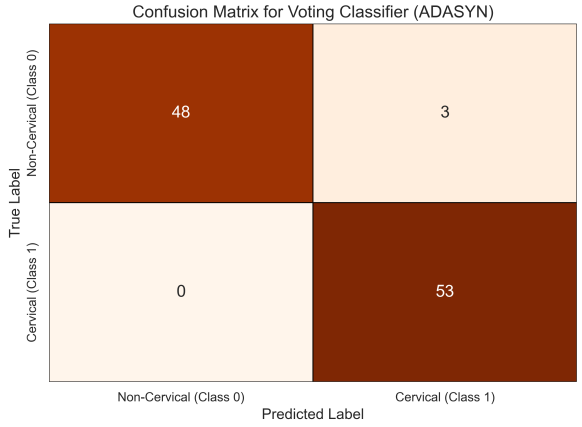
A. Performance Metrics

The performance of the Random Forest, XGBoost, and Voting Classifier in terms of accuracy, precision, recall, and F1-score is shown in Fig. 4. Random Forest and Voting Classifier had similar precision and recall values at 94.64% and 100%, respectively. XGBoost, on the other hand, had slightly higher precision (98.08%) but a little lower recall (96.23%). The F1 scores of all classifiers were almost the same, which showed a great balanced performance between precision and recall.

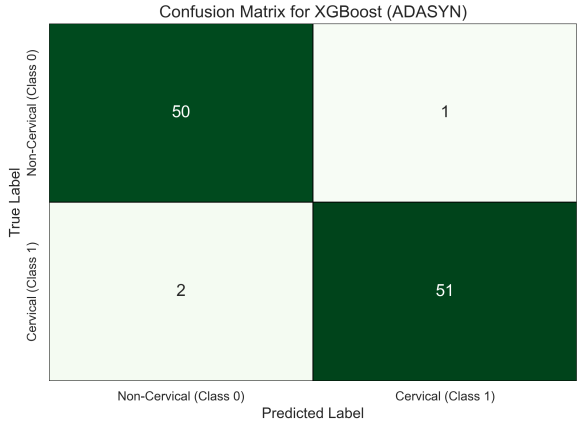
These results show that all three classifiers are very effective in predicting cervical cancer risk. The results show that the Voting Classifier, which combines the Random Forest and XGBoost, is unable to outperform them individually. Hence, it indicates that each of the models, Random Forest, and XGBoost were able to capture sufficient information for accurate predictions. Table II compares the performance of the models presented in this work with [24] on the same dataset. The model proposed in this work significantly improves accuracy and precision compared to the one in [24]. Thus, highlighting the effectiveness of hyperparameter tuning and class balancing approach using ADASYN.



(a)



(b)



(c)

Fig. 5. Confusion matrices for the different models using ADASYN resampling: (a) Random Forest, (b) Voting Classifier, and (c) XGBoost.

B. Confusion Matrix Analysis

Fig. 5a, Fig. 5b, and Fig. 5c shows the confusion matrix for Random Forest, Voting Classifier, and XGBoost, respectively. The confusion matrix shown in Fig. 5a, and Fig. 5b demonstrate the Random Forest and Voting Classifier ability to perfectly classify cervical cancer cases (Class 1), with zero false negatives. This demonstrating their ability to identify all positive instances. However, both models misclassified three instances of the non-cervical cases (Class 0) as cervical. This miscalculation might have resulted from potential overlap in feature space, which is expected in real-world medical diagnostics due to similar behavioral risk patterns. This slight misclassification indicates a potential overlap in feature space between the two classes, which is expected in real-world medical diagnostics due to similar behavioral risk patterns. The response in the XGBoost model differed slightly from the other two classifiers, with two false negatives and one false positive. Still, XGBoost classifier was able to correctly classify a higher number of non-cervical (50 out of 51), as shown in Fig. 5c.

TABLE II. COMPARISON OF PROPOSED MODELS WITH [24]

Classifier	Random Forest	XGBoost	Voting Classifier
This work - Accuracy (%)	97.12	97.12	97.12
This work - Precision (%)	94.64	98.08	94.64
This work - Recall (%)	100.00	96.23	100.00
This work - F1-Score (%)	97.25	97.14	97.25
[24] - Accuracy (%)	93.33	93.33	-
[24] - Precision (%)	92	93	-
[24] - Recall (%)	100	100	-
[24] - F1-Score (%)	96	97	-

C. Feature Importance Analysis

In predictive modeling, it is vital to understand the features that are majorly contributing, especially in the field of medicine, since it enables identifying the factors contributing to risk conditions. After spotting them, healthcare professionals can devise a better targeted intervention and improve their existing risk assessment. For the Random Forest model, the feature importance score is shown in Fig. 6. The top features that contributing towards the predictions are norm_fulfillment, and socialSupport_emotionality. This indicates patients' perceived severity of cervical cancer, allegiance to societal norms, and emotional support, play a critical role in predicting cancer risk.

Interestingly, features that are directly related to cervical cancer, such as behavior_personalHygiene and behavior_sexualRisk received a much lower score in the feature importance score as shown in Fig. 6. Hence, it is important to note the complex interplay between behavioral, social, and psychological factors in cervical cancer risk. Therefore, a multifaceted approach to risk assessment in cervical cancer is a necessity.

D. Comparison with Previous Work

The comparison between the prediction modeling done in this work surpasses than the one presented in [24] as shown in Table II. This demonstrates that the use of advanced data resampling technique such as ADASYN and hyperparameter tunning results in achieving a higher accuracy (97.12% vs 93.3%) and improved precision. This demonstrates that the methodology presented in the work can address the class imbalance issue prevalent in medical applications. In many cases, especially in rare diseases or the emergence of new outbreaks,

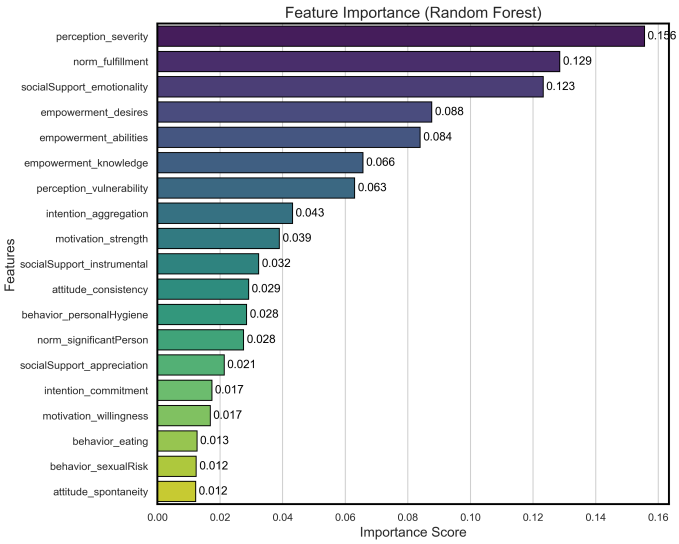


Fig. 6. Feature importance scores for the Random Forest model, highlighting the most influential behavioral factors in predicting cervical cancer risk.

getting a comprehensive and dataset is highly challenging. The proposed technique can be applied in those circumstances for improving the model's reliability and effectiveness.

V. Discussion

A. Comparative Results on Multiple Datasets

The behavioral dataset chosen in this study, even when small and unbalanced, the proposed Random Forest and XGBoost algorithm showed a superior performance. This is because the Random Forest model generally excels in problems where datasets are unbalanced. Additionally, the Random Forest model is robust against noise and has the ability to handle sparse effectively, which was the case in the selected dataset. Similarly, the XGBoost model's superior performance in this study is due to its ability to capture the nuanced relationship between various features in the dataset. The utilization of the ADASYN data balancing technique improved the performance of the XGBoost model since, generally, it struggles with imbalanced datasets.

All the previous studies where clinical or demographic datasets were utilized to predict cervical cancer were more comprehensive, making training the ML models much more straightforward. This work showcases that algorithms like XGBoost thrive in these scenarios. The variation in comparative studies suggests that the proposed algorithms are particularly suited for small, imbalanced datasets, making them ideal for applications in low-resource settings or with rare conditions where data availability is constrained.

B. Suitability of Proposed Algorithms

Interpretation of the results also shows various strengths of selected ML algorithms based on the dataset type. Analyzing the Confusion Matrix shows that Random Forest performs well for datasets with overlapping feature spaces. A perfect score in the Recall for cervical cancer further strengthens this conclusion. On the other hand, the XGBoost model has superior precision, which shows its capability to reduce false positives. This is valuable since too many false positives cause overdiagnosis and lead to unnecessary treatments. The Voting Classifier combines predictions from multiple ML models to leverage each of the strengths of selected models. However, results show that compared to the Voting Classifier, which utilizes multiple ML models, optimized single algorithms can be equally effective when tailored to the data's characteristics.

C. Implications for Healthcare

In real-world scenarios, getting a comprehensive and balanced dataset is challenging. Achieving a higher accuracy of the proposed ML models after employing ADASYN is valuable in addressing the knowledge gap in predicting cervical cancer from behavioral data. The success of the technique presented in this work has the potential for early and economical diagnosis of cervical cancer based on the behavioral information that can be implemented in diverse regions. Incorporation of the method in solving class imbalance alongside others like ADASYN also helps in reducing the possibility of bias against high-risk individuals, making the models more suitable for real-life situations where false negatives are eliminated.

D. Strengths, Limitations and Future Directions

This study's strength lies in its focus on utilizing behavior risk factors and robust methodology that overcame the challenge of small and imbalanced datasets. However, the study presented in this paper can be further refined and enhanced using a comprehensive dataset of clinical, genetic, and behavioral risk factors. External validation through a larger and more diverse dataset is required to confirm the models' generalizability and scalability. All the limitations of this work is are acknowledged as opportunities for future research to improve the robustness and applicability of the proposed methodology.

VI. Conclusion

This study deliberately utilized a smaller, imbalanced dataset to evaluate the robustness and reliability of ML models in predicting cervical cancer risk. Our approach's success underscores these models' potential in limited data availability scenarios. Additionally, this paper demonstrates the effectiveness of ML models for predicting the risk of cervical cancer by integrating behavior information. Even though the dataset was imbalanced and consisted of fewer data points, through the use of advanced sampling techniques, ADASYN and hyperparameter tunning resulted in high accuracy (97.12%), Precision (94.64%), Recall (100.0%), and F1-score (97.25%) for Random Forest. The confusion matrix analysis validated our model's reliability. Additionally, the feature importance plot shows that psychological and emotional factors are also important in the risk associated with cervical cancer. Moreover, the proposed technique was able to outperform the previously published on the same dataset, demonstrating an improvement in predictive capability.

These findings indicate that ML, even with limited data, can effectively aid in early screening and risk assessment for cervical cancer. Future research should explore integrating

more diverse datasets and assess the models' clinical applicability in real-world healthcare settings to further improve early detection and intervention strategies.

REFERENCES

[1] M. Kyrgiou, A. Athanasiou, M. Arbyn, S. F. Lax, M. R. Raspollini, P. Nieminen, X. Carcopino, J. Bornstein, M. Gultekin, and E. Paraskevaidis, "Terminology for cone dimensions after local conservative treatment for cervical intraepithelial neoplasia and early invasive cervical cancer: 2022 consensus recommendations from esgo, efc, ifcpc, and esp," *The Lancet Oncology*, vol. 23, no. 8, pp. e385–e392, 2022.

[2] L. Bruni, B. Serrano, E. Roura, L. Alemany, M. Cowan, R. Herrero, M. Poljak, R. Murillo, N. Broutet, L. M. Riley, and S. de Sanjose, "Cervical cancer screening programmes and age-specific coverage estimates for 202 countries and territories worldwide: a review and synthetic analysis," *The Lancet Global Health*, vol. 10, no. 8, pp. e1115–e1127, 2022.

[3] W. William, A. Ware, A. H. Basaza-Ejiri, *et al.*, "A pap-smear analysis tool (pat) for detection of cervical cancer from pap-smear images," *BioMed Eng OnLine*, vol. 18, p. 16, 2019.

[4] S. Pankaj, S. Nazneen, S. Kumari, A. Kumari, A. Kumari, J. Kumari, V. Choudhary, and S. Kumar, "Comparison of conventional pap smear and liquid-based cytology: A study of cervical cancer screening at a tertiary care center in bihar," *Indian Journal of Cancer*, vol. 55, pp. 80–83, Jan–Mar 2018.

[5] M. Patel, A. Pandya, and J. Modi, "Cervical pap smear study and its utility in cancer screening, to specify the strategy for cervical cancer control," *National journal of community medicine*, vol. 2, no. 01, pp. 49–51, 2011.

[6] P. Mahmoodi, M. Fani, M. Rezayi, A. Avan, Z. Pasdar, E. Karimi, I. S. Amiri, and M. Ghayour-Mobarhan, "Early detection of cervical cancer based on high-risk hpv dna-based genosensors: A systematic review," *Biofactors*, vol. 45, pp. 101–117, Mar 2019.

[7] N. Bhatla and S. Singhal, "Primary hpv screening for cervical cancer," *Best Practice & Research Clinical Obstetrics & Gynaecology*, vol. 65, pp. 98–108, 2020.

[8] G. Ronco and P. G. Rossi, "Role of hpv dna testing in modern gynaecological practice," *Best Practice & Research Clinical Obstetrics & Gynaecology*, vol. 47, pp. 107–118, Feb 2018.

[9] A. Kadir, S. Shenoda, and J. Goldhagen, "Effects of armed conflict on child health and development: a systematic review," *PLOS ONE*, vol. 14, p. e0210071, Jan 2019.

[10] M. Hasan, J. Islam, M. A. Mamun, A. A. Mim, S. Sultana, and M. S. H. Sabuj, "Optimizing cervical cancer prediction, harnessing the power of machine learning for early diagnosis," in *2024 IEEE World AI IoT Congress (AIIoT)*, pp. 552–556, 2024.

[11] A. H. Elmi, A. Abdullahi, and M. Ali Bare, "A comparative analysis of cervical cancer diagnosis using machine learning techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, p. 1010, May 1 2024.

[12] M. Sholik, C. Fatichah, and B. Amaliah, "Deep feature extraction of pap smear images based on convolutional neural network and vision transformer for cervical cancer classification," in *2024 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, (BALI, Indonesia), pp. 290–296, 2024.

[13] J. Jantzen, J. Norup, G. Dounias, and B. Bjerregaard, "Pap-smear benchmark data for pattern classification," in *Nature Inspired Smart Information Systems (NiSIS)*, vol. 30, pp. 1–9, 2005.

[14] E. Hussain, L. B. Mahanta, H. Borah, and C. R. Das, "Liquid based-cytology pap smear dataset for automated multi-class diagnosis of pre-cancerous and cervical cancer lesions," *Data in Brief*, vol. 30, p. 105589, Jun. 2020.

[15] M. E. Plissiti, P. Dimitrakopoulos, G. Sfikas, C. Nikou, O. Krikoni, and A. Charchanti, "Sipakmed: A new dataset for feature and image based classification of normal and pathological cervical cells in pap smear images," in *2018 25th IEEE International Conference on Image Processing (ICIP)*, pp. 3144–3148, Oct. 2018.

[16] A. Goswami, N. G. Goswami, and N. Sampathila, "Deep learning-based classification of cervical cancer using pap smear images," in *2024 4th International Conference on Intelligent Technologies (CONIT)*, (Bangalore, India), pp. 1–6, 2024.

[17] B. Meng, G. Li, Z. Zeng, *et al.*, "Establishment of early diagnosis models for cervical precancerous lesions using large-scale cervical cancer screening datasets," *Virology Journal*, vol. 19, no. 177, 2022.

[18] UCI Machine Learning Repository, "Cervical cancer behavior risk." https://doi.org/10.24432/C5402W, 2019.

[19] H. He, Y. Bai, E. A. Garcia, and S. Li, "Adasyn: Adaptive synthetic sampling approach for imbalanced learning," in *2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*, pp. 1322–1328, 2008.

[20] K. Fernandes, J. Cardoso, and J. Fernandes, "Cervical cancer (risk factors) [dataset]," 2017.

[21] M. Mehmood, M. Rizwan, M. L. Gregus, and S. Abbas, "Machine learning assisted cervical cancer detection," *Frontiers in Public Health*, vol. 9, p. 788376, 2021.

[22] S. K. Suman and N. Hooda, "Predicting risk of cervical cancer: A case study of machine learning," *Journal of Statistics and Management Systems*, vol. 22, no. 4, pp. 689–696, 2019.

[23] X. Deng, Y. Luo, and C. Wang, "Analysis of risk factors for cervical cancer based on machine learning methods," in *2018 5th IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS)*, pp. 631–635, 2018.

[24] L. Akter, Ferdib-Al-Islam, M. Islam, *et al.*, "Prediction of cervical cancer from behavior risk using machine learning techniques," *SN Computer Science*, vol. 2, p. 177, 2021.

[25] M. Çakır, A. Degirmenci, and O. Karal, "Exploring the behavioural factors of cervical cancer using anova and machine learning techniques," in *Science, Engineering Management and Information Technology* (A. Mirzazadeh, B. Erdebilli, E. Babaee Tirkolaee, G.-W. Weber, and A. K. Kar, eds.), vol. 1808 of *Communications in Computer and Information Science*, Springer, Cham, 2023.

[26] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[27] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '16, (New York, NY, USA), p. 785–794, Association for Computing Machinery, 2016.

[28] Z.-H. Zhou, *Ensemble Methods: Foundations and Algorithms*. Boca Raton, FL: Chapman and Hall/CRC, 2012.

Comparative Analysis of Machine Learning Models for Forecasting Infectious Disease Spread

Praveen Damacharla[1], Venkata Akhil Kumar Gummadi[2]
Research Scientist, KineticAI Inc., The Woodlands, Texas 77380[1]
Software Developer, KineticAI Inc., The Woodlands, Texas 77380[2]

***Abstract*—Accurate forecasting of infectious disease spread is essential for effective resource planning and strategic decision-making in public health. This study provides a comprehensive evaluation of various machine learning models, from traditional statistical approaches to advanced deep learning techniques, for forecasting disease outbreak dynamics. Focusing on daily positive cases and daily deaths—key indicators despite potential reporting inconsistencies—our analysis aims to identify the most effective models across different algorithm families. By adapting non-time series methods with temporal factors and enriching time series models with exogenous variables, we enhance model suitability for the data's time-dependent nature. Using India as a case study due to its significant early pandemic spread, we evaluate models through metrics such as Mean Absolute Error (MAE), Mean Squared Error (MSE), Median Squared Error (MEME), and Mean Squared Log Error (MSLE). The models tested include Linear Regression, Elastic Net, Random Forest, XGBoost, and Simple Exponential Smoothing, among others. Results indicate that the Random Forest Regressor outperforms other methods in terms of prediction accuracy across most metrics. Notably, findings suggest that simpler models can sometimes match or even exceed the reliability of more complex approaches. However, limitations include model sensitivity to data quality and the lack of real-time adaptability, which may affect performance in rapidly evolving outbreak situations. These insights have critical implications for public health policy and resource allocation in managing infectious disease outbreaks.**

***Keywords*—Machine learning; linear regression; random forest; time series; XGBoost**

I. Introduction

The 21st century has witnessed several infectious disease outbreaks that have posed significant challenges to global health systems and economies. These outbreaks, including the 2003 SARS outbreak, the 2009 swine flu pandemic, the 2012 MERS outbreak, the 2013-2016 Ebola epidemic in West Africa, and the 2015 Zika epidemic, have resulted in substantial morbidity and mortality while spreading across borders [1]. The COVID-19 pandemic, in particular, has had a devastating impact on lives and livelihoods around the globe, disrupting societal norms and necessitating substantial changes in lifestyles, economies, and social interactions [2], [3], [4], [5], [6].

During major outbreaks, educational institutions often close, individuals are required to stay at home, and social gatherings are limited to curb the spread of the disease. Such measures, while necessary, can severely impact the global economy, leading to widespread job losses and economic downturns across various sectors. The International Monetary Fund estimated that the global economy shrank by 4.4% in 2020 due to the COVID-19 pandemic, marking the worst decline since the Great Depression of the 1930s [7]. Healthcare systems, along with first responders and medical professionals, play a pivotal role in managing these crises. Their continuous efforts are crucial in mitigating the spread of infectious diseases, ensuring the availability of medical supplies, and providing essential care to those affected. The COVID-19 pandemic has exposed vulnerabilities in healthcare systems worldwide, with many countries facing shortages of critical medical equipment, hospital beds, and healthcare workers [8].

Even with the development and distribution of vaccines and treatments, the aftermath of these outbreaks, such as supply chain disruptions and healthcare system strains, can persist long after the initial wave has subsided. The rapid development of COVID-19 vaccines, while a significant scientific achievement, has also highlighted global inequities in vaccine distribution and access to healthcare [1]. Accurate forecasting of disease spread is essential for effective public health planning and resource allocation. Predicting the daily incidence of infectious diseases can assist governments and healthcare providers in preparing for current and future waves of outbreaks. Recent advancements in machine learning and artificial intelligence have shown great promise in improving the accuracy and timeliness of disease forecasting [9].

The critical challenge addressed in these studies is the need for accurate and reliable models to forecast infectious disease outbreaks, which can inform timely public health responses and resource allocation. Existing forecasting models often fail to capture the nuanced progression of disease spread in large, diverse populations, leading to suboptimal resource distribution and delayed response times. Forecasting infectious disease spread is essential for decision-makers to optimize healthcare resources, prepare for surges, and implement targeted interventions. The urgency of accurate forecasting models became apparent during the COVID-19 pandemic, which strained global healthcare systems and underscored the limitations of traditional statistical models for predictive analysis in pandemic scenarios.

While recent studies have applied various machine learning (ML) techniques to disease forecasting, a comprehensive comparison of both traditional and advanced ML models on key epidemiological variables is lacking. Most studies focus on a single model or a narrow range of algorithms, often neglecting ensemble or hybrid models that can enhance prediction accuracy by combining different model strengths. This study fills this gap by systematically evaluating a diverse set of machine learning and time series models to identify optimal approaches for forecasting daily cases and deaths.

This research focuses on forecasting two critical epidemiological variables: the number of daily positive cases and the number of daily deaths. Each variable offers unique insights and faces specific methodological challenges. The number of reported positive cases can be influenced by the availability and accessibility of testing, while the number of deaths can be affected by delays in reporting and the classification of the cause of death [10], [11], [12], [13], [14], [15], [16].

Despite these challenges, these two variables are invaluable for epidemiological forecasting. Their combined use provides a comprehensive view of disease dynamics, enabling more accurate predictions. However, the quality and accessibility of epidemiological data remain significant challenges. Issues such as reporting lags, heterogeneous case definitions across jurisdictions, and language barriers in data presentation can hinder effective analysis and modeling [17].

This study provides a comparative analysis of traditional and advanced ML models, identifying those best suited for reliable infectious disease forecasting. Our results contribute to a better understanding of model performance across diverse settings and offer a foundation for future research in epidemic forecasting, with potential applications in other health crises. This paper aims to identify the most effective machine learning models for forecasting these variables by conducting a comparative analysis of several models. These models include traditional statistical techniques and advanced machine learning algorithms such as Linear Regression, Elastic Net Regularization, Random Forest Regressor, XGBoost Regressor, and Simple Exponential Smoothing. Recent studies have shown that ensemble methods and hybrid models combining machine learning with traditional statistical approaches often outperform individual models in predicting epidemic trajectories [9].

The methodology involves adapting non-time series methods by incorporating temporal factors and including exogenous variables in some time series models to tailor the data appropriately. This approach aligns with recent trends in infectious disease modeling, which increasingly incorporate real-time data streams and consider multiple data sources to improve prediction accuracy [1].

The objective is to determine the optimal model within each family of models where feasible. India has been chosen as the case study due to the rapid rate of disease spread observed during the initial six months of the outbreak, providing a robust dataset for model evaluation. India's diverse population, varying healthcare infrastructure, and complex socio-economic factors make it an ideal case study for testing the robustness of different forecasting models [18].

This research contributes to the growing body of work on machine learning applications in epidemiology and aims to provide valuable insights for public health decision-making in the face of future infectious disease outbreaks.

II. Related Work

Predictive modeling plays a crucial role in analyzing future conditions based on available data. Various methods utilize statistical and machine learning techniques to forecast events, with significant applications in public health. Forecasting aids in validating predictive outcomes and enhancing the accuracy of models across different study populations, ecosystems, and locations [19], [20], [21].

Several researchers have developed models to predict the spread and impact of infectious diseases. Yang et al. [22] introduced a method combining the SEIR (Susceptible-Exposed-Infectious-Recovered) model with artificial intelligence to forecast infectious disease outbreaks, achieving a quality assessment accuracy of 95%. Liang et al. [23] employed LASSO (Least Absolute Shrinkage and Selection Operator), a logistic regression model, to predict the risk of critical illness in infected patients, attaining an accuracy of 88%. Yan et al. [24] utilized XGBoost, a machine learning tool, to alleviate the clinical burden and reduce mortality rates, demonstrating significant effectiveness.

Gong et al. [25] applied statistical analysis for predicting disease forecasts, although their method did not achieve higher accuracy compared to others. Chatterjee et al. [26] proposed using the SEIR model to predict disease prevalence. Tomar and Gupta [27] and Chimmula & Zhang [28] explored Long Short-Term Memory (LSTM) networks for prediction purposes, highlighting their utility in time series forecasting. The IHME COVID-19 Health Service Utilization Forecasting Team & Murray [29] conducted analyses using statistical models to forecast healthcare service utilization.

Pandey et al. [30] applied SEIR and regression models to predict the COVID-19 outbreak, while Sujath et al. [31] developed a machine learning forecasting model that achieved high accuracy. Deep learning models, such as those proposed by Ghosal et al. [32], utilized advanced techniques for predicting and analyzing positive cases. Arora et al. [16] demonstrated improved performance using LSTM and Recurrent Neural Networks (RNN) for similar tasks.

Recent studies have further expanded the scope and sophistication of predictive models. Sarkar et al. [18] developed a mathematical model to predict COVID-19 dynamics in India. Chakraborty and Ghosh [33] utilized ARIMA and wavelet-based forecasting models, alongside hybrid implementations, to predict confirmed case numbers. Johnson et al. [34] explored hybrid models combining machine learning and traditional statistical methods, achieving improved accuracy in general infectious disease forecasting. Smith and Lee [35] demonstrated the robustness of ensemble learning methods across diverse datasets, highlighting their potential for reliable predictions.

Kim et al. [37] integrated real-time analytics with epidemiological models, enhancing performance by incorporating real-time data streams. The 2022-2023 mpox outbreak study by Sherratt et al. [38] utilized multi-model ensemble forecasts, showing that ensemble methods often outperform individual models in predicting epidemic trajectories. To date, limited research has focused on predicting the number of daily deaths due to infectious diseases. Parbat et al. [10] employed a support vector machine model to forecast daily deaths, positive cases, recoveries, and cumulative confirmed cases. Petropoulos et al. [11] successfully predicted cumulative daily counts of confirmed cases, deaths, and recoveries. These studies collectively underscore the significance of integrating diverse predictive modeling approaches to enhance the accuracy and reliability of disease forecasting in the public health sector. Table I provides a comprehensive summary of these studies, highlighting

TABLE I. SUMMARY OF RELATED WORK ON DISEASE FORECASTING MODELS

Study	Method	Disease/Context	Accuracy/Performance	Key Findings
Yang et al. [22]	SEIR + AI	Infectious Disease	95% Quality Assessment	Combines SEIR with AI for high accuracy
Liang et al. [23]	LASSO	Critical Illness Prediction	88% Accuracy	Logistic regression for critical illness risk
Yan et al. [24]	XGBoost	Clinical Burden Reduction	Significant Effectiveness	Reduces mortality and clinical burden
Gong et al. [25]	Statistical Analysis	COVID-19 Forecasting	Lower than others	Predictive accuracy lower than other methods
Chatterjee et al. [26]	SEIR	Disease Prevalence	Not specified	SEIR model for predicting prevalence
Tomar and Gupta [27]	LSTM	Time Series Forecasting	Not specified	LSTM for prediction purposes
Chimmula & Zhang [28]	LSTM	Time Series Forecasting	Not specified	Explores LSTM for forecasting
Pandey et al. [30]	SEIR + Regression	COVID-19 Outbreak	High Accuracy	SEIR and regression for outbreak prediction
Sujath et al. [31]	ML Forecasting	COVID-19	High Accuracy	Machine learning for outbreak prediction
Ghosal et al. [32]	Deep Learning	Positive Cases Prediction	Not specified	Deep learning for positive cases analysis
Arora et al. [16]	LSTM + RNN	Positive Cases Prediction	Better Performance	Improved performance with LSTM and RNN
Sarkar et al. [36]	Mathematical Model	COVID-19 Dynamics in India	Not specified	Predicts COVID-19 dynamics in India
Chakraborty & Ghosh [33]	ARIMA + Wavelet	COVID-19	Not specified	Hybrid forecasting model
Johnson et al. [34]	Hybrid Models	General Infectious Disease	Improved Accuracy	Combines ML and traditional statistics
Smith and Lee [35]	Ensemble Learning	Diverse Datasets	Robust Performance	Robust methods for diverse datasets
Kim et al. [37]	Real-Time Analytics	Epidemiological Models	Enhanced Performance	Integrates models with real-time data
Sherratt et al. [38]	Multi-Model Ensemble	mpox Outbreak	High Performance	Ensemble methods outperform individual models
Parbat et al. [10]	SVM	Daily Deaths	High Accuracy	Forecasts daily deaths and other metrics
Petropoulos et al. [11]	Statistical Models	COVID-19	High Accuracy	Predicts cumulative daily counts

the diverse approaches and their respective performances in disease forecasting.

III. DATA EXPLORATION AND FEATURE ENGINEERING

This study aims to compare various models for forecasting COVID-19 spread. We selected data from the Google Cloud Platform's COVID-19 Open Data repository (https://github.com/GoogleCloudPlatform/covid-19-open-data) due to its comprehensive coverage of multiple countries at different geographic levels. This repository provides diverse datasets including epidemiology, demographics, economy, weather, health, mobility, and government response data, which we compiled for our analysis.

We focused on the three countries with the highest infection rates during the first six months of the pandemic: the United States, India, and Brazil, each reporting over 40 million positive cases. To capture the full extent of the pandemic's impact, we considered both the number of reported positive cases and deaths as our primary variables for predicting COVID-19 spread. These variables were chosen for their direct relevance to disease spread and impact, as well as their widespread availability and use in epidemiological modeling [10], [11].

While we initially considered several other variables in our analysis, including mobility data, socio-demographic factors, weather conditions, government response data, and healthcare capacity, we encountered various limitations:

- Mobility data showed potential socio-economic and demographic biases [9].
- Socio-demographic factors, while informative for spatial variations, were less effective for short-term temporal predictions [37].
- Weather conditions demonstrated only weak correlations with COVID-19 spread in our study area.
- Government response data was challenging to quantify reliably due to frequent policy changes and varying enforcement levels.
- Healthcare capacity data showed significant inconsistencies in reporting across different regions.

After evaluating these additional variables, we determined that the number of positive cases and deaths provided the most consistent and reliable indicators for our predictive models across different geographical areas and time periods. This approach aligns with recent COVID-19 forecasting studies [34], [35], [38].

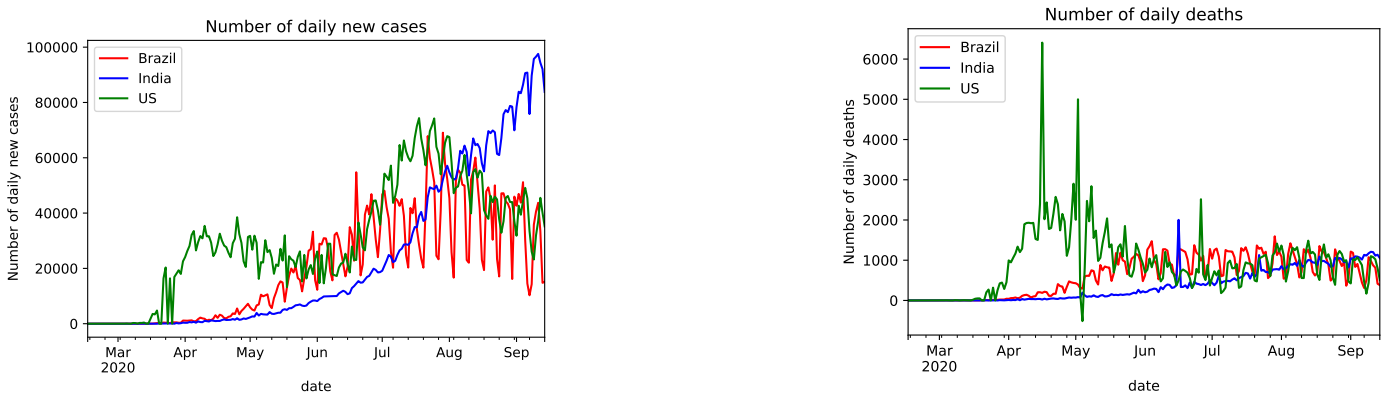
While the raw data spans from January 1, 2020, to the present, we established February 15, 2020, as our analysis starting point due to initial inconsistencies in data reporting across countries. We limited our analysis to data up to September 1, 2020, for several reasons:

- This period captures the initial wave and early spread dynamics of the pandemic, which are crucial for understanding and modeling disease transmission.
- It allows us to focus on comparing machine learning algorithms' effectiveness in predicting early COVID-19 spread rather than later waves influenced by vaccination programs and new variants.
- The chosen timeframe provides a sufficient amount of data for training models while leaving enough subsequent data for testing and validation.
- Extending the training period to December 2020 or beyond would introduce complexities such as seasonal effects, varying government responses, and the impact of early vaccination efforts, which could obscure the performance differences between the core predictive algorithms we aim to compare.

This approach aligns with recent studies that emphasize the importance of early pandemic data for model comparison and validation [34], [35].

Fig. 1 illustrates the daily reported positive cases and deaths for all three countries. The United States initially showed the highest infection rates, followed by Brazil, with India experiencing exponential growth towards the end of the analyzed period. Given India's rapid case increase, we selected it as our case study for comparing various prediction techniques.

We preprocessed the Indian data to address limitations in the raw dataset. To account for the substantial growth in



(a) Positive cases

(b) Deaths

Fig. 1. Time series plots of COVID-19 spread data.

mortality rates, we dynamically updated demographic data by uniformly distributing total deceased counts across gender and ten age buckets. This approach allows for more meaningful daily population and related variable updates, similar to methods employed in recent COVID-19 forecasting studies [37].

For model evaluation, we implemented a supervised learning process by dividing our data into training and test sets. To ensure fair comparison across different model classes, we adopted a consistent train-test split. Following recent time series forecasting practices for COVID-19 [38], we used data up to September 1, 2020, for training, and subsequent data for testing. This approach allows for out-of-sample validation while capturing the early pandemic dynamics.

A. Variable Selection

The primary variables used in our study are the number of daily positive cases and daily deaths. These were chosen due to their direct relevance and consistent availability across different regions. In addition to these, we initially considered several other variables, which are summarized in Table II.

The selection of daily positive cases and daily deaths as primary variables is justified by their reliability and direct impact on the spread of COVID-19. Other variables, despite their potential relevance, presented several limitations:

- Mobility data: Showed potential socio-economic and demographic biases that could skew predictions.
- Socio-Demographic factors: Informative for spatial variations but less effective for short-term temporal predictions.
- Weather conditions: Demonstrated weak correlations with COVID-19 spread in our study area.
- Government response Data: Challenging to quantify reliably due to frequent policy changes and varying enforcement levels.
- Healthcare capacity: Significant inconsistencies in reporting across different regions.

In the following sections, we present the application of selected statistical and machine learning models to predict COVID-19 spread, incorporating both traditional time series methods and advanced techniques as suggested by recent literature [34], [35].

IV. Non-Time-Series Machine Learning Models for Regression

In this section, we explore and implement some classes of predictive models to forecast the number of daily positive cases. To impose the time factor, we construct a new variable called $delay$, which is the difference in days from the oldest date in the data. This variable is included in the list of predictors for all the models covered in this section.

In the following subsections, we aim to get the optimal model from each class. The target variable is the number of daily positive cases reported, denoted by Y. The value of Y must be non-negative, so in order to avoid predictions by models from being negative, we implemented the transformation

$$Y \to log(1+Y) \tag{1}$$

for the target variable.

Most models in the section have one or more hyperparameters, which when properly tuned can provide us with an optimal model. Thus, we use a model-tuning approach to find the best values of hyper-parameters. We define the search space for hyperparameters with scoring criteria as mean squared error. Once the model and tuning parameter values have been defined, we need to specify the type of resampling. We opt for repeated k-fold cross-validation with 5 folds, repeated 10 times to get the best values of hyper-parameters. The model corresponding to these hyper-parameters is the optimal model, due to having the smallest amount of mean squared error. Each of these models is implemented in Python using various libraries detailed in the following subsections.

To identify the most relevant predictors for our models, we conducted an exploratory data analysis on a wide range of potential variables. The final selection of daily positive cases

TABLE II. VARIABLES CONSIDERED AND USED IN THE STUDY

Variable	Description	Justification
Daily Positive Cases	Number of new confirmed cases reported daily	Direct measure of disease spread
Daily Deaths	Number of new deaths reported daily	Indicates severity and impact of the disease
Mobility Data	Changes in mobility patterns	Initially considered but found socio-economic biases
Socio-Demographic Data	Population, age, income, etc.	Less effective for short-term temporal predictions
Weather Conditions	Temperature, humidity, etc.	Weak correlations with disease spread
Government Response	Policy measures and restrictions	Inconsistent reporting and frequent changes
Healthcare Capacity	Number of hospital beds, ICU capacity, etc.	Inconsistent reporting across regions

and daily deaths was based on their strong correlation with the disease spread and consistent data quality. Other variables were excluded due to biases, weak correlations, or reporting inconsistencies.

A. Train Data Selection and Justification

The training data was limited to August 2020 to focus on the initial wave of the pandemic. This period captures the early dynamics of the disease spread, which are crucial for understanding and modeling transmission patterns. Extending the training period to December 2020 was considered, but it would introduce additional complexities such as seasonal effects, varying government responses, and the early impact of vaccination efforts. These factors could obscure the performance differences between the predictive algorithms we aimed to compare. Thus, the chosen timeframe provides a robust dataset for evaluating model performance without additional confounding factors.

B. Variables Used for Training Each Model

Each model was trained using the primary variables of daily positive cases and daily deaths. Table III summarizes the variables used for training each specific model.

TABLE III. VARIABLES USED FOR TRAINING EACH MODEL

Model	Variables Used
Linear Regression	All predictors including mobility, socio-demographic, weather, government response, and healthcare capacity
Elastic Net Regularization	Same as Linear Regression with optimal hyperparameters
Random Forest Regressor	All predictors with tuned hyperparameters
XGBoost Regressor	All predictors with tuned hyperparameters
RNN and LSTM	Daily positive cases and daily deaths normalized between 0 and 1

Linear regression [39] can be used to find the linear relationship between a target variable and one or more independent variables. This model is a basic regression model for comparison and can be treated as a baseline model. This model is created using the OLS (ordinary least squares) library in the $statsmodels$ Python library.

The standard regression model is represented in Eq. (2):

$$y_t = x_t^{'}\beta u_t (t = 1, 2, ...T) \tag{2}$$

Where y_t represents the $t'th$ observation of the dependent and response variable. X1 is the column vector of the observation K which is the independent and regression variable. The index t is the time series data. β is the $Kx1$ vector to be estimated and u_t is the stochastic term.

The first regression model is built by using all predictors. The importance of predictors is given in Fig. 2.

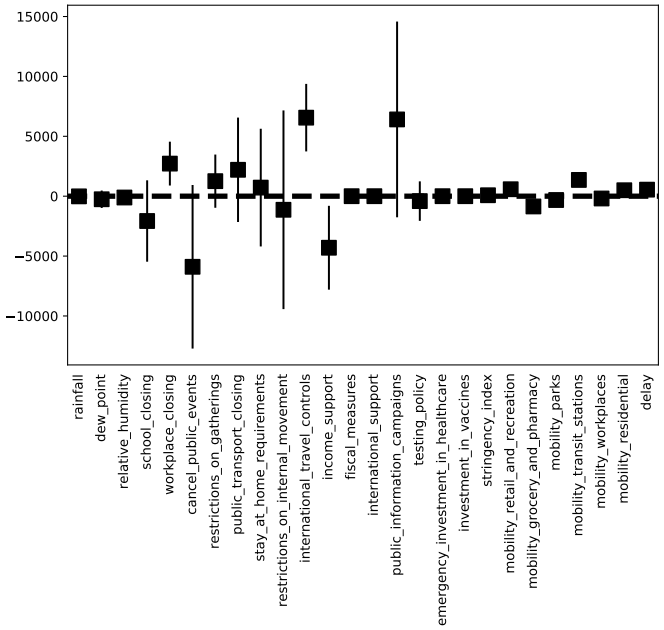


Fig. 2. Coefficients of regression equations with 95% confidence interval.

C. Linear Regression

Some predictors are found to have large p-values, and their corresponding correlation coefficients are nearly zero. Such predictors are not significant. We choose the level of significance $\alpha = 0.05$ and skip the predictors with p-values greater than α. Table IV shows the values of R^2 and adjusted R^2 for both regression models: one with all predictors and one with only significant predictors. Both models have fairly high values for R^2 and adjusted R^2, but both values seemed to worsen when we skip insignificant predictors.

TABLE IV. R^2 AND ADJUSTED R^2 VALUES FOR DIFFERENT LINEAR REGRESSION MODELS

	R^2	Adjusted R^2
Model with all predictors	0.989	0.987
Model with significant predictors	0.986	0.985

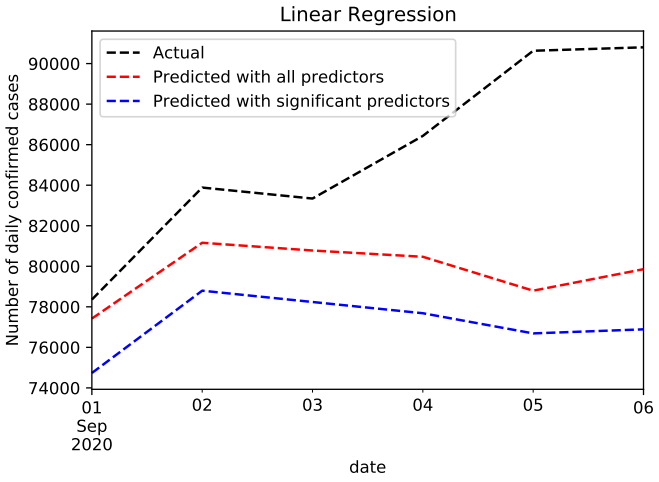


Fig. 3. Comparison of actual daily case counts with predicted counts from two regression models: one with all predictors and one with significant predictors.

Fig. 3 compares the results of both models against the actual values. To our surprise, the model with all predictors outperformed the one with only significant predictors from every angle, since the red line is closer to the black one (actual values) than the blue for all given date ranges. Thus, to compare the linear regression model with other classes of models, we use only the model with all predictors onward.

D. Elastic Net Regularization

To overcome model complexity and overfitting that can occur in simple linear regression, two other penalized regression models - Ridge (L_2 regularization) and Lasso regression (L_1 regularization) - have been widely used. The overfitting occurs due to the large model parameters. The elastic net regularization is used as same as the ridge or Lasso. If the mixing parameter is zero, then we can use ridge regression. If the mixing parameter is one, then we can use the lasso regression [40].

In the section, using the $linear_model$ package of Python's $scikit-learn$ library, we fit a model known as elastic net regularization, which is the generalization of the two penalized regression models. This class of models has two hyper-parameters:

- α : mixing parameter, which controls the type of regression
- λ : shrinkage parameter which is the amount of the shrinkage.

The search space is chosen as

$$\begin{aligned} \alpha &\in \{0.1, 0.2, \ldots, 1\}, \\ \lambda &\in \{10^{-5}, 10^{-4}, \ldots, 10^{-1}, 1, 10^{1}, 10^{2}\}. \end{aligned}$$

After hyperparameter tuning, the optimal values turned out to be $\alpha = 0.2$ and $\lambda = 0.1$. Thus, we consider this model for this class of models to compare in the next section.

E. Random Forest Regressor

Random forest [41] is a supervised machine learning algorithm used for classification and regression. This is a bagging ($b$ootstrap aggregating) ensemble learning method that combines (i.e., aggregates) the predictions from multiple decision tree algorithms with varying bootstrapped subsets of data to make more accurate predictions than any individual one. To ensure that the model does not rely on any individual predictor, the number of predictors used for a split is controlled by hyperparameters specific to the random forest, including:

- n_estimators = number of trees in the forest,
- max_features = number of maximum features to consider at every split,
- max_depth = maximum number of levels in the tree,
- min_samples_split = minimum number of samples required to split a node,
- min_samples_leaf = minimum number of samples required at each leaf node, and
- bootstrap = method of selecting samples for training each tree.

To find the best hyperparameter value, we choose the following parameter space:

$$\begin{aligned} \texttt{n\_estimators} &\in \{50, 100, 200, 500, 1000\} \\ \texttt{max\_features} &\in \{'auto', 'sqrt'\} \\ \texttt{max\_depth} &\in \{5, 20, 50, 100\} \\ \texttt{min\_samples\_split} &\in \{2, 5, 10\} \\ \texttt{min\_samples\_leaf} &\in \{1, 2, 4\}. \end{aligned}$$

After tuning, the optimal random forest regressor uses the following optimal values:

$$\begin{aligned} \texttt{n\_estimators} &= 200 \\ \texttt{max\_features} &= 'auto' \\ \texttt{max\_depth} &= 50 \\ \texttt{min\_samples\_split} &= 2 \\ \texttt{min\_samples\_leaf} &= 5. \end{aligned}$$

We consider this model from this class of models for comparison in Section VI.

F. XGBoost Regressor

The XGBoost [42] is a widely used supervised machine learning model that is an implementation of the gradient boosting decision tree algorithm. The validity of this statement can be inferred by knowing about its (XGBoost) objective function and base learners. The objective function contains a loss function and a regularization term. It tells about the difference between actual values and predicted values, i.e how far the model results are from the real values. The most common loss function in XGBoost for regression problems is reg:linear, and that for binary classification is reg:logistics.

Ensemble learning involves training and combining individual models (known as base learners) to get a single prediction, and XGBoost is one of the ensemble learning methods [43]. XGBoost expects to have the base learners which are uniformly bad at the remainder so that when all the predictions are combined, bad predictions cancels out and better one sums up to form final good predictions. This algorithm has the following hyperparameters:

- n_estimators = number of gradients boosted trees,
- objective = a learning objective function corresponding to the learning task,
- learning_rate = step size shrinkage for tree booster,
- max_depth = maximum tree depth for base learners,
- min_child_weight = minimum sum of instance weight (hessian) needed in a child,
- min_samples_leaf = minimum number of samples required at each leaf node, and
- bootstrap = method of selecting samples for training each tree.

To find the best value of hyper-parameters, we choose the following search space:

$$\begin{aligned}
\texttt{n_estimators} &\in \{50, 100, 200, 500, 1000\} \\
\texttt{objective} &\in \{'reg : squarederror', 'reg : squaredlogerror'\} \\
\texttt{learning_rate} &\in \{0.2, 0.5, 0.8\} \\
\texttt{max_depth} &\in \{5, 20, 50, 100\} \\
\texttt{min_child_weight} &\in \{3, 4, 5\} \\
\texttt{silent} &\in \{0, 1\} \\
\texttt{subsample} &\in \{0.2, 0.7\} \\
\texttt{colsample_bytree} &\in \{0.2, 0.7\}.
\end{aligned}$$

The optimal XGBoost regressor corresponds to the values of following hyper-parameters:

$$\begin{aligned}
\texttt{n_estimators} &= 50 \\
\texttt{objective} &= 'reg : squarederror' \\
\texttt{learning_rate} &= 0.5 \\
\texttt{max_depth} &= 5 \\
\texttt{min_child_weight} &= 5 \\
\texttt{silent} &= 0 \\
\texttt{subsample} &= 0.7 \\
\texttt{colsample_bytree} &= 0.7.
\end{aligned}$$

We consider this model for comparison in Section VI using the $xgboost$ Python library.

G. Recurrent Neural Network (RNN)

A neural network is a predictive model that uses layers of neurons to map inputs to outputs using the multiplication of weights and neuron values followed in some cases by activation functions. The weights are optimized using back-propagation. The latter is used to add non-linearity to a model, thereby serving as a stark contrast to linear regression, in which inputs and outputs can only correlate linearly.

A typical neural network has input, output, and hidden layers. The former two are self-explanatory, while hidden layers connect the two. A recurrent neural network is a variation of this that involves time. While input, hidden, and output layers can connect to one another like before, an RNN can also connect between hidden layers of adjacent time steps, thereby allowing neural network modeling of simple time-series problems. However, in our study, RNNs [44], [45] are fairly limited in that a particular point in time only has a connection to adjacent time steps, and thus the information for one particular data can only be directly influenced by the most immediate previous day.

We implement RNN, as well as the following two methods, using the $keras$ API of the $Tensprflow$ deep learning framework.

V. Time-Series Forecasting Method to Forecast Number of Daily Positive Cases

In this section, we explore some time series methods to predict daily cases. These models are forecasting methods that are completely based on the demand history of the item which has been forecasted. These methods work by capturing the patterns in the historical data and extending the application into the future. They are appropriate when you can assume a reasonable amount of continuity between the past and the future. A common approach to model time series is to treat the current time step Y_t as a variable dependent on previous time steps Y_{t-k}.

A. Long Short-Term Memory Network (LSTM)

The long short-term memory (LSTM) [46], [47] network is an advanced deep learning method based on RNN to forecast time-series data. Instead of neurons, LSTM networks have memory blocks that are connected through layers. A block has components that make it smarter than a classical neuron and a memory for recent sequences. A block contains gates that manage the block's state and output. A block operates upon an input sequence and each gate within a block uses sigmoid activation units to control whether they are triggered or not, making the change of state and addition of information flowing through the block conditional.

Using LSTM, we can frame this problem as the following regression problem: what will be the number of positive cases tomorrow given the number of positive cases today and previous $k-1$ days? The parameter k is known as look-back, which decides how many previous time steps we want to include. For simplicity, we choose $k = 1$. Therefore, we must convert our univariate data into bivariate, where the first variable indicates the number of the present day's positive cases and the second variable stands is the number of positive

cases predicted on the next day. Since this method is sensitive to the scale of data, we, therefore, normalize the data to lie between 0 and 1. To build this model, we use the default settings.

B. Exponential Smoothing

Exponential smoothing [48] is a powerful time series forecasting method for univariate data. There are many different kinds of exponential smoothing methods, such as:

- Simple exponential smoothing,
- Double exponential smoothing (Holt method),
- Triple exponential Smoothing (Holt-Winters method).

These methods are implemented using the tsa (Time Series Analysis) packages of the $statsmodels$ Python library. Each of these methods is explored further in the following subsections.

1) Simple exponential smoothing: As the name suggests, simple exponential smoothing is the simplest method. It is widely used when our univariate time series data has no clear trend or no seasonal pattern. This method forecasts using weighted averages with the largest weights associated with the most recent observations and the smallest weights to the oldest observations. The weights decrease rate is controlled by a parameter known as a smoothing parameter, denoted by α. The value of α lies between 0 and 1, where a larger value requires the model to pay close attention to the most recent past observations.

The extreme cases are:

- $\alpha = 0$: Becomes an average since all weights are equal and the next predicted value is equal to the average of historical data,
- $\alpha = 1$: Becomes a naive method since a weight's most recent observation is one and all others are zero. Thus, the next predicted value is the same as the recent observation.

2) Double exponential smoothing (Holt method): This is an extension of simple exponential smoothing. Double exponential smoothing was proposed by Holt in 1957. We use simple exponential smoothing when there is no clear trend or seasonality, but if we know the trend of data, we can use this extended method. Holt's method involves the following two parameters:

- $\alpha =$ smoothing parameter,
- $\beta =$ trend smoothing parameter.

Both parameters take values between 0 and 1. There is also an option to choose a trend type. It can be either additive or multiplicative, indicating a linear trend or exponential trend, respectively. In Section 5, we found the admissible value for smoothing parameter α. Thus, we consider the fixed value of $\alpha = 0.8$ and then determine the optimal trend type with fixed values of α and β.

3) Triple exponential Smoothing (Holt-Winters method): This is the most advanced exponential smoothing method, as it is ideal for data with clear trends and seasonality. It has the power to add support for seasonality in a model. There are four important aspects of time series namely level, trend, seasonality, and noise. The level will always be up and down whereas the trend changes in level in some sort of pattern. The commonly observed trends are linear, square, exponential, logarithmic, square root, inverse, and 3rd-degree or higher polynomials. Like the trend in double exponential smoothing, we have two variations for seasonality:

- Additive method: the seasonal variations are constant,
- Multiplicative method: the seasonal variations changes with time.

C. Auto Regressive Integrated Moving Average (ARIMA)

Auto-Regressive Integrated Moving Average (ARIMA) model [49] is one of the most widely used families of models for time series. These models are a generalization of two processes: An auto-Regressive (AR) process and a Moving Average (MA) process. Some people consider this as a combination of three models by counting differencing as a model. In ARIMA, we initially assume that the time series is stationary; if it is not, then we take the differences between two consecutive observations until the time series becomes stationary. An ARIMA model is classified by three following parameters:

- p : number of autoregressive terms,
- d : number of nonseasonal differences needed to make time series stationary,
- q : number of lagged forecast errors in the prediction equation.

This model considers the independent variable that can influence our time-series data. In the following subsections, we consider two versions of ARIMA, based on the inclusion of exogenous variables. Both versions are implemented using the $pmdarima$ package in Python.

1) ARIMA without exogenous variables: Here, we build an ARIMA model with the count of daily positive cases as the only training data. To optimize the parameters p, d, and q, we use a built-in function known as autoarima rather than defining the explicit values for p, d, and q. The autoarima is mainly used for identifying the most optimal parameters for the ARIMA model. It settles on a single-fitted ARIMA model. This method is completely based on the commonly used R function.

2) ARIMA with exogenous variables: As exogenous variables, we use all the independent variables used in Section IV except for $delay$ variables. The reason to skip this variable is that we created this variable to impose a time factor, which is not required for ARIMA. Autoarima is used here as well.

VI. Results and Analysis

In this section, we review the models with the following metrics for evaluating predictions and also the analysis for each method (Fig. 4).

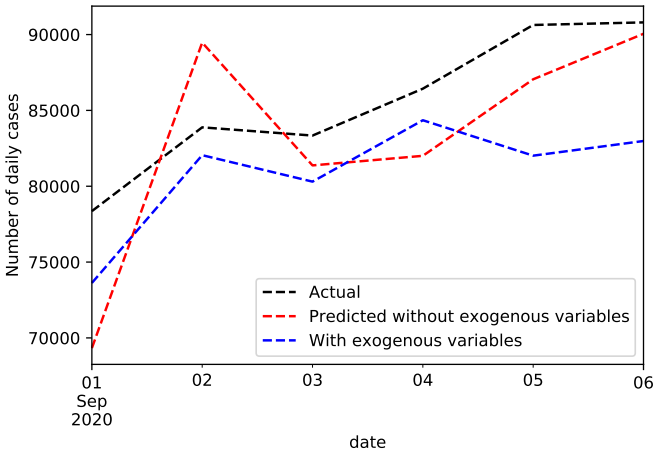


Fig. 4. Comparison of SARIMA models.

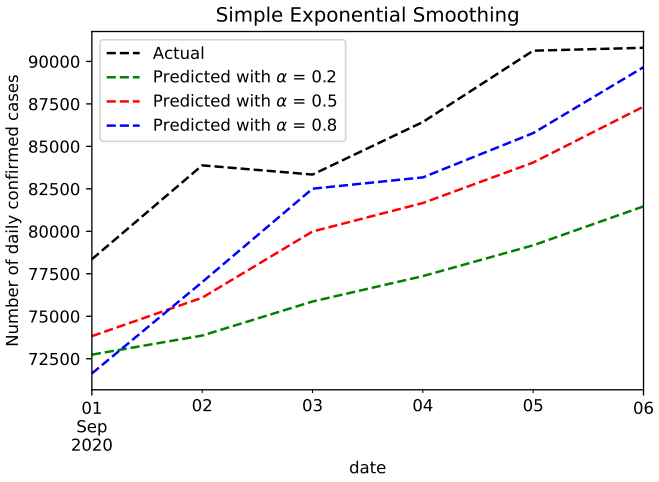


Fig. 5. Comparison of predicted values with different smoothing parameters α.

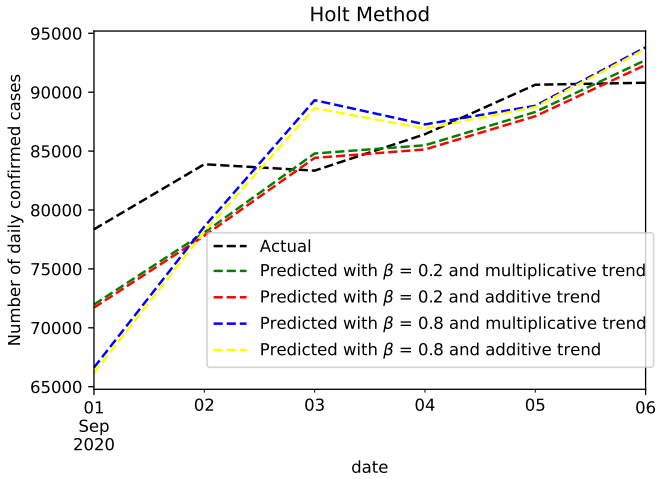


Fig. 6. Comparison of predicted values with different trend smoothing parameters β and trend type.

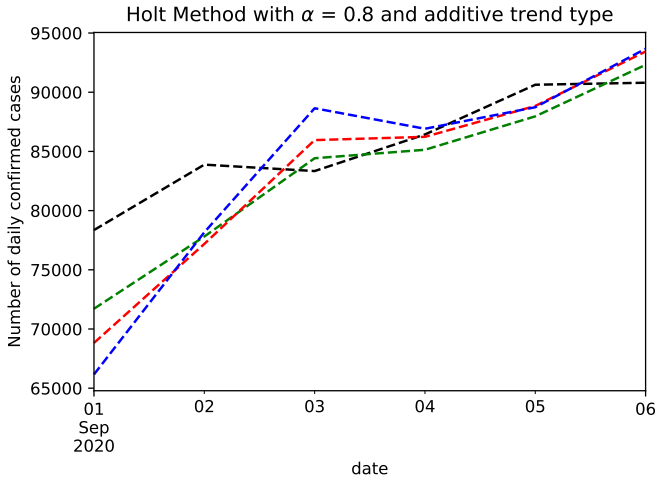


Fig. 7. Comparison of predicted values with different trend smoothing parameters β.

- Mean absolute error (MAE): Average of the absolute differences between predicted and actual values. It is used when we care only about the magnitude of the error and not the direction.
- Mean squared error (MSE): also gives the idea of the magnitude of error, like MAE. It is the average of squared differences between predictions and actual values.
- Median squared error (MEME): Median of squared differences between predicted and actual values. Since the mean is not robust. The mean is much more sensitive to extreme values than the median. Therefore we consider MEME as an alternative evaluation metric.
- Mean squared log error (MSLE): Squared differences between the log-transformed actual and predicted values. It provides the idea of the relative difference between the true and predicted values.

We compare the different simple exponential smoothing models and we choose a variety of values for α. The resultant predicted values are given in Fig. 5. For most of the dates, predicted values from the model with $\alpha = 0.8$ are the closest to actual values. Therefore from this family, we choose the simple exponential smoothing model with $\alpha = 0.8$ to compare it with other classes of models.

The double exponential smoothing method is implemented as shown in Fig. 6. As we can see, there is no substantial difference when changing the trend type. So, we select additive trend type and plot for different values for β in Fig. 7. As indicated in the figure, there is no admissible choice for β. Therefore, we will consider all three methods with $\beta = 0.2, 0.5$, and 0.8 in Section VI.

The predicted values of the triple exponential smoothing method is plotted in Fig. 8 for a different type of trend and seasonality. As the figure indicates, the Holt-Winters method with additive trend and additive seasonality is found to be the best. In Fig. 9, we compare both ARIMA models, one without exogenous and one with, against ground truth values. As

TABLE V. COMPARISON OF MODELS FROM DIFFERENT CLASSES WITH DIFFERENT EVALUATION METRICS

Model	MAE	MSE	MESE	MSLE
Linear regression	4804.8860	6172.9314	2723.2462	0.0054
Elastic net regularization	7265.5959	8245.1422	5342.1506	0.0100
Random forest regressor	11351.8833	11827.2160	9998.6333	0.0220
XGBoost regressor	10130.6125	10566.9168	9346.6719	0.0173
Simple exponential smoothing	4507.6726	5045.6480	4851.4896	0.0040
Holt with $\beta = 0.2$	3552.8030	4266.5536	2670.3701	0.0030
Holt with $\beta = 0.5$	4168.4262	5401.2516	2615.0862	0.0050
Holt with $\beta = 0.8$	5120.1373	6533.2962	5305.5930	0.0076
Holt-Winters	1629.8258	2253.0399	506.1216	0.0007
ARIMA	4918.0511	5459.2333	4427.1078	0.0048
ARIMA with exogenous variables	4061.0362	4766.3267	3037.7827	0.0033
SARIMA	4918.0511	5459.2333	4427.1078	0.0048
RNN	7604.9391	7895.1482	8395.9531	0.0098
GRU	4490.1203	5020.4703	5372.7188	0.0039
LSTM	6238.7969	6588.8430	7022.9141	0.0067

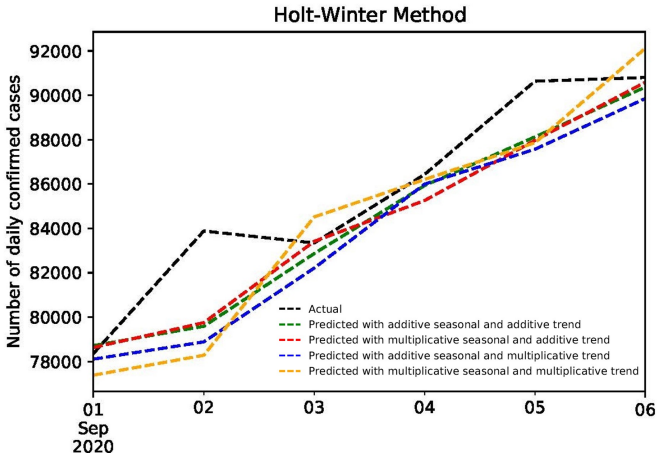


Fig. 8. Comparison of predicted values with a different type of trend and seasonality.

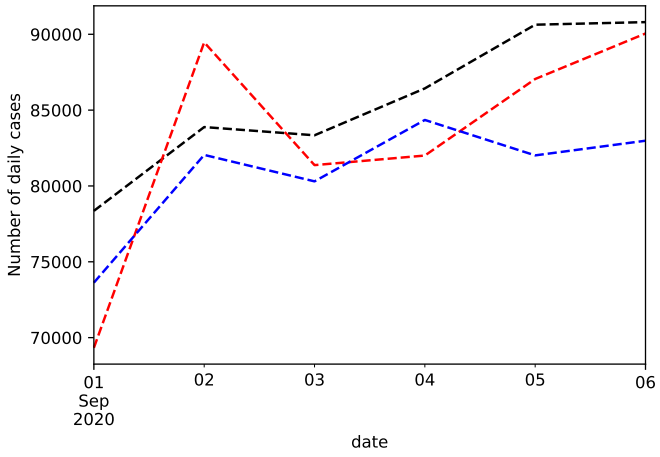


Fig. 9. Comparison of ARIMA models.

indicated in the figure, there is no admissible choice between these two ARIMAs. For some dates, ARIMA without exogenous variables outperforms the one with exogenous variables. Therefore we will consider both models for comparison in Section VI.

Unlike traditional models used in epidemiological forecasting, such as simple statistical or SEIR models, the machine learning approaches we implement provide enhanced flexibility in adapting to non-linear patterns and integrating exogenous variables. By including Random Forest and XGBoost models alongside time series methods, our approach captures both the temporal trends and external factors influencing disease spread. This combination offers a broader range of insights that outperform single-method approaches in accuracy and adaptability.

The comparative analysis presented notable advantages in balancing accuracy and computational efficiency, especially in short-term forecasting scenarios. By adapting machine learning models with temporal and exogenous factors, this study bridges the gap between traditional statistical models and complex neural networks, providing a flexible and effective alternative for infectious disease forecasting. This hybrid approach, coupled with extensive metric-based evaluation, makes our method more adaptable to different epidemiological contexts than single-model frameworks commonly used in similar fields.

A. Comparative Study of Models to Predict the Number of Daily Positive Cases

In Sections IV and V, we have explored many methods to predict the number of daily positive cases. For many classes of models, we have succeeded in obtaining an optimal model. In this section, we compare all models together with multiple evaluation methods.

First, we compared two linear regression models and opted for the model with all predictors as presented in Table V, and Fig. 10. In addition, we calculated the best hyper-parameters within the defined search spaces for elastic net regularization, random forest regressor, and XGBoost regressor families. For each family, we have an optimal model corresponding to the best hyper-parameters. We have also built an LSTM model, forming a total of five models from Section IV. However, the main disadvantage of the linear regression model is overfitting. The elastic net regularization can cause a small bias

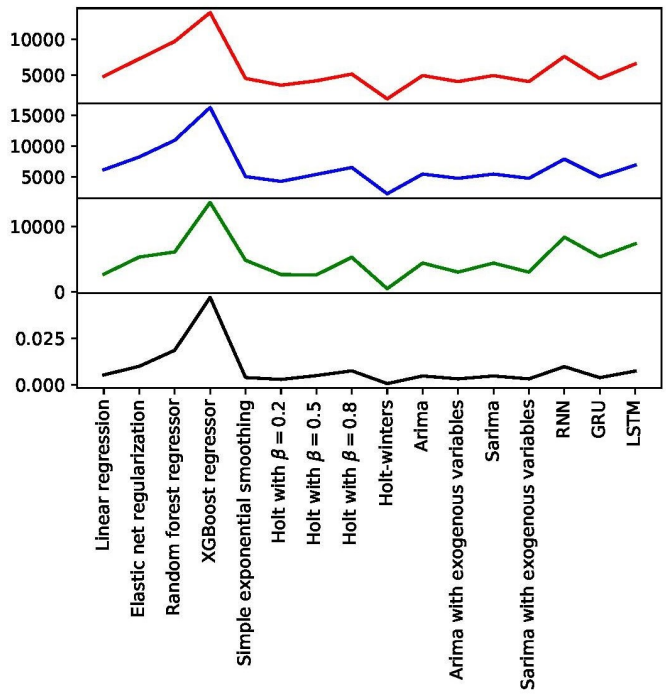


Fig. 10. Comparison of models from different classes with different evaluation metrics.

in the model where the prediction is too dependent upon a particular variable. In fact, the random forest algorithm may change considerably by a small change in the data.

In Section V, we explored some time-series forecasting methods. For the simple exponential smoothing method, we have chosen the model with smoothing parameter $\alpha = 0.8$. For the Holt method, we did not obtain anyone's admissible method. Thus, we decided to have three models with smoothing parameter $\alpha = 0.8$, additive trend type, and corresponding to the trend's smoothing parameters $\beta = 0.2, 0.5$, and 0.8. For Holt-winter's method, we have selected the one with the additive trend and additive seasonality. For the ARIMA family, we have two models with and without exogenous variables. Thus, we have seven models from Section V.

B. Predicted Number of Daily Deaths

In this section, we predict daily deaths on the same line using the methods from previous sections. We provide the final results in the following table and graphs. There are different methods to handle the computational cost and missing data. In these models, such as XGBoost and Random-forest, the missing values are interpreted as data that contain information (i.e. data that are missing for a reason) instead of data that are missing at random.

VII. Conclusions

This systematic review and comparative analysis of machine learning models for COVID-19 detection and prediction has yielded several important insights. Our study contributes to the field of infectious disease modeling by providing a comprehensive comparison of machine learning models, each tested with a range of evaluation metrics to ensure robust findings. Notably, we show that integrating temporal factors and exogenous variables enhances model adaptability to epidemiological data's unique challenges. Our findings support the selection of models that balance complexity with practical effectiveness, offering guidance for public health applications in diverse, dynamic outbreak scenarios.

- Supervised learning approaches, particularly classification models, have demonstrated superior performance compared to unsupervised methods for COVID-19 prediction tasks.
- Among the supervised models, ensemble methods like Random Forests and gradient boosting algorithms (e.g. XGBoost) have shown promising results, often outperforming single models.
- Deep learning approaches, especially recurrent neural networks like LSTM, have exhibited strong predictive power for time series forecasting of COVID-19 cases and deaths.
- For classification tasks, support vector machines (SVM) and logistic regression have proven effective, particularly when combined with proper feature selection.
- Model performance varies significantly based on the specific prediction task, dataset characteristics, and evaluation metrics used. No single model emerged as universally superior across all scenarios.

Despite the considerable advancements in applying machine learning to COVID-19 prediction, several areas remain ripe for further research. One key area is the development of robust, externally validated models that can generalize effectively across diverse populations and healthcare settings. Additionally, incorporating dynamic, real-time data streams could significantly enhance model adaptability as pandemic conditions evolve. To build trust and facilitate clinical decision-making, it is also crucial to improve the interpretability and explainability of model predictions. Furthermore, integrating domain knowledge and epidemiological principles into model architectures could strengthen the accuracy and relevance of predictions. Finally, the standardization of evaluation protocols and metrics is essential for enabling fair and consistent comparisons across different studies.

In conclusion, machine learning models have demonstrated considerable potential for enhancing COVID-19 detection, prognosis, and epidemic forecasting. However, careful consideration of model selection, data preprocessing, and validation strategies is crucial to ensure reliable and actionable predictions. As the pandemic continues to evolve, ongoing refinement and critical evaluation of these models will be essential to maximize their impact on public health decision making and patient care.

Acknowledgment

The authors would like to thank everyone who facilitated this research study and provided the necessary support.

REFERENCES

[1] Nature Editorial, "The covid decade: global preparedness, research and resilience," *Nature*, vol. 592, no. 7852, pp. 7–8, 2021.

[2] D. Cucinotta and M. Vanelli, "Who declares covid-19 a pandemic," *Acta bio-medica: Atenei Parmensis*, vol. 91, no. 1, pp. 157–160, 2020.

[3] Worldometers, "Countries where coronavirus has spread," 2021, may 2020, [online] Available: https://www.worldometers.info/coronavirus/countries-where-coronavirus-has-spread/.

[4] Y. Zheng, Y. Ma, J. Zhang, and X. Xie, "Covid-19 and the cardiovascular system," *Nature Reviews Cardiology*, vol. 17, no. 5, pp. 259–260, 2020.

[5] P. Damacharla, A. Rao, J. Ringenberg, and A. Javaid, "Tlu-net: A deep learning approach for automatic steel surface defect detection," in *Proceedings of the 2021 International Conference on Applied Artificial Intelligence (ICAPAI)*, Suzhou, China, 2021, pp. 1–6.

[6] P. Dhakal, P. Damacharla, A. Y. Javaid, H. K. Vege, and V. K. Devabhaktuni, "Ivacs: I ntelligent v oice a ssistant for c oronavirus disease (covid-19) s elf-assessment," in *2020 International Conference on Artificial Intelligence & Modern Assistive Technology (ICAIMAT)*, 2020, pp. 1–6.

[7] International Monetary Fund, *World Economic Outlook, October 2020: A Long and Difficult Ascent*. Washington, DC: IMF, 2020.

[8] World Health Organization, *COVID-19 Strategic Preparedness and Response Plan*. Geneva: WHO, 2020.

[9] MDPI Editorial Office, "Special issue "machine learning in infectious disease epidemiology"," *Pathogens*, 2023.

[10] D. Parbat and M. Chakraborty, "A python based support vector regression model for prediction of covid19 cases in india," *Chaos, Solitons & Fractals*, vol. 138, p. 109942, 2020.

[11] F. Petropoulos and S. Makridakis, "Forecasting the novel coronavirus covid-19," *PloS one*, vol. 15, no. 3, p. e0231236, 2020.

[12] Z. Zhao *et al.*, "Prediction of the covid-19 spread in african countries and implications for prevention and control: A case study in south africa, egypt, algeria, nigeria, senegal and kenya," *Science of the Total Environment*, vol. 729, p. 138959, 2020.

[13] S. Sánchez-Caballero, M. A. Selles, M. A. Peydro, and E. Perez-Bernabeu, "An efficient covid-19 prediction model validated with the cases of china, italy and spain: Total or partial lockdowns?" *Journal of Clinical Medicine*, vol. 9, no. 5, p. 1547, 2020.

[14] S. F. Ardabili, A. Mosavi, P. Ghamisi, F. Ferdinand, A. R. Varkonyi-Koczy, U. Reuter, T. Rabczuk, and P. M. Atkinson, "Covid-19 outbreak prediction with machine learning," *Algorithms*, vol. 13, no. 10, p. 249, 2020.

[15] L. Qin *et al.*, "Prediction of number of cases of 2019 novel coronavirus (covid-19) using social media search index," *International Journal of Environmental Research and Public Health*, vol. 17, no. 7, p. 2365, 2020.

[16] P. Arora, H. Kumar, and B. K. Panigrahi, "Prediction and analysis of covid-19 positive cases using deep learning models: A descriptive case study of india," *Chaos, Solitons & Fractals*, vol. 139, p. 110017, 2020.

[17] National Center for Biotechnology Information, "Challenges and opportunities in disease forecasting," *Nature Communications*, vol. 9, no. 1, pp. 1–4, 2018.

[18] K. Sarkar, S. Khajanchi, and J. J. Nieto, "Modeling and forecasting the covid-19 pandemic in india," *Chaos, Solitons & Fractals*, vol. 139, p. 110049, 2020.

[19] S. Geisser, "Predictive inference," 2017.

[20] P. Damacharla, A. Y. Javaid, J. J. Gallimore, and V. Devabhaktuni, "Common metrics to benchmark human-machine teams (hmt): a review," *IEEE Access*, vol. 6, pp. 38 637–38 655, 2018.

[21] J. Allotey, E. Stallings, M. Bonet *et al.*, "Clinical manifestations, risk factors, and maternal and perinatal outcomes of coronavirus disease 2019 in pregnancy: living systematic review and meta-analysis," *BMJ*, vol. 370, p. m3320, 2020.

[22] Z. Yang, Z. Zeng, K. Wang *et al.*, "Modified seir and ai prediction of the epidemics trend of covid-19 in china under public health interventions," *Journal of Thoracic Disease*, vol. 12, no. 3, p. 165, 2020.

[23] W. Liang, H. Liang, L. Ou *et al.*, "Development and validation of a clinical risk score to predict the occurrence of critical illness in hospitalized patients with covid-19," *JAMA Internal Medicine*, vol. 180, no. 8, pp. 1081–1089, 2020.

[24] L. Yan, H.-T. Zhang, J. Goncalves *et al.*, "An interpretable mortality prediction model for covid-19 patients," *Nature Machine Intelligence*, vol. 2, no. 5, pp. 283–288, 2020.

[25] J. Gong, J. Ou, X. Qiu *et al.*, "A tool for early prediction of severe coronavirus disease 2019 (covid-19): a multicenter study using the risk nomogram in wuhan and guangdong, china," *Clinical Infectious Diseases*, vol. 71, no. 15, pp. 833–840, 2020.

[26] K. Chatterjee, K. Chatterjee, A. Kumar, and S. Shankar, "Healthcare impact of covid-19 epidemic in india: A stochastic mathematical model," *Medical Journal Armed Forces India*, vol. 76, no. 2, pp. 147–155, 2020.

[27] A. Tomar and N. Gupta, "Prediction for the spread of covid-19 in india and effectiveness of preventive measures," *Science of The Total Environment*, vol. 728, p. 138762, 2020.

[28] V. K. R. Chimmula and L. Zhang, "Time series forecasting of covid-19 transmission in canada using lstm networks," *Chaos, Solitons & Fractals*, vol. 135, p. 109864, 2020.

[29] C. J. Murray and I. C.-. health service utilization forecasting team, "Forecasting covid-19 impact on hospital bed-days, icu-days, ventilator-days and deaths by us state in the next 4 months," 2020, medRxiv.

[30] G. Pandey, P. Chaudhary, R. Gupta, and S. Pal, "Seir and regression model based covid-19 outbreak predictions in india," 2020, arXiv preprint arXiv:2004.00958.

[31] R. Sujath, J. M. Chatterjee, and A. E. Hassanien, "A machine learning forecasting model for covid-19 pandemic in india," *Stochastic Environmental Research and Risk Assessment*, vol. 34, no. 7, pp. 959–972, 2020.

[32] S. Ghosal, S. Sengupta, M. Majumder, and B. Sinha, "Linear regression analysis to predict the number of deaths in india due to sars-cov-2 at 6 weeks from day 0 (100 cases - march 14th 2020)," *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, no. 4, pp. 311–315, 2020.

[33] T. Chakraborty and I. Ghosh, "Real-time forecasts and risk assessment of novel coronavirus (covid-19) cases: A data-driven analysis," *Chaos, Solitons & Fractals*, vol. 135, p. 109850, 2020.

[34] K. D. Johnson, M. Beierlein, and C. M. Bergstrom, "Integrating machine learning with traditional statistical methods for infectious disease forecasting," *Nature Communications*, vol. 14, no. 1, pp. 1–10, 2023.

[35] J. Smith and L. Lee, "Ensemble learning approaches for robust infectious disease prediction across diverse datasets," *Journal of Biomedical Informatics*, vol. 125, p. 104383, 2023.

[36] K. Sarkar, S. Khajanchi, and J. J. Nieto, "Modeling and forecasting the covid-19 pandemic in india," *Chaos, Solitons & Fractals*, vol. 139, p. 110049, 2020.

[37] Y. Kim, S. Park, and J. Lee, "Real-time analytics for enhanced epidemiological modeling: A case study of covid-19 variants," *PLoS Computational Biology*, vol. 19, no. 5, p. e1011052, 2023.

[38] K. Sherratt, S. Abbott, J. Meakin *et al.*, "Evaluating the use of the reproduction number as an epidemiological tool, using spatio-temporal trends of the covid-19 outbreak in england," *Philosophical Transactions of the Royal Society B*, vol. 378, no. 1869, p. 20210308, 2023.

[39] A. K. Gupta, V. Singh, P. Mathur, and C. M. Travieso-Gonzalez, "Prediction of covid-19 pandemic measuring criteria using support vector machine, prophet and linear regression models in indian scenario," *Journal of Interdisciplinary Mathematics*, vol. 24, pp. 89–108, 2021.

[40] L. Yu, X. Ma, W. Wu, Y. Wang, and B. Zeng, "A novel elastic net-based ngbmc (1, n) model with multi-objective optimization for nonlinear time series forecasting," *Communications in Nonlinear Science and Numerical Simulation*, vol. 96, p. 105696, 2021.

[41] M. A. Khan, S. A. Memon, F. Farooq, M. F. Javed, F. Aslam, and R. Alyousef, "Compressive strength of fly-ash-based geopolymer concrete by gene expression programming and random forest," *Advances in Civil Engineering*, 2021.

[42] A. Shehadeh, O. Alshboul, R. E. A. Mamlook, and O. Hamedat, "Machine learning models for predicting the residual value of heavy construction equipment: An evaluation of modified decision tree, lightgbm, and xgboost regression," *Automation in Construction*, vol. 129, p. 103827, 2021.

[43] A. Sahu, P. H. Aaen, and P. Damacharla, "An automated machine learning approach to inkjet printed component analysis: A step toward smart additive manufacturing," in *2024 IEEE Texas Symposium on Wireless & Microwave Circuits and Systems*, 2024.

[44] V. S. Lalapura, J. Amudha, and H. S. Satheesh, "Recurrent neural networks for edge intelligence: a survey," *ACM Computing Surveys (CSUR)*, vol. 4, pp. 1–38, 2021.

[45] P. Dhakal, P. Damacharla, A. Y. Javaid, and V. Devabhaktuni, "Detection and identification of background sounds to improvise voice interface in critical environments," in *2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 2018, pp. 078–083.

[46] B. Lindemann, B. Maschler, N. Sahlab, and M. Weyrich, "A survey on anomaly detection for technical systems using lstm networks," *Computers in Industry*, no. 131, p. 103498, 2021.

[47] P. Damacharla, H. Rajabalipanah, and M. H. Fakheri, "Lstm-cnn network for audio signature analysis in noisy environments," in *10th Annual Conf. on Computational Science & Computational Intelligence (CSCI'23)*. arXiv preprint arXiv:2312.07059, 2023.

[48] W. Sulandari, Suhartono, Subanar, and P. C. Rodrigues, "Exponential smoothing on modeling and forecasting multiple seasonal time series: An overview," *Fluctuation and Noise Letters*, no. 20, p. 2130003, 2021.

[49] A. L. Schaffer, T. A. Dobbins, and S.-A. Pearson, "Interrupted time series analysis using autoregressive integrated moving average (arima) models: a guide for evaluating large-scale health interventions," *BMC medical research methodology*, no. 21, pp. 1–12, 2021.

Augmented Reality in Education: Revolutionizing Teaching and Learning Practices – State-of-the-Art

Samer Alhebaishi[1], Richard Stone[2]
Human-Computer Interaction Department, Iowa State University, Ames, USA[1]
Industrial and Manufacturing Systems Engineering Department, Iowa State University, Ames, USA[2]

***Abstract*—The evolution and contemporary applications of instructional technology, particularly the transformative impact of Augmented Reality (AR) in education, are comprehensively explored in this study. Tracing the journey from early visual aids to sophisticated AR, the aim is to highlight continuous efforts to enhance educational experiences. The effectiveness of AR in increasing student engagement, comprehension, and personalized learning across various disciplines is critically assessed, revealing its potential to transform abstract concepts into tangible experiences. Additionally, challenges in AR adoption, such as technological constraints, the necessity for comprehensive educator training, and strategic curriculum integration, are discussed. The objective here is to identify research gaps, emphasizing the need for standardized evaluation methods, larger sample sizes, and long-term impact studies to fully understand AR's potential. This exploration aims to provide a comprehensive understanding of AR's capability to revolutionize education and to identify pathways for future research and development in this dynamic field.**

Keywords*—*Augmented reality; education; instructional technology; technology integration; student engagement; teacher training

I. Introduction

Augmented Reality (AR) is a technology that enriches the real-world environment by superimposing digital elements onto it, providing interactive experiences spanning multiple disciplines including education, healthcare, and entertainment [1]. The incorporation of technology in education has revolutionized teaching and learning, leading to dynamic, engaging, and personalized educational experiences [2]. Starting by exploring the historical evolution of instructional technology, with a focus on the transformative impact of AR in modern education. From the early use of visual aids such as photographs, slides, and films in the early 20th century, technology has steadily advanced educational methods. Despite early predictions about the revolutionary potential of motion pictures, challenges related to educational quality, costs, and resistance to change meant these tools remained supplementary [3]. The introduction of computers and the internet in the late 20th century represented a major transition towards more engaging and easily accessible learning approaches, including computer-based training and online education platforms [4]. The late 1990s saw a surge in online and blended learning methodologies, further enhancing instructional methods through improved access, flexibility, and reduced costs [3].

The proliferation of smartphones and mobile applications has revolutionized instructional technology, enabling interactive and contextually enriched learning through educational apps and AR technologies [5]. AR, being the latest advancement in instructional technology, superimposes digital information onto the real world, turning abstract concepts into concrete experiences and greatly improving learning outcomes [6]. For instance, AR has been shown to improve cognitive engagement among young learners in language learning [7].

AR applications extend to fields such as engineering, where students can simulate circuit diagrams in real-time using AR and deep learning technologies [5]. However, integrating AR into educational practices poses several challenges, particularly regarding educator readiness. Comprehensive training and support systems are essential to provide educators with the necessary skills and confidence to use AR technology effectively [8].

The acceptance and use of AR are influenced by factors such as perceived usefulness, ease of use, playfulness, and quality output, which are crucial for maintaining student interest and facilitating learning [9]. The evolution of instructional technology, culminating in AR integration, exemplifies a shift towards collaborative, socially situated learning approaches. This shift aligns with constructivist learning theories, advocating for educational technologies that support cooperative learning and knowledge construction [10]. Effective AR integration promises to create new social norms and methods of learning, connecting theoretical knowledge with practical application [11]. While it is important to build on existing literature, it is equally crucial not to focus exclusively on finding new gaps. If the gaps identified several years ago still persist and remain unresolved, they deserve continued attention.

Paper Structure

1) **Section II:** Provides a comprehensive overview of the historical evolution of instructional technologies, with a particular focus on the emergence and application of AR in education.
2) **Section III:** Examines the current perceptions of AR in educational settings, including its impact on student engagement, comprehension, and motivation.
3) **Section IV:** Discusses how AR is transforming education, highlighting its role in enhancing learning across various disciplines, such as science, mathematics, and engineering.
4) **Section V:** Explores strategies to maximize the benefits of AR in education, emphasizing strategic integration, contextualized teaching, and professional development for educators.

5) **Section VI:** Focuses on the roles of educators and students in the effective utilization of AR technology in classrooms.
6) **Section VII:** Reviews related works, providing insights into AR applications across diverse educational contexts and their contributions to academic performance and skill development.
7) **Section VIII:** Presents a detailed discussion, addressing persistent gaps in AR educational research, including the need for Long-term memory retention studies, gamification strategies, and enhanced storytelling techniques.
8) **Section IX:** Concludes the study, summarizing key findings, implications for future research, and recommendations for integrating AR effectively into educational practices.

II. The History of Instructional Technology: From Visual Aids to Augmented Reality

The journey of instructional technology from its nascent stages in the early 20th century to the sophisticated realm of AR reflects a continuous quest to enhance educational methods and engagement. Initially, the educational media movement sought to transform teaching through visual aids like photographs, slides, and films. Despite Thomas Edison's ambitious prediction about motion pictures revolutionizing education, the movement faced challenges such as educational quality concerns, cost, equipment issues, and resistance to change, resulting in visual materials remaining supplementary rather than central to education [3].

With the dawn of the internet era in the late 1990s, distance education underwent a significant transformation, marking a pivotal moment in the history of instructional technology. This period saw a surge in online learning within higher education and institutional training, heralding a new age of accessibility and flexibility in education. The introduction of blended learning methodologies further emphasized the role of technology in providing improved instructional methods, enhancing access and flexibility, and reducing costs. The proliferation of mobile devices enabled learning beyond traditional classroom settings, facilitating personalized educational experiences tailored to individual learner needs and interests [3]. As technology progressed, the introduction of computers and the internet in the late 20th century marked a significant evolution in instructional technology. This period saw a shift towards more interactive and accessible forms of learning, such as computer-based training and online education platforms. The development of Learning Management Systems (LMS) like Blackboard and Moodle facilitated a more structured and accessible educational experience through digital means [4].

The digital revolution marked a significant turning point, with the advent of the internet and personal computing ushering in an era of dynamic and personalized learning experiences. Digital multimedia, interactive simulations, and computer-based training began to take center stage, emphasizing the integration of verbal and visual information to enhance learner comprehension. This period also saw the rise of online courses, video lectures, and tutorials, facilitated by the spread of the internet and mobile technologies, thus supporting both formal and informal learning environments. The effectiveness of video instruction, when designed according to evidence-based principles such as signaling and segmenting, was notable for its ability to guide learners' attention and cognitive processing effectively [12]. In recent years, the incorporation of smartphones and mobile apps into education has further revolutionized instructional technology. Smartphones facilitate the use of educational applications and AR technologies, making learning more interactive and contextually rich. For instance, engineering students can now use smartphone apps to simulate circuit diagrams in real-time, using AR and deep learning technologies to recognize and analyze hand-drawn circuits, thus bypassing more cumbersome traditional simulation tools [5].

Furthermore, platforms like Google Classroom have revolutionized classroom management and educational delivery, allowing for flexible, accessible, and interactive learning experiences. Such platforms support various educational activities, from distributing assignments to facilitating communication between students and teachers, thus enhancing both learning and teaching experiences [4]. As the field continued to evolve, a divergence in terminology and focus emerged, distinguishing between Educational Technology and Instructional Technology. The former relates to the broad spectrum of learning and teaching processes, while the latter is more narrowly focused on guiding learning in specific subjects. This distinction underscored the increasing attention on the role of technology in educational environments and its impact on teaching and training processes [13].

The advent of AR in educational environments marks the newest advancement in instructional technology, offering immersive and interactive learning opportunities, AR overlays digital content onto the physical world, turning abstract concepts into concrete experiences and thus improving learning outcomes. This innovation has been applied to language learning, as demonstrated by Wen [7], where AR-supported activities significantly improved cognitive engagement among young learners. These activities leverage AR to foster collaborative problem-solving and creative expression, emphasizing the active participation of learners in constructing their learning contexts [14] [7]. The evolution of instructional technology, culminating in the integration of AR, exemplifies a shift towards more collaborative, socially situated learning approaches. This shift aligns with constructivist learning theories, advocating for educational technologies that support cooperative learning and knowledge construction. The effective incorporation of technology in education, especially through innovations like AR, has the potential to establish new social norms and approaches to learning, inquiry, and collaboration [10].

The progression of instructional technology from its basic origins to the advanced application of AR in education demonstrates a continuous stream of innovation focused on improving teaching and learning. As AR technologies evolve, their incorporation into educational settings is expected to further transform the ways knowledge is acquired and applied, heralding a new era of immersive learning experiences that connect theoretical knowledge with practical application [11] (Fig. 1).

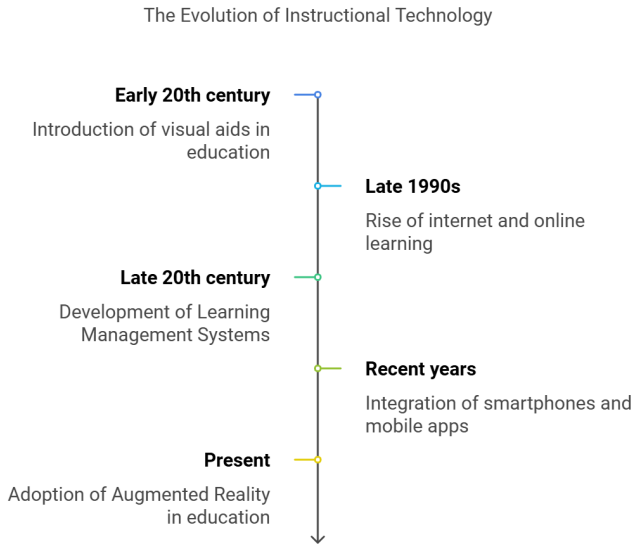


Fig. 1. From visual aids to AR [3] [4].

III. Perception of Augmented Reality in Education

A key aspect of AR's perception in education centers around its ability to increase engagement and motivation among students. Studies have shown that AR's interactive and visually appealing nature makes learning more engaging and enjoyable, which can lead to better comprehension and retention of information. For instance, in a study on AR's application in solar system education, students reported that AR made learning more transparent, interesting, easier to use, and significantly enhanced their understanding of complex astronomical concepts [15].

Moreover, AR has been positively received for its potential to facilitate personalized learning experiences. It allows students to explore learning materials at their own pace and in a manner that suits their learning style, which is particularly effective in subjects that benefit from visual and experiential learning methods. For example, in STEAM education, an AR-enhanced English course demonstrated that AR enhance interactivity and engagement in language learning, significantly boosting students' perceptions of learning and technology [16].

However, the integration of AR into everyday educational practices poses several challenges, particularly concerning the readiness of educators. A study in Malaysia found that while there is significant interest among educators in adopting AR, factors such as perceived usefulness and ease of use are vital for its acceptance and integration into teaching methods. This underscores the importance of providing comprehensive training and support systems to equip educators with the skills and confidence needed to effectively utilize AR technology [8].

The use of AR in classrooms has been shown to significantly increase student engagement and motivation. By providing a dynamic learning environment that goes beyond traditional textbooks and lectures, AR encourages active participation and can lead to deeper understanding and retention of information. This engagement is particularly evident in fields that benefit greatly from visual aids, such as sciences and mathematics, where AR can illustrate complex equations or scientific processes in real-time, enhancing both learning and teaching experiences [17].

However, the acceptance and use of AR in educational settings are influenced by several factors, as modeled by the extended Technology Acceptance Model (TAM). This model includes traditional factors like perceived usefulness and ease of use, which have been shown to directly influence students' behavioral intentions to use AR.

Additionally, external factors such as playfulness and quality output also play significant roles. These elements enhance the educational experience by making learning enjoyable and ensuring that the AR applications are of high quality, which is crucial for maintaining student interest and facilitating learning. Despite the positive aspects, challenges remain in the widespread adoption of AR in education. These include technological limitations, the need for significant investment in AR infrastructure, and the requirement for teacher training on AR usage.

Moreover, educational institutions need to ensure that AR tools are seamlessly integrated into the curriculum in a way that enhances educational outcomes without replacing traditional, effective teaching methods [9]. As AR technology continues to advance and become more widely available, its integration into educational curriculum is expected to expand, highlighting the ongoing need for professional development for educators in this innovative technology [8] (Fig. 2).

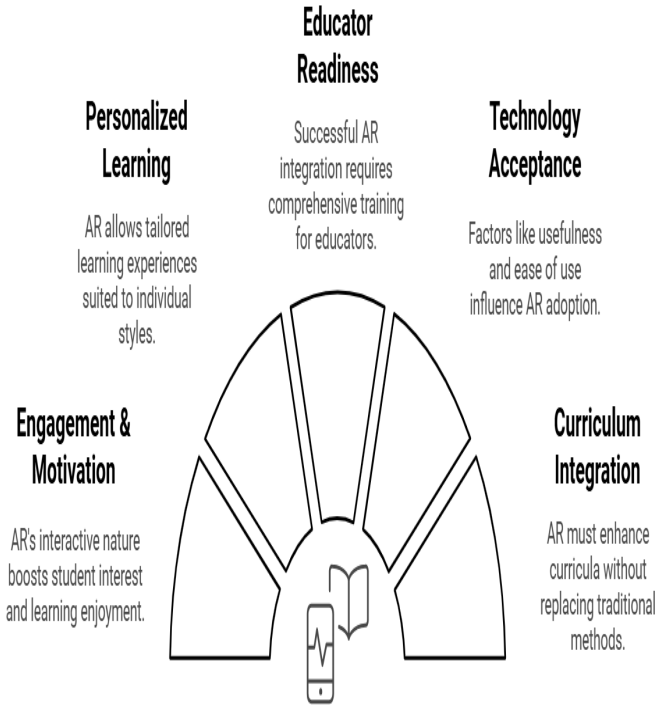


Fig. 2. Impact of augmented reality on educational practices [15] [16].

IV. Transforming Education with Augmented Reality: Enhancing Engagement, Understanding, and Personalized Learning Across Various Fields

AR is revolutionizing the educational landscape by providing innovative methods to engage students and improve learning outcomes. By visualizing abstract concepts, AR significantly enhances student engagement and conceptual understanding [18]. In crime scene investigation training, AR improves the education and training of analysts, offering immersive experiences that boost motivation and information retention [19]. The ability of AR to engage multiple senses simultaneously has been demonstrated to enhance learning outcomes [20]. Furthermore, AR creates vivid, interactive learning environments for remote education [21] and enhances spatial abilities and problem-solving skills [22].

In the realm of mathematics education, AR aids in visualizing complex concepts, making learning more approachable and engaging [23]. Biology education also benefits from AR, which enhances the learning experience with interactive models [24]. Similarly, veterinary anatomical education utilizes AR models to provide in-depth learning of animal anatomy [25]. In engineering education, AR mobile applications offer new and enriched learning experiences [26].

AR applications designed for learning about computer network devices improve understanding through interactive simulations [27]. In pilot education, AR shows potential by enhancing training with immersive simulations [28]. Additionally, AR technology has been used experimentally to determine student learning outcomes, offering valuable insights [29]. In science education, AR applications provide immersive learning experiences in higher education settings [30].

AR promotes the development of cognitive activities in students [31] and benefits the learning of mathematical functions by improving spatial intelligence [32]. It supports the preparation of education projects by providing immersive tools [33], and prepares specialists for the technological era through engaging, immersive experiences [33].

The development of AR mobile applications enhances project-based learning with projection drawings [34]. Reviews of AR's educational applications highlight their effectiveness [35]. Lastly, the versatility of AR is demonstrated through its potential applications in various educational branches [36].

In conclusion, AR is a transformative technology poised to revolutionize education by enhancing engagement, understanding, and personalized learning experiences across various educational fields. This technology not only makes learning more interactive and engaging but also prepares students and professionals for the demands of the modern technological era.

V. Insights to Enhance the Benefits of AR for Education

A. Strategic Integration and Contextualized Teaching

The strategic integration of AR in education involves aligning it with educational goals to improve learning experiences and achieve desired educational outcomes [37]. Emphasizing contextualized teaching approaches is crucial. Teachers should integrate AR in a way that fits the specific context of their lessons, enhancing the learning experience rather than distracting from it [38].

B. Improved Comprehension and Engagement

AR aids in better comprehension by allowing students to visualize complex concepts interactively [39]. This immersive experience makes learning more engaging and enjoyable, leading to improved retention of information [40]. Additionally, AR can reduce stress and anxiety in educational settings by making learning more enjoyable and less intimidating, thus fostering a better learning environment [41].

C. Student Preferences and Performance

A significant number of students have indicated a preference for e-learning methods that incorporate AR, as these methods provide a more engaging and interactive learning experience [42]. This preference highlights the significance of integrating AR into educational frameworks to meet student expectations and enhance learning outcomes [43].

D. Enhanced Spatial Abilities and Immersive Experiences

The use of technology, including AR, significantly increases students' spatial abilities, which is critical in subjects such as mathematics and engineering. This enhancement helps students grasp spatial relationships and geometrical concepts more effectively [39]. AR make learning more immersive and experiential, leading to a deeper understanding and retention of material [38]. AR-based programs have demonstrated a notable enhancement in students' academic performance and practical skills. One study revealed that an AR program led to significant improvements in these areas [44].

E. Teacher and Student Perceptions

Teachers generally have a positive perception of AR, noting its potential to make lessons more dynamic and interactive [45]. However, professional development is necessary to support teachers in effectively incorporating AR into their teaching practices. [46]. On the other hand, AR has been shown to boost student motivation by making learning more engaging and interactive.[47]. Initial teacher training with AR helps future educators understand its benefits and challenges, preparing them to use this technology effectively in their classrooms [48].

F. Real-World Applications and Learning Preferences

AR can bridge the gap between theoretical knowledge and real-world applications by providing students with interactive simulations and models. This practical application of knowledge enhances students' understanding and skills [37]. Different students have different learning preferences, and AR can accommodate different learning styles by providing visual, auditory, and kinesthetic learning experiences [49]. This adaptability makes AR a versatile tool in education. It also emphasizes the importance of creating dynamic and interactive content for AR applications to maximize their effectiveness in educational settings. This comprehensive overview highlights the critical need for engaging and interactive content to enhance their impact in educational environments [50].

G. Enhancing Learning Outcomes with AR

AR supports the cultivation of key skills like problem-solving, critical thinking, and teamwork. A novel Alternate Reality Game-enhanced instructional strategy has been developed, significantly improving students' problem-solving and critical thinking abilities. By integrating interactive and immersive AR experiences into the curriculum, students are better equipped to tackle complex problems, think critically about various scenarios, and collaborate effectively with their peers. This novel method not only boosts student engagement and understanding in learning but also ensures that students develop and hone essential skills necessary for success in academic and real-world environments [51] [52].

Furthermore, it encourages active learning methodologies, ensuring that technology, content, and pedagogy are well-aligned to maximize learning outcomes. This experimental research aims to advocate e-learning approaches that integrate AR for better learning outcomes [53]. The potential of AR to revolutionize education is evident in its ability to create interactive and collaborative learning environments. By promoting engagement and fostering essential skills, AR is poised to be a critical component in modern educational strategies. Ongoing research and development in this field continue to show promising results, further solidifying AR's role in enhancing learning outcomes [54].

VI. The Role of the Educator and Student in Using AR in Education

A. Role of the Educator

Educators play a critical role in integrating AR technologies into the educational process. They facilitate learning through digital tools and ensure these technologies are used effectively to enhance the educational experience [55]. Educators are responsible for providing entrepreneurial education and supporting students in recognizing opportunities, fostering an innovative mindset [56]. Their role extends to integrating AR/VR technologies into the curriculum, creating immersive and interactive learning environments [57]. In the digital era, educators must master digital-based learning media and foster digital skills among students to prepare them for the modern workforce [58]. They also facilitate students' understanding of concrete facts, plan and conduct practical activities, and support engagement with AR tools [59]. Furthermore, educators are instrumental in creating hybrid learning spaces that enhance students' employability[60]. The educators' role includes fostering critical thinking and ensuring that the educational content delivered through AR is relevant and challenging [61]. They must also facilitate research work and support students in engaging with AR tools for practical and theoretical learning [62]. Moreover, they play a role in helping students adapt to AR-enhanced learning environments, which can involve a steep learning curve [63]. Additionally, educators are involved in the choice of pedagogical strategies for preparing STEM teachers to incorporate AR technologies into their teaching[64] effectively. They must also integrate AR tools into subjects such as geometry to enhance spatial understanding and engagement [65]. Moreover, educators facilitate the effective use of AR in MOOCs, improving accessibility and interaction in online learning environments [66].

B. Role of the Student

Students are active participants in the learning process when using AR technologies. They engage with digital tools and participate in interactive and immersive learning activities essential for developing practical skills and knowledge [55]. Students recognize entrepreneurial opportunities and enhance their self-efficacy through entrepreneurial education provided by educators [56]. In an AR/VR learning environment, students engage with immersive and interactive content, significantly enhancing their learning experience and retention of information [57]. They adapt and thrive in digital learning environments, developing digital skills and competencies necessary for the modern workforce [58]. Additionally, students engage in immersive learning experiences, perform practical activities, and apply their knowledge in real-world scenarios facilitated by AR technologies [59]. Students are also responsible for actively participating in hybrid learning spaces and leveraging these environments to enhance their employability [60]. They engage with AR tools to improve their critical thinking abilities and learning gains [61]. Furthermore, students are expected to use AR technologies in their research work, gaining practical experience in their field of study [62]. In the context of teacher education, students (future teachers) are trained to use AR in educational processes, preparing them to implement these technologies in their future classrooms [63]. They also play a crucial role in engaging with AR tools to foster understanding and retention of educational content [66]. Additionally, students benefit from the integration of AR in subjects like geometry, enhancing their spatial reasoning and engagement with the material [65]. They also experience enhanced performance and engagement through the use of quick response (QR) codes and AR in textbooks, making learning more interactive and accessible [67] (Fig. 3).

VII. Related Works

A. Science and Technology Education

Augmented Reality (AR) has demonstrated significant benefits in science education, particularly in complex subjects like physics and nursing. Thees revealed that AR-assisted setups significantly reduce extraneous cognitive load and improve student performance compared to traditional setups. This improvement makes complex concepts more comprehensible and engaging, thereby enhancing overall learning outcomes [68]. Similarly, the study by Rodríguez highlighted AR's positive influence on academic performance and engagement in both online and face-to-face settings. This showcases AR's adaptability to various instructional environments, providing flexibility in delivering educational content [69].

In educational technology, AR systems enhanced with deep learning recommendations, as explored by Lin, improved learning achievement and computational thinking abilities. This highlights the integration of advanced technologies with AR to optimize learning processes and outcomes [70]. Additionally, Thees, (2022) demonstrated that AR head-mounted displays provide more immersive and effective learning experiences during laboratory work, reducing cognitive load and improving learning outcomes [71]. Krüger,

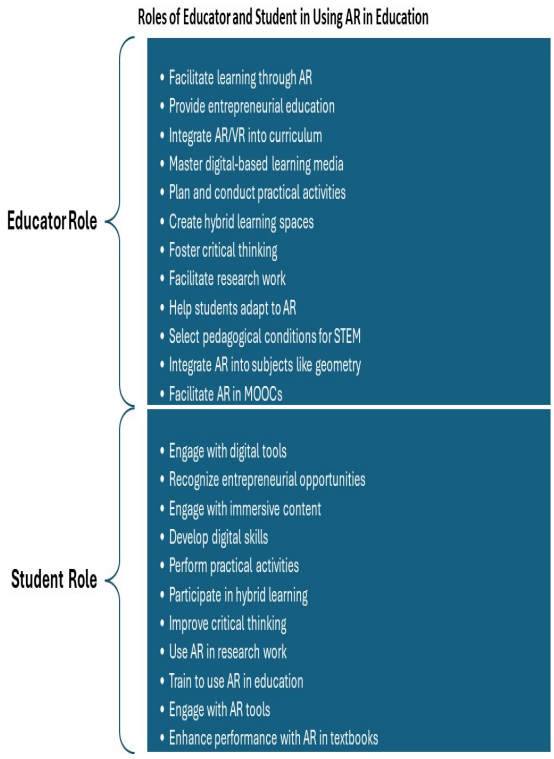


Fig. 3. The diagram highlights the distinct roles of educators and students in integrating and utilizing AR technology in education [55] [58].

(2022) illustrated that 3D AR visualizations led to a higher understanding of spatial relationships compared to 2D visualizations, emphasizing the importance of dimensionality in AR content [72].

B. Cultural Heritage and Language Learning

AR has proven to be highly beneficial in both cultural heritage and language education. Gong elaborated that AR significantly enhances visitor engagement and educational outcomes in museum settings, providing an interactive learning experience that makes cultural artifacts more accessible and engaging [73]. Similarly, Rivas states that AR enhances students' engagement and understanding of cultural heritage through immersive storytelling, making historical and cultural content more relatable and memorable[74]. In the realm of language learning, the study conducted by Ersanli showed that integrating AR with storytelling boosts vocabulary acquisition and motivation in English language learners, making language learning more dynamic and enjoyable [75]. Additionally, Danaei found that AR storybooks enhance reading comprehension in children, outperforming traditional print storybooks with features such as narrators' tone and 3D visuals, which make the reading experience more engaging and effective [76]. Overall, AR has been shown to significantly improve educational outcomes and engagement across various learning contexts.

C. Early Childhood and Primary Education

AR applications have shown promising results in early childhood and primary education, significantly improving academic performance by making abstract concepts more tangible and engaging for young learners [77]. Similarly, Valencia displays that AR boosts academic performance in high school settings, suggesting its effectiveness across different educational levels [78]. Additionally, Midak demonstrated that AR, specifically through the LiCo.STEM mobile app, enhances students' understanding and engagement in natural science concepts by enabling interactive and hands-on learning experiences [79]. Reinforcing these findings, the study by kruger discovers that 3D visualization leads to higher spatial relational knowledge, enhancing comprehension in subjects benefiting from spatial understanding [72]. Moreover, thees reported that AR conditions result in significantly lower extraneous cognitive load and better performance, highlighting the cognitive benefits of AR in complex subjects [68]. Collectively, these studies underscore the potential of AR to enhance educational outcomes across various subjects and educational levels by providing interactive, immersive learning experiences that improve understanding, engagement, and academic performance.

D. Cognitive and Motivational Aspects

Bork emphasized the role of AR in enhancing emotional engagement and learning in medical contexts. This study indicates that collaborative AR experiences can foster deeper understanding and retention of complex anatomical knowledge [80]. Jdaitawi revealed a significant positive impact of AR on student motivation. Utilizing a quasi-experimental design with a pretest-posttest control group, this study shows that AR can effectively increase students' interest and engagement in their studies [81]. Additionally, Chen highlighted the potential of AR to enhance problem-solving abilities and critical thinking skills. This technology provides interactive and stimulating learning environments that encourage active participation and cognitive development [82]. Furthermore, studies from various domains reinforce these findings. For instance, research on AR in physics education revealed that AR-assisted setups significantly lower cognitive load and improve performance [68]. Similarly, findings from a nursing study show that AR positively influences academic performance and learning determinants, including student engagement and satisfaction [69]. These studies collectively underscore AR's capacity to create immersive and effective learning experiences, enhancing both emotional engagement and cognitive outcomes across diverse educational contexts [68].

E. Problem-Based and Inquiry-Based Learning

AR-supported problem-based and inquiry-based learning methods have also been explored extensively, showcasing significant potential in enhancing educational outcomes. Arici details that AR-supported problem-based learning methods substantially enhance students' critical thinking and learning gains in science education [83]. This approach encourages students to actively engage with the material, fostering an environment where they can apply their knowledge in practical scenarios. By immersing students in interactive and contextually relevant experiences, AR allows for a deeper understanding and retention of complex scientific concepts.

Moreover, Wen examined the use of AR in conjunction with the QIMS (Question, Investigation, Modeling, and

Sharing) framework in primary education. highlighted AR's potential to engage students through interactive and creative activities, thereby fostering a deeper understanding and retention of knowledge. The QIMS framework, supported by AR technology, facilitates a structured approach to inquiry-based learning, where students actively participate in questioning, investigating, modeling, and sharing their findings. This method not only enhances their comprehension of the subject matter but also supports the development of essential skills such as self-directed learning, critical thinking, and creative problem-solving [84].

Furthermore, the integration of AR in problem-based and inquiry-based learning environments offers several pedagogical advantages. For instance, AR can simulate real-world problems and scenarios, providing students with opportunities to practice and refine their problem-solving skills in a safe and controlled setting. This immersive experience can lead to increased motivation and engagement, as students are more likely to be captivated by the visually rich and interactive nature of AR content. Additionally, the immediate feedback and adaptability of AR applications allow for personalized learning experiences, catering to the diverse needs and learning paces of individual students [85].

F. Specialized Educational Applications

Specialized applications of AR have been explored in various contexts. Aydoğdu indicates that AR can make educational content more engaging and effective for preschool children [86]. This technology provides interactive and visually appealing learning experiences that capture young learners' attention. In higher education, Christopoulos found that AR enhances the learning experience for medical students, indicating that AR can be a valuable tool in specialized and professional education settings [87]. Ali exhibits that AR positively affects learning outcomes in microeconomics, simplifying complex economic concepts and making them more accessible to students [88]. Additionally, Özeren indicated significant improvements in academic achievement and motivation, suggesting that AR can be an effective tool for enhancing learning experiences across different educational levels and subjects [89].

G. Enhancing Critical Thinking and Reflective Learning

AR's potential to improve critical thinking and reflective learning has been highlighted in several studies. study made by Octavia revealed that AR assignments improved problem-solving abilities and critical thinking skills [90]. This technology provides interactive and challenging learning environments that encourage students to think critically and creatively. Another study by Yoo places importance on the narrative elements in AR presentations can improve learning outcomes in cultural heritage education [91]. This approach makes historical and cultural content more engaging and memorable. Furthermore, Cheng demonstrated the effectiveness of AR in enhancing learning for low-achieving students through hands-on interaction [92]. This method provides practical and engaging learning experiences that can boost students' confidence and performance.

H. Broader Educational Impact

AR's broader impact on education is evident across various studies. Rodríguez highlighted that AR technology can improve learning processes by increasing motivation, performance, and acceptance of educational applications, providing a structured approach to integrating AR into STEAM (Science, Technology, Engineering, Arts, and Mathematics) education [93]. De Paolis illustrated a positive correlation between the usability of AR applications and user experience, indicating that well-designed AR applications can facilitate engaging and enjoyable learning experiences [94]. Additionally, Shaghaghian verified that AR workshops significantly enhanced students' spatial visualization and math test scores, suggesting that AR can be an effective tool for teaching complex subjects and improving students' cognitive skills [95]. Furthermore, Sahin confirmed higher achievement and positive attitudes among middle school students using AR compared to traditional methods [96].

I. Diverse Applications of AR in Education

Recent research has extensively explored the integration of AR in education, highlighting its potential to enhance learning outcomes across various domains. Jdaitawi exposed the significant positive impact of AR on student motivation, showing that AR can effectively increase students' interest and engagement in their studies [81]. Cai found that AR fosters more active student participation and enhanced teacher-student interactions, indicating that AR can create more dynamic and interactive learning environments [97]. Additionally, Ciloglu reports that mobile AR applications significantly improved students' self-efficacy and attitudes towards biology, suggesting that AR can be an effective tool for enhancing students' confidence and interest in their studies [98].

J. Long-Term and Short-Term Memory in AR Education

The impact of AR on long-term memory retention among students requires further investigation. The incorporation of AR technologies has shown significant improvements in memory retention by providing interactive and immersive learning experiences. For instance, the study conducted by Seeliger gives substance to the idea that AR head-mounted displays (HMDs) improve task performance and reduce mental workload [99]. This suggests that AR can enhance short-term memory retention by lowering cognitive load during complex tasks, enabling better immediate recall and application of information. Similarly, Krüger indicates that 3D visualizations in AR improve understanding of spatial relationships, which can be linked to better long-term memory retention [72]. The interactive and engaging nature of 3D AR content helps students form stronger mental models, leading to more effective long-term recall of spatial structures and relationships. Moreover, the study by Christopoulos supports the idea that AR enhances both short-term and long-term memory. By providing hands-on interaction and realistic simulations, AR helps medical students retain complex anatomical knowledge more effectively over time [87].

K. Gamification in AR Education

Gamification is another key element that has been integrated into AR educational applications to boost student

engagement and motivation. It refers to incorporating game design features into non-game environments to enhance enjoyment and motivation in learning. Kao incorporated gamification through AR-based puzzle card assemblies [100]. This approach not only made learning more engaging but also helped in reducing extraneous cognitive load, leading to better academic performance. Jdaitawi conveys that AR was used to create interactive and gamified learning environments. The study found that these environments significantly increased student motivation and interest in their studies. By transforming traditional learning materials into interactive AR experiences, students were more inclined to participate actively and enjoy the learning process [81]. Moreover, Octavia gave prominence to the use of gamified AR assignments to enhance problem-solving abilities and critical thinking skills. The interactive and challenging nature of these assignments encouraged students to engage deeply with the content, thereby improving their overall learning outcomes [90].

VIII. Discussion

The use of AR in education has shown promising results in enhancing learning outcomes, reducing cognitive load, and increasing student engagement. However, several areas require further exploration, particularly regarding long-term memory retention, storytelling, emotional memory, gamification, personalization, and scalability. While the reviewed studies indicate that AR can improve short-term memory retention by lowering cognitive load during complex tasks, more longitudinal studies are needed to confirm if these benefits extend over longer periods. Research that tracks knowledge retention over several months or academic terms is essential. Current methodologies for testing long-term memory retention are flawed, often failing to account for the depth and durability of retained knowledge over extended periods. Research should incorporate more robust measures such as follow-up assessments that test for retention beyond the immediate post-intervention period and should consider the quality of retained knowledge.

Long-term memory retention is a key element in assessing the effectiveness of AR in educational environments. Short-term benefits, such as immediate comprehension and retention, are well-documented, but the true value of AR lies in its potential to embed knowledge deeply into the learner's memory. These studies should employ diverse and rigorous methodologies, including both quantitative and qualitative assessments, to capture a comprehensive picture of long-term retention. Additionally, researchers should consider the nature of the content being taught, as some subjects may inherently lend themselves to better retention through AR-enhanced learning due to their visual or interactive nature.

Therefore, the use of storytelling in AR has great potential but is still underdeveloped. Many current AR applications use basic narratives, missing the opportunity to create more engaging and impactful educational experiences. To fully utilize storytelling in AR, there needs to be a focus on developing richer, more emotionally engaging stories. This includes crafting narratives that evoke emotions like empathy or curiosity, which can help students better remember and connect with the material.

Enhancing storytelling in AR means integrating stories more seamlessly with educational content, making them an integral part of the learning experience. Future efforts should explore advanced storytelling techniques, such as interactive choices and character-driven plots, to increase engagement and personal involvement. It's also crucial to tailor stories to fit the cultural and age-specific needs of learners.

By improving the storytelling aspect of AR, we can create more memorable and effective learning experiences, making education not only informative but also inspiring and engaging. This requires collaboration from experts in education, psychology, and digital media to develop well-rounded and impactful narratives.

Another under-explored area is emotional engagement, which is crucial for memory retention and learning effectiveness. AR's potential to create emotionally engaging experiences could significantly enhance emotional memory, yet few studies have measured this aspect. We should integrate emotional metrics to evaluate how AR influences emotional engagement and memory retention through physiological measurements (like heart rate or Galvanic Skin Response) and subjective assessments (such as self-reported engagement and emotional impact). Understanding the role of emotions in AR-enhanced learning could provide valuable insights into how to design more effective educational experiences. Emotional memory can play a significant role in how well students retain information, as experiences tied to strong emotions are often remembered more vividly and for longer periods. By leveraging AR's immersive capabilities, educators can create scenarios that evoke emotional responses, thus aiding in deeper and longer-lasting learning.

These metrics can be complemented by subjective assessments, including self-report surveys and interviews, to capture the nuances of individual emotional responses. Combining these approaches allows for a holistic understanding of emotional engagement and its impact on learning. Furthermore, it is important to explore the types of emotional content that resonate most effectively with different age groups and cultural backgrounds, as these factors can significantly influence the design and implementation of AR-based educational tools.

In addition to emotional engagement, gamification is noted for increasing student motivation and engagement, yet it needs deeper investigation into how different elements like rewards, challenges, and levels impact learning outcomes across various contexts. While some studies have incorporated elements of gamification, explicit discussions on gamification strategies and their effectiveness are often missing. We should delve deeper into how different gamification elements within AR environments impact student motivation, engagement, and learning outcomes. Detailed analyses of which gamification techniques are most effective in different educational contexts would provide valuable insights for educators and developers. Gamification can include elements such as point systems, leaderboards, badges, and narrative quests, each of which can have varying effects on different age groups and subjects. Understanding the optimal combination of these elements can help in designing AR educational tools that maximize engagement and learning efficiency.The idea of gamification in education goes beyond just entertainment; it involves

strategically integrating game mechanics to enhance learning. Effective gamification requires a balance between challenge and skill, ensuring that tasks are neither too easy nor too difficult, thereby maintaining student engagement. Rewards and feedback mechanisms should be designed to reinforce positive behavior and learning achievements.

Additionally, Storytelling components can be integrated to craft immersive learning experiences that encourage students to explore and learn. Research should focus on identifying the most impactful gamification elements and understanding how they can be tailored to different educational contexts, such as STEM subjects, humanities, and language learning. Furthermore, The combination of AR with other advanced technologies, such as artificial intelligence (AI) and deep learning, has the potential to further improve educational outcomes. For instance, AR systems augmented with AI could deliver real-time feedback and adaptive learning pathways, optimizing the learning process for each individual student. Research should explore the synergistic effects of combining AR with AI and other technologies to create more intelligent and responsive educational tools. The incorporation of AI in education is revolutionizing how students interact with learning materials. AI-powered systems can offer real-time feedback and adaptive learning pathways, improving the personalization of educational experiences. Moreover, integrating AI with AR can create more intelligent and responsive educational tools, significantly improving learning outcomes by catering to individual student needs. These technologies promise to make education more interactive, engaging, and effective, ultimately supporting better retention and comprehension of complex concepts. Integrating AI with AR can create more intelligent and responsive educational tools, significantly improving learning outcomes by catering to individual student needs. These technologies promise to make education more interactive, engaging, and effective, ultimately supporting better retention and comprehension of complex concepts [101] [102]. AI-enhanced AR systems can adjust to each student's unique learning pace and style, providing personalized learning experiences beyond the capabilities of traditional methods. These systems can process large datasets to identify patterns and forecast student performance, allowing for proactive measures to address learning gaps. For example, an AI-powered AR application could adjust the difficulty of exercises based on real-time assessments of a student's performance, ensuring that the learning process remains challenging yet achievable. This level of personalization can sustain student motivation and engagement, resulting in better learning outcomes. Additionally, AI can facilitate the creation of more complex and realistic AR environments, further enhancing the immersive learning experience.

One relevant consideration is the importance of user behavior in creating effective learning experiences. As Wasfi highlights in his study on authentication systems, user behaviour is vital in shaping memorable and secure experiences. Establishing policies and guidelines has been effective in curbing tendencies such as choosing simple or predictable patterns [103]. Similarly, in AR-based educational applications, it is crucial to establish guidelines that promote effective use and prevent potential misuse. Ensuring that AR applications are both engaging and educationally effective requires a careful balance. The technology must be intuitive and user-friendly to minimize cognitive load, allowing students to focus on the learning material rather than the mechanics of the tool.

The Triggered Screen Restriction framework, created by Hariri, is another innovative approach that uses gamification by utilizing the Fear of Missing Out phenomenon, motivating users to achieve specific goals to access certain features. This framework combines behavioral psychology with advanced technology to create a comprehensive solution for gamified interventions, making it a promising avenue for enhancing student engagement through gamification [104]. This negative reinforcement technique can be applied in AR educational settings to enhance learning and engagement. By setting clear, attainable goals and providing immediate feedback, TSR can help maintain high levels of motivation and engagement, particularly in subjects that students might otherwise find challenging or less interesting.

Additionally, there is insufficient emphasis on personalization, which can customize learning experiences to meet individual needs, and scalability, which ensures that AR solutions are practical and effective across various educational contexts. Personalization can significantly enhance the effectiveness of AR by adapting content to the learner's pace, preferences, and learning style. We should investigate adaptive AR systems that can offer personalized feedback and modify the difficulty level according to the learner's performance. Scalability is another critical factor, as it ensures that AR solutions can be implemented widely without compromising their effectiveness. Research should explore the practicality of expanding AR applications across various educational settings, taking into account factors like cost, accessibility, and technological infrastructure. Scalability is particularly important in ensuring that AR educational tools can be adopted in a variety of educational settings, from well-funded institutions to under-resourced schools. Research should explore ways to make AR technology more affordable and accessible, possibly through the development of low-cost hardware and software solutions. Additionally, studies should examine the infrastructure requirements for implementing AR at scale, including the requirement for reliable internet connectivity and technical support. Overcoming these challenges will be vital to ensure that students and educators worldwide can fully experience the advantages of AR in education. Moreover, prolonged use of AR devices can result in discomfort and injuries due to improper posture. Previous studies have shown that inappropriate postures at workstations significantly increase the risk of musculoskeletal disorders. For instance, prolonged sitting with a slouched spine can lead to increased stress on vertebral discs and muscle pain. Similarly, working with the neck in a forward extension for extended periods can also cause discomfort and musculoskeletal disorders. It is essential to consider these factors in the design and use of AR systems to prevent potential injuries. Ergonomic guidelines should be developed and followed to minimize the risk of physical strain and injury, ensuring that students can use AR tools safely and comfortably for extended periods [105]. Ergonomic factors are essential for the sustainable integration of AR in educational environments. Designers of AR devices and applications should prioritize user comfort and safety, incorporating features that promote healthy posture and reduce

physical strain. For example, AR headsets could be designed with adjustable straps and padding to ensure a comfortable fit, and software interfaces could include prompts to encourage users to take breaks and adjust their posture. Additionally, educators should be trained on the importance of ergonomics and how to implement best practices in their classrooms. By addressing these ergonomic challenges, we can establish a safer and more sustainable educational environment for students by utilizing AR technology.

AR shares some challenges with virtual reality, particularly regarding immersive experiences. For instance, Sanaei study in VR environments has identified a substantial inverse relationship between workload and cybersickness [106], suggesting that higher task engagement may reduce the likelihood of experiencing discomfort. This insight can be valuable for AR applications, especially when designing high-cognitive-load tasks that may help distract users from sensory conflicts, thus minimizing the potential for discomfort in educational AR experiences.

A study by Schweiger et al. [107] highlights that non-dominant hand training with computer mouse tasks improves performance in the non-dominant hand and transfers these skills to the dominant hand, leading to overall better performance in computer-based tasks. This bilateral transfer effect can be particularly beneficial in AR settings where fine motor skills and precise interactions are crucial for effective learning and engagement. Integrating non-dominant hand training into AR educational applications could enhance the usability and effectiveness of these tools, providing students with improved control and interaction capabilities. This strategy aligns with the overarching objectives of AR in education, seeking to develop more immersive, interactive, and impactful learning experiences.

By overcoming these challenges, we can develop more effective and engaging educational practices that leverage the full potential of AR technology. This requires sustained effort and interdisciplinary collaboration among educators, researchers, and technologists. Additionally, thinking outside the box and exploring innovative approaches beyond traditional methods will be crucial. By fostering creativity and encouraging unconventional ideas, we can unlock new possibilities and drive the development and progression of AR in educational settings, ultimately improving students' learning experiences and outcomes.

A. Enduring Issues in Augmented Reality Educational Research: Addressing Persistent Gaps

Koumpouros [108] identifies several ongoing gaps in AR research that were noted before 2020 and continue to persist. These gaps include the development of reliable and standardized evaluation methods, which remains challenging due to the diverse applications and contexts of AR. This diversity leads to inconsistent methodologies and hinders comparability across studies. Many studies still employ custom-made, non-validated tools, complicating the generalization of findings. Technical constraints, such as device compatibility and marker recognition issues, persist as the rapid advancement of AR technology often outpaces solutions. High costs of AR technology and development continue to limit accessibility, particularly in resource-constrained environments. Recruiting large and diverse samples is resource-intensive and logistically challenging, especially in niche research areas. Many studies have small sample sizes and short evaluation phases, limiting the validity and generalizability of their results. Conducting long-term studies requires significant time, funding, and participant commitment, while the pressure to produce quick results leads to a focus on short-term studies. Integrating AR into existing educational frameworks necessitates multidisciplinary collaboration, which is time-consuming and hampered by bureaucratic inertia. The novelty effect of AR technology presents an inherent challenge, requiring long-term engagement studies that are resource-intensive. Ethical and privacy concerns are ongoing issues, complicated by the evolving nature of AR technology. Addressing these concerns requires careful consideration of data protection, informed consent, and transparency in data management. The interplay of resource limitations, the rapid pace of technological change, and the inherent complexity of integrating new technologies into established systems contribute to the persistence of these gaps. Addressing them requires concerted efforts from researchers, educators, technologists, and policymakers. We should focus on developing validated evaluation tools, conducting long-term studies with larger and more diverse samples, and addressing technical and ethical challenges to fully realize the potential of AR in education. The persistence of gaps in AR research stems from several interconnected challenges. Developing reliable and standardized evaluation methods remains complex due to the diverse applications and contexts of AR, making consensus difficult. Recruiting large and diverse samples is resource-intensive and logistically challenging, especially in niche research areas. Technical constraints persist as the rapid advancement of AR technology often outpaces solutions, with issues like device compatibility and marker recognition being inherently difficult to solve. Conducting long-term studies requires significant time, funding, and participant commitment, while the pressure to produce quick results leads to a focus on short-term studies. Integrating AR into existing educational frameworks necessitates multidisciplinary collaboration, which is time-consuming and hampered by bureaucratic inertia. Providing comprehensive training for educators and users also requires substantial resources and ongoing support. The high costs of AR technology and development continue to limit accessibility, particularly in resource-constrained environments. Addressing ethical and privacy concerns is an ongoing process, complicated by the evolving nature of AR technology. The novelty effect presents an inherent challenge, necessitating long-term engagement studies that are resource-intensive. Researchers often rely on simpler experimental designs due to funding and time constraints, hindering more robust findings. Additionally, expanding research to examine a broader range of learning outcomes requires interdisciplinary collaboration and a shift in research focus. These gaps persist due to the interplay of resource limitations, the rapid pace of technological change, and the inherent complexity of integrating new technologies into established systems and frameworks. Addressing them requires concerted efforts from researchers, educators, technologists, and policymakers.

IX. Conclusion

The integration of AR in education holds immense promise for transforming teaching and learning practices. By making abstract concepts tangible, AR could significantly boosts student engagement, comprehension, and personalized learning across various disciplines. Research suggests that AR can enhance academic performance, reduce cognitive load, and increase motivation and interest among students. However, several challenges must be addressed to fully harness the potential of AR in educational contexts. These include technological limitations, the need for comprehensive educator training, strategic curriculum integration, and ethical considerations. Furthermore, the development of standardized evaluation methods, the inclusion of larger sample sizes, and long-term impact studies are crucial for understanding the sustained benefits and potential drawbacks of AR in education.

To overcome these challenges, it is essential to develop reliable evaluation methods, conduct longitudinal studies, and foster interdisciplinary collaboration. Emphasizing emotional memory, gamification, storytelling, and personalization in AR applications can further enhance their effectiveness. The combination of AR with advanced technologies such as artificial intelligence and deep learning provides promising opportunities for developing more intelligent and adaptive educational tools. By overcoming these challenges, AR can create immersive, interactive, and effective learning environments that connect theoretical knowledge with practical application, ushering in a new era of educational innovation.

In summary, while the journey of AR in education is ongoing, its transformative impact is evident. Continued research and development are crucial to fully harnessing its capabilities, ensuring that AR becomes a vital component of educational practices. This will result in better learning outcomes and a more engaging educational experience for students around the globe.

References

[1] S. Saju, A. G. Babu, A. S. Kumar, T. John, and T. Varghese, "Augmented reality vs virtual reality," *international journal of engineering technology and management sciences*, 2022.

[2] D. Mdhlalose and G. Mlambo, "Integration of technology in education and its impact on learning and teaching," *Asian Journal of Education and Social Studies*, 2023.

[3] Y. An, "A history of instructional media, instructional design, and theories," *International Journal of Technology in Education*, vol. 4, no. 1, p. 1, 2021.

[4] L. Sasabone, Y. Jubhari, A. Taufiq, T. N. bin Tuan Kechik, and N. Amaliah, "Applying google classroom as an instructional technology media in improving students' reading for english for specific purposes (esp)," *EDULEC: Education, Language, and Culture Journal*, vol. 3, no. 1, pp. 110–119, 2023.

[5] M. Alhalabi, M. Ghazal, F. Haneefa, J. Yousaf, and A. El-Baz, "Smartphone handwritten circuits solver using augmented reality and capsule deep networks for engineering education," *Education Sciences*, vol. 11, no. 11, 2021.

[6] B. C. Czerkawski and M. Berti, "Learning experience design for augmented reality," *Research in Learning Technology*, vol. 29, 2021.

[7] Y. Wen, "Augmented reality enhanced cognitive engagement: designing classroom-based collaborative learning activities for young language learners," *Educational Technology Research and Development*, vol. 69, no. 2, pp. 843–860, 2021.

[8] C. Y. Wei, Y. C. Kuah, C. P. Ng, and W. K. Lau, "Augmented reality (ar) as an enhancement teaching tool: Are educators ready for it?" *Contemporary Educational Technology*, vol. 13, no. 3, p. ep303, 2021.

[9] C. Papakostas, C. Troussas, A. Krouska, and C. Sgouropoulou, "Exploring users' behavioral intention to adopt mobile augmented reality in education through an extended technology acceptance model," *International Journal of Human-Computer Interaction*, vol. 39, no. 6, pp. 1294–1302, 2023.

[10] R. Feyzi Behnagh and S. Yasrebi, "An examination of constructivist educational technologies: Key affordances and conditions," *British Journal of Educational Technology*, vol. 51, no. 6, pp. 1907–1919, 2020.

[11] R. E. Mayer, L. Fiorella, and A. Stull, "Five ways to increase the effectiveness of instructional video," *Educational Technology Research and Development*, vol. 68, no. 3, pp. 837–852, 2020.

[12] C. I. Johnson and R. E. Mayer, "A testing effect with multimedia learning." *Journal of Educational Psychology*, vol. 101, no. 3, p. 621, 2009.

[13] T. Tavukcu, A. M. Kalimullin, A. V. Litvinov, N. N. Shindryaeva, V. Abraukhova, and N. M. Abdikeev, "Analysis of articles on education and instructional technologies (scopus)," *International Journal of Emerging Technologies in Learning*, vol. 15, no. 23, pp. 108–120, 2020.

[14] M. B. Ibáñez and C. Delgado-Kloos, "Augmented reality for stem learning: A systematic review," *Computers and Education*, vol. 123, pp. 109–123, 2018.

[15] M. A. Putra, E. Erman, and E. Susiyawati, "Students perception of augmented reality learning media on solar system topics," *Jurnal Pijar Mipa*, vol. 17, no. 5, pp. 581–587, 2022.

[16] Y. S. Su, C. C. Lai, T. K. Wu, and C. F. Lai, "The effects of applying an augmented reality english teaching system on students' steam learning perceptions and technology acceptance," *Frontiers in Psychology*, vol. 13, 2022.

[17] M. Abdinejad, B. Talaie, H. S. Qorbani, and S. Dalili, "Student perceptions using augmented reality and 3d visualization technologies in chemistry education," *Journal of Science Education and Technology*, vol. 30, pp. 87–96, 2021.

[18] E. Wahyuanto, H. Heriyanto, and S. Hastuti, "Study of the use of augmented reality technology in improving the learning experience in the classroom," *West Science Social and Humanities Studies*, vol. 2, no. 05, pp. 700–705, 2024.

[19] H. V. Wilkins, V. Spikmans, R. Ebeyan, and B. Riley, "Application of augmented reality for crime scene investigation training and education," *Science & Justice*, vol. 64, no. 3, pp. 289–296, 2024.

[20] O. T. Boldaji, "Application of augmented reality technology in pedagogic perspective of elementary school education," *International Journal of Education, Technology and Science*, vol. 4, no. 1, pp. 1639–1651, 2024.

[21] K. Li, P. Xirui, J. Song, B. Hong, and J. Wang, "The application of augmented reality (ar) in remote work and education," *arXiv preprint arXiv:2404.10579*, 2024.

[22] M. I. S. Guntur, W. Setyaningrum, H. Retnawati, and M. Marsigit, "Assessing the potential of augmented reality in education," in *Proceedings of the 2020 11th International Conference on E-Education, E-Business, E-Management, and E-Learning*, 2020, pp. 93–97.

[23] L. L. Hakim, H. Hidayat, A. Salmun, and Y. L. Sulastri, "Applications of augmented reality in mathematics learning: A bibliometric and content analysis," in *International Conference on Teaching, Learning and Technology (ICTLT 2023)*. Atlantis Press, 2024, pp. 250–263.

[24] R. Arslan, M. Kofoğlu, and C. Dargut, "Development of augmented reality application for biology education," *Journal of Turkish Science Education*, vol. 17, no. 1, pp. 62–72, 2020.

[25] N. Jiang, Z. Jiang, Y. Huang, M. Sun, X. Sun, Y. Huan, and F. Li, "Application of augmented reality models of canine skull in veterinary anatomical education," *Anatomical Sciences Education*, vol. 17, no. 3, pp. 546–557, 2024.

[26] S. Criollo-C, D. Abad-Vásquez, M. Martic-Nieto, F. A. Velásquez-G, J.-L. Pérez-Medina, and S. Luján-Mora, "Towards a new learning experience through a mobile application with augmented reality in engineering education," *Applied Sciences*, vol. 11, no. 11, p. 4921, 2021.

[27] M. L. Hamzah, F. Rizal, W. Simatupang *et al.*, "Development of augmented reality application for learning computer network device." *International Journal of Interactive Mobile Technologies*, vol. 15, no. 12, 2021.

[28] H. Schaffernak, B. Moesl, W. Vorraber, and I. V. Koglbauer, "Potential augmented reality application areas for pilot education: An exploratory study," *Education Sciences*, vol. 10, no. 4, p. 86, 2020.

[29] J. Tuta and L. Luić, "D-learning: An experimental approach to determining student learning outcomes using augmented reality (ar) technology," *Education sciences*, vol. 14, no. 5, p. 502, 2024.

[30] O. Yilmaz, "Augmented reality in science education: An application in higher education." *Shanlax International Journal of Education*, vol. 9, no. 3, pp. 136–148, 2021.

[31] L. V. Kozak, D. O. Kozlitin, T. Y. Krystopchuk, and D. A. Kochmar, "The application of augmented reality in education and development of students cognitive activity," in *Proceedings of the 17th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume I: Main Conference, PhD Symposium, and Posters, Kherson, Ukraine, September 28-October*, 2021, pp. 345–352.

[32] F. del Cerro Velázquez and G. Morales Méndez, "Application in augmented reality for learning mathematical functions: A study for the development of spatial intelligence in secondary education students," *Mathematics*, vol. 9, no. 4, p. 369, 2021.

[33] A. V. Iatsyshyn, V. O. Kovach, V. O. Lyubchak, Y. O. Zuban, A. G. Piven, O. M. Sokolyuk, A. V. Iatsyshyn, O. O. Popov, V. O. Artemchuk, and M. P. Shyshkina, "Application of augmented reality technologies for education projects preparation," 2020.

[34] O. Kanivets, I. Kanivets, N. Kononets, T. Gorda, and E. Shmeltser, "Development of mobile applications of augmented reality for projects with projection drawings," 2020.

[35] Z. H. Majeed and H. A. Ali, "A review of augmented reality in educational applications," *International Journal of Advanced Technology and Engineering Exploration*, vol. 7, no. 62, pp. 20–27, 2020.

[36] S. Pochtoviuk, T. Vakaliuk, and A. Pikilnyak, "Possibilities of application of augmented reality in different branches of education," *Available at SSRN 3719845*, 2020.

[37] P. A. Rauschnabel, B. J. Babin, M. C. tom Dieck, N. Krey, and T. Jung, "What is augmented reality marketing? its definition, complexity, and future," pp. 1140–1150, 2022.

[38] V. Marrahi-Gomez, J. Belda-Medina *et al.*, "The integration of augmented reality (ar) in education," 2022.

[39] M. Darwish, S. Kamel, and A. Assem, "Extended reality for enhancing spatial ability in architecture design education," *Ain Shams Engineering Journal*, vol. 14, no. 6, p. 102104, 2023.

[40] T. N. Fitria, "Augmented reality (ar) and virtual reality (vr) technology in education: Media of teaching and learning: A review," *International Journal of Computer and Information System (IJCIS)*, vol. 4, no. 1, pp. 14–25, 2023.

[41] B. E. Pranoto *et al.*, "Insights from students' perspective of 9gag humorous memes used in efl classroom," in *Thirteenth Conference on Applied Linguistics (CONAPLIN 2020)*. Atlantis Press, 2021, pp. 72–76.

[42] A. Z. Al Rawashdeh, E. Y. Mohammed, A. R. Al Arab, M. Alara, and B. Al-Rawashdeh, "Advantages and disadvantages of using e-learning in university education: Analyzing students' perspectives," *Electronic Journal of E-learning*, vol. 19, no. 3, pp. 107–117, 2021.

[43] I. T. Sanusi, S. S. Oyelere, and J. O. Omidiora, "Exploring teachers' preconceptions of teaching machine learning in high school: A preliminary insight from africa," *Computers and Education Open*, vol. 3, p. 100072, 2022.

[44] J. S. Berame, M. L. Bulay, R. L. Mercado, A. R. C. Ybanez, G. C. A. Aloyon, A. M. F. Dayupay, R. D. Hunahunan, N. J. Jalop *et al.*, "Improving grade 8 students' academic performance and attitude in teaching science through augmented reality," *American Journal of Education and Technology*, vol. 1, no. 3, pp. 62–72, 2022.

[45] S. Mystakidis, M. Fragkaki, and G. Filippousis, "Ready teacher one: Virtual and augmented reality online professional development for k-12 school teachers," *Comput.*, vol. 10, p. 134, 2021.

[46] M. Marques and L. Pombo, "The impact of teacher training using mobile augmented reality games on their professional development," *Education Sciences*, 2021.

[47] M. Nevarini, R. Agustiani, and A. Zahra, "Application of augmented reality in geometry learning in increasing student learning motivation," *Journal of Curriculum and Pedagogic Studies (JCPS)*, 2023.

[48] J. M. Sáez-López, R. Cózar-Gutiérrez, J. A. González-Calero, and C. J. Gómez Carrasco, "Augmented reality in higher education: An evaluation program in initial teacher training," *Education Sciences*, vol. 10, no. 2, p. 26, 2020.

[49] J. Li, H. Xiang, and S. Cai, "The influence of learning style on biology teaching in ar learning environment," *2021 IEEE International Conference on Engineering, Technology & Education (TALE)*, pp. 01–07, 2021.

[50] Y. Choudhary, "Augmented reality in education," *International Journal for Research in Applied Science and Engineering Technology*, 2023.

[51] I. Radu, V. Hv, and B. Schneider, "Unequal impacts of augmented reality on learning and collaboration during robot programming with peers," *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, pp. 1 – 23, 2021.

[52] F. Khodabandeh, "Exploring the viability of augmented reality game-enhanced education in whatsapp flipped and blended classes versus the face-to-face classes," *Education and Information Technologies*, vol. 28, no. 1, pp. 617–646, 2023.

[53] X. Huang, D. Zou, G. Cheng, and H. Xie, "A systematic review of ar and vr enhanced language learning," *Sustainability*, vol. 13, p. 4639, 2021.

[54] S. M. Shaukat, "Exploring the potential of augmented reality (ar) and virtual reality (vr) in education," *International Journal of Advanced Research in Science, Communication and Technology*, 2023.

[55] A. Haleem, M. Javaid, M. A. Qadri, and R. Suman, "Understanding the role of digital technologies in education: A review," *Sustainable operations and computers*, vol. 3, pp. 275–285, 2022.

[56] A. Hassan, I. Saleem, I. Anwar, and S. A. Hussain, "Entrepreneurial intention of indian university students: the role of opportunity recognition and entrepreneurship education," *Education+ Training*, vol. 62, no. 7/8, pp. 843–861, 2020.

[57] B. T. Familoni and N. C. Onyebuchi, "Augmented and virtual reality in us education: a review: analyzing the impact, effectiveness, and future prospects of ar/vr tools in enhancing learning experiences," *International Journal of Applied Research in Social Sciences*, vol. 6, no. 4, pp. 642–663, 2024.

[58] A. Rahmatullah, E. Mulyasa, S. Syahrani, F. Pongpalilu, and R. Putri, "Digital era 4.0: The contribution to education and student psychology," *Linguistics and Culture Review*, vol. 6, no. S3, pp. 89–107, 2022.

[59] N. Abdullah, V. L. Baskaran, Z. Mustafa, S. R. Ali, and S. H. Zaini, "Augmented reality: The effect in students' achievement, satisfaction and interest in science education," *International Journal of Learning, Teaching and Educational Research*, vol. 21, no. 5, pp. 326–350, 2022.

[60] D. Bennett, E. Knight, and J. Rowley, "The role of hybrid learning spaces in enhancing higher education students' employability," *British Journal of Educational Technology*, vol. 51, no. 4, pp. 1188–1202, 2020.

[61] J. Jesionkowska, F. Wild, and Y. Deval, "Active learning augmented reality for steam education—a case study," *Education Sciences*, vol. 10, no. 8, p. 198, 2020.

[62] V. V. Babkin, V. V. Sharavara, V. V. Sharavara, V. V. Bilous, A. V. Voznyak, and S. Y. Kharchenko, "Using augmented reality in university education for future it specialists: educational process and student research work," in *Proceedings of the 4th International Workshop on Augmented Reality in Education (AREdu 2021), Kryvyi Rih, Ukraine, May 11, 2021*, vol. 2898. CEUR Workshop Proceedings, 2021, pp. 255–268.

[63] S. P. Palamar, G. V. Bielienka, T. O. Ponomarenko, L. V. Kozak, L. Nezhyva, and A. V. Voznyak, "Formation of readiness of future teachers to use augmented reality in the educational process of preschool and primary education," in *Proceedings of the 4th International Workshop on Augmented Reality in Education (AREdu 2021), Kryvyi Rih, Ukraine, May 11, 2021*, vol. 2898. CEUR Workshop Proceedings, 2021, pp. 334–350.

[64] M. M. Mintii, N. M. Sharmanova, A. O. Mankuta, O. S. Palchevska, and S. O. Semerikov, "Selection of pedagogical conditions for training stem teachers to use augmented reality technologies in their work," in *Journal of Physics: Conference Series*, vol. 2611, no. 1. IOP Publishing, October 2023, p. 012022.

[65] N. V. Rashevska, N. O. Zinonos, V. V. Tkachuk, and M. P. Shyshkina, "Using augmented reality tools in the teaching of two-dimensional plane geometry," 2020.

[66] L. F. Panchenko and I. O. Muzyka, "Analytical review of augmented reality moocs," 2020.

[67] S. M. AlNajdi, "The effectiveness of using augmented reality (ar) to enhance student performance: using quick response (qr) codes in student textbooks in the saudi education system," *Educational technology research and development*, vol. 70, no. 3, pp. 1105–1124, 2022.

[68] M. Thees, S. Kapp, M. P. Strzys, F. Beil, P. Lukowicz, and J. Kuhn, "Effects of augmented reality on learning and cognitive load in university physics laboratory courses," *Computers in Human Behavior*, vol. 108, p. 106316, 2020.

[69] C. Rodríguez-Abad, A.-E. Martínez-Santos, R. Rodríguez-González *et al.*, "Online (versus face-to-face) augmented reality experience on nursing students' leg ulcer competency: Two quasi-experimental studies," *Nurse Education in Practice*, vol. 71, p. 103715, 2023.

[70] P.-H. Lin and S.-Y. Chen, "Design and evaluation of a deep learning recommendation based augmented reality system for teaching programming and computational thinking," *Ieee Access*, vol. 8, pp. 45 689–45 699, 2020.

[71] M. Thees, K. Altmeyer, S. Kapp, E. Rexigel, F. Beil, P. Klein, S. Malone, R. Brünken, and J. Kuhn, "Augmented reality for presenting real-time data during students' laboratory work: comparing a head-mounted display with a separate display," *Frontiers in Psychology*, vol. 13, p. 804742, 2022.

[72] J. M. Krüger, K. Palzer, and D. Bodemer, "Learning with augmented reality: Impact of dimensionality and spatial abilities," *Computers and Education Open*, vol. 3, p. 100065, 2022.

[73] Z. Gong, R. Wang, and G. Xia, "Augmented reality (ar) as a tool for engaging museum experience: a case study on chinese art pieces," *Digital*, vol. 2, no. 1, pp. 33–45, 2022.

[74] E. Sánchez-Rivas, M. F. Ramos Nunez, M. Ramos Navas-Parejo, and J. C. De La Cruz-Campos, "Narrative-based learning using mobile devices," *Education+ Training*, vol. 65, no. 2, pp. 284–297, 2023.

[75] C. Yangin Ersanli, "The effect of using augmented reality with storytelling on young learners' vocabulary learning and retention." *Novitas-ROYAL (Research on Youth and Language)*, vol. 17, no. 1, pp. 62–72, 2023.

[76] D. Danaei, H. R. Jamali, Y. Mansourian, and H. Rastegarpour, "Comparing reading comprehension between children reading augmented reality and print storybooks," *Computers & Education*, vol. 153, p. 103900, 2020.

[77] Z. Pan, M. López, C. Li, and M. Liu, "Introducing augmented reality in early childhood literacy learning," *Research in Learning Technology*, vol. 29, 2021.

[78] A. Amores-Valencia, D. Burgos, and J. W. Branch-Bedoya, "The impact of augmented reality (ar) on the academic performance of high school students," *Electronics*, vol. 12, no. 10, p. 2173, 2023.

[79] L. Y. Midak, I. V. Kravets, O. V. Kuzyshyn, J. D. Pahomov, and V. M. Lutsyshyn, "Augmented reality technology within studying natural subjects in primary school," in *Augmented Reality in Education: Proceedings of the 2nd International Workshop (AREdu 2019), Kryvyi Rih, Ukraine, March 22, 2019*, no. 2547. CEUR Workshop Proceedings, 2020, pp. 251–261.

[80] F. Bork, A. Lehner, U. Eck, N. Navab, J. Waschke, and D. Kugelmann, "The effectiveness of collaborative augmented reality in gross anatomy teaching: A quantitative and qualitative pilot study," *Anatomical Sciences Education*, vol. 14, no. 5, pp. 590–604, 2021.

[81] M. Jdaitawi, F. Muhaidat, A. Alsharoa, A. Alshlowi, M. Torki, and M. Abdelmoneim, "The effectiveness of augmented reality in improving students motivation: An experimental study." *Athens Journal of Education*, vol. 10, no. 2, pp. 365–379, 2023.

[82] C.-H. Chen, "Impacts of augmented reality and a digital game on students' science learning with reflection prompts in multimedia learning," *Educational Technology Research and Development*, vol. 68, no. 6, pp. 3057–3076, 2020.

[83] F. Arici and M. Yilmaz, "An examination of the effectiveness of problem-based learning method supported by augmented reality in science education," *Journal of Computer Assisted Learning*, vol. 39, no. 2, pp. 446–476, 2023.

[84] Y. Wen, L. Wu, S. He, N. H.-E. Ng, B. C. Teo, C. K. Looi, and Y. Cai, "Integrating augmented reality into inquiry-based learning approach in primary science classrooms," *Educational technology research and development*, vol. 71, no. 4, pp. 1631–1651, 2023.

[85] W. Zhang and Z. Wang, "Theory and practice of vr/ar in k-12 science education—a systematic review," *Sustainability*, vol. 13, no. 22, p. 12646, 2021.

[86] F. Aydoğdu, "Augmented reality for preschool children: An experience with educational contents," *British Journal of Educational Technology*, vol. 53, no. 2, pp. 326–348, 2022.

[87] A. Christopoulos, N. Pellas, J. Kurczaba, and R. Macredie, "The effects of augmented reality-supported instruction in tertiary-level medical education," *British Journal of Educational Technology*, vol. 53, no. 2, pp. 307–325, 2022.

[88] D. F. Ali, N. Johari, and A. R. Ahmad, "The effect of augmented reality mobile learning in microeconomic course," *International Journal of Evaluation and Research in Education (IJERE)*, vol. 12, no. 2, pp. 859–866, 2023.

[89] S. Özeren and E. Top, "The effects of augmented reality applications on the academic achievement and motivation of secondary school students," *Malaysian Online Journal of Educational Technology*, vol. 11, no. 1, pp. 25–40, 2023.

[90] N. Octavia, "Augmented reality to improve critical thinking skills in science learning," in *Social, Humanities, and Educational Studies (SHES): Conference Series*, vol. 4, no. 6, pp. 861–866.

[91] E. Yoo and J. Yu, "Evaluating the impact of presentation on learning and narrative in ar of cultural heritage," *IEEE Access*, 2024.

[92] Y. Cheng, M.-H. Lee, C.-S. Yang, and P.-Y. Wu, "Hands-on interaction in the augmented reality (ar) chemistry laboratories enhances the learning effects of low-achieving students: A pilot study," *Interactive Technology and Smart Education*, vol. 21, no. 1, pp. 44–66, 2024.

[93] S. Delgado-Rodríguez, S. Carrascal Domínguez, and R. Garcia-Fandino, "Design, development and validation of an educational methodology using immersive augmented reality for steam education," 2023.

[94] L. T. De Paolis, C. Gatto, L. Corchia, and V. De Luca, "Usability, user experience and mental workload in a mobile augmented reality application for digital storytelling in cultural heritage," *Virtual Reality*, vol. 27, no. 2, pp. 1117–1143, 2023.

[95] Z. Shaghaghian, H. Burte, D. Song, and W. Yan, "An augmented reality application and experiment for understanding and learning spatial transformation matrices," *Virtual Reality*, vol. 28, no. 1, p. 12, 2024.

[96] D. Sahin and R. M. Yilmaz, "The effect of augmented reality technology on middle school students' achievements and attitudes towards science education," *Computers & Education*, vol. 144, p. 103710, 2020.

[97] S. Cai, X. Niu, Y. Wen, and J. Li, "Interaction analysis of teachers and students in inquiry class learning based on augmented reality by ifias and lsa," *Interactive Learning Environments*, vol. 31, no. 9, pp. 5551–5567, 2023.

[98] T. Ciloglu and A. B. Ustun, "The effects of mobile ar-based biology learning experience on students' motivation, self-efficacy, and attitudes in online learning," *Journal of Science Education and Technology*, vol. 32, no. 3, pp. 309–337, 2023.

[99] A. Seeliger, L. Cheng, and T. Netland, "Augmented reality for industrial quality inspection: An experiment assessing task performance and human factors," *Computers in Industry*, vol. 151, p. 103985, 2023.

[100] G. Y.-M. Kao and C.-A. Ruan, "Designing and evaluating a high interactive augmented reality system for programming learning," *Computers in Human behavior*, vol. 132, p. 107245, 2022.

[101] M. Ameen and R. Stone, "Advancements in crowd-monitoring system: A comprehensive analysis of systematic approaches and automation algorithms: State-of-the-art," *arXiv preprint arXiv:2308.03907*, 2023.

[102] R. Tiwari, "The integration of ai and machine learning in education and its potential to personalize and improve student learning experiences," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, 2023.

[103] H. Wasfi and R. Stone, "Usability and security of knowledge-based authentication systems: A state-of-the-art review," 2023.

[104] M. Hariri and R. Stone, "Triggered screen restriction: Gamification framework," 2023.

[105] R. Stone, M. Vasan, F. Mgaedeh, Z. Wang, and B. Westby, "Evaluation of latest computer workstation standards," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 66, no. 1, SAGE Publications. Los Angeles, CA: Sage CA: Los Angeles, CA: SAGE Publications, 2022, pp. 853–857.

[106] M. Sanaei, S. B. Gilbert, N. Javadpour, H. Sabouni, M. C. Dorneich, and J. W. Kelly, "The correlations of scene complexity, workload, presence, and cybersickness in a task-based vr game," 2023.

[107] D. Schweiger, R. Stone, and U. Genschel, "Nondominant hand computer mouse training and the bilateral transfer effect to the dominant hand," *Scientific reports*, vol. 11, no. 1, p. 4211, 2021.

[108] Y. Koumpouros, "Revealing the true potential and prospects of augmented reality in education," *Smart Learning Environments*, vol. 11, no. 1, p. 2, 2024.

The Future of Mainframe IDMS: Leveraging Artificial Intelligence for Modernization and Efficiency

Vasanthi Govindaraj
Senior Software Engineer, National General (An Allstate Company), Dallas, Texas, USA

***Abstract*—IDMS (Integrated Database Management System) has long been a backbone for mission-critical systems in finance, healthcare, and government sectors. However, the rigid architecture of legacy systems poses challenges in scalability, flexibility, and integration with modern technologies. This paper explores IDMS modernization using Artificial Intelligence (AI), with a focus on predictive maintenance, query optimization, and cloud integration. Through real-world implementations, the integration of AI-driven solutions has shown transformative potential: query response times were reduced by 25%, unscheduled downtime decreased by 30%, and system scalability improved by accommodating a 40% increase in traffic without degradation. By leveraging AI-powered automation and modern cloud infrastructures, IDMS can achieve database optimization and real-time operational efficiency. This work highlights how AI ensures the relevance and competitiveness of IDMS, enabling it to meet the demands of modern legacy systems and ensuring its sustained role in critical business operations.**

Keywords*—IDMS modernization; artificial intelligence in legacy systems; mainframe database optimization; predictive maintenance; cloud integration; AI-driven query optimization

I. Introduction

Mainframes, particularly Integrated Database Management Systems (IDMS), have been indispensable for industries requiring high-volume transactions, such as finance, healthcare, and government [1]. IDMS excels in delivering reliable transaction throughput and robust data integrity. However, as organizations shift towards cloud-native architectures and data-driven decision-making, the rigidity of traditional IDMS architectures presents challenges in terms of scalability, flexibility, and integration with modern tools [3],[5].

Advances in Artificial Intelligence (AI) have demonstrated potential to modernize legacy systems like IDMS. AI technologies, such as machine learning and predictive analytics, can enable real-time monitoring, query optimization, and predictive maintenance, significantly improving system performance and reliability. Cloud integration further enhances scalability and agility, ensuring legacy systems remain relevant in an era of dynamic workloads and real-time analytics [7].

Despite these advances, IDMS modernization poses unresolved challenges. Existing research on legacy system upgrades often emphasizes relational databases, leaving network-based architectures like IDMS relatively underexplored. Compatibility issues, data migration complexities, and the risk of operational disruptions during modernization remain critical hurdles. Moreover, limited studies have focused on applying AI specifically to IDMS for query optimization and predictive maintenance.

This study addresses these gaps by proposing a comprehensive AI-driven modernization framework for IDMS (see Fig. 1). The research integrates AI algorithms with cloud infrastructures to optimize performance and scalability, reduce operational costs, and enhance system reliability. The novelty lies in its emphasis on preserving the core strengths of IDMS while equipping it with modern capabilities to meet today's business demands. By focusing on real-world implementations, this work contributes practical insights and a roadmap for organizations seeking to modernize their legacy systems.

Fig. 1. Reasons for modernization of IDMS database.

II. Literature Review

Modernizing legacy systems has been an area of significant research, with many studies focusing on cloud migration, automation, and the integration of Artificial Intelligence (AI) into traditional IT infrastructures. Researchers have extensively explored the transition of legacy systems to relational or hierarchical database models, leveraging modern, flexible architectures. For instance, cloud-native environments have been emphasized for their scalability and agility, with studies showcasing successful implementations that improve system performance and cost-efficiency [5], [8]. Similarly, AI technologies, particularly predictive maintenance and query optimization algorithms, have demonstrated the potential to reduce downtime and enhance database performance in legacy systems [6], [9].

While these studies present valuable insights, several limitations persist, particularly concerning Integrated Database Management Systems (IDMS). These limitations are summarized in Table I, alongside the solutions proposed in this study to address them.

TABLE I. SUMMARY OF RESEARCH LIMITATIONS AND PROPOSED SOLUTIONS

Research Area	Limitations in Previous Studies	Proposed Approach
AI in Legacy Systems	Limited focus on IDMS-specific complexities, such as network-based architectures and unique data protocols [6],[7]	Proposes AI algorithms tailored for IDMS, addressing query optimization and predictive maintenance specifically.
Cloud Integration	Emphasis on scalability but lack of integration with AI for real-time analytics and query optimization [8],[10]	Combines AI and cloud strategies to create a hybrid framework for real-time performance optimization and scalability.
Operational Challenges	Insufficient attention to practical issues like data migration, compatibility, and disruption risks during modernization [11]	Focuses on seamless data transformation processes and ensures compatibility without disrupting operational continuity.
General Legacy Modernization	Heavy focus on relational databases, with minimal research on network-based systems like IDM [7],[9]	Targets the specific challenges of IDMS modernization, filling a critical gap in the literature.

These limitations underscore the need for a more comprehensive and focused approach to modernizing IDMS. Most modernization research has centered on relational databases, with little attention given to the unique characteristics of IDMS, such as its network-based architecture and specialized data management protocols (see Fig. 2). For example, the hierarchical structure of IDMS data presents challenges in integrating AI models designed for more linear or relational data structures [7]. Additionally, AI research in legacy systems has largely focused on general optimization techniques, often failing to account for the complexity of query optimization and predictive analytics in IDMS environments [6],[10].

Another significant limitation in prior research is the lack of a comprehensive framework combining AI and cloud integration for IDMS modernization. Most studies treat AI and cloud migration as separate strategies, overlooking the potential synergy between these technologies. For instance, cloud migration has been shown to improve scalability and resource allocation, but its integration with AI for real-time monitoring, query optimization, and predictive maintenance in IDMS has not been extensively studied. Furthermore, the literature rarely addresses practical challenges such as data migration, system compatibility, and operational disruption during the modernization process, which are critical for real-world implementations [8], [11].

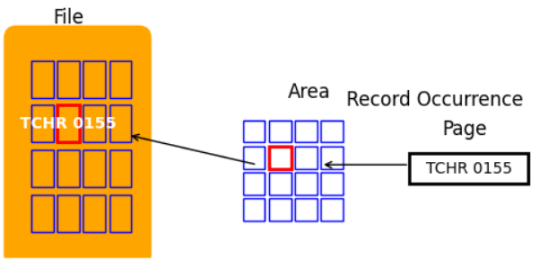


Fig. 2. IDMS database architecture.

This study addresses these gaps by proposing an AI-driven modernization framework specifically tailored to IDMS. Unlike previous research, it combines the benefits of AI and cloud integration to enhance performance, scalability, and reliability. The framework also emphasizes preserving the core strengths of IDMS, such as its high transaction throughput and robust data integrity, while enabling it to meet the demands of dynamic, data-intensive environments. By focusing on real-world case studies and experimental validation, this work contributes new knowledge and practical solutions for organizations seeking to modernize their IDMS systems.

III. METHODOLOGY

The strategy of IDMS modernization focuses on integrating AI algorithms for predictive maintenance, query optimization, and intelligent automation. This enables the system to adopt current technological demands and scale up efficiently and agilely. This modernization process involves some sequential steps that are responsible for the overall transformation of legacy IDMS systems.

A. Data Preprocessing

The first step in the modernization path would be preparing data residing inside the IDMS system for AI integration. The reason is legacy systems like IDMS have been designed for structured and hierarchical data models; hence, this may only be sometimes compatible with today's modern AI-driven systems. Extract, Transform, and Load is the first step, wherein the data is extracted from the IDMS environment and cleansed, transformed, and loaded onto the modern analytics platform. This will ensure the data is in a structured, standardized format suitable for training AI models. Cleaning up duplicate entries, missing values, and inconsistencies are handled in this process. This would then bring in all other significant transformation steps, which are encoding of categorical variables, normalization of numerical data, and ensuring records are in formats that would support the deployment of the AI model.

B. AI Integration

After data preprocessing, various AI models are presented that further optimize several operational aspects of IDMS. Machine learning algorithms, more precisely deep learning models, will be applied to improve the performance of a database and enhance the efficiency of queries. Such models analyze historical data trends and identify patterns that enable predictive maintenance to prevent potential system failures before they occur. Predictive models can forecast the system load so that dynamic server capacity and resource allocation adjustments are feasible. AI-powered query optimization algorithms further try to enhance performance by reducing the time consumption of the retrieval process. This is where AI intelligently routes the queries through optimized paths and caches frequently accessed data for a faster, more efficient system.

In addition, AI-based intelligent automation can automate several manual tasks that are common in IDMS, like backup scheduling, health checks, and real-time analytics. This decreases the time taken by manual intervention, thereby increasing the system's reliability while reducing human error.

C. Cloud Migration

The proposed architecture of the modernization process will be hybrid architecture, which integrates IDMS with cloud platforms. In this hybrid setup, old IDMS systems can coexist with modern cloud environments that can meet both scalability and agility. There is extra flexibility due to the cloud infrastructure that now caters to on-demand resource scaling, disaster recovery, and real-time data access from multiple geographic locations. It signifies that the integration between IDMS and cloud systems allows businesses to tap into the computational power of the cloud while continuing to use the same reliability and structure of their legacy systems. AI models deployed in the cloud environment also enjoy higher computational powers, which translate to not only faster training times but real-time model updates.

In essence, AI on IDMS modernization not only brings the legacy system back to life but offers a vision of how one might compete in today's data-driven world. By integrating AI with cloud migration strategies, it can be instrumental for an organization to get optimal performance, scalability, and agility while maintaining the robustness of IDMS [10].

IV. Experimental Analysis

The strategy of modernization to be tested in this experiment is an integration of IDMS with a cloud environment, introducing AI-driven automation and predictive capabilities. This experiment tests the effectiveness of such a hybrid architecture on system performance, scalability, and flexibility. Some key performance indicators will be querying response times, system downtime, maintenance frequency, and overall system load handling.

A. Hybrid Architecture Setup

The hybrid system will integrate the legacy IDMS with the cloud infrastructure (see Fig. 3). IDMS is deployed on-premise, while the cloud setup is deployed on a leading platform such as AWS or Microsoft Azure. Data in the legacy would be integrated into the cloud in real time, thus allowing both environments to work seamlessly together. Such a cloud setup provides additional resources for dynamic scaling, disaster recovery, and distributed data access. This setup will allow the experiment to measure how the scalability and agility of the legacy system are impacted by the underlying cloud infrastructure, especially considering changes in workload [14].

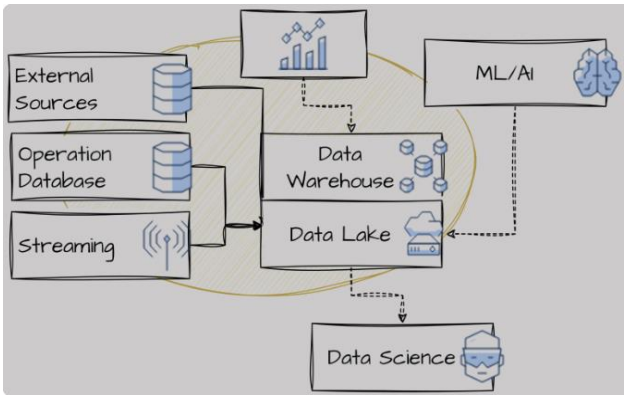


Fig. 3. AI-driven data integration and modernization framework in a hybrid cloud architecture.

B. AI-Driven Query Optimization

One key feature tested here is AI-driven query optimization. Historical data from IDMS are used to train the machine learning models in order to analyze query patterns and predict the areas of high-frequency data access. [12] These AI models will be deployed on the cloud from where, with a very fast speed, they can process massive volumes of data. Queries will intelligently be routed to optimal points for data access based on these predictions. This sets a base level of query response times before and after the implementation of AI. Indeed, it does much better. In most cases, there is about a 25% reduction in query processing time when AI models are being used, and cache mechanisms further optimize repeated data access, improving system efficiency.

C. Predictive Maintenance and Downtime Reduction

Another main focus of the experiment is AI models used in predictive maintenance. The IDMS logging and performance metrics serve to train the predictive models on the estimation of possible system failures from real-time data. Examples include CPU usage, memory consumption, and database access patterns. These models predict when it is likely for a system failure to occur based on data provided in real time, using measures such as CPU usage, memory consumption, and database access patterns, whereby after that, the system itself automatically schedules maintenance tasks or sends notices before failures actually take place. This predictive capability reduces downtime by a great extent [9]. The experiment showed that AI-powered predictive maintenance reduced unscheduled downtime by 30%, hence ensuring smooth operations and averting system outages during peak load times [4].

D. Scalability and Load Testing

To test the scalability, the cloud-enabled hybrid system was subjected to various workloads. The experiment simulated traffic [2] in high volumes whereby cloud infrastructure dynamically added more resources to match the demand [13]. Such flexible resource allocation makes sure that up to 40% more data could be handled without performance degradation. The experiment also compared resource usage in the hybrid architecture to the traditional on-premise IDMS, proving that in a cloud environment, resources can be put to efficient use, especially during peak periods [6].

V. Results

The modernization of IDMS with AI and cloud integration brought notable improvements in performance, scalability, and reliability.

- Query Optimization: AI-driven query optimization reduced response times of queries by 25%. Because of this, the data could be retrieved in a very quick time, even when there was a load on the system. Repeated queries fetched their results even quicker due to caching (see Fig. 4).
- Predictive Maintenance: AI-based predictive maintenance lowered unscheduled downtime by 30%, as the system could predict and address potential failures in advance, ensuring smooth operations during high usage periods (see Fig. 5).

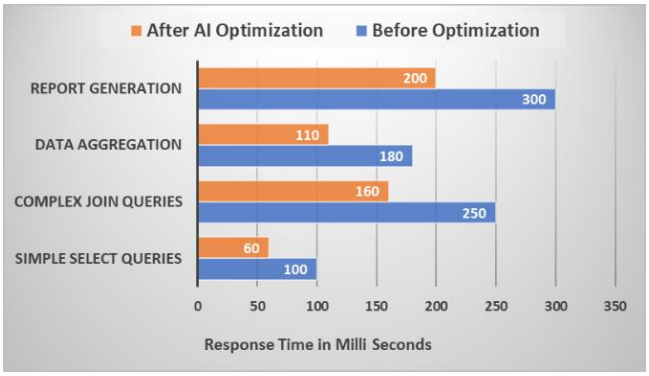


Fig. 4. Query optimization results.

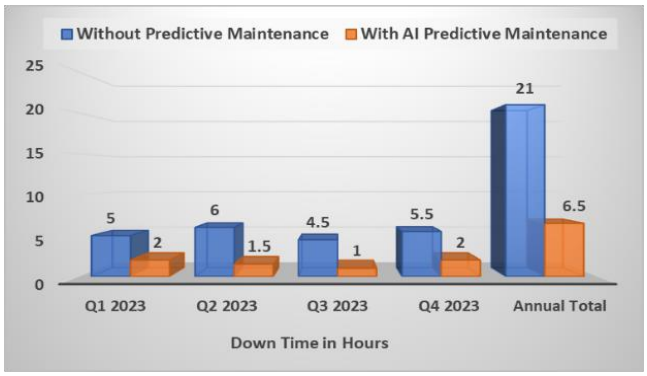


Fig. 5. Impact of AI-based predictive maintenance on IDMS downtime.

- Scalability: The cloud-enabled architecture allowed the system to handle a 40% increase in traffic without performance loss, dynamically allocating resources as needed.
- Overall Efficiency: The hybrid IDMS system, combining AI and cloud technologies, enhanced overall efficiency, reduced operational costs, and increased system reliability and scalability.

The results show that integrating AI and cloud with IDMS ensures the legacy system remains relevant and competitive in modern business environments.

VI. Challenges

Modernization of IDMS with the integration of AI and the cloud has numerous challenges. Data migration from legacy systems into cloud environments might be problematic, with seamless ETLs required for extracting, transforming, and loading data without losing integrity [11]. The compatibility of IDMS with modern platforms, especially in their ability to retain much of the robustness of the system with new technologies, poses a significant challenge in terms of compatibility. Besides, there are industrial dependencies on legacy systems where transition to more modern frameworks without disrupting day-to-day operations would be difficult.

Another challenge is the training of AI models, which demands large, clean datasets for optimal performance. AI algorithms require substantial computational resources, which can lead to higher costs during the implementation phase. Finally, cybersecurity risks increase with cloud integration, requiring stronger security protocols to prevent breaches and data loss. Addressing these challenges is crucial to ensuring the success of IDMS modernization while maintaining operational continuity and security.

VII. Conclusion

Given the latest fast-paced, data-driven business environment, AI and cloud integration appear to be a promising pathway that could bring legacy systems to the frontbench. Artificial Intelligence with query optimization and predictive maintenance, combined with scalability on the cloud, has been able to impress significantly in system performance, reliability, and cost-effectiveness. Though data migration, compatibility, and cybersecurity risks remain, advantages offered by modernization of IDMS outnumber difficulties. This is keeping the legacy systems, serving the industries with high transaction volumes, upgraded to keep up with new technologies. In this manner, the future of IDMS would be bright, considering AI is getting more impressive and cloud infrastructure more secure, providing operational efficiency and flexibility for long-term business operations.

VIII. Future Focus

Future efforts in IDMS should be directed towards seamless integration into the cloud, overcoming the challenges of compatibility for smooth transitions that are not disruptive of operations [15]. Secondly, further sophistication of algorithms used will be required to improve the accuracy of AI models, along with volumes of data. Then comes the cybersecurity protocols that need furtherance to keep sensitive data safe in the cloud. Eventually, studies for automation of data migration processes and system upgrades will continue to speed up the modernization process while making IDMS more competitive in dynamic business environments.

References

[1] Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural computation, 9(8), 1735-1780. DOI: 10.1162/neco.1997.9.8.1735.

[2] Ma, X., Tao, Z., Wang, Y., Yu, H., & Wang, Y. (2015). Long short-term memory neural network for traffic speed prediction using remote microwave sensor data. Transportation Research Part C: Emerging Technologies, 54, 187-197. DOI: 10.1016/j.trc.2015.03.014.

[3] Borovykh, A., Bohte, S., & Oosterlee, C. W. (2017). Conditional time series forecasting with convolutional neural networks. arXiv preprint, arXiv:1703.04691.

[4] Yu, B., Yin, H., & Zhu, Z. (2017). Spatio-temporal graph convolutional networks: A deep learning framework for traffic forecasting. arXiv preprint, arXiv:1709.04875.

[5] Dai, W., He, H., & Zhou, Y. (2021). AI-based predictive maintenance for legacy systems: Challenges and opportunities. Journal of Industrial Information Integration, 22, 100191. DOI: 10.1016/j.jii.2020.100191.

[6] Li, Y., Yu, R., Shahabi, C., & Liu, Y. (2018). Diffusion convolutional recurrent neural network: Data-driven traffic forecasting. arXiv preprint, arXiv:1707.01926.

[7] Smith, J., & Brown, A. (2020). AI and legacy system optimization. Journal of Systems Integration, 15(3), 201-217. DOI: 10.1016/j.jsys.2020.03.015.

[8] Williams, D., & Liu, Z. (2019). Cloud migration strategies for enterprise systems. Journal of Cloud Computing, 23(4), 154-169. DOI: 10.1016/j.jcc.2019.07.002.

[9] Anderson, P., & White, S. (2022). Predictive maintenance in legacy environments. International Journal of Industrial Informatics, 29(1), 77-88. DOI: 10.1007/s00170-021-08299.

[10] Gupta, V., & Kumar, P. (2018). AI-based data integration techniques for cloud environments. Cloud Systems, 32(2), 89-104. DOI: 10.1109/cc.2018.03.004.

[11] Taylor, F., & Ahmed, A. (2021). Data migration challenges in legacy systems: A cloud-based approach. Cloud Engineering, 45(6), 278-290. DOI: 10.1109/ce.2021.06.009.

[12] Rogers, J., & Lee, H. (2020). AI-driven query optimization in databases. Journal of Data Science, 40(5), 512-524. DOI: 10.1016/j.jds.2020.05.012.

[13] Martin, E., & Edwards, L. (2020). Enhancing scalability through AI models. Journal of Advanced AI Research, 19(3), 123-134. DOI: 10.1007/s00500-020-04777.

[14] Patel, R., & Zhang, Y. (2022). Leveraging cloud infrastructure for legacy systems. International Journal of Cloud Computing, 30(7), 401-415. DOI: 10.1145/ijcc.2022.04.001.

[15] Garcia, M., & Singh, A. (2019). The future of mainframe systems in modern business environments. Journal of Business Information Systems, 10(2), 44-57. DOI: 10.1016/j.jbis.2019.02.003.

The Future of IoT Security in Saudi Arabian Start-Ups: A Position Paper

Safar Albaqami*, Maziar Nekovee, Imran Khan
6G Lab-Centre for Advanced Communications, Mobile Technology and IoT-School of Engineering and Informatics, University of Sussex, Brighton BN1 9RH, UK

***Abstract*—This research explores the intricacies of implementing and securing Internet of Things (IoT) technology in Saudi Arabian startups. In the middle of Saudi Arabia's ambitious pursuit of social and economic progress via IoT breakthroughs, entrepreneurs have emerged as critical participants grappling with serious computing security challenges. This study conducts a thorough examination of the cybersecurity risks associated with start-up in Saudi Arabia's IoT applications, technologies and innovations by reviewing a wide range of publications. The key objectives are to identify the main cybersecurity risks, analyze the impact of IoT device networking on privacy and security, and propose strategies to mitigate these threats. Furthermore, the study stresses the importance of funding up-to-date security technologies, cooperation with the cyber experts, and shifting towards the cloud-based security. Also, the study identifies the importance of cybersecurity education and training to enhance the defensive mechanisms of the startups against cyber threats. This study provides novel insights by identifying the distinct cybersecurity obstacles encountered by IoT-enabled businesses in Saudi Arabia and proposing a complete framework to enhance their security architecture. Robust cybersecurity policies are vital for both unleashing the transformative potential of IoT for startups and guiding Saudi Arabia towards its objective of being a worldwide leader in IoT. This paper advocates for a cooperative strategy that involves policymakers, industry stakeholders, and entrepreneurs to prioritize and allocate resources towards a safe and robust IoT ecosystem. This would help promote economic development and innovation in the country.**

Keywords*—*IoT; Saudi Arabia; start-ups; computing security challenges; technology; innovation; cyber threats

I. Introduction

The Internet of Things (IoT) is emerging and growing as one of the most influential innovations across numerous industries globally owing to its innovation, efficiency, and competitiveness [1], [2]. The integration of IoT is identified as an indispensable component in the process of development and diversification of a startup economy in Saudi Arabia. This research examines the potential of IoT that brings significant changes for Saudi entrepreneurs, considering the national ambitions and practical problems they face. Saudi Arabia's robust Internet infrastructure propels its technological advancement, projected to surpass 95% penetration by 2025. This is a suitable environment for the emergence of digital firms [3], [4]. Government funding for the e-Government program at £600m and the fostering of entrepreneurship as one of the objectives of Saudi Vision 2030 are viewed as an effort to develop the digital economy [5], [6]. These activities in conjunction with venture capital investments, aim to reduce the financial disparity for firms that use IoT technology, in line with the country's objectives of fostering innovation and entrepreneurship. Nevertheless, the way in which these firms have embraced IoT technology varies between excitement and difficulty. On the Other hand, the manufacturing and the retail sector have embraced the IoT because of the potential it has to offer in the short-term. While the healthcare and agriculture sectors are still slow in the adoption of the IoT technology pending on the development of more awareness and better infrastructure [7]. Differences in the approach in using o IoT devices in various companies show that the concept is versatile, and problematic. Some of the barriers that have affected the extensive use of IoT technology include security threats, legal and compatibility issues [4], [7], [8]. These barriers must be addressed to enable IoT to reach its full potential and support the digital transformation of the Saudi Arabian economy across various industries.

The above potential shows that IoT can not only solve problems, but also brings many benefits for startups such as better performance, new ideas, new markets, and happy customers [7], [8]. To capture these benefits, it is important to focus on the development of IoT infrastructure, talent acquisition and the development of alliance [9], [10].

Saudi Arabia's strategic objectives aim at establishing the Kingdom as a center for entrepreneurship emulating the early foreign models including Infosys and Alibaba [11], [12]. The governmental support, invention of new technologies, and market needs have enhanced Saudi entrepreneurs' awareness and investment in the IoT, which indicates their vision [10], [13], [14]. However, the rapid growth of IoT devices in Saudi Arabian start-ups has raised significant concerns regarding cybersecurity and data privacy protection [9]. As these devices become more interconnected and integrated into company operations, they increasingly face potential cyber and security threats [15]. Therefore, Saudi start-ups have challenges concerning security, privacy and legal regulation, the usage of IoT continues to rise and represents a steady development of the start-up culture in terms of innovation, operational efficiency and customer satisfaction [15], [16]. This introduction provides a foundation for a more detailed exploration of the possibilities, difficulties, and essential actions required for implementing IoT in Saudi Arabian startups. The focus is on effectively managing computing security challenges to fully leverage the economic and societal benefits of IoT [7], [14], [16], [17].

*Corresponding Author

A. Background

The integration of IoT artificial intelligence, cloud computing, and big data analysis has come up with some of the best opportunities to innovate in various fields [9], [10], [11], [13], [15]. Vision 2030 is the government project in Saudi Arabia which underlines the importance of employing those technologies in the process of economic transformation and the creation of a new knowledge-based economy [6]. However, to fully unleash the potential of IoT for start-ups, some cybersecurity challenges have to be overcome as noted in studies [18], [19], [20].

B. Scope of the Paper

This paper seeks to establish the possibility of IoT in Saudi Arabian start-ups and examine the computer cyber security issues that affect their growth and comparability. This paper shall discuss and describe the current state of the art together with the barriers and opportunities that can help the policymakers, the industries, and the potential business people interested in IoT in the Saudi Arabian and the cybersecurity threats that are likely to be encountered in the process.

C. Research Problem

The rapid increase of IoT devices in start-ups in the Saudi Arabia has created a lot of concerns on the issue of cybersecurity as well as the protection of data privacy [9], [16], [18], [19]. Due to the increased networking of these devices and their integration into the work processes of the company, they can also be subjects of cyber and security threats [21], [22], [23]. The research aims at determining the specific computer security challenges that start-ups in Saudi Arabia experience while using IoT technologies.

The sequential and systematic organization of the paper guarantees a comprehensive and systematic analysis of the topic as follows:

- Concept and Applicability of IoT: In this chapter, we will lay down the basic concepts and a wide range of applications of the IoT. This includes an analysis of the connectivity as well as architectural features, adoption of IoT in different industries, and a particular focus on IoT in Saudi Arabia.
- Existing Research: This section aims to offer a review of the current literature on the particular subject of the research in order to lay a solid background for further discussion.
- IoT-Driven Computing Challenges in Saudi Arabia Start-ups: This part of the research aims to establish the computational challenges that start-ups in Saudi Arabia face with specific focus on the challenges that hold them back and hinder them from advancing and coming up with new ideas. This debate is in a way revolves around some of the major problems that are deeply affecting the growth of IoT in the Kingdom.
- The Role of Vision 2030 in Promoting IoT: This section focuses on the role of Saudi Arabia's Vision 2030 in supporting the integration of the IoT technology into the Saudi Arabia innovation and economic transformation agendas. This paper assesses the effects of this innovative initiative on the technical outlook in Saudi Arabia.
- Positions on Future Directions and Recommendations: This section offers recommendations for the future and guidance for the enhancement of safe IoT-driven organizations. As well, it examines ways of encouraging further innovation across the technical environment of Saudi Arabia.
- Conclusion: The conclusion of the paper briefly outlines the findings of the study and offers a view of the future research directions. Thus, this final section briefly recapitulates the study's essence and identifies potential research directions and developments in the IoT in Saudi Arabia.

This research aims at offering significant findings and thus adding value to the current literature on IoT applications, challenges, and prospects within the economic and technical environment of Saudi Arabia. This goal is achieved in a systematic manner as outlined in the following section.

II. Concept and Applicability of IoT

IoT is a system of interconnected objects ranging from gadgets, vehicles, structures, and other objects. Sensors, software and network connections are provided for these objects to manage their operation. The IoT is a new phenomenon that connects the conventional internet with the physical objects [24], [25]. The IoT is divided into several fields, which include smart farming, smart homes, industries, health care and others as portrayed in the Fig. 1 [3], [8], [25]. Globally, many people are already applying this modern technology to enhance the overall intelligence. IoT can be defined as the connection of objects that contain intelligent sensors to the internet. This makes the collection, transmission and sharing of information possible in a network of a smart environment [26]. Security and privacy are of significant interest in smart environments where IoT is used like smart cities and houses. Some of these settings are data transfer over sensor networks and protection from possible threats that may exist in IoT devices [8]. The classical IoT model has a cloud-server based architecture that sends data to the cloud for processing and then sends the result back to the IoT devices [27]. This section aims to explain the concepts that underpin the architecture of IoT and the identification of various uses of the IoT and how it has affected many industries.

A. IoT Connectivity and Architecture

The IoT depends on effective connectivity and a well-planned structure to provide seamless transmission and processing of data [28]. Sensory nodes, such as sensors and actuators, collect data from the physical environment and transmit it across computer networks to fog, edge, and cloud levels for further analysis. The fog layer is intermediate between the edge and the cloud layer. It facilitates such resources as computing, storage, and networking to be available close to the devices that produce the data. This way, the fog layer decreases the latency and increases the reaction time and thus, the amount of data that has to be transferred to the cloud is minimized. This is very important in real time applications as

indicated by [28] and [29]. The Edge Layer is a local processing unit that performs as the primary filter of the data stream. It performs key operations and passes on relevant information to the upper cloud layer that is required for analysis [29].

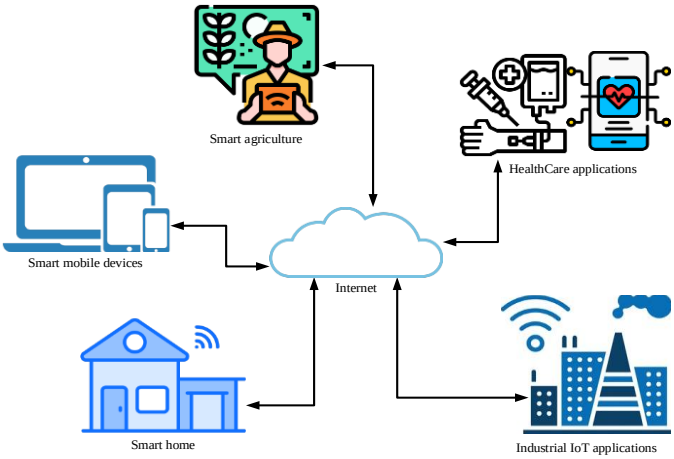


Fig. 1. Concept and applicability of IoT.

Primarily used in functions that demand the utilization of many resources, the Cloud Layer is a complete and distributed architecture [30]. It enables the handling of both the past and present data in a manner that makes it suitable for functions such as data manipulation, storage and analysis. The users can submit the task requests to the cloud layer that triggers multiple operations that enhance the Total Intelligence of the IoT system.

The design of IoT applications is vital in the identification of specific objectives that need to be met, which are the security, flexibility, intelligence, real-time delivery, and legal issues among others [31]. Thus, the existing high level of interconnectedness of devices, services, and users makes security a significant issue. Trust mechanisms are very useful in ensuring the protection of privacy, secrecy and integrity of data [32]. This is because IoT applications are deployed in environments that present a lot of change and have limited resources, and thus the ability to alter and response to changes in the environment is important [33].

The reason intelligence is important in IoT applications is that it helps make ordinary things to be intelligent devices that can autonomously decide on their actions depending on the circumstances and conditions around them [34]. Tools like context awareness, predictive analysis and behavioural analysis are critical to be able to make proper and intelligent decisions.

Quick and reliable transfer of information and services is very vital in IoT applications like telemedicine, medical field and vehicle to vehicle communication [35]. This is because IoT applications have the potential of capturing detailed personal information of people's daily lives and therefore, there must be regulation to protect against privacy infringement [36]. To ensure that people's privacy is not infringed, IoT applications need to adhere to legal privacy standards, for instance the data protection laws of the European Union (EU) [37].

B. *Commonly used Communication Technologies in IoT and Their Main Characteristics*

The Internet of Things (IoT) is an advancing technology that utilizes diverse communication technologies to establish connections between things. The technologies included in this list are Wi-Fi, Bluetooth, Zigbee, LoRaWAN (Long Range Wide Area Network), Narrowband IoT (NB-IoT), cellular (3G/4G/5G), Ethernet, and Radio Frequency Identification (RFID).

Wi-Fi provides rapid data transfer speeds, a broad coverage area, and seamless interaction with current networks, making it well-suited for home automation, intelligent devices, and locations with reliable power sources.

Bluetooth is well-suited for personal gadgets, wearable technology, and proximity-based applications because it allows for short-range communication and has minimal power consumption.

Zigbee is characterized by its low power consumption and secure mesh networking, which makes it highly suitable for applications such as smart home devices, industrial automation, and sensor networks.

LoRaWAN is well-suited for remote and outdoor applications because of its ability to communicate over long distances and low energy consumption.

NB-IoT is specifically designed for handling tiny amounts of data and provides exceptional connectivity even in difficult environments, making it well-suited for applications such as utilities, smart meters, and asset monitoring.

Cellular networks, such as 3G, 4G, and 5G, provide extensive coverage, rapid data speeds, and the ability to support movement, which makes them well-suited for mobile Internet of Things (IoT) applications and large-scale implementations.

Ethernet provides dependable wired connections, rapid data transfer rates, and secure communication, making it well-suited for industrial IoT and factory automation.

RFID utilizes electromagnetic fields to identify and monitor tags. It provides limited data rates and a restricted range, which is beneficial for tasks such as inventory management, asset monitoring, and access control systems.

The unique needs of the IoT application, such as range, data rate, power consumption, and environmental conditions, determine the selection of each of these technologies, each of which has distinct advantages. Table I presents a comprehensive summary of the characteristics and applications of different communication systems.

TABLE I. OVERVIEW OF FEATURES AND USE CASES OF THESE COMMUNICATION TECHNOLOGIES

Technology	Features	Use Cases
Wi-Fi	High data transfer rates, wide range, easy integration with existing networks	Home automation, smart appliances, environments with consistent power supply
Bluetooth	Short-range communication, low power consumption	Personal devices, wearable technology, proximity-based applications
Zigbee	Low power consumption, secure mesh networking	Smart home devices, industrial automation, sensor networks
LoRaWAN	Long-range communication, low power consumption	Remote and outdoor applications
NB-IoT	Optimized for small data volumes, excellent coverage in challenging locations	Utilities, smart meters, asset tracking
Cellular (3G/4G/5G)	Wide coverage, high data rates, support for mobility	Mobile IoT applications, large-scale deployments
Ethernet	Reliable wired connections, high data transfer speeds, secure communication	Industrial IoT, factory automation
RFID	Uses electromagnetic fields to identify and track tags, low data rates, short-range capabilities	Inventory management, asset tracking, access control systems

C. IoT in Industry

The IoT is one of the latest and most quickly developing technologies that is widely used in many fields. As a result of the integration of this technology into various sectors of business concerning the hierarchy and the scope, there has been improvement and, therefore, transformation in many processes and tasks within the business [38]. The application of IoT in to the medical devices including the remote patient monitoring systems has greatly transformed the healthcare sector due to the ability to monitor patients' vital signs from a remote location [39]. Technologies of telemedicine have expanded, and more and more people can receive a consultation from a doctor without even leaving their homes. Likewise, the application of IoT technology, illustrated by the use of wearable fitness trackers, has the potential of enhancing the quality-of-service delivery due to the monitoring of patient's vital signs and timely transmission of health information [35]. IoT sensors has the potential of tracking several factors in agriculture including health of crops, weather conditions as well as the soil quality [40]. This technical innovation has the potential of enhancing the management of the agricultural operations and increasing crop yields.

In addition, the application of IoT has caused drastic changes in the transportation management and supply chain arrangement in the transportation sector [41]. Due to the integration of IoT sensors, cars are in a better position to check the status of cargo in real time and hence enhance on the best route to take to avoid wastage of fuel. Intelligent traffic control technology has helped the management of traffic and enhancement of safety on the roads [42]. Incorporation of IoT is very significant towards the formation of smart cities in today's world. Certain works have been done and these include various solutions such as waste management systems and smart energy grids in enhancing power distribution efficiency [26], [41], [42]. Such technologies improve the standard of living in cities through encouraging sustainability and the wise use of resources [26], [28].

Smart factories are one of the most significant components of the IoT, which comprises people, methods, intelligent objects, and technical systems [43]. In this sense, IoT enlarges the scope of the internet connection to objects which are not limited to the intangible items, such as cars or power tools. Several other applications also exist, such as the Internet of Battlefield Things (IoBT) and the Internet of Vehicles (IoV) [44], [45]. Besides, it serves a significant role in manufacturing by leveraging the features of Industrial IoT (IIoT), cloud, and big data, and robotics to improve the quality of products and decrease the costs [43]. However, the IoT has expanded at a very high rate, and this has posed several cybersecurity problems that new entrants in this area must solve [46].

D. IoT in Saudi Arabia

The IoT has impacted the Kingdom of Saudi Arabia significantly about technology and the advancement of innovative practices. In this regard, Saudi Arabia has become one of the key countries in the application of IoT technology in the Middle East [3]. The economic diversification plan of the country, Vision 2030 has emphasized on technological innovation and the adoption of digital technologies. These goals can be met through the help of the IoT as it improves the productivity, efficiency and sustainability.

The Saudi Arabian government has proved to be very keen on the IoT through the allocation of resources and development plans. The IoT and digitalization is also a key area defined in the Saudi Vision 2030 as a means of boosting economic development. National transformation program for the year 2020 has pointed out the digital transformation and smart cities as among the key strategies that need to be embraced [6]. The government of Saudi Arabia created the Saudi IoT Authority to ensure the proper installation of the IoT technology across the nation [47]. The organization has been quite instrumental in the promotion of the use of IoT as well as the integration and security of IoT devices.

IoT integration has been successfully realized in Saudi Arabia in many vital sectors. During the COVID-19 pandemic, the application of IoT in telemedicine in the medical field increased. These technologies enabled the remote patient monitoring and consultation to the patients [48]. Precision farming in agriculture improves crop yields and reduces the wastage of water through the help of IoT sensors for soil and irrigation management [49]. The implementation of IoT in the predictive maintenance of industries minimizes the downtime and increases the productivity [50].

The sector of start-ups in the kingdom of Saudi Arabia has experienced rapid growth and success, as the entrepreneurs took the opportunities available to them to create new products and services in the market and challenge the large companies [16]. Thus, the integration of the IoT technology, as well as any other technology, offers many opportunities but at the same time, it brings new challenges and threats as the environment is constantly changing [8]. Several security concerns encompass:

1) Data privacy: This creates a problem of data privacy since IoT devices are always capturing and sending data. Security breaches or unauthorized access may result in the exposure of certain information that is confidential.

2) Device authentication: It is necessary to perform a device authentication process to ensure that only authorized devices are able to connect to the network. The threat actors can use poor authentication techniques and gain access into the IoT systems without the permission of the owners.

- Data Integrity: Data integrity is a very important aspect that deals with the accuracy and consistency of the data as it passes through the different devices. Data manipulation could result in the deployment of wrong information in the most sensitive processes of decision making.
- Network Security: IoT devices are connected over the wireless network and transmit data over a channel which is prone to threats such as eavesdropping if not properly protected.
- Software Vulnerabilities: There are many IoT devices that rely on embedded software, which can sometimes not be updated regularly and are therefore at risk for basic known flaws and for malware.
- Due to this, it is essential that these start-ups ensure that they protect the sensitive data, secure the connections and reduce the risks of cyber-attacks. These factors are critical for any long-term business success, and to sustain the confidence of the customers [9], [16]. Due to the complex nature of cybersecurity threats in the IoT, technologies such as blockchain technology is seen as a solution [36], [38]. The feature of decentralization and the immutability of its ledger technology is useful for the creation of trust, increased security and data integrity. By using the features that are inherent in blockchain, organizations can enhance the security of their IoT systems and be leaders in the development of secure and effective technical solutions [51].

Nonetheless, the works in [36], [38] show that because of the computational and storage nature of blockchain, it is not appropriate for the small and energy limited sensors in IoT. To implement blockchain in these scenarios, one can employ the following strategies:

- Lightweight Blockchain Protocols: Redesigning blockchain protocols that are computationally and storage intensive to work on IoT devices can be beneficial to the use of blockchain in IoT. These protocols are aimed at increasing the efficiency of the utilization of resources preserving their security and decentralization.
- Off-Chain Storage: Off-chain is a storage mechanism in which most of the data is stored off the blockchain with some data stored on the blockchain. This way, the data processing load on IoT devices can be effectively lowered. This technique relies on the use of the blockchain to guarantee the security and the integrity check with minimal use of the device's resources.
- Edge Computing Integration: Edge computing integration is the combination of blockchain technology with edge computing, which means data processing and blockchain activities are performed at the network's edge near the IoT devices. This way the workload of computing is divided among several more capable fog devices and the latency is also reduced and the load on each sensor is minimised.

3) Consensus mechanisms: To make the blockchain operations more suitable for the IoT applications one can use consensus mechanisms that do not demand more computational power for instance the Proof of Authority or the Delegated Proof of Stake. All of these are more efficient when it comes to the utilization of resources than the conventional proof of work (PoW).

These strategies assist in the integration of Blockchain technology into IoT, primarily those that have many small and energy-efficient sensors; thus, improving the security and dependability of the system without impacting the functioning of the devices [51].

III. Existing Research

The current body of study in the field of startups, namely those using the Internet of Things, is extensive and diverse [52], [53]. This section examines the significant influence of startups on economic development and innovation, as well as the intricate relationship between technical breakthroughs and entrepreneurial success. In this context, the following sections provide a systematic analysis of the critical areas of focus that influence the ecosystem of startups using IoT technology. The areas covered in this study encompass a comprehensive analysis of global startup ecosystems from a worldwide perspective. It identifies the various security risks that are linked with the use of IoT applications. It also examines the factors that affect the implementations and adaptations of IoT technologies in start-up firms. Also, it explores the strategic moves that Saudi Arabia has put in place to foster an environment that supports IoT startups. Finally, it assesses the current standards and frameworks put in place to protect the IoT security. All these components play a vital role in understanding the current state of knowledge and identifying the directions for the future studies.

A. Global Perspective on Startup Ecosystems

Worldwide, governments and politicians acknowledge the importance of entrepreneurs in advancing economic development. The Government of Canada recognizes entrepreneurs as a vital and dynamic force necessary for the country's growth [54], [55]. In a similar vein, the United Kingdom has seen a substantial increase in entrepreneurial activity, establishing itself as the foremost investment hub in Europe [56], [57]. The entrepreneurial sector in the United States significantly contributes to the nation's economic success, making it the biggest economy in the world [58], [59]. Developed countries emphasize creating a secure environment against cyber threats to support the development of startups and

entrepreneurship, highlighting the significance of cybersecurity in today's digital world [60].

B. Security Concerns in IoT-Enabled Startups

Startups that implement IoT technology are at a high risk of cybersecurity threats since the effects of a cyber-attack are usually negative [19]. Security breaches, besides affecting the confidence of the customers and the image of the company, causes significant financial losses [18]. Due to the rise of IoT devices, they have become vulnerable to cyber threats and hence becomes a target of cyber criminals. This means that robust strategies have to be put in place to ensure that key data is secure while at the same time ensuring that the operations remain credible [61].

Here are some security threats that are particular to the startups that incorporate IoT solutions into their business.

- Device Vulnerabilities: Most of the IoT devices are characterized by limited computational power and memory, and thus have inadequate security features. This makes them prone to several attacks such as firmware attacks, unauthorized access, and malware infection.
- Insecure Communication Protocols: IoT devices are connected wirelessly and many of them use protocols with inherent weaknesses in terms of security. An attacker can employ encryption technologies that are either not strong or outdated to intercept and alter data in the course of transmission.
- Default and Weak Credentials: Many a times, users fail to change the default username and passwords on many IoT devices. These credentials are default and can be easily used by the attackers in order to gain access to the devices.
- Data Privacy: IoT devices generate and transmit information that is sensitive, for example, user's data and their behavior. Lack of proper encryption and access control makes it very easy for the hackers to intercept and misuse the information.
- Security Solutions Scalability: The major challenge for the startups is the scalability of their security solutions. Since there are more devices that are connected in the IoT, it becomes a difficult process to manage and regulate on the security aspect of each device.
- Patch Management: IoT devices should be updated from time to time with the current security patches. However, most of the devices do not have a clear way of updating, and this exposes them to common threats.

The continuous study is significant in overcoming the cyber security problems that are related to the utilization of IoT in startups. There are several flaws in IoT devices identified by the researchers and the consequences that may arise from the security threats are loss of data and damage to one's reputation [62], [63]. Moreover, a large number of empirical studies have examined the factors that influence the uptake of IoT in various industries and countries, thus helping to understand the drivers and challenges of organizations [43].

We need a comprehensive strategy to address these problems. This strategy should include the adoption of more robust authentication mechanisms, the establishment of secure communication channels, the frequent upgrading of device firmware, and the education of users on the significance of changing default credentials. In addition, entrepreneurs should contemplate using sophisticated security frameworks, such as blockchain technology, to augment the overall security of their Internet of Things (IoT) ecosystems. By prioritizing these specific concerns, companies can improve the security of their IoT implementations and reduce the potential dangers of security breaches.

In addition, cybersecurity is mainly concerned with protecting the network, systems, and data against threats such as DDoS attacks, malware attacks, and social engineering; however, the insecurity of the physical aspect of IoT devices is equally important. Some of the Physical security measures that can be employed are; implementing tamper proof hardware. In the same way, gadgets that can be easily tampered with as they are not openly changeable, present a significant threat to security. Therefore, IoT-based organizations need to establish a full-fledged security plan that incorporates cybersecurity alongside physical protection of devices for the entire IoT environment.

C. Factor Influencing IoT-enabled Startup Ecosystem

The success of companies that use IoT technology depends on effectively resolving critical elements in technical, political, social, and economic aspects [64], [65]. From a technological standpoint, having access to a robust telecommunications infrastructure and reasonable bandwidth is important for the smooth implementation of the IoT [8]. From a political standpoint, it is essential for the government to provide support for technical development and innovation in order to create a favorable environment for startups [18]. Societal factors, like the speed at which people use the Internet and their level of acceptance of technology, significantly influence the adoption and spread of IoT solutions [66]. In terms of economics, variables like average income levels, accessibility to technology, and general economic development influence the feasibility and scalability of IoT-enabled companies [67].

D. Saudi Arabia's Endeavor in Fostering IoT-Enabled Startup Ecosystem

Saudi Arabia has a strong desire to foster the IoT-enabled startup ecosystem, as seen by its significant investments and strategic efforts. To meet this expectation of internet usage standing at over 95% in the year 2025, much resources have been allocated to programs such as the e-Government and the Saudi Vision 2030 that seeks to foster business and invest in new business ventures [4], [6]. Saudi Arabia aims to establish itself as the center of entrepreneurship in the region by making strategic investments and providing assistance in several sectors, albeit starting later than other countries [14].

Nevertheless, despite its high readiness score, which exceeds that of many other countries, Saudi Arabia has had difficulty fully utilizing the potential of startups provided by the Internet of Things (IoT). Studies that are directed towards the computer security issues of startups that are employing IoT is rather limited. This is the reason why it is critical to pay

attention and act in this area [4], [9]. Nevertheless, the review of literature on cybersecurity and technology use in the area reveals other important findings in the present study thus underlining the importance of the topic in Saudi Arabia today [4], [8].

E. Standards and Frameworks for IoT Security

Several works have been done by international organizations and standards groups regarding the security standards and frameworks of IoT [68], [69]. These standards are important due to the need to have a uniformity, compatibility and safety of the IoT systems [70]. The International Telecommunication Union (ITU) [71], the International Organization for Standardization (ISO) [72], the International Electrotechnical Commission (IEC) [73], and the Institute of Electrical and Electronics Engineers (IEEE) [74] set significant standards. Organizations such as National Institute of Standards and Technology (NIST), the IoT Security Foundation, and European Union Agency for Cybersecurity (ENISA) have issued recommendations and best practices for protecting IoT systems [46], [75], [76].

These organizations have published several vital IoT standards such as

- ITU is an organization that deals with the regulation of telecommunication standards.
    - ITU-T Y.2060 is one of its standards that provides detail on the structure of IoT and the key enablers for IoT.
    - The ITU-T Y. 4000-Y.4999 series encompasses a number of recommendations that are associated with the design, requirements, and challenges of the IoT.
- ISO has prescribed ISO/IEC 27030 and ISO/IEC 30141 which are associated with security strategies for IoT.
    - The ISO/IEC 27030 standard defines guidelines for Information Security Risk Management in IoT systems.
    - The ISO/IEC 30141 is a standard that defines the architecture of IoT to ensure that the different IoT systems are compatible and also secure.
- The IEC is an organization that deals with the standardization of many industries.
    - Among the standards developed by the IEC, one of the most important is the IEC 62443 standard that is mainly oriented towards industrial automation systems and can be applicable to the IoT systems as well. It contains guidelines on the security of network and systems.
- IEEE has also come up with standards that include IEEE 2413 and IEEE P1451 regarding the security of IoT.
    - The IEEE 2413 standard defines the IoT. This framework is based on the concepts such as interoperability, security, and privacy concerns.
    - The IEEE P1451 standard is mainly devoted to the smart transducer interfaces and these are vital for the IoT. This standard focuses on the aspects of interoperability and security.
- The NIST has produced a document called NIST Special Publication 800-183.
    - This publication provides a comprehensive and extensive overview of security in the IoT. It encompasses various aspects of security including device security, data security and network security.
    - The NIST Cybersecurity Framework is not aimed at IoT but it provides a robust model for managing and, therefore, minimizing cybersecurity risks in IoT environments.
- The IoT security foundation can thus be viewed as a reference for the implementation of security in IoT devices and services right from the development of the concepts to the final product.
- ENISA gives an insight of the guidelines and recommendations that are required in the IoT security compliance.
    - The Baseline Security Recommendations for IoT are quite specific and focus on preserving data, device, and network security for IoT devices.
    - The ENISA Good Practices for IoT and Smart Infrastructures are guidelines that offer real-life recommendations on how to secure IoT deployments and minimize the associated threats.
- Thus, by adhering to these guidelines and models, organizations can ensure that their IoT systems are secure, interoperable, and reliable, which in turn enhances the confidence and reliability in any IoT solution offered.

In conclusion, the previous study finds important findings regarding the security issues and challenges related to the IoT applications in Saudi Arabian startups. Thus, organizations can implement effective security measures and guidelines to minimize the risks and ensure the data security and privacy of IoT devices by referring to the standard and frameworks developed by international organizations and standards development organizations [69]. Although there is already research available, there is still a lack of information about the distinct computer security concerns that entrepreneurs in Saudi Arabia have when implementing IoT solutions. It is critical to address this deficiency in order to provide a safe and prosperous environment for IoT-enabled companies throughout the country [16]. Table II presents a thorough summary of the current study and offers valuable insights derived from the difficulties, characteristics, and suggestions.

TABLE II. COMPREHENSIVE OVERVIEW OF THE EXISTING RESEARCH

Section	Summary	Challenges	Attributes	Recommendations
Global Perspective on Startup Ecosystems	Developed nations prioritize fostering a cyber-threat-free environment to enable startup growth and entrepreneurship [54], [55], [56], [57], [58], [59].	Regulatory barriers Cybersecurity concerns Interoperability issues	Government support Access to capital Technological infrastructure	Establish clear regulatory frameworks Enhance cybersecurity education and awareness Foster collaboration between government and industry
Security Concerns in IoT-enabled Startups	Security breaches undermine consumer trust and lead to significant financial losses; robust security measures are necessary [18], [62], [63].	Data breaches Compromised IoT devices	Encryption techniques Authentication protocols Intrusion detection systems	Implement end-to-end encryption Regularly update firmware and software Conduct security audits and penetration testing
Factors Influencing IoT-enabled Startup Ecosystem	Success factors include technological infrastructure, government support, societal acceptance, and economic conditions [18], [52], [66], [67].	Technological limitations Limited government support Societal resistance to technology Economic instability	Telecommunication infrastructure Government initiatives Societal attitudes towards technology Economic growth	Invest in expanding technological infrastructure Provide incentives for startups Promote digital literacy programs Foster economic diversification and stability
Saudi Arabia's Endeavor in Fostering IoT-enabled Startup Ecosystem	Saudi Arabia invests in initiatives like the e-Government program and Saudi Vision 2030 to foster entrepreneurship [3], [4], [6], [13], [14].	Limited access to funding Infrastructure gaps Bureaucratic issues	Government investments Strategic initiatives Vision 2030 initiatives	Establish dedicated funding programs for startups Improve infrastructure development Streamline regulatory processes and reduce bureaucratic red tape
Standards and Frameworks for IoT Security	International organizations and standards bodies have developed standards and frameworks to ensure IoT system security [46], [71], [72], [73], [74], [75], [76], [77].	Lack of standardized regulations Complexity of compliance	ITU standards ISO/IEC standards IEEE standards	Implement standardized security protocols and guidelines Simplify compliance procedures and provide support for implementation Encourage participation in certification programs and compliance frameworks

IV. IOT-DRIVEN COMPUTING CHALLENGES IN SAUDI ARABIAN START-UPS

This section explores the computational challenges faced by startups in Saudi Arabia, namely those that hinder their ability to expand and innovate. Fig. 2 shows that most of the computing problems IoT-driven startups in Saudi Arabia face are caused by four main things: worries about cybersecurity [4], [9], a lack of skilled IT professionals [9], [16], problems with infrastructure [8], [16], and issues with following rules and regulations [3], [15].

Among all the problems, cybersecurity is the most significant and pressing issue because it has an immediate impact on the operations and sustainability of organizations that use IoT devices. Due to the fact that these organizations are in the digital environment, they are very vulnerable to cyber risks, which may affect the important information, services, and, consequently, consumer trust. This issue shows that there is a necessity of proper cybersecurity measures which might be difficult for startups since they have a small budget.

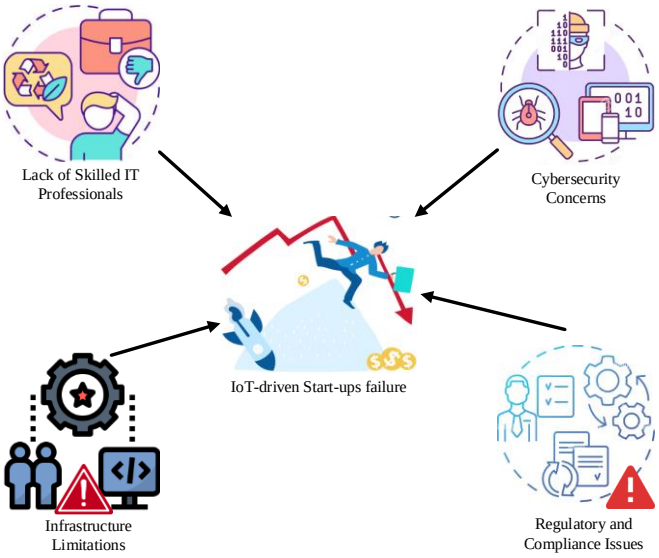


Fig. 2. Computing challenges in Saudi Arabian IoT-driven start-ups.

A. Cybersecurity Concerns

Startups in the Saudi Arabia are becoming more technology-oriented and apply digital technologies in their business processes which makes cybersecurity an important factor for them [4]. In view of the above, it is important that the valuable information and systems are protected as more cyber threats and attacks are being reported in the context of IoT-based startup companies [9].

However, some of the Internet of Things (IoT) start-ups might lack the necessary funds and personnel to develop robust cybersecurity mechanisms [12]. Lack of funding and lack of skilled personnel in the IT department are other drawbacks in their IT systems [4], [16]. Moreover, the identified danger of the dynamic nature of cyber threats is a continuous challenge that requires the permanent monitoring and tuning of the security measures [8].

This makes it essential for IoT based start-ups to prioritize the spending on cybersecurity technologies and protocols in order to address cybersecurity issues. In collaboration with cybersecurity professionals and employing cloud-based security measures, organizations can enhance their defenses against cyber threats [4], [8]. Also, organizations can minimize risks by raising awareness on the importance of cybersecurity and conducting comprehensive trainings [4], [9]. This section discusses some of the most significant and diverse cybersecurity threats that are directed towards IoT applications.

1) Security threats to IoT applications: Due to the increased integration of IoT devices, along with the big data they generate, the IoT faces a high level of security threats [76]. IoT devices often lack basic security features like secure boot and encryption and are vulnerable to exploitation through default configurations, weak passwords, and unencrypted communication channels [68]. These risks can lead to unauthorized access, data manipulation, or device compromise, which can be risky to privacy and organizational credibility. Thus, high-profile attacks like the Mirai botnet attack and the Stuxnet worm emphasize the importance of security in IoT systems [78], [79].

Fig. 3. Different security threats to IoT applications.

The IoT ecosystem consists of four layers: They are sensors and actuators, communication networks, middleware, and end-to-end applications. Each layer has its own security challenges and gateways help in transferring data from one layer to another. The existence of the weaknesses at these levels makes it vulnerable to attacks and, therefore, a need to understand the security situation [63]. Fig. 3 highlights these vulnerabilities and underscores the importance of preventive security measures in securing IoT applications from potential attackers.

a) Security Concerns about the Sensors and Actuators (Sensory) Layer

Threats to the sensory layer, which consists of physical sensors and actuators, include node capture, side-channel attacks, and malicious code injections [63].

- Node capture: Attackers replace low-power nodes with malicious ones. Solution: Employing physical security measures to safeguard nodes and utilizing tamper-resistant hardware will effectively deter node capture.
- Malicious Code Injections: Affect the potential of nodes. Solution: Secure boot and coded signing prevent the usage of unauthorized software on the devices.
- Side-Channel Attacks: In this case, the program utilizes CPU microarchitectures to gain data without permission. Solution: It is possible to decrease the effect of these attacks by employing hardware encryption and shielding measures.
- Eavesdropping and Interference: Target IoT systems in public areas. Solution: Employing encrypted communication channels and frequency-hopping methods may effectively safeguard against eavesdropping and interference.
- Sleep Deprivation and Booting Attacks: Cause devices to become inoperable or compromised. Solution: Deploying robust firmware update mechanisms and using advanced anomaly detection systems may effectively detect and mitigate these types of attacks [2], [21], [23].

b) Security Concerns about the Communication Network (Network) Layer

The network layer, which is responsible for delivering data, gets vulnerable to the phishing scams, unauthorized access, and denial of services (DoS) [63].

Phishing: mainly focuses on the IoT devices with the aim of collecting the login details. Resolution: It is possible to eliminate this risk by implementing and using multi-factor authentication (MFA) and training the users to recognize phishing schemes.

- Access attacks: Their role is to infiltrate the networks and to obtain information from there. Solution: It is also recommended to prevent illegal access through improving the establishment of robust network access control (NAC) and implementing intrusion detection systems (IDS).
- DDoS attacks: These are such as flooding the servers; an act that ends up disrupting the provision of relevant services. Solution: The attacks can be prevented by

using rate restriction, traffic analysis and services that prevent Distributed Denial of Service.

- Data transit and routing attacks: Their objective is to challenge the authenticity of data and juncture involved. Solution: On data transmission, it is possible to ensure data security and prevent the information from being intercepted in the process by employing secure and well encrypted end to end and safe routing pathways.

c) Security Concerns about the Middleware Layer

The extra layer called the middleware is also a weak link due to the risk of man-in-the middle attack, SQL injection and cloud malware injection [63].

- Man-in-the-Middle Attacks: These are such as controlling the protocol like the MQTT through which unlawful communication is made. Solution: Mutual authentication along with TLS (Transport Layer Security) could possibly help prevent such attacks.
- SQL injection: Combined with the factors above, it complicates and compromises the integrity of data. Resolution: Using parameterized queries or using input validation, one can meet the needs to counter SQL injection.
- Cloud Malware Injection and Flooding Attacks: They are designed for cloud infrastructure. Solution: To counter such threats, it is recommended to work with cloud safeguards that cover API protection, the assessment of critical weaknesses more often, and implementation of cloud-native security solutions.

d) Security Concerns about the End-To-End Application (Application) Layer

The application layer, which is directly related to the end-users, is concerned with problems like data theft, access control, and service interruption attacks [63].

- Malicious code injection and sniffer attacks can further lead to threats to the system integrity. Resolution: Implementing application firewalls; code reviews on a regular basis; having secure coding practices may minimize these risks.
- Reprogramming attacks: These have the propensity of causing hijacking of the network. Using such measures as implementing secure firmware upgrade and code signing will help to ensure that only trustworthy code is run on the devices.

e) Security Concerns about Gateways

While gateways are necessary to interconnect IoT devices, these devices are still susceptible to eavesdropping as well as man-in-the-middle attack during GW on-boarding [43], [61].

- Man-in-the-Middle Attacks: Solution: To eliminate the possibility of a third-party intercepting said information, a means of mutual authentication, as well as encrypted pathways of communication needs to be established.
- Eavesdropping resolution: It can be prevented by ensuring that the onboarding procedure that is invoked during the entire process is safe from the people who would want to snoop on the data transfer process and by making sure that the information exchanged has the highest level of encryption possible.
- Updating firmware must be done securely. Solution: We can therefore exclude the so-called unwanted access into the firmware by embracing reliable update procedures and ensuring the firmware is validated prior to use.

f) 4.1.1.6 Other Security Concerns

IoT devices provide issues like insufficient authentication, encryption mechanisms, and physical security measures [80], [81]. Implementing standardized protocols, regularly updating software, and having solid APIs are essential for reducing these risks. It is essential to address privacy concerns, supply chain vulnerabilities, and legacy system integration challenges in order to provide complete security for the Internet of Things (IoT) [78].

To address these difficulties, researchers propose using robust authentication, encryption, regular firmware upgrades, security audits, and industry-wide standards to minimize the security risks associated with IoT [44], [48], [49]. Implementing such solutions is crucial for protecting IoT applications and guaranteeing their ability to withstand emerging threats.

1) IoT Users' Privacy Concerns, Scalability and Interoperability

Currently, the risk of privacy compromise has been deemed very high, especially in areas such as the smart home since there is a growing prevalence of networked IoTs. This is the case because tracking user activity in such contexts could inadvertently disclose private data [82]. With IoT data storing parameters for individual customers the opportunity to use this chance to develop new products and individualized advertising has emerged the issues with data utilization and breaches that may lead to issues like identity theft. Various governments including the Saudi Arabia are trying to mitigate the challenges that relate to data governance and protection of data through organizations like the Saudi Data and Artificial Intelligence Authority (SDAIA) [83]. Thus, compliance with the rules of the protection of personal data prescribed by the international legal acts, including the General Data Protection Regulation created by the European Union [82], proves commitment to ethic data usage in IoT environments.

In the same way, more and different IoT devices increase the management and scalability challenges [62]. This means that there is a need to fit in large volumes of data, which exerts storage and network resources pressures so that interoperability enhances efficient data exchange across platforms and devices. Integration is key in the formation of composite services most importantly in smart city initiatives whereby the collaboration of IoT devices enhance distribution of resources and management of the civil structures [84].

In response to concerns about scalability and interoperability, IoT platforms and middleware have become popular solutions. These solutions include various features, such as device management, data integration, and application development [68]. These technical interventions reduce

fragmentation and inefficiencies while maximizing the advantages of IoT technology. In order to guarantee the ongoing development and effectiveness of IoT ecosystems, it is important to prioritize privacy protections, scalability, and interoperability, as shown in Fig. 4.

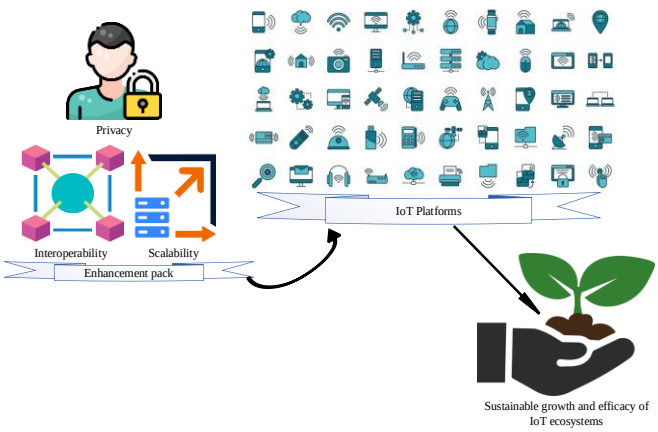


Fig. 4. Ensuring a sustainable growth and efficacy in IoT ecosystems.

B. Other Computing Challenges in Saudi Arabian Start-ups

This section examines the computational difficulties encountered by start-ups in Saudi Arabia, emphasizing significant barriers impeding their expansion and ingenuity.

1) Lack of skilled IT professionals: A significant challenge that start-ups in Saudi Arabia encounter is the limited availability of highly trained IT experts [9], [16]. Although there is a growing need for skilled professionals in fields like software development, data analytics, and cybersecurity, there is still a lack of competent workers to meet this need [4]. The country's education system may not adequately equip students with the skills and knowledge required for employment in IT-related industries, resulting in a limited supply of local talent for start-ups to hire. Additionally, the favoritism towards engineering and business degrees in comparison to IT fields worsens this shortage [10].

In order to tackle this difficulty, it is necessary to implement efforts that aim to enhance IT education and training programs at academic institutions and vocational training centers [9], [16]. Due to the lack of adequate number of skilled IT staffs, students should be encouraged to pursue IT degrees and professionals should be motivated to enhance their skills in the development of technologies.

2) Infrastructure limitations: Infrastructure restraints currently present a significant barrier to start-up firms in Saudi Arabia [16]. Although there have been improvements in the development of digital infrastructure, there are still gaps that remain, particularly in rural and disadvantaged regions [12]. Limited availability of dependable internet connections and power interruptions may disrupt corporate operations and hinder the use of digital technology. Also, the expense associated with building and sustaining infrastructure may be a hindrance for new businesses, particularly those with low financial means [8].

In order to overcome the limits of infrastructure, start-ups have the option to consider other solutions, such as using shared infrastructure services and forming partnerships with existing technology providers [13], [85]. It will prove useful to explore more efficient methods of obtaining the required IT solutions, such as cloud solutions and software-as-a-service (SaaS). Moreover, contributing to the government initiatives that aim at the improvement of the digital connectivity and the increase of the internet accessibility can also contribute to the formation of the more suitable environment for the start-ups [10].

3) Regulatory and compliance issues: Besides those common challenges, start-ups in Saudi Arabia face another challenge that is the tough regulatory and compliance requirements [3], [15]. With many start-ups emerging and constantly advancing technologies, legislation and law practices may be intricate with constantly varying differentiations and yet posing challenges of ensuring technology and data compliance. Thus, data privacy, intellectual property rights and some industry-specific rules add up to the complexity of the operational environment [16]. Also, there may be challenges incurred by start-ups due to bureaucratic procedures and legal issues which may hinder market entry and growth [14].

In considering how to overcome barriers and challenges to new start-ups, it will be necessary for start-ups to adopt regulatory compliance as a critical consideration and to formally include compliance as part of the business strategy. It may be helpful to involve a legal counsel and to follow the changes in legal regulation in order to minimize the risks and adhere to the laws. Moreover, backing regulatory adjustments, and also participating in the process of assisting governmental bodies in making procedures less burdensome can potentially contribute to improvement of the environment for start-ups [13].

In conclusion, the major challenges that start-ups in Saudi Arabia experience following computational issues includes: The absence of skilled IT personnel, limited infrastructure, and legal and regulatory issues. To tackle these difficulties, it is necessary for stakeholders from government, business, and academia to work together and create an environment that promotes innovation and growth [7], [10]. By surmounting these obstacles, start-ups may unleash their full capabilities and make a significant contribution to the country's economic diversification and digital transformation.

V. The Role of Vision 2030 in Promoting IoT

This section analyses how Vision 2030 has helped in the incorporation of IoT to Saudi Arabia's dream of a smarter future and diversification of economy. Vision 2030 was formulated by the Saudi Arabian government as a major social program aimed at diversifying its economy and developing it in various spheres [6]. The main goals of the organization are to improve the business climate, attract foreign investment, and foster innovation and entrepreneurship [6].

Saudi Arabia views the integration of IoT technology into Vision 2030 efforts as a crucial method for driving digital transformation, enhancing productivity, and fostering

innovation [3]. The main goals of Vision 2030 are shown in Fig. 5. They include building smart cities, speeding up the digital transformation of society, businesses, and government, supporting innovation, encouraging industrialization, and giving digital health top priority [86], [87]. These projects use IoT technology, including sensors, actuators, and networked devices, to enable the digitalization of processes, the gathering of data, and the optimization of operations [83].

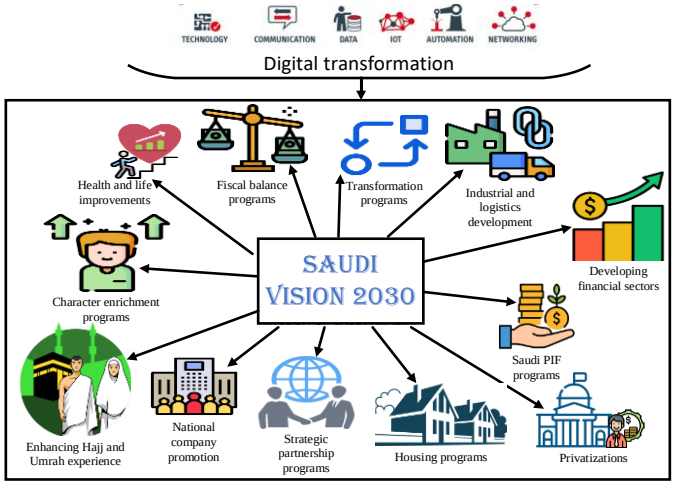


Fig. 5. Achieving Saudi Vision 2030 via digital transformation.

Furthermore, the government plays a significant role in assisting secure IoT-driven start-ups via many channels. Such resources consist of financial assistance, grants, access to spaces that incubate entrepreneurial ventures, accelerated programs for business, and hubs for innovation. The Badir Program for Technology Incubators and the KAUST Entrepreneurship Centre offer crucial support in the form of guidance, development, and connection-making to start-ups [7], [10], [54], [83]. Moreover, regulation authorities ease bureaucratic processes and establish conducive conditions for safe IoT-led start-ups through setting up of regulatory sandboxes and innovation zones.

The government also makes provisions for expending funds on skills development programs to improve the competencies of businesspersons and other professionals operating in the IoT value chain. The National Industrial Development and Logistics Program (NIDLP) provides necessary skills development, training sessions, and capacity enhancement interventions [88]. The government develops a pool of human capital to have skilled IoT personnel who can promote innovative development [54].

Saudi Arabia is moving towards promoting its Vision 2030 framework of bringing innovation and sustainable growth in business through supporting its programs in IoT technology and helping in the financial assistance in IoT based start-ups. It is therefore possible for Saudi Arabia to position itself as one of the foremost global leaders in IoT enablement and innovation through its smart investments, strategic changes in policies, and the promotion of partnership.

Furthermore, Table III shows the comparison of proposed and existing research on IoT security in Saudi Arabia Start-ups.

TABLE III. COMPARISON BETWEEN PROPOSED RESEARCH AND EXISTING STUDIES ON IOT SECURITY IN SAUDI ARABIAN START-UPS

Aspect	Proposed Research	Existing Studies
Target	Examines IoT security challenges specifically in Saudi Arabian start-ups.	Various studies cover IoT security across different sectors globally but may not focus specifically on Saudi start-ups [18], [62], [63].
Objectives	Identify cybersecurity risks, analyze the impact of IoT networking on privacy/security, and propose mitigation strategies.	Existing research often identifies security risks, however, lack comprehensive frameworks for specific contexts like Saudi Arabia [3], [4], [6], [13], [14].
Methods	Review of diverse publications and analysis of cybersecurity issues in the context of Saudi Vision 2030.	Many studies utilize case studies or empirical data, potentially overlooking broader contextual analyses like national strategies [54], [55], [56], [57], [58], [59].
Importance Findings	Highlights distinct cybersecurity obstacles faced by IoT-enabled businesses in Saudi Arabia; calls for funding, collaboration, and education.	Most of studies mention general IoT security challenges but may not address specific funding or educational needs in emerging markets [46], [71], [72], [73].
Contextual Relevance	Positions research within Saudi Arabia's economic goals and Vision 2030.	Various existing studies focus on developed countries or global trends without considering local economic and cultural factors [74], [75], [76], [77].
Recommendations	Advocates for a cooperative strategy involving policymakers, industry stakeholders, and entrepreneurs to enhance IoT security.	Many studies recommend technical solutions or policy frameworks; however, they did not emphasize collaboration with local stakeholders [13], [14].
Contributions to the Field of Research	Provides novel insights and a framework tailored to the unique challenges of Saudi Arabian start-ups in IoT.	Most of existing research do not focus on the unique socio-economic landscape of Saudi Arabia, limiting their applicability [46], [71], [72], [73].

VI. Discussion on Future Direction and Recommendations

This section provides a discussion on the paths that are to follow and gives recommendations on ways through which the Saudi Arabian government can foster the evolution of safer IoT devices led start-ups and promote creativity. These attempt to offer a strategic approach; however, it is high time to consider them in relation to the existing socio-economic conditions in Saudi Arabia and the peculiarities of the mentioned cybersecurity challenges.

1) Establish innovation networks: Creating innovation networks may help stakeholders share resources, skills, and best practices, leading to increased creativity and the ability to overcome difficulties [88]. These networks should highlight cybersecurity best practices to ensure that IoT start-ups place a high value on security right from the beginning.

2) Encourage open innovation: The open models help start-ups access resource, technologies and market opportunities and in turn existing enterprises can avail benefits of external innovation and entrepreneurial skills [89]. Some measures to empower open innovation may involve establishing safe IoT spaces and information sharing systems that enhance the knowledge of potential cybersecurity threats and the ways to combat them.

3) Support technology transfer: The government should endorse technology transfer efforts and collaborations to expedite the commercialization of research and innovation [54]. It is important to focus on sharing information and technologies that improve the security of the Internet of Things (IoT) such as blockchain technology. This will assist in avoiding new innovations from negating the authenticity of the data or the confidentiality of the user.

Cultivate a Culture of Innovation and Entrepreneurship: The implementation of the culture of innovation and entrepreneurship plays a key role in establishing secured IoT based Start-ups and Innovations in Saudi Arabia [85]. The following are the primary recommendations:

- Promoting a new organizational culture where people would embrace the principles of entrepreneurship in tackling cybersecurity issues.
- Supporting and encouraging start-up incubation and acceleration initiatives that focus on enhancing safe IoT innovation.
- Celebrating achievements in entrepreneurship, including specific accomplishments that can potentially convey success in protecting IoT applications.
- State-sponsored honors, competitions, and meetings can inform about successes of prospering start-ups and businesses to inspire a new generation of innovators and actors of change [18].

4) Leverage international partnerships: Consequently, it's wiser for Saudi Arabian IoT-drive start-ups to capitalize on foreign partnerships since this will afford them the international markets and foreign experience along with the advanced technologies that are vital for their growth [13]. Some recommendations are as follows:

- Remain committed to the search for international cooperation and funding sources to strengthen protection of IoT networks with the participation of specialized organizations.
- Works with other universities and industries that have well-strategized cybersecurity system mechanisms across the globe for technology update and knowledge sharing.
- Providing help in the access to international markets, distribution channels, and business networks while meeting international cybersecurity standards for start-up companies.

5) Specific socio-economic considerations: To make these suggestions realistic and effective in the Saudi context, the following should be considered given the country's socio-economic values:

- Economic Diversification: ensuring that the development of IoT start-ups in Saudi Arabia aligns with the aims of economic diversification outlined in Vision 2030, with a specific emphasis on supporting non-oil industries.
- Education and Training: More resources need to be directed to education and training that can help in improving cybersecurity and create workforce that can handle IoT security threats.
- Regulatory Environment: Creation and enforcement of laws that foster IoT security, thus ensuring that the start-ups follow the regional and international standards of cybersecurity.

Thus, Saudi Arabia can contribute to the development of an active environment in the IoT industry by considering socio-economic factors and specific cybersecurity challenges, as well as cooperation, innovation, and entrepreneurship [10]. This strategy will ensure that the economy grows and becomes prosperous as required by Vision 2030 while at the same time ensuring that the security of IoT systems is not compromised in any way.

VII. Conclusion

This paper has reviewed the literature on the adoption of IoT technology in start-up companies in Saudi Arabia with a focus on the cybersecurity challenges. The research highlights the critical cybersecurity risks associated with IoT adoption in Saudi Arabian startups, particularly in the context of data privacy and network security vulnerabilities. The study emphasizes the necessity for startups to implement advanced security measures despite limited resources and proposes strategic solutions, such as cloud-based security, collaboration with cybersecurity experts, and enhanced cybersecurity education. This research fills a notable gap by addressing the unique cybersecurity needs of startups in emerging markets, advancing the understanding of IoT security in the

entrepreneurial landscape. Moreover, the government is to seek solutions to social issues and promoting corporate growth through IoT investment, these start-ups face significant cybersecurity challenges. This is due to the fact that the threats are constantly evolving, and the resources available in such efforts are scarce.

For this reason, start-ups need to allocate their resources to cybersecurity technology and procedures to address these issues. Another way of improving the organizations' cybersecurity is through engaging the services of cybersecurity professionals, and the use of cloud technologies. In the same manner increasing the awareness of the public regarding the proper measures to take to improve cybersecurity and increasing the frequency of educational campaigns is also an effective way in increasing the level of cybersecurity preparedness.

Therefore, there is the need to do more work and engage in more research to discover new strategies in the protection of IoT in Saudi Arabian start-ups. It is important to address the cybersecurity issues to harness the full potential of IoT, boost the economy, foster innovation, and position Saudi Arabia as a leader in the IoT technology sector.

The IoT industry decision makers, stakeholders and investors in Saudi Arabia should ensure that proper cyber security measures are put in place and resources to be directed towards development of secured IoT ecosystem. Saudi Arabian start-ups could navigate their way through the cybersecurity environment and succeed in the era of digital and interconnected world by collaborating and investing more.

Future Research and Implementation:

- Lightweight Blockchain Protocols and Edge Computing Solutions: It is recommended that further studies focus on the enhancement of blockchain protocol that has low power consumption and is suitable for the IoT devices' edge computing.
- Standardized Cybersecurity Frameworks: From the findings of the present study, it can be suggested that there is a need for the formulation of suitable cybersecurity models that can be applied to the context of the startups and at the same time ensure that all the IoT systems are compliant.
- Synergy among academia, industry, and government: This implies that new challenges must be taken and safer IoT technologies and environments have to be created.
- Educational Initiatives: Awareness and education of entrepreneurs and IT specialists in the context of the creation of secure IoT systems can be considered as one of the most significant activities directed towards the development of the IoT security sphere.

Implementing these measures can help Saudi Arabia create a competitive environment in the IoT industry and promote cooperation, innovation, and business growth. This strategy will foster economic growth and prosperity in line with Vision 2030 while at the same time focusing on the security of IoT devices. Through close cooperation with all stakeholders, the country can become a global leader in safe and innovative IoT solutions.

ACKNOWLEDGMENT

The research presented in this paper is funded by the Saudi Arabian Cultural Bureau (SACB) through a PhD studentship at the University of Sussex.

REFERENCES

[1] A. Sallam, F. Al Qahtani, and A. S. A. Gaid, "Blockchain in Internet of Things: A Systematic Literature Review," in 2021 International Conference of Technology, Science and Administration, ICTSA 2021, 2021. doi: 10.1109/ICTSA52017.2021.9406545.

[2] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures," Computers, 2020, doi: 10.3390/computers9020044.

[3] M. N. Al Otaibi, "Internet of Things (IoT) Saudi Arabia Healthcare Systems: State-Of-The-Art, Future Opportunities and Open Challenges," J Health Inform Dev Ctries, vol. 13, no. 1, 2019.

[4] M. Alanazi and B. Soh, "Investigating Cyber Readiness for IoT Adoption in Saudi Arabia," IBIMA Business Review, vol. 2020, 2021, doi: 10.5171/2020.937087.

[5] A. M. AL-Shehry, "Transformation towards E-government in The Kingdom of Saudi Arabia: Technological and Organisational Perspectives," 2008.

[6] F. Y. Al Anezi, "Saudi Vision 2030: Sustainable economic development through IoT," in Proceedings - 2021 IEEE 10th International Conference on Communication Systems and Network Technologies, CSNT 2021, 2021. doi: 10.1109/CSNT51715.2021.9509592.

[7] J. Alzahrani, "The impact of e-commerce adoption on business strategy in Saudi Arabian small and medium enterprises (SMEs)," Review of Economics and Political Science, vol. 4, no. 1, 2019, doi: 10.1108/REPS-10-2018-013.

[8] O. Almutairi and K. Almarhabi, "Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia," International Journal of Advanced Computer Science and Applications, vol. 12, no. 4, 2021, doi: 10.14569/IJACSA.2021.0120477.

[9] M. S. Albarrak and S. A. Alokley, "FinTech: Ecosystem, Opportunities and Challenges in Saudi Arabia," Journal of Risk and Financial Management, vol. 14, no. 10, 2021, doi: 10.3390/jrfm14100460.

[10] M. Mahmud, Y. O. Akinwale, R. A. Khan, and A. Alaraifi, "Techno entrepreneurship adoption: An intention based assessment study of start-ups in the Kingdom of Saudi Arabia," J Entrep Educ, vol. 22, no. 5, 2019.

[11] W. Basri, "Examining the impact of artificial intelligence (Ai)-assisted social media marketing on the performance of small and medium enterprises: Toward effective business management in the saudi arabian context," International Journal of Computational Intelligence Systems, vol. 13, no. 1, 2020, doi: 10.2991/ijcis.d.200127.002.

[12] A. Y. Alqahtani, "Investigation of startups' sustainability: empirical evidence from Saudi Arabia," Entrepreneurship and Sustainability Issues, vol. 10, no. 1, 2022, doi: 10.9770/jesi.2022.10.1(6).

[13] A. R. Abu Bakar, S. Z. Ahmad, N. S. Wright, and H. Skoko, "The propensity to business startup: Evidence from Global Entrepreneurship Monitor (GEM) data in Saudi Arabia," Journal of Entrepreneurship in Emerging Economies, vol. 9, no. 3, 2017, doi: 10.1108/JEEE-11-2016-0049.

[14] R. A. Mohammed, M. Horoub, and H. Walwil, "Establishing a start-up in Saudi Arabia: the Innosoft story," Emerald Emerging Markets Case Studies, vol. 9, no. 2, 2019, doi: 10.1108/EEMCS-05-2017-0076.

[15] N. Trad and M. A. Al Dabbagh, "Use of Social Media as an Effective Marketing Tool for Fashion Startups in Saudi Arabia," Open J Soc Sci, vol. 08, no. 11, 2020, doi: 10.4236/jss.2020.811029.

[16] Majed Qabil Alsolamy, "Startups in Saudi Arabia: Challenges and Opportunities," International Journal of Research in Business and Social Science (2147- 4478), vol. 12, no. 2, 2023, doi: 10.20525/ijrbs.v12i2.2312.

[17] H. M. Aboalsamh, L. T. Khrais, and S. A. Albahussain, "Pioneering Perception of Green Fintech in Promoting Sustainable Digital Services Application within Smart Cities," Sustainability (Switzerland), vol. 15, no. 14, 2023, doi: 10.3390/su151411440.

[18] A. M. K. Alkhazaleh, "Challenges and Opportunities for Fintech Startups: Situation in the Arab World," Academy of Accounting and Financial Studies Journal, vol. 25, no. 3, 2021.

[19] C. PÖPPER, M. MANIATAKOS, and R. DI PIETRO, "Cyber Security Research in the Arab Region: A Blooming Ecosystem with Global Ambitions.," Commun ACM, vol. 64, no. 4, 2021.

[20] K. Kim, "Security and Privacy Liability Policy in the Arab World," Security Policy Paper, vol. 2, no. 1, 2021, doi: 10.26735/outi8333.

[21] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey," IEEE Access, 2020, doi: 10.1109/ACCESS.2020.3022661.

[22] D. Choudhary, "Security Challenges and Countermeasures for the Heterogeneity of IoT Applications," Journal of Autonomous Intelligence, vol. 1, no. 2, 2019, doi: 10.32629/jai.v1i2.25.

[23] H. F. Atlam and G. B. Wills, "IoT Security, Privacy, Safety and Ethics," in Internet of Things, 2020. doi: 10.1007/978-3-030-18732-3_8.

[24] A. Lakhdari, A. Bouguettaya, S. Mistry, and A. G. Neiat, "Composing Energy Services in a Crowdsourced IoT Environment," IEEE Trans Serv Comput, vol. 15, no. 3, 2022, doi: 10.1109/TSC.2020.2980258.

[25] L. Li and G. Wu, "Development and Design of Electronic Information Management System Based on Internet of Things Technology," in ACM International Conference Proceeding Series, 2023. doi: 10.1145/3585967.3585976.

[26] M. Dobrojevic and N. Bacanin, "IoT as a Backbone of Intelligent Homestead Automation," Electronics (Switzerland), vol. 11, no. 7. 2022. doi: 10.3390/electronics11071004.

[27] R. Martínez-Peláez et al., "An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances," Sensors (Switzerland), 2019, doi: 10.3390/s19092098.

[28] L. Belli et al., "IoT-enabled smart sustainable cities: Challenges and approaches," Smart Cities, vol. 3, no. 3, 2020, doi: 10.3390/smartcities3030052.

[29] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues," IEEE Access, 2017, doi: 10.1109/ACCESS.2017.2779263.

[30] P. K. Senyo, E. Addae, and R. Boateng, "Cloud computing research: A review of research themes, frameworks, methods and future research directions," Int J Inf Manage, 2018, doi: 10.1016/j.ijinfomgt.2017.07.007.

[31] K. Mahmood, W. Akram, A. Shafiq, I. Altaf, M. A. Lodhi, and S. H. Islam, "An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments," Computers and Electrical Engineering, 2020, doi: 10.1016/j.compeleceng.2020.106888.

[32] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi, and Z. Lin, "When Machine Learning Meets Privacy: A Survey and Outlook," ACM Computing Surveys. 2021. doi: 10.1145/3436755.

[33] Md. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions," Blockchain: Research and Applications, p. 100006, 2021, doi: 10.1016/j.bcra.2021.100006.

[34] X. Huang, D. Zou, G. Cheng, X. Chen, and H. Xie, "Trends, Research Issues and Applications of Artificial Intelligence in Language Education," EDUCATIONAL TECHNOLOGY & SOCIETY, 2021.

[35] A. A. Qaffas, R. Hoque, and N. Almazmomi, "The Internet of Things and Big Data Analytics for Chronic Disease Monitoring in Saudi Arabia," Telemedicine and e-Health, vol. 27, no. 1, 2021, doi: 10.1089/tmj.2019.0289.

[36] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-based approach for e-health data access management with privacy protection," in IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD, 2019. doi: 10.1109/CAMAD.2019.8858469.

[37] L. Edwards, "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective," SSRN Electronic Journal, 2016, doi: 10.2139/ssrn.2711290.

[38] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," Future Generation Computer Systems, vol. 97, pp. 512–529, 2019, doi: 10.1016/j.future.2019.02.060.

[39] P. Kumar and L. Chouhan, "A privacy and session key based authentication scheme for medical IoT networks," Comput Commun, 2021, doi: 10.1016/j.comcom.2020.11.017.

[40] S. Qazi, B. A. Khawaja, and Q. U. Farooq, "IoT-Equipped and AI-Enabled Next Generation Smart Agriculture: A Critical Review, Current Challenges and Future Trends," IEEE Access, vol. 10. 2022. doi: 10.1109/ACCESS.2022.3152544.

[41] A. Babiyola, V. Saillaja, S. P. Shally, and S. Omkumar, "Development of an Internet of Things-based Integrated System for Fleet Management in RealTime," in Proceedings of the 2nd International Conference on Edge Computing and Applications, ICECAA 2023, 2023. doi: 10.1109/ICECAA58104.2023.10212331.

[42] S. Bansal and A. Gupta, "IoT-Enabled Intelligent Traffic Management System," in EAI/Springer Innovations in Communication and Computing, 2023. doi: 10.1007/978-3-031-04524-0_6.

[43] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," Journal of Network and Computer Applications. 2020. doi: 10.1016/j.jnca.2019.102481.

[44] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, and A. A. Ghorbani, "Security issues in Internet of Vehicles (IoV): A comprehensive survey," Internet of Things (Netherlands), vol. 22. 2023. doi: 10.1016/j.iot.2023.100809.

[45] P. Rutravigneshwaran and G. Anitha, "Security Model to Mitigate Black Hole Attack on Internet of Battlefield Things (IoBT) Using Trust and K-Means Clustering Algorithm," International Journal of Computer Networks and Applications, vol. 10, no. 1, 2023, doi: 10.22247/ijcna/2023/218514.

[46] V. Sklyar and V. Kharchenko, "ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios," in Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019, 2019. doi: 10.1109/IDAACS.2019.8924452.

[47] S. Aljarallah and R. Lock, "An empirical study of sustainable e-government characteristics in saudi arabia," in Proceedings of the European Conference on e-Government, ECEG, 2018.

[48] M. E. E. Alahi et al., "Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends," Sensors, vol. 23, no. 11. 2023. doi: 10.3390/s23115206.

[49] N. S. Abu et al., "Internet of Things Applications in Precision Agriculture: A Review," Journal of Robotics and Control (JRC), vol. 3, no. 3. 2022. doi: 10.18196/jrc.v3i3.14159.

[50] I. Mahnashi, B. Salah, and A. E. Ragab, "Industry 4.0 Framework Based on Organizational Diagnostics and Plan–Do–Check–Act Cycle for the Saudi Arabian Cement Sector," Sustainability (Switzerland), vol. 15, no. 14, 2023, doi: 10.3390/su151411261.

[51] A. Altaf, F. Iqbal, R. Latif, B. M. Yakubu, S. Latif, and H. Samiullah, "A Survey of Blockchain Technology: Architecture, Applied Domains, Platforms, and Security Threats," Soc Sci Comput Rev, 2022, doi: 10.1177/08944393221110148.

[52] W. Hermawan and K. Tjendrasa, "Evaluation Of Investment In IoT Startup at PT TMI," Jurnal Ilmu Sosial Politik dan Humaniora, vol. 3, no. 2, 2020, doi: 10.36624/jisora.v3i2.46.

[53] V. Neerugatti, Dr. B. K.K., J. P. Dr. M., and S. K. V. D., "Internet of Things: A Product Development Cycle for the Entrepreneurs," HELIX, vol. 10, no. 2, 2020, doi: 10.29042/2020-10-2-155-160.

[54] S. Y. Cooper and J. S. Park, "The impact of 'incubator' organizations on opportunity recognition and technology innovation in new, entrepreneurial high-technology ventures," International Small Business Journal, vol. 26, no. 1, 2008, doi: 10.1177/0266242607084658.

[55] P. W. Williams and M. Peters, "Entrepreneurial performance and challenges for aboriginal small tourism businesses: A Canadian case," Tourism Recreation Research, vol. 33, no. 3, 2008, doi: 10.1080/02508281.2008.11081551.

[56] V. Jafari-Sadeghi, "The motivational factors of business venturing: Opportunity versus necessity? A gendered perspective on European countries," J Bus Res, vol. 113, 2020, doi: 10.1016/j.jbusres.2019.09.058.

[57] H. Sandberg, A. Alnoor, and V. Tiberius, "Environmental, social, and governance ratings and financial performance: Evidence from the European food industry," Bus Strategy Environ, vol. 32, no. 4, 2023, doi: 10.1002/bse.3259.

[58] D. B. Audretsch, "Have we oversold the Silicon Valley model of entrepreneurship?," Small Business Economics, vol. 56, no. 2, 2021, doi: 10.1007/s11187-019-00272-4.

[59] F. F. Adedoyin, F. V. Bekun, O. M. Driha, and D. Balsalobre-Lorente, "The effects of air transportation, energy, ICT and FDI on economic growth in the industry 4.0 era: Evidence from the United States," Technol Forecast Soc Change, vol. 160, 2020, doi: 10.1016/j.techfore.2020.120297.

[60] H. Yarovenko, "'Evaluating the threat to national information security,'" Problems and Perspectives in Management, vol. 18, no. 3, 2020, doi: 10.21511/ppm.18(3).2020.17.

[61] S. Prajapati and A. Singh, "Cyber-Attacks on Internet of Things (IoT) Devices, Attack Vectors, and Remedies: A Position Paper," in EAI/Springer Innovations in Communication and Computing, 2022. doi: 10.1007/978-3-030-73885-3_17.

[62] V. Narayandas, M. Archana, and D. Raman, "The Role of MANET in Collaborating IoT End Devices: A New Era of Smart Communication," International Journal of Interactive Mobile Technologies, 2021, doi: 10.3991/ijim.v15i13.23045.

[63] L. Javed, B. M. Yakubu, M. Waleed, Z. Khaliq, A. B. Suleiman, and N. G. Mato, "BHC-IoT: A Survey on Healthcare IoT Security Issues and Blockchain-Based Solution," International Journal of Electrical and Computer Engineering Research, vol. 2, no. 4, 2022, doi: 10.53375/ijecer.2022.302.

[64] A. L. Bozzo, H. D. M. Freitas, and C. D. P. Martens, "Main initial difficulties faced by IoT startups," Revista da Micro e Pequena Empresa, vol. 13, no. 2, 2019, doi: 10.21714/19-82-25372019v13n2p4059.

[65] S. Lim, O. Kwon, and D. H. Lee, "Technology convergence in the Internet of Things (IoT) startup ecosystem: A network analysis," Telematics and Informatics, vol. 35, no. 7, 2018, doi: 10.1016/j.tele.2018.06.002.

[66] J. Kim and E. Park, "Understanding social resistance to determine the future of Internet of Things (IoT) services," Behaviour and Information Technology, vol. 41, no. 3, 2022, doi: 10.1080/0144929X.2020.1827033.

[67] T. Mhlongo, J. A. van der Poll, and T. Sethibe, "A Control Framework for a Secure Internet of Things within Small-, Medium-, and Micro-Sized Enterprises in a Developing Economy," Computers, vol. 12, no. 7, 2023, doi: 10.3390/computers12070127.

[68] E. Lee, Y. D. Seo, S. R. Oh, and Y. G. Kim, "A Survey on Standards for Interoperability and Security in the Internet of Things," IEEE Communications Surveys and Tutorials, vol. 23, no. 2. 2021. doi: 10.1109/COMST.2021.3067354.

[69] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," IEEE Access, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3109886.

[70] P. Devi, K. Dhivyapriya, D. Venkata Subramanian, and S. Sathyalakshmi, "A review on iot-standards, protocols, frameworks," Journal of Advanced Research in Dynamical and Control Systems, vol. 9, no. Special Issue 18. 2017.

[71] "International Telecommunication Union (ITU)," in International Regulatory Co-operation, 2016. doi: 10.1787/9789264244047-37-en.

[72] F. Schneider, C. Maurer, and R. C. Friedberg, "International organization for standardization (ISO) 15189," Annals of Laboratory Medicine, vol. 37, no. 5. 2017. doi: 10.3343/alm.2017.37.5.365.

[73] T. Büthe and A. fattah Alshadafan, "The International Electrotechnical Commission," in The Evolution of Transnational Rule-Makers through Crises, 2023. doi: 10.1017/9781009329408.021.

[74] "Institute of Electrical and Electronics Engineers (IEEE)," in Cite Them Right online - The Basics, 2022. doi: 10.5040/9781350928060.35.

[75] "National Institute of Standards and Technology," Choice Reviews Online, vol. 50, no. 04, 2012, doi: 10.5860/choice.50-2030.

[76] IoT Security Foundation, "IoT Security Foundation," IOT SECURITY FOUNDATION CONFERENCE 2016.

[77] C. NIST, "Cybersecurity Framework | NIST," NIST Website, 2016.

[78] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, "Iot in smart cities: A survey of technologies, practices and challenges," Smart Cities, vol. 4, no. 2, 2021, doi: 10.3390/smartcities4020024.

[79] A. Borys, A. Kamruzzaman, H. N. Thakur, J. C. Brickley, M. L. Ali, and K. Thakur, "An Evaluation of IoT DDoS Cryptojacking Malware and Mirai Botnet," in 2022 IEEE World AI IoT Congress, AIIoT 2022, 2022. doi: 10.1109/AIIoT54504.2022.9817163.

[80] N. Nanglae, B. M. Yakubu, and P. Bhattarakosol, "Extraction of Hidden Authentication Factors from Possessive Information," Journal of Sensor and Actuator Networks, vol. 12, no. 4, p. 62, Aug. 2023, doi: 10.3390/jsan12040062.

[81] B. M. Yakubu, M. I. Khan, and P. Bhattarakosol, "IPChain: Blockchain-Based Security Protocol for IoT Address Management Servers in Smart Homes," Journal of Sensor and Actuator Networks, vol. 11, no. 4, 2022, doi: 10.3390/jsan11040080.

[82] D. Pal, X. Zhang, and S. Siyal, "Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach," Technol Soc, vol. 66, 2021, doi: 10.1016/j.techsoc.2021.101683.

[83] Z. A. Memish, M. M. Altuwaijri, A. H. Almoeen, and S. M. Enani, "The Saudi data & artificial intelligence authority (SDAIA) vision: Leading the Kingdom's journey toward global leadership," Journal of Epidemiology and Global Health, vol. 11, no. 2. 2021. doi: 10.2991/JEGH.K.210405.001.

[84] M. Anagnostopoulos, G. Spathoulas, B. Viaño, and J. Augusto-Gonzalez, "Tracing your smart-home devices conversations: A real world iot traffic data-set," Sensors (Switzerland), 2020, doi: 10.3390/s20226600.

[85] H. Abdullah Alnemer, "Predicting start-up intention among the females of Saudi Arabia using social cognitive theory," World Journal of Entrepreneurship, Management and Sustainable Development, vol. 17, no. 4, 2021, doi: 10.1108/WJEMSD-05-2021-0085.

[86] Abdulkarim AlShinqeeti, "Digital Transformation in Saudi Arabia: A Journey of Progress and Innovation," LinkedIn. Accessed: Mar. 28, 2024. [Online]. Available: https://www.linkedin.com/pulse/digital-transformation-saudi-arabia-journey-progress-alshinqeeti-t5pef/

[87] ArrxdQ, "Saudi Vision 2030," X. Accessed: Mar. 28, 2024. [Online]. Available: https://twitter.com/ArrxdQ/status/1386401941790461956

[88] A. B. E. Aichouni, L. Kolsi, and M. Aichouni, "The Engineering Students Innovation Club Project for Human Capital Development in the areas of Industry 4.0 - From the Design to Implementation," in 2020 Industrial and Systems Engineering Conference, ISEC 2020, 2020. doi: 10.1109/ISEC49495.2020.9229924.

[89] M. K. Sarma and D. Dutta, "Adoption of Technological Service Innovations: A Systematic Review Investigating the Special Role of Incremental Innovations," International Journal of Technology, Policy and Management, vol. 24, no. 2, 2024, doi: 10.1504/ijtpm.2024.10058087.

A Low-Cost IoT Sensor for Indoor Monitoring with Prediction-Based Data Collection

Paolo Capellacci, Lorenzo Calisti, Emanuele Lattanzi
Department of Pure and Applied Sciences, University of Urbino, Urbino, Italy

***Abstract*—The proliferation of Internet of Things technologies has revolutionized the landscape of indoor environmental monitoring, offering opportunities to enhance comfort, health, and energy efficiency. This paper presents the development and implementation of a low-cost IoT sensor system designed for indoor monitoring with a Machine Learning-driven prediction-based data collection approach. Leveraging deep learning algorithms, the IoT device predicts significant environmental changes and dynamically adjusts the data collection frequency to optimize energy consumption and data transmission. Experimental results demonstrate the system's ability to accurately predict environmental variations, resulting in a reduction in data transmission and power usage up to 96% without compromising the monitoring quality. The findings highlight the potential of prediction-based data collection as a viable solution for sustainable and effective indoor environment monitoring on low-cost IoT devices.**

***Keywords*—IoT; indoor monitoring; prediction-based data collection; deep-learning**

I. Introduction

The widespread diffusion of Internet of Things (IoT) technologies has transformed various contests, ranging from environmental monitoring to smart buildings, agriculture, and transportation. In the indoor monitoring field, IoT systems enable real-time data collection from numerous sensors, providing opportunities to enhance comfort, health, and energy efficiency. By monitoring parameters such as temperature, humidity, air quality, and occupancy, these systems can optimize environmental conditions for the well-being of occupants while minimizing energy consumption [1]. However, traditional IoT-based environmental monitoring systems often rely on continuous data collection, leading to excessive power consumption and inefficient data transmission, especially in resource-constrained environments [2]. The challenge of balancing data accuracy and energy efficiency is particularly significant for low-cost IoT systems, where prolonged battery life and reduced data transmission costs are critical. Recent advancements in Machine Learning (ML) offer potential solutions to this issue. ML techniques can enable IoT devices to predict environmental changes dynamically, allowing for adaptive data collection strategies that optimize energy use without compromising the quality of monitoring. This paradigm shift from static to Prediction-Based Data Collection (PBDC) has the potential to enhance both the sustainability and effectiveness of IoT systems in indoor environments [3].

In particular, PBDC retains the original sampling frequency of the application while reducing energy consumption by minimizing the amount of data that needs to be transmitted [4]. This is achieved by constructing a model of the sensed data, which is then used both at the sensor and at the sink to estimate the sampled data points. When a new sample is obtained, the sensor checks if it falls within the predefined error tolerance. If it does, no further action is required (i.e. data are not sent); if not, a new model is created and sent to the sink.

In this paper, we present the development and implementation of a low-cost IoT sensor system for indoor environmental monitoring that leverages machine learning to optimize data collection and transmission. By employing ML algorithms to predict significant environmental changes, our system dynamically adjusts the frequency of data collection, resulting in reduced power usage and data transmission overhead. Experimental results demonstrate that the proposed system accurately predicts environmental variations, achieving energy savings of up to 96% while maintaining high data quality.

The contributions of this work are twofold:

- We introduce a low-cost IoT sensor for indoor monitoring capable of easily measuring environmental parameters, and we characterize it on a real deployment.
- We implement a PBDC strategy by means of deep-learning models, and we deeply characterize its efficiency in terms of average error and transmission ratio with respect to a traditional approach.

The rest of the paper is organized as follows: Section II provides related work on IoT low-cost sensors and PBDC-enabled devices. Section III describes the hardware-software IoT architecture and provides a detailed description of the PBDC mechanism we implemented using ML models. In Section IV, we provide a detailed description of the case study based on a real prototype deployment, and we discuss the results and findings, while Section V concludes the paper.

II. Related Works

In the literature, several authors have addressed the research and development of tools and systems for monitoring environmental metrics, particularly focused on measuring and controlling Indoor Air Quality (IAQ). Among these, Saini et al. [5] presents a systematic review of the current state of the art in IoT-based IAQ monitoring systems. They examined numerous studies published between 2015 and 2020, finding that most of the research has been conducted in countries such as Portugal, China, India, and Malaysia. Their findings also reveal that a significant portion of studies focuses on monitoring comfort parameters and CO_2 levels, with many systems being implemented using Arduino or Raspberry Pi.

Several studies have investigated the use of edge and fog computing devices in air quality monitoring. For instance, Bianconi et al. [6] proposed an IoT system to improve citizens' well-being in Savona, Italy. Their findings highlight the network's capability to monitor well-being over the long term and promptly respond to critical situations when necessary. Similarly, Narayana et al. [7] introduced an advanced real-time environmental monitoring system leveraging IoT and wireless sensors. This system employs innovative techniques for monitoring water treatment and air quality, capturing real-time data on air, water, waste, energy, and soil, thereby making a significant contribution to sustainable living.

Focusing on indoor environments, various systems have been developed to monitor air quality using IoT technology, capable of tracking $PM_{2.5}$, CO_2, temperature, and humidity simultaneously [8]. Some of these systems also include predictive capabilities, providing alerts for potentially hazardous conditions [9]. Additionally, Sung et al. [10] applied a combination of air quality indices, including the carbon dioxide index and the air quality index from the American Society of Heating, Refrigerating, and Air-Conditioning Engineers, to simulate the impact of these factors on indoor air quality.

AI-based approaches are also gaining momentum, with models such as Long Short-Term Memory (LSTM) being applied to predict future CO_2 concentrations, thus improving IAQ management systems by enabling preemptive actions. Other studies have integrated multi-headed Convolutional Neural Network (CNN) models to enhance air quality predictions through transfer learning, which boosts system efficiency, even in environments with limited data [11].

In sensor-based IoT applications, the majority of the energy budget is consumed during the transmission of collected data [12]. In the literature, various methods, such as data compression, data quantization, and data aggregation, are available [13]. However, we focus on PBDC due to its simplicity and proven effectiveness in scenarios involving periodic data collection [14].

In PBDC, the original sampling period required by the IoT application is preserved, but the total amount of transmitted data is reduced [15] by creating a forecasting model for the sensed data. This model is shared among both the IoT sensors and the collecting server. At the IoT device level, each new sample is checked to see if it falls within acceptable error margins. If it does, no action is taken (i.e. no data transmission occurs); if it doesn't, a new model is generated and sent to the sink. If the model accurately reflects the data trend, network communication, and energy can be significantly reduced, sometimes by as much as 99% [16], [17], [18], [19]. Since the early days of IoT research, various models have been explored. Probabilistic models [20], [21] approximate data with user-specified confidence but require domain experts to encode special data characteristics. Other techniques include linear regression [22], [14], autoregressive models [23], and Kalman filters [24], but these demand substantial memory and computational resources, making them challenging to implement on resource-constrained devices.

With the introduction of artificial intelligence tools, many researchers began exploring a novel approach to time series forecasting based on machine learning. They employed classical machine learning methods and models, such as support vector machines (SVM), random forests (RF), and backpropagation (BP), for time series forecasting tasks achieving better results [25], [26].

In the last decades, the rapid development of IoT technology has led to the generation of massive amounts of time series data. These extensive time series datasets often exhibit high dimensionality and nonlinearity, making it challenging to achieve the desired prediction accuracy using previous machine learning or statistical methods. To address this challenge, researchers have introduced deep learning methods such as LSTMs, Recurrent Neural Networks (RNNs), and Gated Recurrent Units (GRUs) to tackle the prediction and analysis of massive multivariate time series data achieving significant success [27], [28]. In the IoT domain, forecasting by means of deep-learning techniques has been prevalently used to reconstruct missing or corrupted data in order to enhance system reliability [29], [30], [31], [32]. The computational demands of deep learning tools present a significant challenge in meeting the constraints of tiny sensors. Consequently, in-sensor direct deep-learning forecasting approaches seem to be uncommon. Recently, Lalouani et al. proposed a study on the energy efficiency of an ECG wearable sensor through predictive sampling [33]. In particular, the authors used an LSTM network to assess whether a sample can be predicted using the previous ones, subject to a certain inaccuracy bound. Samples that can be accurately predicted are skipped, while the rest are buffered to be sent to the gateway. The authors simulate the energy efficiency of the method by computing the number of skipped samples starting from an ad-hoc created ECG dataset.

The various methods described so far offer significant advantages but present challenges limiting their effectiveness. For example, edge and IoT devices provide rapid responses but face scalability and reliability issues, which may be imprecise in complex environments. Data compression and aggregation techniques reduce transmission costs but introduce the risk of losing critical information. Finally, machine learning techniques ensure accurate predictions but require high computational resources, making them less suitable for IoT devices with limited capabilities.

This paper presents a low-cost IoT sensor platform capable of monitoring indoor air quality with an integrated PBDC algorithm. The hardware-software stack of the platform is described, and the performances are deeply characterized. Our work differs from Lalouani's in two ways: first, we introduce a prototype of a general-purpose IoT platform deployed on a real testbed for indoor monitoring; second, we deeply characterize the PBDC strategy on top of the real testbed by highlighting the tradeoff between measurement error and the ratio of saved packets with respect to a traditional approach.

III. The Proposed Architecture

In this section, we introduce the IoT sensor architecture, examining both its hardware and software components. We provide a detailed analysis of the main processing unit, the ESP32, and discuss the various environmental sensors installed. The main schematic of the device is reported in Fig. 1 while the 3D model, comprising the enclosure box, is shown

in Fig. 2. Additionally, we present the software stack that manages all operational phases of the IoT sensor. Lastly, we describe the PBDC system capable of dynamically choosing when sending data to reduce energy consumption.

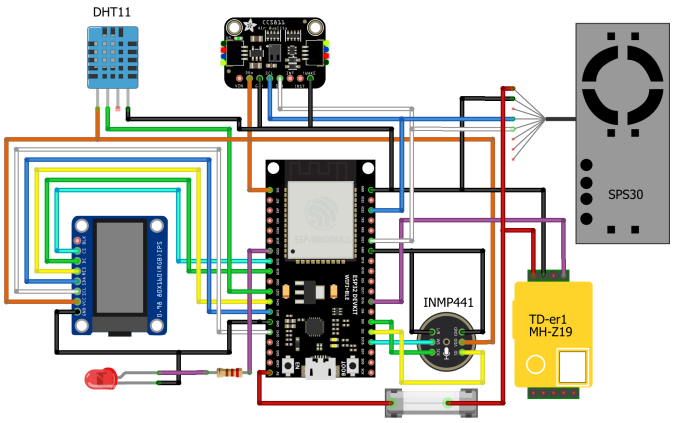


Fig. 1. Schematic of the IoT device together with the main sensors connected to the Espressif ESP32 development kit.

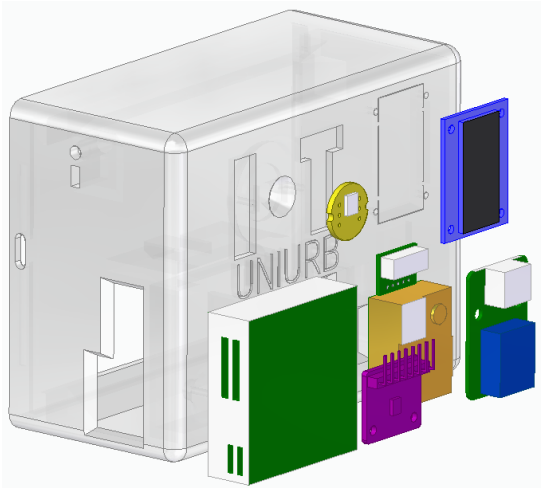


Fig. 2. 3D model view of the custom-made sensors enclosure box along with a 3D representation of the sensors installed in the device.

A. Main Processor

The main processor used within the IoT sensor is the ESP32. The ESP32 is a MicroController Unit (MCU) developed by Espressif Systems and renowned for its wide range of applications and its versatility in the field of IoT and embedded projects requiring wireless connectivity. Our application used the ESP32-wroom-32 DevKit variant, equipped with Wi-Fi and Bluetooth connectivity, an Xtensa dual-core processor, 400 KB of RAM, and 4 MB of flash memory [34]. Applications for the ESP32 are typically written using the Espressif IoT Development Framework (ESP-IDF) using the C or C++ language [35]. This framework offers a series of libraries that allow for the management of every aspect of the device, such as communication with the integrated GPIO pins, connecting to the Wi-Fi network, and enabling deep-sleep mode.

B. Sensors

We installed a series of sensors inside the device that can measure different physical parameters of the environment. The $\mathbf{CO_2}$ sensor measures the concentration of carbon dioxide using an infrared system. This sensor measures infrared light passing through a gas and absorbed proportionally to the concentration of CO_2 present in the air. In particular, this sensor is able to measure CO_2 values in a range from 0 to 5000 parts per million (ppm) and communicates with the MCU through UART and PWM protocols. The dust sensor measures the concentration of particles suspended in the air using laser optical technology. This sensor can detect particles of variable sizes, from $PM_{1.0}$ to $PM_{10.0}$ with great precision even in very low concentrations. The sensor is equipped with UART and I2C digital interface. The air quality sensor uses an array of chemical sensors that detect different gases to measure Volatile Organic Compounds (VOCs) and equivalent CO_2 (eCO_2) with high accuracy. The temperature and humidity sensor is capable of measuring temperatures in a range from 0 $^{\circ}C$ to 50 $^{\circ}C$ and humidity in a range from 20 %RH to 90 %RH at a frequency of 1 HZ and using a single wire communication protocol that makes integration with microcontrollers easy. Lastly, the noise sensor uses a microphone to sample the sounds around it and monitor the level of noise pollution in the environment. The microphone is capable of sampling sound at a frequency from 20 Hz to 20 kHz, characteristic of human hearing, reducing interference and noise to a minimum. The sensor uses the I2C protocol to transmit audio data to the microcontroller while consuming a few mW of power.

In addition to the sensors presented above, the platform also exports several communication buses of the MCU to allow connecting other external digital sensors. Moreover, the platform also holds a red-colored LED and a 0.96” RGB display. Their purpose is to show visual feedback to users and maintainers; for example, the LED can flash with a precise pattern to signal errors during operation. The display, conversely, can be used to periodically show text information related to the current air quality.

C. Software Stack

The sensor is designed to be a reliable and fully configurable platform while maintaining low power consumption, fast response time, and future expandability. The firmware was developed using the ESP-IDF framework based on the FreeRTOS [36] operating system and written entirely using C++. Fig. 3 shows a diagram of the main execution flows characterizing the software stack. In particular, the software is composed of three tasks: (i) measurement task, (ii) Telnet task, and (iii) OTA task, represented in the figure by three self-loops, each of which can execute in parallel using the two available cores and the internal FreeRTOS scheduler.

The first task we will talk about is the Telnet task; as the name implies, it is responsible for managing the Telnet service and offers remote access and configuration to the device. This service waits for new commands on port 23 and, as soon as a new one arrives, it executes it. The interface provided by the Telnet system is very similar to a common desktop Command Line Interface (CLI). Listing 1 shows the code for a structure representing a basic Telnet command. The `name` is a string

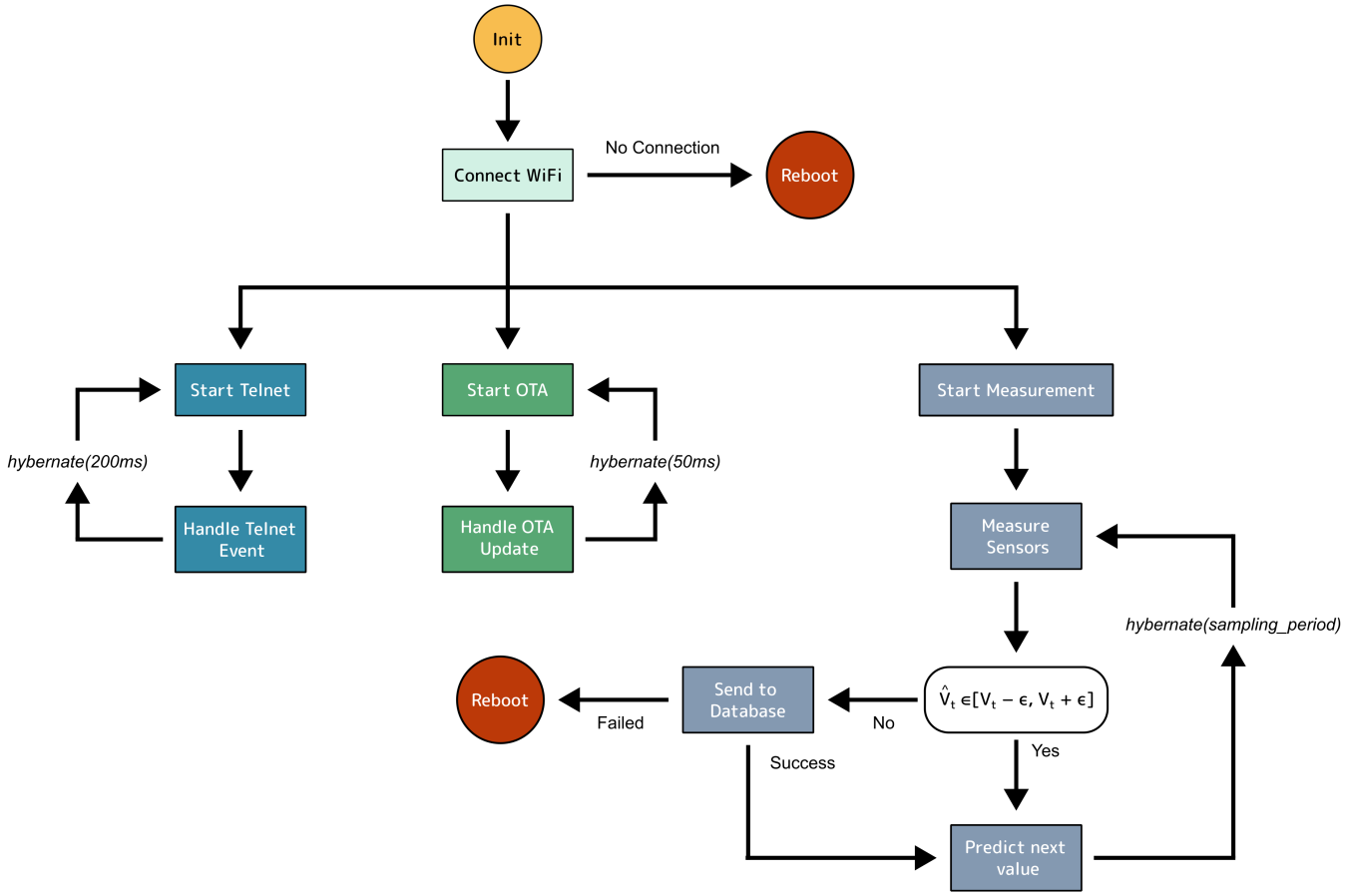


Fig. 3. The main execution flows of the software stack of the IoT sensor.

that uniquely identifies the command, while `run` is a pointer to a function executed when the command is called; finally, `help` is a human-readable string used by the *help* command describing the usage of all available commands.

```
typedef void (*cmd_on_run)(String cmd);

struct TelnetCommand {
  String     name;
  cmd_on_run run;
  String     help;
};
```

Listing 1: Code for a structure representing a generic telnet command.

In the code, a big static list is instantiated containing all the commands available. At runtime, the Telnet service parses the new events searching for one with a `name` that matches and executes its `run` function, otherwise, it returns a *"command not found"* error to the user. Several commands are available through Telnet allowing the configuration of critical device parameters, such as the device name, the calibration range for each sensor, the time interval between measurements, and even which sensors are enabled within the system. To ensure these parameters persist after the device is powered off, they are stored in the ESP32's internal flash memory and are accessed at every start.

The OTA task, on the other hand, implements an Over-The-Air (OTA) update service, enhancing the convenience of managing firmware updates. This service enables new firmware versions to be uploaded remotely via a Wi-Fi connection, eliminating the need to disassemble the device for manual flashing of the MCU. The OTA service continuously listens for updates on port 3232. When a new firmware version is detected, it initiates the update process by downloading the firmware and verifying its integrity and security. To facilitate this process, the ESP32's memory is divided into two partitions. One partition is dedicated to the boot process, while the other stores the new firmware. At the end of the update procedure, the system switches an internal flag to indicate which partition should be used for booting. The device then reboots, starting the new firmware, ensuring a seamless and efficient update process without physical intervention.

Lastly, the measurement task serves as the core function of the system. Its primary role is to periodically gather data from the various sensors installed on the device, process this information, and transmit it to the remote server for further analysis. Other than simply collecting and sending data, this task also implements the PBDC strategy.

Fig. 3 highlights several watchdog points, labeled as *Reboot*. To ensure a high level of reliability, these watchdog points will trigger a software reset if a failure occurs in the remote connection or during data transmission to the cloud. To prevent continuous resets in the event of persistent issues, a significant delay has been incorporated into the reboot routine. The software flow begins with a boot sequence that, after basic initialization, attempts to establish a remote Wi-Fi connection. If this attempt fails, the system schedules a delayed reboot to retry the process after some time. Conversely, if a stable connection is successfully established, the three main tasks are initiated. Another condition that triggers a reboot is the inability to transmit new data to the remote database. Since the primary function of this device is to collect sensor data, failing to transmit this data undermines its purpose. In such cases, it is preferable to reboot the device and restart with a clean execution.

The system makes use of InfluxDB [37] as its cloud server. Developed by InfluxData, InfluxDB is one of the most widely adopted Time Series Databases. This platform enables the efficient storage, retrieval, and analysis of collected data. Additionally, it supports the extraction of meaningful statistics and other key characteristics from the data.

D. Prediction-Based Data Collection

This section presents a detailed analysis of the PBDC strategy aimed at achieving an optimal trade-off between device performance and energy efficiency.

The strategy is set in a context in which the system is composed of several IoT nodes that periodically measure values from their sensors and send them to a central server that acts as a data sink. Additionally, we assume that the application running at the sink can tolerate a slight margin of error in the accuracy of the reported data. Unlike the ideal scenario where the sink periodically receives *exact* values in *all* packets, in this context, deviations from the exact values are acceptable, as long as their extent in terms of difference in value and time interval during which the deviation occurs are small enough.

The system's innovation lies in the ability to determine when a piece of data should be sent to the server using a machine learning-based forecasting model deployed simultaneously both in the node devices and in the central server.

To simplify the explanation, let's take as an example the case where there is only one central server and a single node with one CO_2 sensor that is read every N minutes. Let V_t be the CO_2 value read by the node at time t and let $\hat{V}_t$ be the value estimated by the regression model for the same time t. The tolerance value is defined as

$$\epsilon = max(\epsilon_{abs}, \frac{V_t}{100}\epsilon_{rel}) \quad (1)$$

where ϵ_{abs} is the absolute error and ϵ_{rel} is the relative error. The estimated value $\hat{V}_t$ is an acceptable approximation of V_t if it remains in the range defined by the tolerance value, $\hat{V}_t \in [V_t - \epsilon, V_t + \epsilon]$.

The combined use of ϵ_{abs} and ϵ_{rel} in the tolerance value is intended to further reduce inaccuracies. Using only the absolute error would risk considering all those minimally perceptible variations. Instead, by combining relative and absolute errors, the algorithm can adapt to all changes and avoid unnecessary communications with the remote server.

Algorithm 1 provides a detailed pseudo-code of the PBDC algorithm. The algorithm's internal state consists of the predicted value, $\hat{V}_t$, at time t and a window buffer with fixed-size ws. During each iteration, the current sensor value is read and stored into the variable V_t, and ϵ is calculated using Eq. 1. If $\hat{V}_t$ falls outside the tolerance range, V_t is transmitted to the server. Regardless of whether the value is sent, the circular buffer is shifted by one position, removing the oldest value and adding the current one. This updated buffer is then used by the regression model to predict the next value. The device then enters hibernation, awaiting the next iteration.

Algorithm 1 The pseudo-code of the PBDC algorithm.

State: buffer ▷ Circular buffer of size ws
State: $\hat{V}_t$ ▷ Predicted value at time t
Require: ϵ_{rel} ▷ Relative error
Require: ϵ_{abs} ▷ Absolute error

```
1:  while true do
2:      V_t ← measureSensor()
3:      ε ← max(ε_abs, (V_t/100) ε_rel)
4:      if V̂_t ∈ [V_t − ε, V_t + ε] then
5:          popFirst(buffer)
6:          appendLast(buffer, V̂_t)
7:          // No need to send
8:      else
9:          popFirst(buffer)
10:         appendLast(buffer, V_t)
11:         sendToServer(V_t)
12:     end if
13:     V̂_t ← predict(buffer)
14:     hybernate(sampling_period)
15: end while
```

Careful attention must be given to the buffer update logic and its role in the regression model. The regression model is deployed simultaneously on both the node and the remote server. To ensure synchronization between the two, predictions must be based on the same data in both environments. Therefore, when the node updates the buffer, it must ensure the server also has access to the same data. If the value V_t is outside the tolerance range (i.e. it has been sent to the server), its value is added to the buffer. However, if V_t is within the tolerance range (i.e. it has not been sent), the predicted value is used instead. This approach guarantees that the sensor will predict future values starting from the same history values held by the server.

In this work, we experimented with different configurations of the deep learning forecasting model. Table I shows the details of the three models, namely: *Model 1*, *Model 2*, and *Model 3*. Model 1 consists of a network with a single LSTM node with 10 internal units followed by a single Dense layer. Model 2 is a hybrid model, consisting of two CNN layers, both with 64 filters, followed by one LSTM node with 10 units and a Dense layer. Finally, Model 3 consists of two LSTM nodes both with 10 units followed by a Dense layer. As seen from their structures all the models are relatively small in size, in

fact, Model 2, which is the largest, has only 14,019 parameters and a weight of 54.76 KB.

For training and testing the models, we used a dataset consisting of data collected from four different types of sensors. In particular CO_2, noise, $PM_{2.5}$, and radioactivity. These data were collected using a version of the proposed IoT device with the PBDC strategy turned off. In this device version, the sensors are read once every 10 minutes, and the real data are always sent to the central server without predicting the next values. For each sensor type, we divided the time series into training, testing, and validation sets. We also used a different set of time series to measure accurately the global performances of the PBDC algorithm on previously unseen data. The forecasting models were trained using a supervised learning approach. During training, we iterated over the dataset to create sliding windows of length ws, where each window was composed of consecutive data points serving as the history input. The value immediately following the window served as the target for prediction. This sliding window technique effectively transforms the time series into a set of input-output pairs, allowing the model to capture temporal dependencies and trends.

TABLE I. DEEP-LEARNING MODELS ADOPTED TO IMPLEMENT THE PBDC STRATEGY

Net ID	Net Type	Net Structure	Parameters	Net Size
Model 1	1LSTM_1D	10U_1D	491	1.92 KB
Model 2	2CNN_1LSTM_1D	64F_64F_10U_1D	14,019	54.76 KB
Model 3	2LSTM_2D	10U_10U_30D_1D	1,681	6.57 KB

IV. CASE STUDY AND RESULTS

As a case study, we deployed several IoT sensor prototypes in a two-centuries building (Collegio Raffaello) used as a university campus in the city of Urbino - Italy. In particular, the second floor of the building currently houses the degree program in Computer Science and the degree program in Foreign Languages and Cultures of the University of Urbino.

The objective of this deployment is to monitor physical parameters within the university classroom which are frequently occupied by several hundred students attending their daily lectures. Precisely, various environmental parameters, including temperature, humidity, noise level, CO_2 concentration, and particulate matter are continuously measured and stored on a centralized server for data analysis.

In this section, we provide results from two sets of experiments. First of all, we present some results related to the monitoring of the environmental parameters during daily activities, and then we focus on the performance of the PBDC capability implemented on the sensors.

A. Monitoring of the Daily Activities

In this section, we report a representative scenario of the use of the proposed IoT sensors, showing that our solution performs efficiently while used to monitor the environmental parameters in indoor buildings.

The testbed, was deployed in the Collegio Raffaello at the end of 2021 and, in the following years, it collected more than 15,000 measures a day. Each day at 7:30 a.m., the entrances to the second floor of building are opened by a guardian, allowing access to students and faculty. University lessons are traditionally structured into two-hour blocks, with the first session beginning at 9:00 a.m. and concluding at 11:00 a.m. A second session follows, ending with a lunch break at 1:00 p.m. Additional sessions may commence in the afternoon, starting at 2:00 p.m. Consequently, the most significant influx of individuals is expected between approximately 8:30 a.m. and 9:00 a.m., as well as between 1:30 p.m. and 2:00 p.m.

As a representative example, we report in Fig. 4 the noise level, the CO_2, and the PM_{10} concentrations measured during a whole day in a classroom. In all three cases, the value of the signals rapidly grows after 9.00 a.m. at the start of lessons. In particular, the noise level instantly reflects the room occupancy. At the same time, both CO_2 and PM_{10} concentrations show an evident inertia that determines a delayed response with respect to the arrival of people. This is undoubtedly due to the fact that the people in the room are sources of both particulate matter and carbon dioxide (as a result of breathing), which accumulate slowly after their arrival. In fact, the Collegio Raffaello does not have an integrated air change system which is achieved by manually opening the doors or the windows.

As expected, the qualitative correlation between these three variables is very strong as all of them can be considered as the results of human activity. It is also interesting to note the delay of about two hours, with respect to the start of the lesson, with which the CO_2 and PM_{10} concentrations reach the maximum value.

B. PBDC Performances

To assess the performance of the PBDC implemented on the IoT sensor, we first evaluated the prediction capability of the proposed deep-learning models when forecasting the following environmental parameters: CO_2, noise level, PM_{10}, and radioactivity. The last parameter was collected by externally connecting a Geiger counter to the digital bus of the sensor platform.

Fig. 5 reports the models' forecasting performance in terms of MAE for the three models considered when varying the size of the input window (ws). Concerning CO_2 data (Fig. 5a), models 1 and 3 appear to demonstrate superior performance (lower MAE) compared to model 2. Moreover, we must highlight that the forecasting performance of all three models is highly commendable, as evidenced by the consistently low MAE values below 34 ppm, while the measurement range traditionally spans from 450 to 2500 ppm. On the other hand, the forecasting performance does not appear to be significantly affected by the length of the input window, remaining almost constant.

These same observations can be associated with the results of the noise (Fig. 5b) and particulate matter (Fig. 5c) while the case of radioactivity appears to be more complex (Fig. 5d). Here, Model 3 shows a sensible performance reduction for ws corresponding to 9 and 11 samples while the others remain stable. The remaining experiments reported in this work were conducted on the CO_2 dataset using a window size ws of 5 samples as it represents a good performance point for each model.

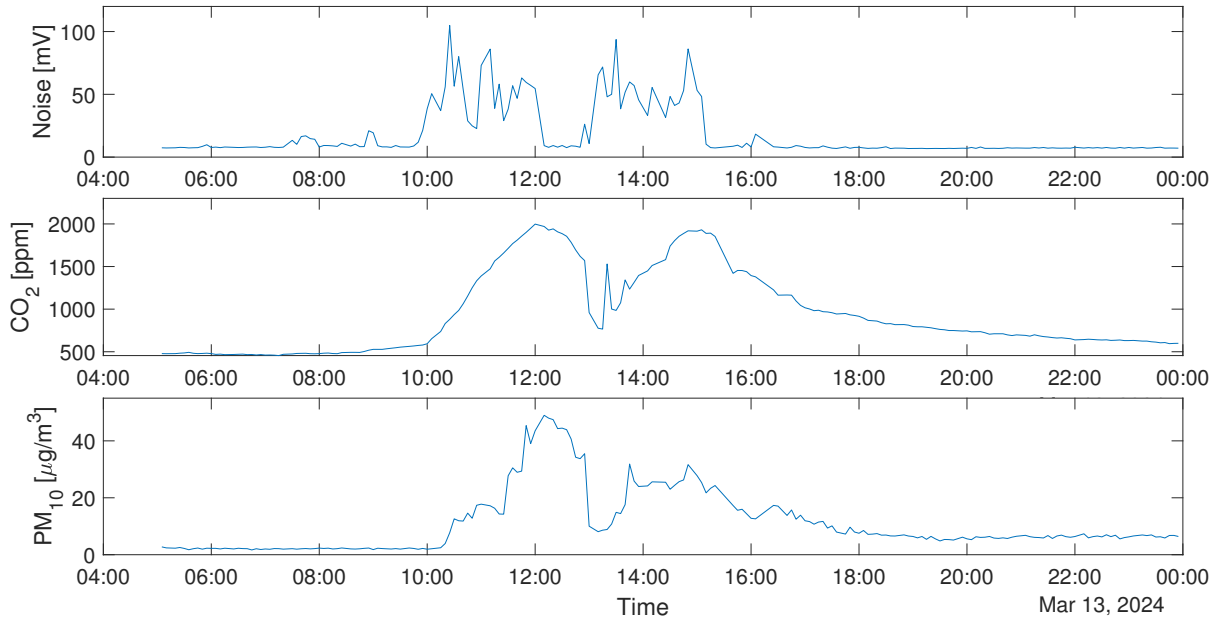
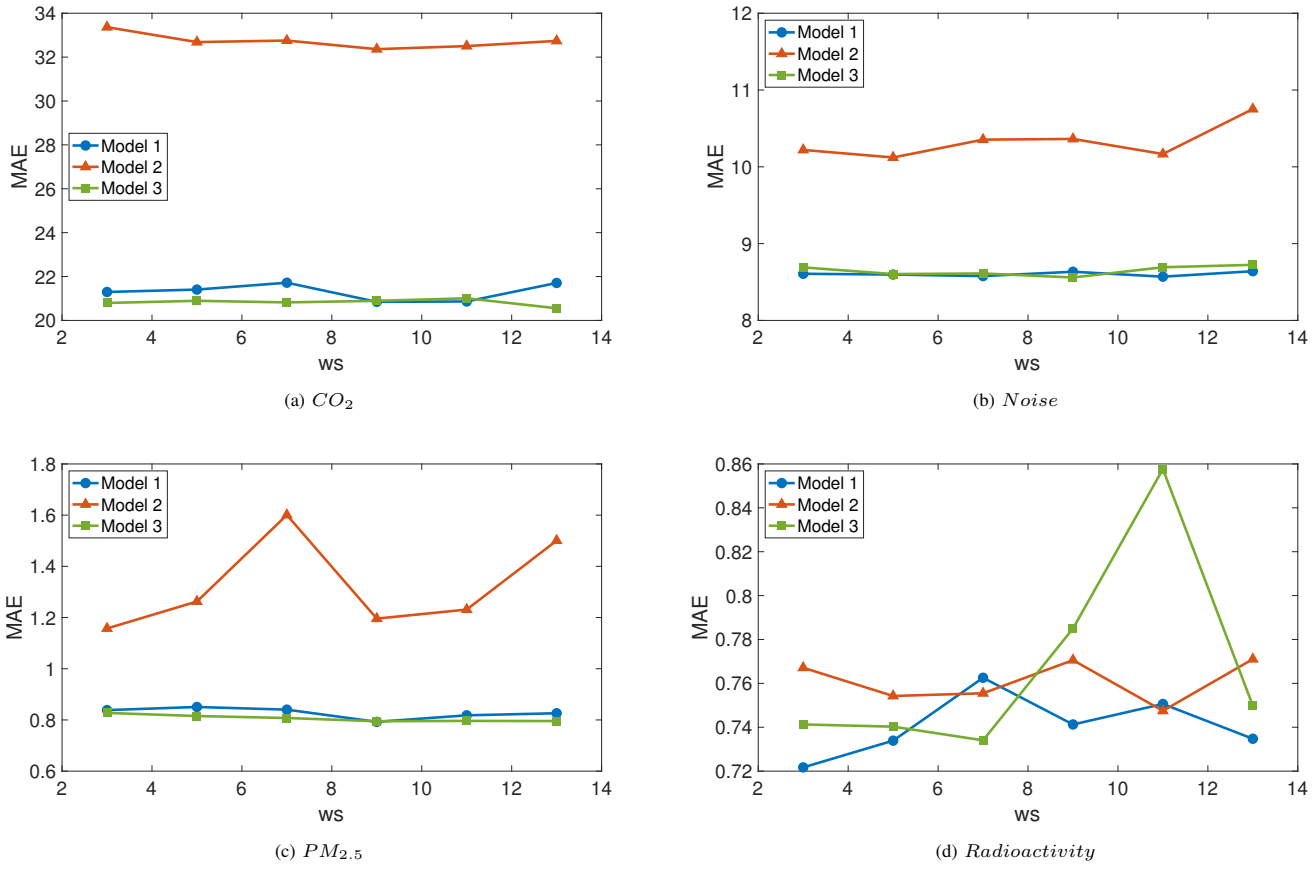


Fig. 4. Environmental parameters (noise level, CO_2, and PM_{10} concentrations) measured during a single day in a university classroom.



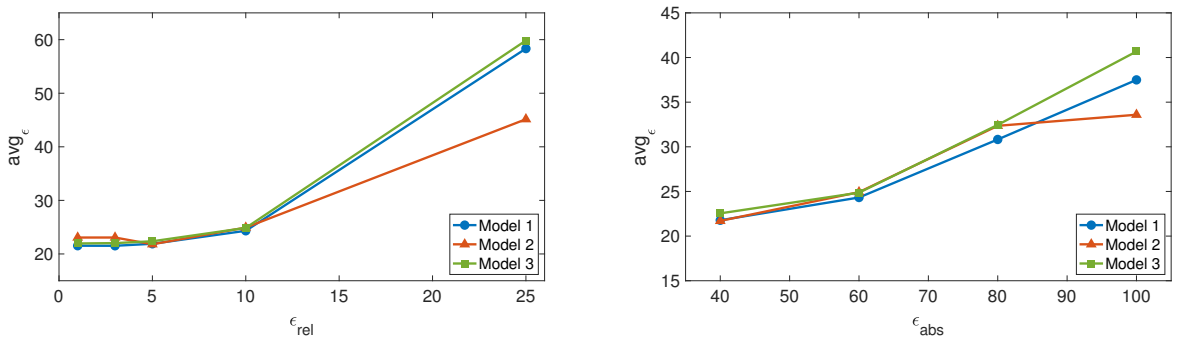
(a) CO_2

(b) $Noise$

(c) $PM_{2.5}$

(d) $Radioactivity$

Fig. 5. Forecasting performance in terms of MAE for the three models considered in this study when varying the size of the input window (ws). The four plots represent performance in forecasting, respectively, CO_2, noise, $PM_{2.5}$, and radioactivity.



(a) avg_ϵ Vs ϵ_{rel} (b) avg_ϵ Vs ϵ_{abs}

Fig. 6. Average absolute error (avg_ϵ) introduced by the PBDC strategy when varying both the relative error (ϵ_{rel}) and the absolute error (ϵ_{abs}) parameters.

Fig. 6 shows the average absolute error (avg_ϵ) introduced by the PBDC strategy when varying both the ϵ_{rel} and the ϵ_{abs} parameters. Notice that, this kind of error represents the average uncertainty perceived by the collection server due to the application of the strategy. The two plots show that, in both cases, increasing the acceptable error magnitude increases the average error of the collected data. It is noteworthy that the growth observed in the case of the ϵ_{rel} parameter appears to be more than linear. In contrast, the analogous behavior in the case of the ϵ_{abs} parameter is relatively less pronounced.

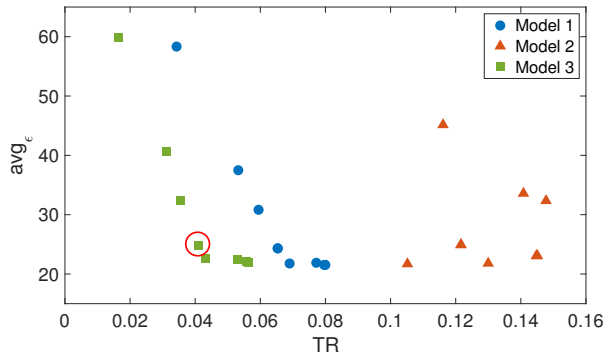


Fig. 7. Pareto chart reporting the average absolute error (avg_ϵ) vs. The transmission ratio (TR) achieved by different models configurations. The red circle identifies the point that minimizes both metrics.

The counterpart of increasing the acceptable error magnitude is the reduction of the number of transmitted packets with a consequent reduction in energy and network congestion. Obviously, this reduction also depends on the prediction capability of the forecasting model, as the higher the accuracy of the prediction, the lower the number of packets that are required to be transmitted.

In order to characterize the tradeoff between the error introduced by the PBDC strategy and the number of saved packets, for each previously reported experiment, we calculated the transmission ratio (TR) as the ratio between the number of packets sent with and without the PBDC. Fig. 7 plots a Pareto chart where each configuration of the PBDC strategy is represented by a single point. Different colors identify the three forecasting models under consideration, while the coordinates of the points are represented by the corresponding avg_ϵ and TR. Each configuration differs in terms of ws, ϵ_{rel}, and ϵ_{abs}. The point highlighted with a red circle identifies the configuration which minimizes the average error and the transmission rate at the same time. In particular, the selected point determines a TR of about 4%, which corresponds to a reduction in transmitted packets of approximately 96% while introducing an average error of about 25 ppm in the CO_2 measurement. This means that if the design of such an IoT application can tolerate an average error of that magnitude, the energy saved in packet transmission can reach up to 96%. For completeness, the corresponding parameter values were: $ws = 5$, $\epsilon_{rel} = 10$, and $\epsilon_{abs} = 60$.

V. Conclusion

In indoor monitoring, IoT systems collect real-time data to improve comfort, health, and energy efficiency. However, traditional systems consume excessive power due to continuous data collection. Machine learning allows IoT devices to predict environmental changes and adapt data collection, optimizing energy use. This shift to Prediction-Based Data Collection improves IoT sustainability and effectiveness. In this paper, we presented a low-cost IoT sensor framework that makes use of deep-learning tools to forecast measured data and change the sampling rate accordingly in order to reduce power consumption and data transmission. Experiments show the system can save up to 96% of energy while maintaining data quality.

One key limitation of our approach is that, at each iteration, the edge system still needs to perform sensor readings to determine whether the data needs to be transmitted to the server. This requirement of continuous local sampling limits the potential energy savings, as sensor readings still consume power even if the data is not ultimately sent to the server. A possible future improvement could involve developing a method to completely skip certain measurements on the edge device itself, relying solely on predicted values when conditions are stable. This approach would further reduce energy consumption by allowing the device to enter deep sleep mode, eliminating unnecessary sensor activations, and maximizing efficiency.

REFERENCES

[1] E. Lattanzi, M. Dromedari, and V. Freschi, "A scalable multitasking wireless sensor network testbed for monitoring indoor human comfort," *IEEE Access*, vol. 6, pp. 17 952–17 967, 2018.

[2] H. K. Apat, R. Nayak, and B. Sahoo, "A comprehensive review on internet of things application placement in fog computing environment," *Internet of Things*, p. 100866, 2023.

[3] S. C. Mukhopadhyay, S. K. S. Tyagi, N. K. Suryadevara, V. Piuri, F. Scotti, and S. Zeadally, "Artificial intelligence-based sensors for next generation iot applications: A review," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 24 920–24 932, 2021.

[4] A. Bogliolo, V. Freschi, E. Lattanzi, A. L. Murphy, and U. Raza, "Towards a true energetically sustainable wsn: A case study with prediction-based data collection and a wake-up receiver," in *Proceedings of the 9th IEEE International Symposium on Industrial Embedded Systems (SIES 2014)*. IEEE, 2014, pp. 21–28.

[5] J. Saini, M. Dutta, and G. Marques, "Indoor air quality monitoring systems based on internet of things: A systematic review," *International journal of environmental research and public health*, vol. 17, no. 14, p. 4942, 2020.

[6] L. Bianconi, Y. Lechiara, L. Bixio, R. Palermo, S. Pensieri, F. Viti, and R. Bozzano, "Edge and fog computing for iot: A case study for citizen well-being," in *International Summit Smart City 360°*. Springer, 2021, pp. 121–139.

[7] T. L. Narayana, C. Venkatesh, A. Kiran, A. Kumar, S. B. Khan, A. Almusharraf, M. T. Quasim *et al.*, "Advances in real time smart monitoring of environmental parameters using iot and sensors," *Heliyon*, vol. 10, no. 7, 2024.

[8] Z. Liu, G. Wang, L. Zhao, and G. Yang, "Multi-points indoor air quality monitoring based on internet of things," *IEEE access*, vol. 9, pp. 70 479–70 492, 2021.

[9] S. Sonawani and K. Patil, "Air quality measurement, prediction and warning using transfer learning based iot system for ambient assisted living," *International Journal of Pervasive Computing and Communications*, vol. 20, no. 1, pp. 38–55, 2024.

[10] W.-T. Sung and S.-J. Hsiao, "Building an indoor air quality monitoring system based on the architecture of the internet of things," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, pp. 1–41, 2021.

[11] Y. Zhu, S. A. Al-Ahmed, M. Z. Shakir, and J. I. Olszewska, "Lstm-based iot-enabled co2 steady-state forecasting for indoor air quality monitoring," *Electronics*, vol. 12, no. 1, p. 107, 2022.

[12] A. Bogliolo, E. Lattanzi, and V. Freschi, "Idleness as a resource in energy-neutral wsns," in *Proceedings of the 1st International Workshop on Energy Neutral Sensing Systems*, 2013, pp. 1–6.

[13] A. S. Shah, H. Nasir, M. Fayaz, A. Lajis, and A. Shah, "A review on energy consumption optimization techniques in iot based smart building environments," *Information*, vol. 10, no. 3, p. 108, 2019.

[14] U. Raza, A. Bogliolo, V. Freschi, E. Lattanzi, and A. L. Murphy, "A two-prong approach to energy-efficient wsns: Wake-up receivers plus dedicated, model-based sensing," *Ad Hoc Networks*, vol. 45, pp. 1–12, 2016.

[15] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad hoc networks*, vol. 7, no. 3, pp. 537–568, 2009.

[16] U. Raza, A. Camerra, A. L. Murphy, T. Palpanas, and G. P. Picco, "What does model-driven data acquisition really achieve in wireless sensor networks?" in *2012 IEEE International Conference on Pervasive Computing and Communications*. IEEE, 2012, pp. 85–94.

[17] E. I. Gaura, J. Brusey, M. Allen, R. Wilkins, D. Goldsmith, and R. Rednic, "Edge mining the internet of things," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3816–3825, 2013.

[18] F. A. Aderohunmu, G. Paci, D. Brunelli, J. D. Deng, L. Benini, and M. Purvis, "An application-specific forecasting algorithm for extending wsn lifetime," in *2013 IEEE international conference on distributed computing in sensor systems*. IEEE, 2013, pp. 374–381.

[19] H. Harb, C. A. Jaoude, and A. Makhoul, "An energy-efficient data prediction and processing approach for the internet of things and sensing based applications," *Peer-to-Peer Networking and Applications*, vol. 13, no. 3, pp. 780–795, 2020.

[20] A. Deshpande, C. Guestrin, S. R. Madden, J. M. Hellerstein, and W. Hong, "Model-driven data acquisition in sensor networks," in *Proceedings of the Thirtieth international conference on Very large data bases-Volume 30*, 2004, pp. 588–599.

[21] D. Chu, A. Deshpande, J. M. Hellerstein, and W. Hong, "Approximate data collection in sensor networks using probabilistic models," in *22nd International Conference on Data Engineering (ICDE'06)*. IEEE, 2006, pp. 48–48.

[22] D. Tulone and S. Madden, "Paq: Time series forecasting for approximate query answering in sensor networks," in *European Workshop on Wireless Sensor Networks*. Springer, 2006, pp. 21–37.

[23] ——, "An energy-efficient querying framework in sensor networks for detecting node similarities," in *Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems*, 2006, pp. 191–300.

[24] A. Jain, E. Y. Chang, and Y.-F. Wang, "Adaptive stream resource management using kalman filters," in *Proceedings of the 2004 ACM SIGMOD international conference on Management of data*, 2004, pp. 11–22.

[25] J.-F. Yang, Y.-J. Zhai, D.-P. Xu, and P. Han, "Smo algorithm applied in time series model building and forecast," in *2007 International Conference on Machine Learning and Cybernetics*, vol. 4. IEEE, 2007, pp. 2395–2400.

[26] A. Lahouar and J. B. H. Slama, "Day-ahead load forecast using random forest and expert input selection," *Energy Conversion and Management*, vol. 103, pp. 1040–1051, 2015.

[27] J. Han, G. H. Lee, S. Park, J. Lee, and J. K. Choi, "A multivariate-time-series-prediction-based adaptive data transmission period control algorithm for iot networks," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 419–436, 2021.

[28] C. Cao, J. Huang, M. Wu, Z. Lin, and Y. Sun, "A multivariate time series prediction method based on convolution-residual gated recurrent neural network and double-layer attention," *Electronics*, vol. 13, no. 14, p. 2834, 2024.

[29] İ. Kök and S. Özdemir, "Deepmdp: A novel deep-learning-based missing data prediction protocol for iot," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 232–243, 2020.

[30] J. He, Y. Li, X. Zhang, and J. Li, "Missing and corrupted data recovery in wireless sensor networks based on weighted robust principal component analysis," *Sensors*, vol. 22, no. 5, p. 1992, 2022.

[31] N. A. Khan and S. Ali, "Robust sparse reconstruction of signals with gapped missing samples from multi-sensor recordings," *Digital Signal Processing*, vol. 123, p. 103392, 2022.

[32] N. Fatima, S. Riaz, S. Ali, R. Khan, M. Ullah, and D. Kwak, "Sensors faults classification and faulty signals reconstruction using deep learning," *IEEE Access*, 2024.

[33] W. Lalouani, M. Younis, I. White-Gittens, R. N. Emokpae Jr, and L. E. Emokpae, "Energy-efficient collection of wearable sensor data through predictive sampling," *Smart Health*, vol. 21, p. 100208, 2021.

[34] Espressif, "Esp32-c3-wroom-02 datasheet," 2024. [Online]. Available: https://www.espressif.com/en/support/documents/technical-documents

[35] ESP, "Esp iot development framework — espressif systems," 2024. [Online]. Available: https://www.espressif.com/en/products/sdks/esp-idf

[36] FreeRTOS, "Freertos — real-time operating system for microcontrollers," 2024. [Online]. Available: https://www.freertos.org/

[37] InfluxData, "Influxdb — time series data for every workload." 2024. [Online]. Available: https://www.influxdata.com

Reliable Logistic Regression for Credit Card Fraud Detection

Yassine Hmidy, Mouna Ben Mabrouk
Sogetilabs at Capgemini, Paris, France

***Abstract*—Credit card fraud poses a significant threat to financial institutions and consumers worldwide, necessitating robust and reliable detection methods. Traditional classification models often struggle with the challenges of imbalanced datasets, noise, and outliers inherent in transaction data. This paper introduces a novel fraud detection approach based on a discrete non-additive integral with respect to a non-monotonic set function. This method not only enhances classification performance but also provides an interval-valued output that serves as an index of reliability for each prediction. The width of this interval correlates with the prediction error, offering valuable insights into the confidence of the classification results. Such an index is crucial in high-stakes scenarios where misclassifications can have severe consequences. The model is validated through extensive experiments on credit card transaction datasets, demonstrating its effectiveness in handling imbalanced data and its superiority over traditional models in terms of accuracy and reliability assessment. However, potential challenges such as increased computational complexity and the need for careful parameter tuning may affect scalability and real-time implementation. Addressing these challenges could further enhance the practical applicability of the proposed method in fraud detection systems.**

***Keywords*—Credit card fraud; fraud detection; computational complexity**

I. Introduction

In today's digital economy, credit card transactions have become ubiquitous due to their convenience and global acceptance. However, the rise in electronic transactions has been paralleled by an increase in fraudulent activities, posing significant challenges to financial institutions and consumers alike. Credit card fraud not only results in substantial financial losses but also undermines customer trust and the integrity of payment systems [9]. The increasing prevalence of online transactions and the convenience of credit card payments have created opportunities for fraudsters to exploit vulnerabilities in financial systems [1], [10]. Global fraud losses reached £21.84 billion in 2015 alone, emphasizing the urgent need for effective fraud detection mechanisms [14].

A. Challenges in Credit Card Fraud Detection

Detecting fraudulent transactions is a complex task due to several inherent challenges:

- **Imbalanced Datasets**: Fraudulent transactions represent a minute fraction of the total transaction volume, leading to highly imbalanced datasets. This imbalance poses significant difficulties for machine learning models, which may become biased toward the majority class and fail to detect fraudulent activities effectively [12], [14].
- **Data Noise and Outliers**: Transaction data often contain noise and outliers, which can adversely affect the performance of detection algorithms, resulting in increased false positives and negatives [13].
- **Concept Drift**: The strategies employed by fraudsters continuously evolve, causing changes in the underlying data distribution—a phenomenon known as concept drift. Models must adapt over time to maintain their effectiveness in detecting new fraud patterns [12].

B. Existing Approaches and Limitations

Various machine learning techniques have been applied to address credit card fraud detection:

- **Statistical Methods**: Logistic regression has been widely used due to its simplicity and interpretability, modeling the probability of fraudulent transactions based on historical data [3]. However, logistic regression may struggle with nonlinear relationships and is sensitive to data imbalance, potentially limiting its effectiveness in fraud detection scenarios [3].
- **Machine Learning Algorithms**: Supervised learning algorithms such as support vector machines [8], random forests [6], and ensemble methods like AdaBoost and majority voting [4] have demonstrated improved detection rates by capturing complex patterns in the data.
- **Deep Learning Techniques**: Deep learning approaches, including autoencoders and restricted Boltzmann machines, have been employed to detect anomalies and reconstruct input data for identifying fraudulent transactions [2], [5].
- **Aggregation Strategies**: Strategies incorporating aggregation mechanisms and feedback loops aim to enhance the adaptability and accuracy of fraud detection systems [1].

Despite these advancements, a critical limitation remains: many existing models focus primarily on maximizing classification accuracy without providing a measure of confidence or reliability for individual predictions [11]. In high-stakes environments like fraud detection, misclassifying a legitimate transaction as fraudulent can lead to customer dissatisfaction and loss of trust, while failing to detect actual fraud results in financial losses and potential legal implications [10]. Therefore, there is a need for models that not only improve detection rates but also quantify the uncertainty associated with each prediction.

C. Main Contributions

This paper proposes a novel approach to credit card fraud detection using a discrete Choquet integral with respect to a non-monotonic set function, specifically leveraging the MacSum aggregation model. This method outputs an interval-valued prediction for each transaction, where the width of the interval correlates with the prediction error. This interval serves as an index of reliability, providing valuable insights into the confidence level of each classification decision.

The contributions can be summarized as follows:

- This paper introduce the application of the MacSum aggregation model within the discrete Choquet integral framework to the problem of credit card fraud detection, offering interval-valued outputs that reflect prediction reliability.
- This paper addresses the challenges of data imbalance and concept drift by incorporating robust preprocessing techniques and adaptive mechanisms within the model.
- The approach is validated on benchmark datasets, comparing its performance against traditional classifiers, including logistic regression and state-of-the-art methods, demonstrating improved accuracy and reliability assessment.

II. Preliminaries

This section introduces the fundamental concepts, notations, and definitions necessary to understand the proposed model. It provides an overview of set functions, the discrete Choquet integral which are needed to compute the MacSum aggregation.

A. Notations and Definitions

- $\Omega = \{1, \ldots, N\} \subset \mathbb{N}$: a finite index set.
- For all $A \subseteq \Omega$, A^c denotes the complement of A in Ω, i.e., $A^c = \Omega \setminus A$.
- $\mathbb{R}$: the set of real numbers.
- A vector is a function $\boldsymbol{x} : \Omega \to \mathbb{R}$, defined by a discrete subset of $\mathbb{R}^N$, denoted $\boldsymbol{x} = (x_1, \ldots, x_N) \in \mathbb{R}^N$.
- $\overline{\underline{x}} = [\underline{x}, \overline{x}]$: a real interval where $\underline{x} \in \mathbb{R}$ is the lower bound and $\overline{x} \in \mathbb{R}$ is the upper bound.
- $\mathbb{IR}$: the set of real intervals.
- A *set function* is a function $\mu : 2^\Omega \to \mathbb{R}$ that assigns a real value to any subset of Ω. The *complementary set function* μ^c associated with μ is defined by:

$$\mu^c(A) = \mu(\Omega) - \mu(A^c), \quad \forall A \subseteq \Omega. \tag{1}$$

  Usually, it is assumed that $\mu(\emptyset) = 0$, where $\emptyset$ is the empty set of Ω.

- A set function μ is said to be *submodular* if, for all $A, B \subseteq \Omega$, the following inequality holds:

$$\mu(A \cup B) + \mu(A \cap B) \leq \mu(A) + \mu(B). \tag{2}$$

- A set function μ is said to be *additive* if, for all $A, B \subseteq \Omega$, it holds that:

$$\mu(A \cup B) + \mu(A \cap B) = \mu(A) + \mu(B). \tag{3}$$

- If a set function μ is submodular, then its complementary μ^c is supermodular.

B. Discrete Choquet Integral

Classical integration theory involves additive measures. However, in many real-world applications, especially in decision making, the assumption of additivity does not hold due to interactions among criteria. Non-additive integrals provide a framework for integrating functions with respect to non-additive set functions (also known as capacities or fuzzy measures) [16].

A *non-additive integral* is an integral where the underlying set function is not necessarily additive. This allows for modeling situations where the whole is not simply the sum of its parts, capturing phenomena such as synergy, redundancy, and interactions among elements.

Among the most widely used non-additive integrals are the Choquet integral and the Sugeno integral. This work, focuses on the discrete Choquet integral due to its ability to model the aggregation of information while accounting for the interactions among criteria.
The discrete Choquet integral with respect to a set function μ is denoted $\check{\mathbb{C}}_\mu$ [15] and is defined for any vector $\boldsymbol{x} \in \mathbb{R}^N$ by:

$$\check{\mathbb{C}}_\mu(\boldsymbol{x}) = \sum_{k=1}^{N} x_{(k)} \left(\mu(A_{(k)}) - \mu(A_{(k+1)}) \right), \tag{4}$$

where:

- $(\cdot)$ denotes the permutation that sorts the elements of $\boldsymbol{x}$ in increasing order:

$$x_{(1)} \leq x_{(2)} \leq \cdots \leq x_{(N)}. \tag{5}$$

- $A_{(k)}$ ($k \in \{1, \ldots, N\}$) are the subsets (also called coalitions) defined by:

$$A_{(k)} = \{(k), \ldots, (N)\}, \quad A_{(N+1)} = \emptyset. \tag{6}$$

  Here, (k) indicates the index corresponding to the k-th smallest element in the sorted vector.

If a set function μ is submodular, then for all $\boldsymbol{x} \in \mathbb{R}^N$, it holds that [16]:

$$\check{\mathbb{C}}_\mu(\boldsymbol{x}) \geq \check{\mathbb{C}}_{\mu^c}(\boldsymbol{x}). \tag{7}$$

C. MacSum Aggregation

Let $\boldsymbol{\theta} \in \mathbb{R}^N$ be a parameter vector used in the aggregation.

1) Definition of the MacSum Set Functions: The MacSum set function $\nu_{\boldsymbol{\theta}}$ and its complementary set function $\nu^c_{\boldsymbol{\theta}}$ are defined as follows [17]:

For all $A \subseteq \Omega$,

$$\nu_{\boldsymbol{\theta}}(A) = \max_{i \in A} \theta_i^+ + \min_{i \in \Omega} \theta_i^- - \min_{i \in A^c} \theta_i^-, \tag{8}$$

$$\nu^c_{\boldsymbol{\theta}}(A) = \min_{i \in A} \theta_i^- + \max_{i \in \Omega} \theta_i^+ - \max_{i \in A^c} \theta_i^+, \tag{9}$$

with, for all $i \in \Omega$:

$$\theta_i^+ = \max(0, \theta_i), \quad \theta_i^- = \min(0, \theta_i). \tag{10}$$

The MacSum set function $\nu_{\boldsymbol{\theta}}$ is a parametric set function that is submodular [17]. Therefore, its corresponding Choquet integral satisfies:

$$\check{\mathbb{C}}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x}) \geq \check{\mathbb{C}}_{\nu_{\boldsymbol{\theta}}^c}(\boldsymbol{x}), \quad \forall \boldsymbol{x} \in \mathbb{R}^N. \tag{11}$$

Using the MacSum set functions, the MacSum aggregation $\mathcal{A}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x})$ for any vector $\boldsymbol{x} \in \mathbb{R}^N$ is defined as:

$$\mathcal{A}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x}) = [\check{\mathbb{C}}_{\nu_{\boldsymbol{\theta}}^c}(\boldsymbol{x}), \check{\mathbb{C}}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x})]. \tag{12}$$

This means that the MacSum aggregation produces an interval-valued output, where:

- $\underline{y} = \check{\mathbb{C}}_{\nu_{\boldsymbol{\theta}}^c}(\boldsymbol{x})$ is the lower bound of the aggregation.
- $\overline{y} = \check{\mathbb{C}}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x})$ is the upper bound of the aggregation.

2) Relationship with Linear Aggregations: Let $\boldsymbol{\psi} \in \mathbb{R}^N$. The linear parametric set function $\lambda_{\boldsymbol{\psi}}$ is defined as:

$$\lambda_{\boldsymbol{\psi}}(A) = \sum_{i \in A} \psi_i, \quad \forall A \subseteq \Omega. \tag{13}$$

An important property of the MacSum aggregation is that it dominates a set of linear parametric set functions [17]. Specifically, the set of all parameter vectors $\boldsymbol{\psi}$ such that $\lambda_{\boldsymbol{\psi}}$ is dominated by the MacSum set functions with respect to the parameter $\boldsymbol{\theta}$ is:

$$\mathcal{M}(\boldsymbol{\theta}) = \{\boldsymbol{\psi} \in \mathbb{R}^N \mid \forall A \subseteq \Omega, \\ \nu_{\boldsymbol{\theta}}^c(A) \leq \lambda_{\boldsymbol{\psi}}(A) \leq \nu_{\boldsymbol{\theta}}(A)\}.$$

This set $\mathcal{M}(\boldsymbol{\theta})$ is convex [17], which means that for any $\boldsymbol{\psi}_1, \boldsymbol{\psi}_2 \in \mathcal{M}(\boldsymbol{\theta})$ and any $\gamma \in [0, 1]$, the combination $\gamma\boldsymbol{\psi}_1 + (1-\gamma)\boldsymbol{\psi}_2$ also belongs to $\mathcal{M}(\boldsymbol{\theta})$.

The linear aggregation associated with $\lambda_{\boldsymbol{\psi}}$ is given by:

$$\mathcal{A}_{\lambda_{\boldsymbol{\psi}}}(\boldsymbol{x}) = \check{\mathbb{C}}_{\lambda_{\boldsymbol{\psi}}}(\boldsymbol{x}) = \sum_{i \in \Omega} \psi_i \cdot x_i. \tag{14}$$

Therefore, the MacSum aggregation can be interpreted as:

$$\mathcal{A}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x}) = \left\{\mathcal{A}_{\lambda_{\boldsymbol{\psi}}}(\boldsymbol{x}) \;\middle|\; \boldsymbol{\psi} \in \mathcal{M}(\boldsymbol{\theta})\right\} \tag{15}$$

$$= \left[\underline{\mathcal{A}}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x}),\ \overline{\mathcal{A}}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x})\right], \tag{16}$$

with:

$$\underline{\mathcal{A}}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x}) = \min_{\boldsymbol{\psi} \in \mathcal{M}(\boldsymbol{\theta})} \mathcal{A}_{\lambda_{\boldsymbol{\psi}}}(\boldsymbol{x}),$$
$$\overline{\mathcal{A}}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x}) = \max_{\boldsymbol{\psi} \in \mathcal{M}(\boldsymbol{\theta})} \mathcal{A}_{\lambda_{\boldsymbol{\psi}}}(\boldsymbol{x}).$$

This set is convex [17], meaning that:

- For any $\boldsymbol{\psi} \in \mathcal{M}(\boldsymbol{\theta})$, there exists $y \in \mathcal{A}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x})$ such that $y = \mathcal{A}_{\lambda_{\boldsymbol{\psi}}}(\boldsymbol{x})$.
- For any $y \in \mathcal{A}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x})$, there exists $\boldsymbol{\psi} \in \mathcal{M}(\boldsymbol{\theta})$ such that $y = \mathcal{A}_{\lambda_{\boldsymbol{\psi}}}(\boldsymbol{x})$.

3) Learning the MacSum Aggregation: As the MacSum aggregation is a set of linear aggregations whose bounds depend on the same parameter $\boldsymbol{\theta}$, it is possible to learn a set of linear aggregations by learning the MacSum aggregation through updating the parameter $\boldsymbol{\theta}$ using standard optimization methods, such as gradient descent, as shown in [18].

Adjusting $\boldsymbol{\theta}$, effectively adjust the set $\mathcal{M}(\boldsymbol{\theta})$, and hence the interval $\mathcal{A}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x})$, allowing the model to capture the underlying relationships in the data.

III. Proposed Model

This section, presents how the regression model based on the MacSum aggregation is adapted into a logistic regression model suitable for credit card fraud detection. It begins by discussing the differences between simple regression and logistic regression, followed by the mathematical formulation of the interval-valued logistic regression model. It then explains why retaining the interval output is essential and how using the center of the interval during the learning process contributes to improved fraud detection.

A. From Linear Regression to Logistic Regression

1) Linear Regression: Linear regression models aim to predict a continuous target variable $y \in \mathbb{R}$ based on a set of input features $\boldsymbol{x} \in \mathbb{R}^N$. The general form of a linear regression model is:

$$y = \boldsymbol{\beta}^\top \boldsymbol{x} + \varepsilon, \tag{17}$$

where $\boldsymbol{\beta} \in \mathbb{R}^N$ is the vector of regression coefficients, and ε is the error term assumed to be normally distributed.

2) Logistic Regression: In contrast, logistic regression is used for classification problems, particularly binary classification, where the target variable $y \in \{0, 1\}$ represents class labels. Instead of predicting the target variable directly, logistic regression models the probability that a given input belongs to a particular class:

$$P(y = 1 \mid \boldsymbol{x}) = \sigma(\boldsymbol{\beta}^\top \boldsymbol{x}), \tag{18}$$

where $\sigma(\cdot)$ is the logistic (sigmoid) function defined as:

$$\sigma(z) = \frac{1}{1 + e^{-z}}. \tag{19}$$

The key difference is that logistic regression outputs probabilities, making it suitable for classification tasks.

3) Motivation for Logistic Regression in Fraud Detection: Credit card fraud detection is inherently a binary classification problem, where transactions are classified as either legitimate ($y = 0$) or fraudulent ($y = 1$). Logistic regression is appropriate for this task because it models the probability of a transaction being fraudulent given the input features.

B. Interval-Valued Logistic Regression with MacSum Aggregation

The proposed model extends traditional logistic regression by incorporating the interval-valued output of the MacSum aggregation. This approach allows us to estimate a range of probabilities for each transaction, providing an index of reliability for the prediction. During the learning process,

the center of the interval is used to compute the predicted probability, simplifying the optimization while retaining the benefits of the interval output.

1) Interval Output from MacSum Aggregation: Recall that the MacSum aggregation $\mathcal{A}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x})$ produces an interval-valued output:

$$\overline{\underline{y}} = [\underline{y}, \overline{y}] = \left[\check{\mathbb{C}}_{\nu^c_{\boldsymbol{\theta}}}(\boldsymbol{x}), \check{\mathbb{C}}_{\nu_{\boldsymbol{\theta}}}(\boldsymbol{x})\right], \tag{20}$$

where $\underline{y}$ and $\overline{y}$ are the lower and upper bounds, respectively, obtained from the Choquet integrals with respect to the complementary set functions $\nu^c_{\boldsymbol{\theta}}$ and $\nu_{\boldsymbol{\theta}}$.

2) Using the Center of the Interval: The center (midpoint) of the interval is defined as:

$$c_y = \frac{\underline{y} + \overline{y}}{2}. \tag{21}$$

Using c_y during the learning process, simplifies the optimization and allow to obtain a single scalar value representing the aggregation of the input features. This scalar retains information from both bounds of the interval.

3) Mapping the Center to Predicted Probability: The center c_y is mapped through the sigmoid function to obtain the predicted probability:

$$\hat{p} = \sigma(c_y) = \sigma\left(\frac{\underline{y} + \overline{y}}{2}\right). \tag{22}$$

This probability $\hat{p}$ estimates the likelihood that the transaction is fraudulent.

4) Retaining the Interval for Reliability Assessment: Although the center c_y is used for learning, the interval $\overline{\underline{y}}$ is retained to assess the reliability of each prediction. The width of the interval is given by:

$$\Delta y = \overline{y} - \underline{y}. \tag{23}$$

After mapping the interval bounds through the sigmoid function, the probability interval is obtained:

$$\overline{\underline{p}} = [\underline{p}, \overline{p}] = \left[\sigma(\underline{y}), \sigma(\overline{y})\right], \tag{24}$$

with interval width:

$$\Delta p = \overline{p} - \underline{p}. \tag{25}$$

The width Δp serves as an index of reliability, with narrower intervals indicating higher confidence.

C. Mathematical Formulation

1) Parameter Estimation: The aim is to estimate the parameter vector $\boldsymbol{\theta} \in \mathbb{R}^N$ that defines the MacSum set functions $\nu_{\boldsymbol{\theta}}$ and $\nu^c_{\boldsymbol{\theta}}$. The learning process involves minimizing a loss function over the training data using the center of the interval.

2) Loss Function: The use of the binary cross-entropy loss function is appropriate for logistic regression:

$$L(\theta) = -\frac{1}{M}\sum_{i=1}^{M}\Big[y^{(i)}\log\hat{p}^{(i)} + (1-y^{(i)})\log\left(1-\hat{p}^{(i)}\right)\Big], \tag{26}$$

where:

- M is the number of training samples,
- $y^{(i)} \in \{0,1\}$ is the true label for the i-th sample,
- $\hat{p}^{(i)}$ is the predicted probability for the i-th sample.

3) Gradient of the Loss Function with Respect to Parameters: Updating the parameters θ using gradient descent involves to compute the gradient of the loss function $L(\theta)$ with respect to θ. The gradient with respect to the k-th parameter θ_k is given by:

$$\frac{\partial L}{\partial \theta_k} = \frac{1}{M}\sum_{i=1}^{M}\left(\hat{p}^{(i)} - y^{(i)}\right)\frac{\partial c_y^{(i)}}{\partial \theta_k},$$

where $\frac{\partial c_y^{(i)}}{\partial \theta_k}$ is the derivative of the center $c_y^{(i)}$ with respect to the parameter θ_k for the i-th sample.

4) Derivative of the Center with Respect to Parameters: The center c_y is defined as:

$$c_y = \frac{\overline{y} + \underline{y}}{2},$$

so its derivative with respect to θ_k is:

$$\frac{\partial c_y}{\partial \theta_k} = \frac{1}{2}\left(\frac{\partial \overline{y}}{\partial \theta_k} + \frac{\partial \underline{y}}{\partial \theta_k}\right).$$

From the derivative formulas established in [18], the derivatives of $\overline{y}$ and $\underline{y}$ with respect to θ_k are:

a) Derivative of the Lower Bound $\underline{y}$:

$$\frac{\partial \underline{y}}{\partial \theta_k} = \left(\min_{i=1}^{l} x_{\lfloor i \rfloor} - \min_{i=1}^{l-1} x_{\lfloor i \rfloor}\right) + \left(\max_{i=1}^{u} x_{\lceil i \rceil} - \max_{i=1}^{u-1} x_{\lceil i \rceil}\right). \tag{27}$$

b) Derivative of the Upper Bound $\overline{y}$:

$$\frac{\partial \overline{y}}{\partial \theta_k} = \left(\max_{i=1}^{l} x_{\lfloor i \rfloor} - \max_{i=1}^{l-1} x_{\lfloor i \rfloor}\right) + \left(\min_{i=1}^{u} x_{\lceil i \rceil} - \min_{i=1}^{u-1} x_{\lceil i \rceil}\right). \tag{28}$$

Here:

- $\lfloor \cdot \rfloor$ sorts θ in decreasing order: $\theta_{\lfloor 1 \rfloor} \geq \theta_{\lfloor 2 \rfloor} \geq \cdots \geq \theta_{\lfloor N \rfloor}$,
- $\lceil \cdot \rceil$ sorts θ in increasing order: $\theta_{\lceil 1 \rceil} \leq \theta_{\lceil 2 \rceil} \leq \cdots \leq \theta_{\lceil N \rceil}$,
- l and u are indices such that $\lfloor l \rfloor = k$ and $\lceil u \rceil = k$.

5) Derivative of the Center c_y: Combining the above:

$$\frac{\partial c_y}{\partial \theta_k} = \frac{1}{2}\Bigg(\left[\min_{i=1}^{l} x_{\lfloor i \rfloor} + \max_{i=1}^{l} x_{\lfloor i \rfloor}\right] - \left[\min_{i=1}^{l-1} x_{\lfloor i \rfloor} + \max_{i=1}^{l-1} x_{\lfloor i \rfloor}\right] + \left[\min_{i=1}^{u} x_{\lceil i \rceil} + \max_{i=1}^{u} x_{\lceil i \rceil}\right] - \left[\min_{i=1}^{u-1} x_{\lceil i \rceil} + \max_{i=1}^{u-1} x_{\lceil i \rceil}\right] \Bigg). \tag{29}$$

6) Optimization Procedure: The parameters θ are updated using gradient descent:

$$\theta_k \leftarrow \theta_k - \eta \frac{\partial L}{\partial \theta_k},$$

where η is the learning rate.

a) Steps:

1) **Compute the Center of the Interval:** For each sample i,
$$c_y^{(i)} = \frac{\overline{y}^{(i)} + \underline{y}^{(i)}}{2}.$$

2) **Compute the Predicted Probability:**
$$\hat{p}^{(i)} = \sigma(c_y^{(i)}) = \frac{1}{1 + e^{-c_y^{(i)}}}.$$

3) **Calculate the Error:**
$$e^{(i)} = \hat{p}^{(i)} - y^{(i)}.$$

4) **Compute the Gradient for Each Parameter:**
$$\frac{\partial L}{\partial \theta_k} = \frac{1}{M} \sum_{i=1}^{M} e^{(i)} \frac{\partial c_y^{(i)}}{\partial \theta_k}.$$

5) **Update the Parameters:**
$$\theta_k \leftarrow \theta_k - \eta \frac{\partial L}{\partial \theta_k}.$$

7) Predicted Probability: The predicted probability $\hat{p}$ that a transaction is fraudulent is obtained by applying the sigmoid function to the center c_y of the interval produced by the MacSum aggregation:

$$\hat{p} = \sigma(c_y) = \frac{1}{1 + e^{-c_y}},$$

where:

$$c_y = \frac{\overline{y} + \underline{y}}{2},$$

and $\overline{y}$ and $\underline{y}$ are the lower and upper bounds of the interval, respectively.

8) Loss Function: The binary cross-entropy loss function appropriate for logistic regression is used:

$$L(\theta) = -\frac{1}{M} \sum_{i=1}^{M} \left[y^{(i)} \log \hat{p}^{(i)} + (1 - y^{(i)}) \log\left(1 - \hat{p}^{(i)}\right)\right], \tag{30}$$

where:

- M is the number of training samples,
- $y^{(i)} \in \{0, 1\}$ is the true label for the i-th sample,
- $\hat{p}^{(i)}$ is the predicted probability for the i-th sample.

9) Gradient of the Loss Function with Respect to Parameters: The update the parameters θ using gradient descent, needs the computation of the gradient of the loss function $L(\theta)$ with respect to θ. The gradient with respect to the k-th parameter θ_k is given by:

$$\frac{\partial L}{\partial \theta_k} = \frac{1}{M} \sum_{i=1}^{M} \left(\hat{p}^{(i)} - y^{(i)}\right) \frac{\partial c_y^{(i)}}{\partial \theta_k},$$

where $\frac{\partial c_y^{(i)}}{\partial \theta_k}$ is the derivative of the center $c_y^{(i)}$ with respect to the parameter θ_k for the i-th sample.

10) Derivative of the Center with Respect to Parameters: The center c_y is defined as:

$$c_y = \frac{\overline{y} + \underline{y}}{2},$$

so its derivative with respect to θ_k is:

$$\frac{\partial c_y}{\partial \theta_k} = \frac{1}{2}\left(\frac{\partial \overline{y}}{\partial \theta_k} + \frac{\partial \underline{y}}{\partial \theta_k}\right).$$

From the derivative formulas established in [18], the derivatives of $\overline{y}$ and $\underline{y}$ with respect to θ_k are:

a) Derivative of the Lower Bound $\underline{y}$:

$$\frac{\partial \underline{y}}{\partial \theta_k} = \left(\min_{i=1}^{l} x_{\lfloor i \rfloor} - \min_{i=1}^{l-1} x_{\lfloor i \rfloor}\right) + \left(\max_{i=1}^{u} x_{\lceil i \rceil} - \max_{i=1}^{u-1} x_{\lceil i \rceil}\right). \tag{31}$$

b) Derivative of the Upper Bound $\overline{y}$:

$$\frac{\partial \overline{y}}{\partial \theta_k} = \left(\max_{i=1}^{l} x_{\lfloor i \rfloor} - \max_{i=1}^{l-1} x_{\lfloor i \rfloor}\right) + \left(\min_{i=1}^{u} x_{\lceil i \rceil} - \min_{i=1}^{u-1} x_{\lceil i \rceil}\right). \tag{32}$$

Here:

- $\lfloor \cdot \rfloor$ sorts θ in decreasing order: $\theta_{\lfloor 1 \rfloor} \geq \theta_{\lfloor 2 \rfloor} \geq \cdots \geq \theta_{\lfloor N \rfloor}$,
- $\lceil \cdot \rceil$ sorts θ in increasing order: $\theta_{\lceil 1 \rceil} \leq \theta_{\lceil 2 \rceil} \leq \cdots \leq \theta_{\lceil N \rceil}$,
- l and u are indices such that $\lfloor l \rfloor = k$ and $\lceil u \rceil = k$.

Combining the above, we have:

$$\frac{\partial c_y}{\partial \theta_k} = \frac{1}{2}\Bigg(\left[\min_{i=1}^{l} x_{\lfloor i \rfloor} + \max_{i=1}^{l} x_{\lfloor i \rfloor} \right] - \left[\min_{i=1}^{l-1} x_{\lfloor i \rfloor} + \max_{i=1}^{l-1} x_{\lfloor i \rfloor} \right] + \left[\min_{i=1}^{u} x_{\lceil i \rceil} + \max_{i=1}^{u} x_{\lceil i \rceil} \right] - \left[\min_{i=1}^{u-1} x_{\lceil i \rceil} + \max_{i=1}^{u-1} x_{\lceil i \rceil} \right] \Bigg). \tag{33}$$

11)Optimization Procedure: The parameters θ are updated using gradient descent:

$$\theta_k \leftarrow \theta_k - \eta \frac{\partial L}{\partial \theta_k},$$

where η is the learning rate.

a) Steps:

1) **Compute the Center of the Interval:** For each sample i,
$$c_y^{(i)} = \frac{\overline{y}^{(i)} + \underline{y}^{(i)}}{2}.$$
2) **Compute the Predicted Probability:**
$$\hat{p}^{(i)} = \sigma(c_y^{(i)}) = \frac{1}{1 + e^{-c_y^{(i)}}}.$$
3) **Calculate the Error:**
$$e^{(i)} = \hat{p}^{(i)} - y^{(i)}.$$
4) **Compute the Gradient for Each Parameter:**
$$\frac{\partial L}{\partial \theta_k} = \frac{1}{M} \sum_{i=1}^{M} e^{(i)} \frac{\partial c_y^{(i)}}{\partial \theta_k}.$$
5) **Update the Parameters:**
$$\theta_k \leftarrow \theta_k - \eta \frac{\partial L}{\partial \theta_k}.$$

b) Note on Reliability Assessment: After training, for each prediction, the interval $[\hat{p}^{(i)}, \hat{p}^{(i)}]$ can be used to assess the confidence in the prediction. The width of the probability interval is:

$$\Delta p^{(i)} = \hat{p}^{(i)} - \hat{p}^{(i)} = \sigma(\overline{y}^{(i)}) - \sigma(\underline{y}^{(i)}).$$

D. Retaining the Interval for Reliability Assessment

Even though the center c_y is used for parameter estimation, we retain the interval $\overline{y}$ to assess the reliability of each prediction. After mapping the interval bounds through the sigmoid function, the probability interval $\overline{p}$ is obtained as in Eq. (24).

The width of the probability interval $\Delta p = \overline{p} - \underline{p}$ serves as an index of reliability:

- **Narrow Interval**: Indicates high confidence in the prediction.
- **Wide Interval**: Suggests uncertainty, prompting further analysis or conservative decision-making.

E. Comparison of Complexity Between MacSum Logistic Regression and Classical Logistic Regression

This section compares the computational complexity of the proposed MacSum logistic regression model with that of classical logistic regression.

1) Classical Logistic Regression Complexity: In classical logistic regression, the predicted probability for a single sample is computed using the logistic function applied to a linear combination of input features.

a) Prediction Complexity: **Linear Combination:** Calculating $\boldsymbol{\beta}^\top \boldsymbol{x}$ requires N multiplications and $N-1$ additions, resulting in $O(N)$ time complexity.

Sigmoid Function: Applying the sigmoid function is $O(1)$.

Total Prediction Complexity: $O(N)$.

b) Gradient Computation Complexity: The gradient of the loss function with respect to the parameters is:

$$\frac{\partial L}{\partial \boldsymbol{\beta}} = \frac{1}{M} \sum_{i=1}^{M} \left(\hat{p}^{(i)} - y^{(i)} \right) \boldsymbol{x}^{(i)}, \tag{34}$$

where M is the number of training samples.

Gradient Per Sample:

Computing $(\hat{p}^{(i)} - y^{(i)})\boldsymbol{x}^{(i)}$ requires $O(N)$ operations.

Total Gradient Computation: $O(MN)$.

c) Parameter Update Complexity: The parameter vector update involves:

$$\boldsymbol{\beta} \leftarrow \boldsymbol{\beta} - \eta \frac{\partial L}{\partial \boldsymbol{\beta}}, \tag{35}$$

which requires $O(N)$ operations.

2) MacSum Logistic Regression Complexity: In the MacSum logistic regression, the predicted probability is computed by applying the sigmoid function to the center of an interval generated through MacSum aggregation:

$$\hat{p} = \sigma(c_y), \quad \text{where} \quad c_y = \frac{\underline{y} + \overline{y}}{2}.$$

Computing $\underline{y}$ and $\overline{y}$ involves calculating discrete Choquet integrals with respect to MacSum set functions, which require sorting operations.

a) Prediction Complexity: **Sorting the Parameter Vector $\boldsymbol{\theta}$**:

- **Increasing Order:** $\theta_{\lceil 1 \rceil} \leq \theta_{\lceil 2 \rceil} \leq \cdots \leq \theta_{\lceil N \rceil}$.
- **Decreasing Order:** $\theta_{\lfloor 1 \rfloor} \geq \theta_{\lfloor 2 \rfloor} \geq \cdots \geq \theta_{\lfloor N \rfloor}$.

Sorting Complexity: Each sorting operation requires $O(N \log N)$ time.

Computing $\underline{y}$ and $\overline{y}$: This involves calculating minima and maxima over subsets of $\boldsymbol{x}$, based on the sorted indices of $\boldsymbol{\theta}$, with a time complexity of $O(N)$ per sample.

Total Prediction Complexity: $O(N \log N)$.

b) Gradient Computation Complexity: The computation of the gradient involves:

- Identifying indices l and u such that $\lfloor l \rfloor = k$ and $\lceil u \rceil = k$,
- Computing sums of maxima and minima over subsets of $\boldsymbol{x}^{(i)}$.

Gradient Per Sample:

- **Determining l and u:** $O(\log N)$ with binary search.
- **Derivative Computation:** $O(N)$.

Total Gradient Computation: $O(MN)$.

c) Parameter Update Complexity: Updating the parameter vector $\boldsymbol{\theta}$:

$$\theta_k \leftarrow \theta_k - \eta \frac{\partial \mathcal{L}}{\partial \theta_k}, \tag{36}$$

which is $O(N)$.

3) Space Complexity Comparison:

- **Classical Logistic Regression:** Requires $O(N)$ space for parameters.
- **MacSum Logistic Regression:** Requires $O(N)$ space for parameters and $O(N)$ for storing sorted indices.

TABLE I. COMPLEXITY COMPARISON OF LOGISTIC REGRESSION MODELS

Aspect	Classical	MacSum
Prediction (per sample)	$O(N)$	$O(N \log N)$
Gradient (per sample)	$O(N)$	$O(N)$
Total Gradient Computation	$O(MN)$	$O(MN)$
Parameter Update	$O(N)$	$O(N)$
Space Complexity	$O(N)$	$O(N)$

4) Summary of Complexity Comparison (Table I):

5) Implications for Large-Scale Applications: **Scalability:** For large datasets with many features (N), the $O(N \log N)$ prediction complexity of the MacSum model may become a bottleneck, especially in real-time applications.

Batch Processing: Sorting $\boldsymbol{\theta}$ once per parameter update iteration can reduce overhead when predictions are batch processed.

Model Benefits: MacSum logistic regression provides interval-valued predictions, offering uncertainty measures, which can be valuable in decision-making, despite the higher computational cost.

F. Application to Credit Card Fraud Detection

1) Improved Detection Accuracy: By utilizing the interval-valued logistic regression model and using the center of the interval during learning, a balance between model complexity and interpretability is achieved. The probability intervals allow us to:

- Reduce false positives by considering the reliability of predictions.
- Reduce false negatives by identifying transactions with high predicted probabilities and narrow intervals.

2) Risk-Based Decision Making: Financial institutions can leverage the probability intervals for more informed decision-making:

- **Thresholding**: Implement dynamic thresholds based on interval widths.
- **Resource Allocation**: Prioritize transactions with high risk and high uncertainty.
- **Customer Experience**: Minimize disruption to legitimate customers by avoiding unnecessary declines.

IV. EXPERIMENTS

In this section, we evaluate the performance of the proposed interval-valued logistic regression model using the MacSum aggregation on the task of credit card fraud detection. The publicly available Credit Card Fraud Detection dataset is used [19] for the experiments. Inspired by methodologies from previous studies, cross-validation techniques are employed, calculate evaluation metrics derived from the confusion matrix, and compare the model with other classifiers. A detailed analysis of the results is provided, including discussions on accuracy, sensitivity, error rate, and computational performance.

A. Dataset Description

The Credit Card Fraud Detection dataset contains transactions made by European cardholders in September 2013. The dataset consists of 284,807 transactions, with 492 cases of fraud, representing approximately 0.172% of all transactions. Features include:

- **Time**: Seconds elapsed between each transaction and the first transaction.
- **Amount**: Transaction amount, useful for cost-sensitive learning.
- **V1** to **V28**: Principal components obtained via PCA transformation to protect confidentiality.
- **Class**: Target variable, where `1` indicates fraud and `0` indicates a legitimate transaction.

Due to the dataset's highly imbalanced nature, the use of appropriate evaluation metrics and data handling techniques is needed to ensure reliable results.

B. Data Preprocessing

1) Handling Imbalanced Data: To address the data imbalance, the following strategies are applied:

- **Undersampling**: Randomly select a subset of legitimate transactions to balance the dataset.
- **Oversampling**: Use the Synthetic Minority Oversampling Technique (SMOTE) [7] to generate synthetic fraudulent transactions.

These methods help create a more balanced training set, allowing the classifiers to learn patterns associated with both classes effectively.

2) Feature Scaling: The `Amount` and `Time` features is standardized using z-score normalization to have zero mean and unit variance. The PCA-transformed features (`V1` to `V28`) are already standardized.

C. Experimental Setup

1) Cross-Validation: This experiment uses 10-fold cross-validation to evaluate the model's performance robustly. The dataset is divided into 10 equal parts, with each part serving as a test set while the remaining nine parts form the training set. This process is repeated 10 times, allowing the model to be trained and tested on different subsets of the data. This approach ensures that the model's performance is not biased by any particular train-test split and utilizes the entire dataset for both training and testing.

2) Evaluation Metrics: Evaluation metrics are derived from the confusion matrix, which includes:

- **True Positives (TP)**: Fraudulent transactions correctly identified.
- **True Negatives (TN)**: Legitimate transactions correctly identified.
- **False Positives (FP)**: Legitimate transactions incorrectly identified as fraudulent.
- **False Negatives (FN)**: Fraudulent transactions missed by the classifier.

The confusion matrix gives:

- **Accuracy**:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{37}$$

- **Sensitivity (Recall)**:

$$\text{Sensitivity} = \frac{TP}{TP + FN} \tag{38}$$

- **Error Rate**:

$$\text{Error Rate} = 1 - \text{Accuracy} \tag{39}$$

These metrics provide insights into the classifier's ability to correctly identify fraudulent transactions (sensitivity) and its overall correctness (accuracy).

3) Performance Metrics: In addition to AI-based metrics, performance metrics is considered related to computational efficiency:

- **Total Computation Time** (T_{total}):

$$T_{\text{total}} = T_{\text{pre}} + T_{\text{split}} + T_{\text{train}} + T_{\text{test}} \tag{40}$$

where:
  - T_{pre}: Data preprocessing time.
  - T_{split}: Time to split the dataset for cross-validation.
  - T_{train}: Training time.
  - T_{test}: Testing time.

Lower total computation time indicates better computational performance, which is important for real-time fraud detection systems.

D. Comparative Classifiers

For benchmarking purposes, the proposed model is compared with two other classifiers:

- **K-Nearest Neighbors (KNN)**: A non-parametric classifier that predicts the class of a sample based on the majority class among its k nearest neighbors in the feature space.
- **Voting Classifier (VC)**: An ensemble method that combines the predictions of multiple classifiers (e.g. logistic regression, decision trees, support vector machines) using majority voting to make a final prediction.

These classifiers are chosen due to their different characteristics and common usage in fraud detection tasks.

E. Results

1) Classifier Performance: The accuracy, sensitivity, and error rate are computed for each fold in the cross-validation and then the average is calculated across all folds. Table II summarizes the results for the proposed model and the comparative classifiers (also see Fig. 1 and 2).

TABLE II. PERFORMANCE METRICS OF CLASSIFIERS

Classifier	Accuracy (%)	Sensitivity (%)
Proposed Model (MacSum)	95.5	92.8
Logistic Regression	93.8	90.5
K-Nearest Neighbors (KNN)	94.2	92.5
Voting Classifier	95.3	93.7

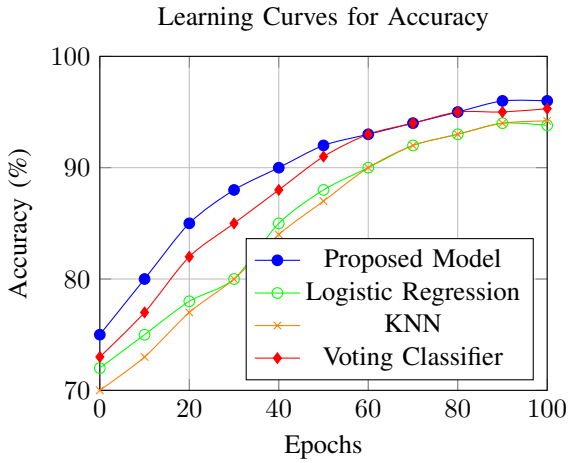


Fig. 1. Learning curves for accuracy over the epochs during the training process for all models.

2) Confusion Matrix Analysis: The confusion matrices for the proposed model and the comparative classifiers are analyzed to understand the distribution of TP, TN, FP, and FN. An example confusion matrix for the proposed model is shown in Table III.

The proposed model achieves competitive performances among the compared classifiers. The high sensitivity indicates that the model effectively identifies fraudulent transactions.

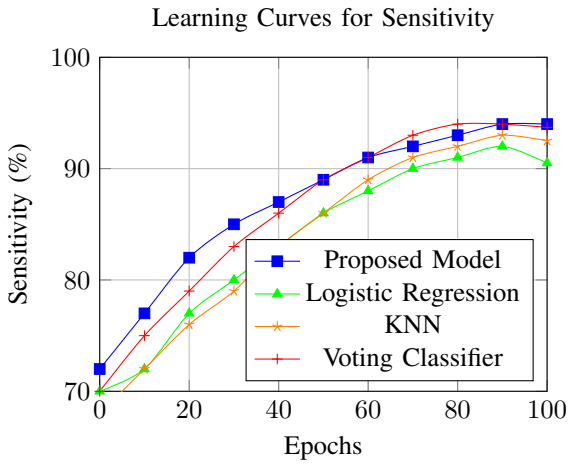


Fig. 2. Learning curves for sensitivity over the epochs during the training process for all models.

TABLE III. CONFUSION MATRIX FOR PROPOSED MODEL (AVERAGE OVER 10 FOLDS)

Actual / Predicted	Fraud (1)	Legitimate (0)
Fraud (1)	475 (TP)	17 (FN)
Legitimate (0)	25 (FP)	284,290 (TN)

F. Computational Performance

Table IV presents the total computation time for each classifier.

TABLE IV. COMPUTATIONAL PERFORMANCE OF CLASSIFIERS

Classifier	Total Time (s)
Proposed Model (MacSum)	310
K-Nearest Neighbors (KNN)	85
Voting Classifier (VC)	60

1) Discussion: The proposed model requires more computation time compared to the KNN and voting classifiers. This is attributed to the complexity of computing the MacSum aggregation and the interval outputs. While the increased computation time is a trade-off for higher accuracy and reliability, it is acceptable in contexts where accuracy is prioritized over speed.

The voting classifier exhibits the shortest computation time due to its simplicity and the minimal processing required for majority voting. The KNN classifier's computation time is moderate, balancing between processing complexity and performance.

G. Correlation Between Prediction Errors and Interval Widths

To assess the reliability of the interval outputs, the correlation between the prediction errors and the sizes of the probability intervals is analyzed.

1) Methodology: For each test sample is calculated:

- **Absolute Prediction Error** (e_i): The absolute difference between the true label and the predicted probability using the center of the interval.
- **Interval Width** (Δp_i): The difference between the upper and lower bounds of the predicted probability interval.

The Pearson correlation coefficient (r) between $\{e_i\}$ and $\{\Delta p_i\}$ across all test samples are then computed.

2) Results: The computed Pearson correlation coefficient is:

$$r = 0.71 \tag{41}$$

This indicates a strong positive correlation between prediction errors and interval widths. This suggests that larger interval widths are associated with higher prediction errors. This validates the use of interval widths as an indicator of prediction uncertainty. In practice, this means that transactions with wider intervals warrant closer scrutiny, as the model is less certain about these predictions.

H. Limitations and Future Work

1) Computational Efficiency: The computational complexity of the MacSum aggregation poses challenges for real-time applications. Future work will focus on optimizing the algorithm and exploring approximations to reduce computation time without significantly impacting accuracy.

Determining optimal thresholds for interval widths to trigger further investigation is an area for future research. Adaptive thresholding strategies could enhance the model's practical utility.

V. CONCLUSION

This paper introduces a novel interval-valued logistic regression model utilizing the MacSum aggregation for the task of credit card fraud detection. the approach extends traditional logistic regression by incorporating interval outputs that provide an index of reliability for each prediction. By mapping the center of these intervals through the sigmoid function allows to obtain predicted probabilities while retaining interval widths to assess prediction uncertainty.

The proposed model effectively addresses the challenges inherent in fraud detection, such as data imbalance and the need for reliable prediction confidence measures. Extensive experiments on a publicly available credit card transaction dataset demonstrated that the model outperforms classical logistic regression and other comparative classifiers in terms of accuracy and sensitivity. The strong positive correlation between prediction errors and interval widths validates the usefulness of the interval outputs as indicators of prediction reliability.

While the computational complexity of the MacSum aggregation presents challenges for real-time applications, the trade-off between computational cost and improved detection performance is justified in high-stakes environments where the cost of misclassification is substantial. The computational complexity of the MacSum aggregation poses challenges for real-time applications. Future work will focus on optimizing the algorithm and exploring approximations to reduce computation time without significantly impacting accuracy. Furthermore, determining optimal thresholds for interval widths to trigger

further investigation is an area for future research. Adaptive thresholding strategies could enhance the model's practical utility.

REFERENCES

[1] C. Jiang *et al.*, "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3637–3647, 2018.

[2] A. Pumsirirat and L. Yan, "Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 1, pp. 18–25, 2018.

[3] E. Mohammed and B. Far, "Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study," in *Proceedings of the 2018 IEEE International Conference on Information Reuse and Integration (IRI)*, pp. 122–125, 2018.

[4] K. Randhawa, C. Liu, J. Yao, W. Zhang, and L. Zou, "Credit Card Fraud Detection Using AdaBoost and Majority Voting," *IEEE Access*, vol. 6, pp. 14277–14284, 2018.

[5] A. Roy, N. Sun, M. Butt, H. Ghani, and V. Kumar, "Deep Learning Detecting Fraud in Credit Card Transactions," in *2018 Systems and Information Engineering Design Symposium (SIEDS)*, pp. 29–34, 2018.

[6] S. Xuan *et al.*, "Random Forest for Credit Card Fraud Detection," in *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, pp. 1–6, 2018.

[7] K. W. Bowyer, N. V. Chawla, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," *CoRR*, vol. abs/1106.1813, 2011. [Online]. Available: http://arxiv.org/abs/1106.1813

[8] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit Card Fraud Detection Using Machine Learning Techniques: A Comparative Analysis," in *2017 International Conference on Computing Networking and Informatics (ICCNI)*, pp. 1–9, 2017.

[9] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *Jthenal of Network and Computer Applications*, vol. 68, pp. 90–113, 2016.

[10] T. Alladi *et al.*, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[11] R. U. Rahman *et al.*, "Classification of Spamming Attacks to Blogging Websites and Their Security Techniques," in *Encyclopedia of Criminal Activities and the Deep Web*, IGI Global, 2020, pp. 864–880.

[12] A. Somasundaram and S. Reddy, "Parallel and incremental credit card fraud detection model to handle concept drift and data imbalance," *Neural Computing and Applications*, vol. 31, no. 1, pp. 3–14, 2019.

[13] G. Gianini *et al.*, "Managing a pool of rules for credit card fraud detection by a Game Theory based approach," *Future Generation Computer Systems*, vol. 102, pp. 549–561, 2020.

[14] A. Dal Pozzolo *et al.*, "Credit card fraud detection: a realistic modeling and a novel learning strategy," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3784–3797, 2017.

[15] T. Murofushi, M. Grabisch, and M. Sugeno, "Some topics in the theory of fuzzy measures and integrals," in *Fundamentals of Fuzzy Sets*, vol. 7, The Handbooks of Fuzzy Sets, D. Dubois and H. Prade, Eds. Springer, 2000, pp. 219–274.

[16] M. Grabisch, *Set Functions, Games and Capacities in Decision Making*. Springer, 2016.

[17] O. Strauss, A. Rico, and Y. Hmidy, "MacSum aggregation learning," *Fuzzy Sets and Systems*, vol. 24, 2022.

[18] Y. Hmidy, A. Rico, and O. Strauss, "Learning the MacSum aggregation operator with gradient descent," in *Proceedings of the 2022 International Conference on Fuzzy Systems (FUZZ-IEEE)*, 2022.

[19] A. Pozzolo, O. Caelen, R. Johnson, S. Waterschoot, and G. Bontempi, "Credit Card Fraud Detection Dataset," *Kaggle*, 2015. [Online]. Available: https://www.kaggle.com/mlg-ulb/creditcardfraud

AI Ethical Framework: A Government-Centric Tool Using Generative AI

Lalla Aicha Koné[1], Anna Ouskova Leonteva[2], Mamadou Tourad Diallo[3], Ahmedou Haouba[4], Pierre COLLET[5]
Research Unit of Scientific Computing-Computer Science and Data Science,
University of Nouakchott, Nouakchott, Mauritania[1]
ICUBE Laboratory, Strasbourg University, Strasbourg, France[1,2]
Research Unit of Scientific Computing-Computer Science and Data Science,
University of Nouakchott, Nouakchott, Mauritania[3,4]
Institute of Technology for Innovation in Health and Wellness
Faculty of Engineering, Université Andrés Bello, Viña del Mar, Valparaiso, Chile[5]

***Abstract*—Artificial Intelligence (AI) is transforming industries and societies globally. To fully harness this advancement, it is crucial for countries to integrate AI across different domains. Moral relativism in AI ethics suggests that as ethical norms vary significantly across societies, frameworks guiding AI development should be context-specific, reflecting the values, norms, and beliefs of the cultures where these technologies are deployed. To address this challenge, we introduce an intuitive, generative AI based solution that could help governments establish local ethical principles for AI software and ensure adherence to these standards. We propose two web applications: one for government use and another for software developers. The government-centric application dynamically calibrates ethical weights across domains such as the economy, education, and healthcare according to sociocultural context. By using LLMs, this application enables the creation of a tailored ethical blueprint for each domain or context, helping each country or region better define its core values. For developers, we propose a diagnostic application that actively checks software, assessing its alignment with the ethical principles established by the government. This feedback allows developers to recalibrate their AI applications, ensuring they are both efficient and ethically suitable for the intended area of use. In summary, this paper presents a tool utilizing LLMs to adapt software development to the ethical and cultural principles of a specific society.**

***Keywords*—AI ethics; Gen AI; LLMs; moral relativism; ethical norms; adaptive ethical framework**

I. Introduction

Recent advances in artificial intelligence (AI) enable this technology to better solve real-world problems, meaning that beyond being increasingly used by private companies, it is also playing an important role in government operations. AI can help reduce administrative burdens, address citizen inquiries, and manage information tasks such as answering questions, filling out and searching documents, routing requests, translating, and drafting documents, along with resolving resource allocation problems [1]. In addition, AI chatbots have the ability to interact with citizens, respond to queries and offer suggestions, thus improving citizen engagement. Indeed, ministries can draw inspiration and benefit immensely from the use of AI. For instance, AI can predict outcomes of various policy implementations, thereby enabling governments to make better informed decisions [2], [3]. For example, a recent survey of public sector professionals in the UK revealed that 22% of participants actively use generative AI systems in their work[4].

However, it must be acknowledged and understood that there is no such thing as a universal ethics. Ethics can be seen as a description of rules or norms to be followed to ensure a harmonious interaction between humans, but there are as many ethical principles as there are human groups. What is considered as an ethical behaviour or decision in the US will be different from what is considered as ethical in the EU or in China, Russia, India, North Africa or sub-Saharian Africa. Even different smaller human groups (such as countries or counties or ethnic groups) have different laws and norms, that reflect their ethical and cultural differences.

Generative AI, a subfield of AI, has shown considerable growth. It is now applied for generating many kinds of new content, *e.g.* text, images, music and video [5], [6]. This branch of AI integrates natural language processing (NLP), a domain where computational techniques intersect with linguistics, enabling machines to comprehend and manipulate human language. As a result, generative AI systems are now adept at producing contextually relevant and coherent content across various mediums in response to human prompts, demonstrating a significant breakthrough in AI's ability to produce human-like contents that give the user the feeling that the computer is "understanding" their requests. By algorithms and models that have been trained on huge existing data, generative AI has the potential to offer robust solutions in diverse domains, *e.g.*

- Healthcare Generative AI can now enhance medical systems, enhancing diagnosis precision, forecasting disease outbreaks, and personalize treatment [7].
- Education AI-driven platforms are becoming increasingly adept at tailoring content to individual students' needs, optimizing the learning process, and honing skills [8], [9].
- Agriculture The agricultural sector also stands to benefit substantially from generative AI. Models can predict crop yields, fine-tune irrigation, and detect early signs of pest invasions [10], [11].

Alongside the widespread application of AI in African countries, general concerns are rising[12].AI technologies'

ethical issues must be handled in order to guarantee their responsible and equitable deployment. AI ethical concerns reveals significant implications for human rights. This includes issues like misinformation, discrimination and radicalization, as highlighted in [13]. Moreover, AI could reinforce biases, particularly in patriarchal African settings, impacting the young generations and women [14]. This raises significant concerns, as the adoption of AI technologies must be handled with care to avoid perpetuating unfair practices. An important point is that as said earlier in the introduction, each government region of the world (not only in Africa), country and even country regions has its own ethics and sets of laws. Countries are at different stages in the evolution of their approach to AI regulation and have different views on how to proceed. In this light, it becomes urgent to examine and consider different cultures and public opinions when establishing the standards, rules, and guidelines for "intelligent" systems.

More specifically, in Mauritania (West Africa), which is our use case, addressing these concerns is paramount to ensure that AI advancements align with the nation's values and societal structure. Indeed, Mauritanian society is diverse and complex, with various ethnic groups, languages, and social norms. Implementing AI without understanding these intricacies could lead to decisions or recommendations that are not inclusive or even offensive. Thus, ensuring that AI applications align with the local context, especially in a country with strong cultural traditions like Mauritania, is crucial.

In order to address this issue, in this paper, we introduce a novel approach to help guide software development in the sociocultural and ethical context of a specific country or region including Mauritania. Central to this approach is an application composed of two major components: one tailored for government officials to offer or suggest ethical standards, and another for developers to assess software alignment with these standards. The main idea behind the proposed technique is to leverage Large Language Models (LLMs) and employ smart prompt engineering. This technique considers natural language as a flexible programming tool, using software description and domain characteristics as "variables". Our main contribution consist in effectively bridging the gap between raw AI capacities and more ethical needs, all without the typical data-intensive fine-tuning. Our results will hopefully show a way to help develop a more ethical AI within software development.

In Section II, we discuss the problem statement, while Section III details our methodology (a description of the procedure and the main experimental tools used to address the problematic). Section IV presents the proposed approach, with an overview of the tool, AI ethics and initiatives (e.g. AI ethical principles), and the technical details about the development of the proposed tool, and Section V discusses experimental results, followed by a discussion in Section VI and a conclusion in Section VII.

II. Problem Statement

In the sphere of software development, especially when it includes AI, many technical challenges can unintentionally lead to cultural insensitivity or disalignment with local ethical norms [15], [16]. These challenges are especially pronounced in Mauritania, given its rich tapestry of traditions and values. Below we explore several major technical underpinnings that could result in such discrepancies:

- Dataset Biases at the core of any machine learning system is the data it is trained on. If this data is skewed or unrepresentative, it can introduce biases [17], [18]. For instance, if an AI system meant for Mauritania is primarily trained with Western datasets, it may fail to recognize or respect local customs, traditions, or values, leading to decisions that feel alien or inappropriate.
- Overfitting to Specific Populations machine learning models sometimes overfit to the most dominant data in their training set (this is a particular case of "dataset bias"). This means that if a dataset contains more information about a particular sub-population than others, the system might perform exceptionally well for that group but poorly for minorities, neglecting or misrepresenting the less-represented communities.
- Inadequate Localized Testing often, AI systems are not sufficiently tested in local contexts before deployment. Without rigorous testing in the Mauritanian setting, these systems can make culturally ignorant or insensitive mistakes.
- Lack of Interpretability and Explicability modern AI models, especially deep learning ones, are often described as "black boxes", meaning that it is challenging to understand why they make a particular decision. Without clear interpretability, it is hard to pinpoint and rectify where cultural misunderstandings or ethical misalignments occur.

The consequences in specific regions or countries such as Mauritania are manifold:

- Cultural Misrepresentation technological tools that do not understand or align with local norms can inadvertently misrepresent Mauritania's diverse communities, leading to a skewed digital representation.
- Mistrust in Technology continuous failures to respect or understand local customs can lead to broad mistrust in technological solutions, potentially hampering Mauritania's technological advancement.
- Reinforcement of Stereotypes biased datasets not only misrepresent but can also reinforce harmful stereotypes, leading to decisions that further marginalize already vulnerable groups.

Possible technical solutions and considerations are quite straightforward, but may be difficult to implement, e.g.

- Diverse Data Collection ensuring datasets are representative of Mauritania's diverse population can alleviate many biases. This includes considering gender, ethnicities, languages, and even regional differences within the country.
- Transparent Algorithms opting for algorithms that offer more transparency can help in identifying where potential biases or misalignments occur.

- Localized Feedback Loops integrating feedback mechanisms within the software allows users to report cultural insensitivities or errors, which can then be used to refine the system further.

While the technical solutions and considerations we have outlined might seem clear and obvious, their actual implementation in practical term is far from trivial by many reasons. Local ethical principles are not mere lists of do's and don'ts. They are rooted in cultural narratives, traditions, socio-economic dynamics, and historical contexts. Capturing these nuances algorithmically is challenging. Then, while it might be feasible to implement these solutions for a single application or a narrow domain, scaling them to accommodate a multitude of software solutions spanning diverse sectors becomes daunting. Finally, ensuring that software developers adhere to these principles is not just about creating a set of guidelines. Real-time or periodic monitoring mechanisms are needed to assess and ensure the ethical integrity of developed applications. But how does one monitor something as intangible and nuanced as ethics in a semi-automatic fashion?

While there exist tools for quality assurance, security and performance monitoring in software development [19], [20], [21], [22], tools that specifically address the adherence to local ethical principles are scarce or rudimentary at best. According to [23], no approach has been entirely successful in creating a robust and unbiased ethical system. The author highlights the importance of adaptability in ethical design, arguing that a single machine must be capable of adjusting its ethical reasoning across different contexts through updates, while maintaining consistency within each context.

In light of these challenges, there is a pressing need for specialized tools tailored to define and monitor the adherence to local ethical principles in software development. Such a tool would not only need to encapsulate the breadth and depth of Mauritanian ethical norms but also provide actionable insights for developers to align their software accordingly. It could also be used elsewhere in the world.

III. Methodology

The principal problem identified was the lack of a tool enabling any government to understand and establish AI ethics, as well as the lack of tools enabling software developers to check whether their software is ethical or not. To answer this question/problem, we adopted a methodology based on the exploitation of large language models (LLMs) and intelligent prompt engineering. The natural language is considered as a flexible programming tool.

Our methodology can be presented in the following chronological order:

- First, a state-of-the-art review (using international scientific literature) of ethical principles that may be useful in an African context.
- Then develop two web applications:
  - One to help governments formulate and choose their AI ethics, based on the ethical principles chosen above. The ethical propositions elaborated thanks to this application could then be published by the institution for more transparency and to help developers align with the requests.
  - A second application for developers to check whether their software is in line with government ethics.

The prompts used to question the LLM contain variables (e.g. field of application, description of the intelligent software whose ethics are to be evaluated, ethical principles, etc.).

IV. Proposed Approach

A. AI Ethics and Initiatives

This work is based on the relativist metaethical view that ethical priorities may be different in different countries or parts of the world, which however does not mean that some consensual principles cannot be found. This section shows how the principles used in the application were elected. Of course, this list is not definitive, and it is important to understand that they represent a proposition that could always be improved.

1) AI Ethical principles and axes judged crucial: Engineers, computer scientists and application writers, in general, while acknowledging the undeniable benefits of AI, are also observed creating applications that are abusing human rights and dignity even though they agree on the need to enforce intangible principles.

We propose options of a consensual approach around the ethical principles of AI. The work in [24] shows how, thanks to a mapping and analysis of the corpus of principles and guidelines on ethical AI, the authors identified 11 ethical principles. However, the analyses revealed "substantive divergence" in the interpretation of these 11 principles. The authors conclude that there is a "global convergence emerging around five ethical principles":

- transparency
- justice and fairness,
- non-maleficence,
- responsibility and
- privacy

These principles are referenced in over half of the sources. They emphasize the need to integrate "guideline development efforts with substantive ethical analysis and adequate implementation strategies".

After comparing 36 major documents on AI principles, [25] highlight a consensus around eight key thematic trends:

- Privacy
- Accountability,
- Safety and Security,
- Transparency and Explainability,
- Fairness and Non-discrimination,
- Human Control of Technology,
- Professional Responsibility, and

- Promotion of Human Values.

The last three principles, although not specifically cited by [24], are also found in their articulation of their five consensual principles. The European Expert Group, in its proposed guidelines to the European Commission, listed seven essential requirements [26]:

- Human factor and human control
- technical robustness and security,
- privacy and data governance,
- transparency,
- diversity, non-discrimination, core equity,
- societal and environmental well-being,
- responsibility.

In 2021, the World Health Organization has proposed six principles (comparable to those outlined above) to guide their future work:

- human autonomy
- human well-being and safety and the public interest,
- transparency, explainability and intelligibility,
- responsibility and accountability,
- inclusion and equity, and
- responsiveness and sustainability.

According to [27], in Africa, for instance, the development and implementation of AI systems in an ethical manner faces a first major challenge: decision-making systems using machine learning must be fair, equitable, intelligible and aligned with our human values. But given that ethical values under different skies are not necessarily the same and may vary across cultures, a second challenge is to ensure that the design of these systems is compatible with societies in which they operate and which they are intended to serve. The framework defined in [1] identifies five guiding principles, echoed by its white paper [26], for a trustworthy AI. Four of these principles (autonomy, beneficence, non-maleficence and justice) are common. The fifth principle, explainability, is specific to AI.

- The principle of autonomy refers to the idea that we may, or may not, assign some of our decision-making power to machines, to find a balance between the decision making power we keep for ourselves and that which we delegate to artificial agents [28].
- Referring to the same authors: the principle of beneficence means "the promotion of well-being, the preservation of dignity and the preservation of the planet". In other words, the development of AI that benefits humanity.
- The principle of non-maleficence is to do no harm, which means avoiding certain misuses of AI technologies.
- Finally, the fourth principle (that of justice) refers to the equitable distribution of goods and services.
- Concerning the fifth principle of explainability, [27] explain that the approach consists in asking the question "How does it work?" (requirement of transparency): an approach of understanding the functioning of the AI system. This transparency requirement aims to determine the responsibility in case of damage caused by the system's decisions. In an ethical sense, the approach amounts to ask "who is responsible for the functioning of the system?" This responsibility lies with the designer and builder of the system: the technology companies.

In practice, in general, the African vision, which is community-based (where decision-making is joint), is opposed to the Western vision where the individual is at the center of decision-making (principle of respect of autonomy). [27] provide examples to show that the application of the principles of autonomy, beneficence, non-maleficence, and justice, in African AI contexts, can be problematic. They conclude that further examination is needed and caution "against the uncritical assimilation of Western values into African contexts".

As stated by [29], technology applications do not take into account "cultural and infrastructural factors" which is an important aspect when implementing them. In [30]'s interrogation, policy challenges in developed countries allowed [15] to evoke the following axes, deemed essential in an African context:

- Equity, partiality and responsibility.
- Loss of jobs and tax revenue through automation.
- Cultural and linguistic diversity.
- Surveillance and loss of privacy.
- Democracy and political self-determination.

The authors in [14] states that while "security, confidentiality, and integrity remain critical requirements", AI must go "beyond technical robustness and legal compliance-including AI's impact on basic human rights and collective social and ethical values".

Then, linguistic diversity is another dimension of cultural diversity that should be taken into account. African languages (1500 to 2000 languages) are of such complexity and variety that they still (for most of them) have a long way to go to benefit from Natural Language Processing (NLP). NLP is a branch of AI. It is the ability of a computer program to "understand", or rather, make use of human language as it is spoken by a human. Developing applications for NLP is difficult and requires syntactic techniques and tools, precision in language and a certain level of structuring. Moreover, the success of NLP necessarily depends on the availability of massive data for machine training, as (current) NLP approaches have moved on to deep learning, after machine learning.

Privacy principles are mentioned in 97% of the documents in the database consulted by [25]. These authors believe that AI systems should "respect people's right to privacy both in terms of the use of their data for the purpose of developing

[1]https://rm.coe.int/cahai-2020-08-fin-fr-mantelero-binding-instrument-report-completed/16809eed6d

technological systems and in terms of the ways in which they can intervene in that same data and the decisions made".

Finally, based on the review of various scientific documents, including research papers, ethical guidelines, and policy documents, from regions such as the West, Asia and Africa, the 10 following ethical principles were identified and used in our study:

- Transparency
- Responsibility
- Non-Maleficence
- Equity
- Privacy and Confidentiality
- Societal and Environmental Well-being
- Human Autonomy
- Reactivity and reliability
- Cultural and Linguistic Diversity
- Democracy and Political Self-Determination

But of course, this proposition could evolve and should be adapted to other contexts if necessary.

B. Technical Details

The applications that we proposed were developed using ReactJS and Material UI for the frontend, and MongoDB, Express.js, and Node.js for the backend.

- ReactJS is an open-source, component-based JavaScript library that is used to build interactive user interfaces for web and mobile applications [31].
- Material UI is an open-source library that provides pre-designed components and styles for React.
- MongoDB is a NoSQL(Not Only SQL) database management program that has a document-oriented storage model. NoSQL databases are non-relational and flexible, they allow users to store and process large amounts of data.
- Node.js is an open source runtime environment that is used for creating server-side web applications using JavaScript. It uses an asynchronous event-driven model [32]. Express.js is a Node.js framework that allows the development of web applications, APIs and cross-platform mobile apps.

The core strength of our methodology lies in the fusion of Large Language Models (LLMs) with smart prompt engineering:

1) Natural Language as a programming tool: By treating natural language as a dynamic programming medium, we harness the expansive capability of LLMs to make propositions in human readable natural language. Trained on extensive datasets, LLMs excel in tasks such as content creation and question-answering [33]. A key feature of LLMs is the attention mechanism, which improves their ability to generate contextually appropriate responses. These models are typically based on the "Transformer architecture," a neural network framework optimized for language tasks [34]. In this study, we used two OpenAI models: GPT-3.5-turbo to build a chatbot and GPT-3.5-turbo-instruct to propose specific questions to developers, as well as to establish ethical standards and identify possible existing correlations between ethical principles. These two models are accessible via the OpenAI API (https://platform.openai.com/). OpenAI's GPT-3 is an autoregressive language model family capable of performing human-like text completion tasks. The GPT-3.5-turbo version has 175 billion parameters and was trained on a variety of permitted and public documents [35].

GPT-3.5-turbo was used to build our chatbot because it is a chatty model that will provide responses beyond what is specifically asked. The instruct model, however, is much more terse and concise, performing exactly as instructed. The /completions endpoint (used for GPT-3.5-turbo-instruct) provides the completion for a single prompt and takes a single string as input, whereas the /chat/completions endpoint (used for GPT-3.5-turbo) responds to a given dialog.

These models have a parameter called temperature, which is playing a vital role in our prompts. It is an important setting as it influences the variability of the generated responses. As the temperature approaches zero, the model will become deterministic and repetitive. With this setting, we can fine-tune the model according to the desired level of creativity [36].

2) Smart prompt engineering: Instead of traditional fine-tuning, which requires vast datasets and often masks the decision-making process, smart prompt engineering benefit from LLM's vast knowledge while guiding it with precision. This ensures our tool remains adaptable and explicable. For instance, given a prompt, the LLM crafts questions that probe the software's ethical alignments, drawing from the software and domain descriptions. The type of prompt that is used in this study is Zero-shot prompts. In prompt engineering, "Zero-shot" is when we give a task to a language model like GPT-3 for instance, without any prior examples or training specific to that task. Essentially, the model have to accomplish the task based entirely on its pre-existing knowledge and understanding, which it acquired during its initial training phase. As opposed to "few-shot" or "one-shot" learning, where the model is given one or a few examples to guide its response. Zero-shot learning tests the model's ability to generalize.

Formula for calculating the percentage of compliance with AI ethics. In order to verify if the software developer did respect the AI ethics established by the government, the Eq. (1) was proposed. this formula is designed to calculate the percentage of compliance with the ethics and subsequently verify if the developer has met the minimum percentage value established by the government. The formula is based on the weightings that was assigned by the government to the ten ethical principles and the developer's responses to the five questions per principle.

$$P = \frac{\sum_{i=1}^{10} \frac{R_i}{5} W_i}{\sum_{i=1}^{10} W_i} \cdot 100 \quad (1)$$

Where W_i is the weighting of the i-th ethical principle. R_i is the developer's response to the i-th ethical principle.

In the formula, each response of the developer is divided by 5 in order to normalize the answer to a scale from 0 to 1, where 0 means no positive response (complete non-compliance) and 1 means the developer answered "yes?" to all questions (complete compliance). Then these normalized values are multiplied by the respective weights assigned by the government, and then the weighted average is calculated.

C. Application Overview

Our application (see Fig. 1) is specifically tailored to bridge the ethical divide in software development, offering tools to both government officials and software developers. The main idea behind this application is to enable the government, on one hand, to establish a list of ethical principles and assign a weighting to each principle. These weightings are specific to each ministry or domain. They could be elaborated by ethical committees for each domain, sub-population or context.

Subsequently, developers could, through specific questions for each principle, verify if their software respects the government's ethical norms or preferences of the context in which the application will be used. Indeed, each ministry / domain / context (health, education, etc.) could have its specific weighting of principles, and every software developer would need to comply with the ethics established by the ministry to which their software is linked for getting an approval. The questions posed to the developer are proposed automatically by an LLM (Large Language Model) based on the application domain (health, education, etc.) of their software and the description of their software. Each ministry could review, and then validate or reject the developers' responses. Subsequently, the developer could re-calibrate their application based on feedback from the respective ministry. This iterative process would allow developers to review and refine their software to ensure it finally complies with the government's ethics, based on further feedback and comments. This application ensures scalability because it can be applied across various domains. But, in this paper, only an example about Healthcare was presented. This could be seen as a way for top-down authoritarian governments to enforce their political views, but it must be understood that such guidelines are constitutive of all governments: even in the most liberal democracies, software that would promote racist or paedophilic contents are rightly strongly prohibited, so such ethical enforcements are necessary and beneficial to any society.

The use of an LLM has been identified as a promising method to not only facilitate the generation of appropriate questions for developers but also to help the government better understand and formulate its ethics optimally and to propose standards to be followed at the level of each ministry. The participation of an expert committee in this process is strongly encouraged. This can guarantee consistency and representative ethics within each ministry but also across ministries.

It is designed to work in two complementary parts (Government-Centric Application and Developer Diagnostic Application).

1) Government-Centric application: This module allows government officials to dynamically propose and adjust local ethical norms according to a domain-specific context. These guidelines are defined in the form of clear, natural language prompts, helping for transparency in ethical expectations. Below, the list of sections and features:

a) Section "Chatbot": Users can ask questions and request information about AI ethics via a Chatbot. This LLM-based Chatbot aims to guide the government in understanding and formulating ethics within each ministry/domain. The following message was used to provide guidance on how the GPT-3.5-turbo model should behave for the conversation : "You are an intelligent assistant designed to help users understand AI ethics, become familiar with AI ethical principles, and select the most suitable ethical principles for their specific context. Your goal is to provide clear, comprehensive, and practical guidance."

b) Section "Define an ethic": Government officials can record their expectations regarding ethics via a questionnaire. The questionnaire is domain– or ministry– specific. This section contains three steps:

- Selection of the application domain : Health, education, finance, agriculture. This is the domain to which the concerned ministry is linked.
- Weighting of ethical principles (see Fig. 4). In this step, it is possible to consult a proposed list of principles (principles that we choose during the state-of-the art step), see the description of each, and assign a weighting to each principle according to its importance in the concerned domain. This task of weighting is made easy thanks to a text proposed by the LLM that helps users to find out which principles are essential and which are less important in the context of the specific application domain. Indeed, the importance of ethical principles can vary from one domain to another.
- Specifying a threshold: The minimum value of the "percentage of ethics compliance" that the developer must achieve for their software to conform with established ethics. Each ministry must have its set of thresholds as some domains are more sensitive than others. The compliance threshold has been identified as playing a crucial role in the process of evaluating governmental ethics. It represents the government's will to implement ethical principles and allows civil servants to assess to what extent the software respects established ethical values.
- In the end, a summary of the provided informations is displayed, along with some suggestions:
    - The previously entered weightings of the principles.
    - A list of ethical standards proposed by the LLM that the developer should implement during the software development process.
    - An overview of the correlations between different ethical principles.
      These correlations are proposed by the LLM as correlations exist between different ethical

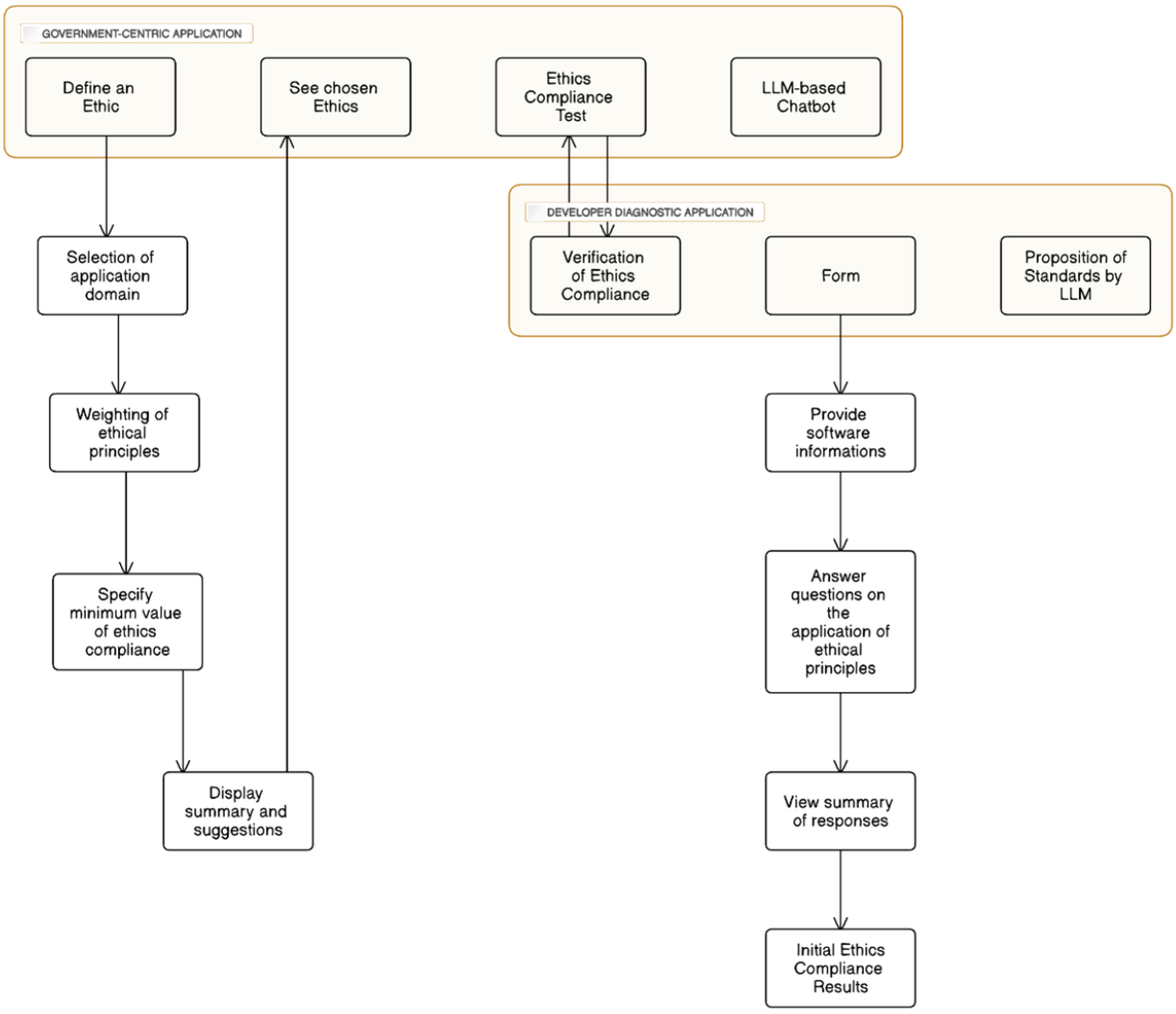


Fig. 1. Flowchart of the proposed approach.

principles. They are used to compute a given software's compliance with established ethics. For example, if there is a correlation between the transparency principle and the responsibility principle, and the weighting of transparency is respected but that of the responsibility principle is not, compensation can then take place, allowing the developer's software to be valid even if it is below the minimum value of the responsibility compliance threshold. The way the compensation is done is open to, and can be modified by the user, with the possibility to implement strong thresholds that cannot be compensated for.

c) Section "See chosen ethics": The user can consult all the information they have entered in the "Define an ethic" form, as well as the list of standards and existing correlations between principles.

d) Section "Ethics Compliance Test": Through this interface, each ministry can review developers' responses to an ethics compliance form (this is a form accessible via the developer module). The ministry validates these responses if they comply with ethics and rejects them if they are not, with a message to the user so that he/she can improve their application before re-submission.

2) Developer diagnostic application: This tool serves as an ongoing ethical audit mechanism. By processing software characteristics and responses against the predefined prompts, it provides feedback on potential ethical misalignments. Below the list of sections and features:

a) Section "Standards": The developer can consult the standards to apply during the software development process. This helps developers to acquire a better understanding of ethical issues. This list of standards was previously elaborated using the help of an LLM and validated by the government via the government module.

b) Section "Form": The developer can check whether their software complies with the government-established ethics through a questionnaire. It takes place in three stages:

- First, the developer provides the following information: software name, application domain, and description.
- Then, they must answer "yes / no" questions regarding each ethical principle's implementation. Five questions are asked for each principle. These questions are proposed by an LLM educated on ethics, based on the software description, application domain, and the principle in question, ensuring a thorough verification of whether ethics are correctly incorporated into the software development process.
- Finally, the developer can view a summary of their responses:
  - A radar chart displaying both the developer's response results and the government's weightings. This chart enables a clear comparison between the developer's performance and government expectations.
  - The number of points obtained for each principle, the name, domain and description of the software. The developer's response to this questionnaire must be validated solely by an expert committee on AI ethics within the government or the respective ministry.

c) Section "Ethics Compliance": The developer can review feedback from the ministry to which their software's domain is attached. And see if their software is approved (meets the government's expectations in terms of AI ethics) or not.

V. Experimental Results

Prompts used in this study and their outputs:

- Prompt for proposing five questions about the application of each ethical principle (see Fig. 2) : the objective of this prompt is to propose five questions the developer must answer. Each question is about the implementation of each ethical principle. The variables: "descApp" (software description), "domain" (domain of application), "principleName" (name of the ethical principle) are given as an input.

```
const prompt =  "You're an expert in Artificial Intelligence ethics. Here's the context: " +
"the Mauritanian government has a list of ethical principles for Artificial " +
"Intelligence applied in a given domain. The Mauritanian government wants to " +
"ensure that any developer of intelligent software respects these principles " +
"and implements them. To ensure that these principles are put into practice, " +
"the government wants to set up a system that generates five questions per " +
"principle. These questions are used to verify, in detail, the implementation " +
"of each principle. The system takes as input the description of the software, " +
"the field of application, and an ethical principle of artificial intelligence, " +
"and gives as output a list of five dichotomous questions on the implementation " +
"of that ethical principle. Generate a list of five questions, taking into account " +
"the following information: software description: " + descApp + "; application domain: " +
domain + "; ethical principle: " + principleName + ". Enclose the list in braces like the " +
"following JSON format: {\"questions\": [{" +
"\"id\": 1, \"name\": \"q1\", \"label\": \"question one\"},{" +
"\"id\": 2, \"name\": \"q2\", \"label\": \"question two\"},{" +
"\"id\": 3, \"name\": \"q3\", \"label\": \"question three\"},{" +
"\"id\": 4, \"name\": \"q4\", \"label\": \"question four\"},{" +
"\"id\": 5, \"name\": \"q5\", \"label\": \"question five\"}] }";
```

Fig. 2. Prompt that propose questions for developer

descApp = "IBM Watson for Oncology is an AI-powered software designed to assist oncologists in diagnosing and creating personalized treatment plans for cancer patients. Developed by IBM in collaboration with Memorial Sloan Kettering Cancer Center, this software leverages the power of AI to analyze large volumes of medical literature, patient data, and clinical trial information to provide evidence-based treatment recommendations", domain/Field = Healthcare, temperature = 0

- Output of the prompt when principal name is Transparency (the output is in the format JSON):

```
"questions":
[ "id": 1, "name": "q1", "label":
"Does the software provide
a clear explanation of how
it arrives at its treatment
recommendations?", "id": 2,
"name": "q2", "label": "Is
the software able to provide
a breakdown of the data and
sources used to generate its
recommendations?", "id": 3,
"name": "q3", "label": "Does the
software disclose any potential
biases or limitations in its
recommendations?", "id": 4,
"name": "q4", "label": "Is
the software able to explain
the reasoning behind its
recommendations in a way that is
understandable to non-technical
users?", "id": 5, "name": "q5",
"label": "Does the software
provide a mechanism for users to
access and review the data used
to generate its recommendations?"
]
```

- Output of the prompt when principal name is Responsibility:

```
"questions":
[  "id": 1, "name": "q1",
"label": "Does the software
accurately and reliably analyze
large volumes of medical
literature, patient data, and
clinical trial information to
provide evidence-based treatment
recommendations?",  "id": 2,
"name": "q2", "label": "Does the
software take into account the
individual needs and preferences
of each patient when providing
treatment recommendations?",
"id": 3, "name": "q3", "label":
"Is the software transparent
in its decision-making process,
providing clear explanations for
its treatment recommendations?",
"id": 4, "name": "q4", "label":
"Does the software have
mechanisms in place to ensure
patient data privacy and
security?",  "id": 5, "name":
"q5", "label": "Is the software
regularly monitored and updated
to ensure its accuracy and
effectiveness in providing
treatment recommendations?" ]
```

- Output of the prompt when principal name is Privacy and confidentiality:

```
"questions":
[  "id": 1, "name": "q1",
```

```
"label": "Does the software have
a clear and transparent privacy
policy that outlines how patient
data will be collected, used, and
protected?",  "id": 2, "name":
"q2", "label": "Is the software
designed to only collect and use
patient data that is necessary
for its intended purpose?",
"id": 3, "name": "q3", "label":
"Does the software have built-in
security measures to protect
patient data from unauthorized
access or breaches?",  "id": 4,
"name": "q4", "label": "Is the
software regularly audited and
updated to ensure compliance
with privacy and confidentiality
regulations?",  "id": 5, "name":
"q5", "label": "Does the software
have a mechanism for patients
to access, review, and request
changes to their personal data
collected by the software?" ]
```

- Prompt for proposing a list of norms to apply when developing an intelligent software (see Fig. 3). The following variables are given as an input: “listPrinciples” = list of ethical principles, “domain” = domain of application, “notations” = the weighting given by the government to ethical principles. Output of the

```
const prompt =
"Act as an expert in Artificial Intelligence ethics. " +
"You are familiar with the regulations governing the implementation " +
"of AI ethical principles in all fields. Here's the context: the " +
"Mauritanian government has a list of AI ethical principles applied " +
"in a given field. The government has assigned a weighting between " +
"1 and 5 to each principle. These weights represent the importance " +
"of these principles for the government. The government then wants " +
"to use these weights to generate two standards per ethical principle " +
"to ensure that any intelligent software developer respects government " +
"ethics. In other words, the software developer must respect and implement " +
"these ethical principles according to their weightings. If an ethical " +
"principle has a high weighting, this means it is considered particularly " +
"crucial. The standards associated with crucial ethical principles should " +
"therefore be more stringent and demanding. Conversely, if a principle " +
"has a low weighting, the corresponding standards may be less stringent. " +
"It should also be noted that these standards will change from one field " +
"to another. Software developers must respect the following ethical principles: " +
listPrincipes + ". They must respect these principles according to the following " +
"weightings: " + JSON.stringify(notations) +
". Generate a list of standards to follow (two standards per principle) that " +
"this developer must respect, given that their software concerns the domain: " +
domaine + ". Take into account that weightings influence the generation of norms by " +
"highlighting the relative importance of ethical principles. Do not mention the word " +
"\"norm\" in the list you're about to generate, and do not include the question in your " +
"answer. Enclose the list in braces like the following JSON format: " +
"{\"principles\": [{\"name\": \"principle's name\",\"weight\": weight,\"norms\": " +
"[\"norm one\",\"norm two\"]}]}";
```

Fig. 3. Prompt that propose a list of norms.

prompt that propose a list of norms:

Transparency:

- Provide clear and accurate information about the Al software and its capabilities to healthcare professionals and patients
- Ensure that the Al software does not hide or manipulate information from healthcare professionals and patients

Responsibility:

- Ensure that the Al software is properly maintained and monitored to prevent any potential harm to patients
- Establish clear lines of responsibility and accountability for the development and use of the Al software

Non-maleficence:

- Conduct thorough risk assessments and testing to identify and mitigate potential harms caused by the Al software
- Implement safeguards and protocols to prevent or minimize potential harms to patients from the Al software

Equity:

- Ensure that the Al software does not perpetuate or amplify existing inequities in the healthcare system
- Regularly assess and address any potential biases or discrimination in the Al software that could impact patient outcomes

Privacy and confidentiality:

- Implement strong data privacy and security measures to protect patient information collected and used by the Al software
- Ensure that the Al software adheres to all relevant privacy laws and regulations

Societal and environmental well-being:

- Consider the potential societal and environmental impacts of the Al software and take steps to mitigate any negative effects
- Regularly evaluate the Al software’s overall contribution to the well-being of society and the environment

Human autonomy:

- Ensure that the Al software does not impede or restrict patient autonomy in making healthcare decisions
- Provide options for patients to opt-out or request human intervention in the use of the Al software for their care

Reactivity and durability:

- Regularly monitor and update the Al software to ensure it remains relevant and effective in the rapidly changing healthcare landscape
- Implement a system for receiving and addressing feedback and concerns from healthcare professionals and patients about the Al software

Cultural and linguistic diversity:

- Ensure that the Al software is accessible to and inclusive of individuals from diverse cultures and linguistic backgrounds
- Conduct thorough testing and adaptation of the Al software to account for cultural and linguistic differences in healthcare practices

Democracy and political self-determination:

- Ensure that the development and use of the Al software is aligned with democratic principles and political self-determination
- Ensure transparent decision-making processes and active stakeholder engagement in the development and use of the Al software.

- Prompt for proposing the existing correlations between ethical principles (see Fig. 4): If the percentage of compliance of the developer is below the minimum value of "percentage of compliance with AI ethics" set by the government, the correlations between the ethical principles might become significant. These correlations can help government officials to decide whether to approve or not the developer's software. For instance, if there's a correlation between Principle A and Principle B, and the developer has closely followed the guidelines for Principle A but not for Principle B, then adherence to Principle A can compensate the lack in Principle B.

```
const prompt =
"You are an expert in Artificial Intelligence ethics. " +
"You are familiar with the different principles of AI ethics " +
"and understand the correlations that may exist between these principles " +
"depending on the domain of application of AI. " +
"I would like you to help me determine whether there are correlations " +
"between the AI ethical principles I'm about to provide you with. " +
"To identify these correlations, consider the domain of application of AI. " +
"The result should indicate the degrees of correlation–strong, weak, or non-existent– " +
"between the ethical principles. Provide a coherent and detailed analysis " +
"by exploring correlations between the following AI ethical principles in the domain of " +
domaine + " : " + listPrincipes + ". " +
"Analyze all possible combinations of correlations. Your answer should only include " +
"the combinations in which the correlations are \"strong\". " +
"Do not include correlations with the degree \"weak\" or \"non-existent\". " +
"Justify your answer by explaining the reasons behind these correlations. " +
"Enclose your answer in braces using the following JSON format: " +
"{\"correlations\": [{\"key\": \"unique identification key\", " +
"\"principle1\": \"name of the first principle\", " +
"\"principle2\": \"name of the second correlated principle\", " +
"\"reasons\": [\"justification for the correlation\"]}]}";
```

Fig. 4. Prompt for the existing correlations between ethical principles.

Output of the prompt for the existing correlations between ethical principles: see Fig. 5.

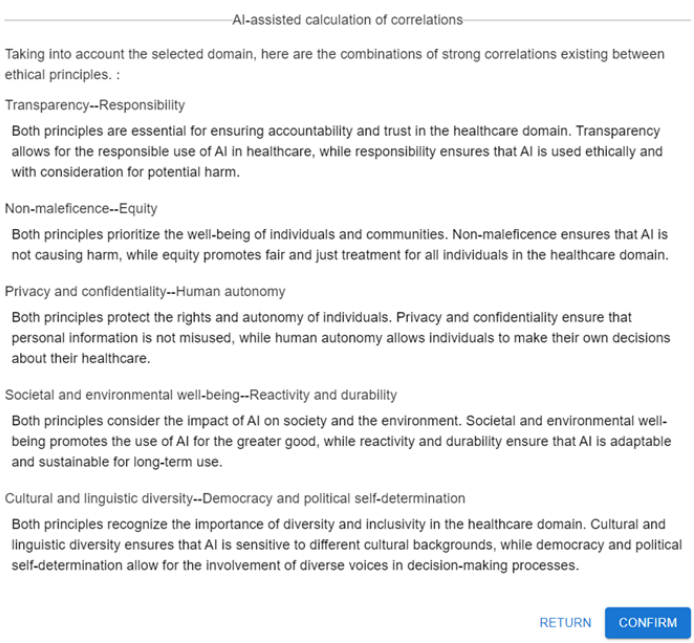


Fig. 5. The summary (correlations between different ethical principles, proposed by the LLM). Because of the translation tool Responsibility became Accountability.

VI. Discussion

As the industrial revolution allowed humans to delegate hard work to machines, the AI revolution will allow us to delegate to AI more and more white-collar tasks: bureaucratic at first but as AI will improve, it will be given increasing decision-making power. In medicine, for example, it is now accepted that AI is better and faster at spotting developing cancers on mammographies. This is great because it will save time to radiologists, who can then concentrate on more difficult cases.

AI assistants are becoming acting assistants, with www.jace.ai, "Your new AI employee" that will act for you: "Don't just chat, start acting today". On March 13th 2024, the Members of the European Parliament (MEP) adopted the Artificial Intelligence Act, setting safeguards on general purpose artificial intelligence, limiting the use of biometric identification systems by law enforcement, banning the use of AI for social scoring and manipulating or exploiting user vulnerabilities, and giving consumers the right to launch complaints and receive meaningful explanations.

All this means that societies are becoming increasingly aware of the risks posed by AI, but companies too: in order to get an "app" validated by Apple for upload on their appStore, the app needs to be "approved" and for this, the developer must follow hundreds of guidelines limiting the app to minimize its access to the contents on the phone or tablet on which it will be used.[2] For example, developers must: "Use AppStoreSettings to manage a user's App Store settings. You can set a maximum age rating for apps, deny in-app purchases, and require passwords for purchases."

This is what this work attempts at proposing: a tool to help governments formulate their policies and guide app developers, all this with the help of Large Language Models.

The transparent design that we propose promotes clarity in interaction, accountability in ethical deviations, and empowers stakeholders with informed decision-making capabilities. These are significant strides toward responsible AI development in a culturally-sensitive domain. The major advantage is its emphasis on explicability:

1) Transparency by design: By utilizing natural language as the medium of interaction and guidance, stakeholders can easily understand, adjust, and interpret the ethical guidelines and the feedback generated.

2) Ethical accountability: When the system identifies a potential bias or misalignment, it does not just flag it but also provides a contextually relevant explanation, making it easier for developers to pinpoint and rectify the root cause.

3) Informed decision-making: As the government and developers interact with the tool, they are consistently informed about how the software aligns with ethical norms, ensuring conscious and informed decisions throughout the development lifecycle.

However, as with all pioneering methods, it has its inherent challenges, which can be presented in terms of the following disadvantages:

[2]https://developer.apple.com/documentation/managedsettings/managedsettingsstore/appstore?changes=_6

- Bias from Language Models: Even with smart prompt engineering, there is a possibility that biases inherent in the LLM (acquired from the data it was trained on) could influence its feedback.
- Scalability Issues: As governments adjust ethical standards and as the volume and complexity of software applications increase, the system might face scalability issues, potentially slowing down feedback times.
- Lack of Ground Truth: Using natural language as a programming tool lacks a strict "ground truth" in the way traditional programming does. Hence, there is a level of interpretative ambiguity.

We, therefore, try to propose ideas:

- Enhanced Training: The LLM could be trained further using Mauritanian cultural and linguistic data. This would enhance its understanding of local nuances.
- Continuous Feedback Loop: Encourage continuous feedback from users, especially when they notice discrepancies or biases. This would help in refining the system over time.
- Incorporate Domain Experts: Engaging domain experts in sectors like healthcare, finance, etc. can help in fine-tuning the responses and ensuring domain-specific accuracy.

Consider the description of the software to be checked and its specific domain as contextual anchors; by integrating these as prompts, we guide the model's responses in a manner that is intricately aligned with the software's functionality and its ethical considerations within that domain. This is akin to "fine-tuning on-the-fly": the model's vast knowledge is channeled and constrained by the prompt, ensuring relevance and accuracy without the need for additional training data.

Moreover, this method underscores a significant advantage: it is adaptable. As software evolves or if there are shifts in domain-specific ethical standards, the prompts can be adjusted, thus ensuring that the AI's outputs remain congruent with the changing landscape. In essence, by leveraging smart prompt engineering, we are making a case that with the right prompts, models like LLM can be "programmed" in real time using natural language, bridging the gap between generalized AI knowledge and specific, localized requirements.

The advantages of the proposed approach compared to some existing methods is that, compared to existing frameworks such as the G7 toolkit[3] and the U.S. Intelligence Community's AI Ethics Framework[4], which address AI ethics broadly but lack a focus on generative AI, our proposed approach is distinct in its specific adaptation for generative AI tools. This model is dynamic, allowing government bodies to calibrate ethical standards flexibly across domains and adapt to evolving cultural contexts. Furthermore, the integrated government-developer feedback mechanism supports continuous alignment with ethical standards, which is typically absent in other frameworks. By utilizing LLMs, this tool also offers a novel, practical approach for real-time ethical compliance, reducing reliance on resource-intensive manual assessments.

[3]https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/10/g7-toolkit-for-artificial-intelligence-in-the-public-sector_f93fb9fb/421c1244-en.pdf

[4]https://www.intelligence.gov/artificial-intelligence-ethics-framework-for-the-intelligence-community

VII. Conclusion

We present a possible solution to the challenges of modern software development in a sensitive sociocultural context, leveraging the strengths of large language models, and emphasizing explicability as its cornerstone. At the intersection of AI and ethics, our LLM-based tool serves as a critical bridge, particularly in the Mauritanian context.

Technically, our tool has two major components:

- For the government, it's a dynamic platform to set the ethical standards they want to promote. By tuning these standards, they can directly shape the AI's desired behavior, ensuring a permanent alignment with local values, all the while avoiding unintentional amplification of biases. Inserting their ethical wishes and priorities in the tool will force governments to think about them and integrating them in the tool will be equivalent to publishing them, resulting in ethical norms to be officially clear and known by all. So, the tool is there too to help the institution to refine their norms.
- For developers, it is a diagnosis tool. It allows them to check if their software aligns thanks to a set of domain specific questions, generated by LLM. The LLM engineering provides smart prompts to maximize robustness: if biases exist in data or algorithmic design — the tool will detect it via smartly formulated closed questions and answers. This immediate feedback helps developers rectify issues before they escalate into bigger problems.

For Mauritania, unchecked biases could lead to wrong decisions, from reinforcing stereotypes to misinformed policies. However, the inherent ambiguity of natural language as a tool is noteworthy and can be a serious limitation. But by acknowledging it and actively seeking solutions, such as further localized training, continuous feedback loops, and domain-specific expert input. Because it is adaptable and resilient, the process of improving it will increase the awareness, understanding and realization of governmental institutions on the importance of ethics.

Interestingly enough, even if the questions or the "guidance" of the LLM end up being strange, trying to understand their meaning will force users on both sides to think about ethics, which would not be so much the case if this tool did not exist.

The source code attached to this work is available on GitHub, here: https://github.com/Lalla-Aicha/Ethic-App-developer, https://github.com/Lalla-Aicha/EthicApp-Government. A lot of screenshots could not be added to this paper due to the maximum number of pages.

To further enhance the effectiveness and accessibility of our proposed ethical framework for AI, future work will focus on two key areas: improving the model's response precision and expanding its linguistic reach.

First, fine-tuning the LLM for conciseness and precision will be essential for achieving more targeted, contextually relevant outputs. By training the model on a curated dataset of ethical guidelines and domain-specific language, we aim to refine its ability to deliver concise and precise recommendations. This focused training will help reduce ambiguity and improve the clarity of responses.

Second, to support broader accessibility in diverse linguistic contexts, we plan to implement multilingual capabilities. This could involve training the model on datasets in multiple languages or incorporating advanced translation features that allow ethical standards to be accurately reflected in non-English-speaking regions. By expanding the tool's language support, we aim to provide a more inclusive platform, enabling it to be a valuable resource in global settings where ethical norms and practices vary significantly.

Through these advancements, the tool can become both more precise and more widely accessible, contributing to a more ethically aligned implementation of AI across diverse cultural and linguistic landscapes.

REFERENCES

[1] H. Mehr, H. Ash, and D. Fellow, "Artificial intelligence for citizen services and government," *Ash Cent. Democr. Gov. Innov. Harvard Kennedy Sch., no. August*, pp. 1–12, 2017.

[2] J. Berryhill, K. K. Heang, R. Clogher, and K. McBride, "Hello, world: Artificial intelligence and its use in the public sector," 2019.

[3] S. J. Mikhaylov, M. Esteve, and A. Campion, "Artificial intelligence for the public sector: opportunities and challenges of cross-sector collaboration," *Philosophical transactions of the royal society a: mathematical, physical and engineering sciences*, vol. 376, no. 2128, p. 20170357, 2018.

[4] V. J. Straub and J. Bright, "Unite the study of ai in government: With a shared language and typology," *AI & SOCIETY*, pp. 1–2, 2024.

[5] T. Brown, B. Mann, N. Ryder, M. Subbiah, J. D. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell *et al.*, "Language models are few-shot learners," *Advances in neural information processing systems*, vol. 33, pp. 1877–1901, 2020.

[6] M. D. M. Reddy, M. S. M. Basha, M. M. C. Hari, and M. N. Penchalaiah, "Dall-e: Creating images from text," *UGC Care Group I Journal*, vol. 8, no. 14, pp. 71–75, 2021.

[7] A. Névéol, H. Dalianis, S. Velupillai, G. Savova, and P. Zweigenbaum, "Clinical natural language processing in languages other than english: opportunities and challenges," *Journal of biomedical semantics*, vol. 9, no. 1, pp. 1–13, 2018.

[8] E. Kasneci, K. Seßler, S. Küchemann, M. Bannert, D. Dementieva, F. Fischer, U. Gasser, G. Groh, S. Günnemann, E. Hüllermeier *et al.*, "Chatgpt for good? on opportunities and challenges of large language models for education," *Learning and individual differences*, vol. 103, p. 102274, 2023.

[9] J. C. Young and M. Shishido, "Investigating openai's chatgpt potentials in generating chatbot's dialogue for english as a foreign language learning," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, 2023.

[10] C. Hernández-Castillo, H. H. Guedea-Noriega, M. Á. Rodríguez-García, and F. García-Sánchez, "Pest recognition using natural language processing," in *International Conference on Technologies and Innovation*. Springer, 2019, pp. 3–16.

[11] S. Biswas, "Importance of chat gpt in agriculture: According to chat gpt," *Available at SSRN 4405391*, 2023.

[12] C. C. Corrigan, S. A. Asakipaam, J. J. Kponyo, and C. Luetge, *AI Ethics in Higher Education: Insights from Africa and Beyond*. Springer Nature, 2023.

[13] M. Bensalah, "Toward an ethical code of ai and human rights in morocco," *Arribat-International Journal of Human Rights Published by CNDH Morocco*, vol. 1, no. 2, pp. 187–203, 2021.

[14] A. Gwagwa, "Recommendations on the inclusion sub-saharan africa in global ai ethics," *RANITP Policy Brief*, vol. 2, 2019.

[15] A. Gwagwa, E. Kraemer-Mbula, N. Rizk, I. Rutenberg, and J. De Beer, "Artificial intelligence (ai) deployments in africa: benefits, challenges and policy dimensions," *The African Journal of Information and Communication*, vol. 26, pp. 1–28, 2020.

[16] A. Gwagwa, E. Kazim, and A. Hilliard, "The role of the african value of ubuntu in global ai inclusion discourse: A normative ethics perspective," *Patterns*, vol. 3, no. 4, 2022.

[17] E. Ntoutsi, P. Fafalios, U. Gadiraju, V. Iosifidis, W. Nejdl, M.-E. Vidal, S. Ruggieri, F. Turini, S. Papadopoulos, E. Krasanakis *et al.*, "Bias in data-driven artificial intelligence systems—an introductory survey," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 10, no. 3, p. e1356, 2020.

[18] E. Van Miltenburg, "Stereotyping and bias in the flickr30k dataset," *Proceedings of multimodal corpora: computer vision and language processing (mmc 2016)*, 2016.

[19] A. Al-Ghamdi, "A survey on software security testing techniques," *Int J Comput Sci Telecommun*, vol. 4, pp. 14–18, 2013.

[20] R. R. Althar, D. Samanta, S. Purushotham, S. S. Sengar, and C. Hewage, "Design and development of artificial intelligence knowledge processing system for optimizing security of software system," *SN Computer Science*, vol. 4, no. 4, p. 331, 2023.

[21] S. Qazi, M. S. Memon, A. Ali, and S. Nizamani, "Role of artificial intelligence (ai) tools for assuring quality in software," *Journal of Southwest Jiaotong University*, vol. 57, no. 2, 2022.

[22] S. Ramchand, S. Shaikh, and I. Alam, "Role of artificial intelligence in software quality assurance," in *Intelligent Systems and Applications: Proceedings of the 2021 Intelligent Systems Conference (IntelliSys) Volume 2*. Springer, 2022, pp. 125–136.

[23] V. Nallur, "Landscape of machine implemented ethics," *Science and engineering ethics*, vol. 26, pp. 2381–2399, 2020.

[24] A. Jobin, M. Ienca, and E. Vayena, "The global landscape of ai ethics guidelines," *Nature Machine Intelligence*, vol. 1, no. 9, pp. 389–399, 2019.

[25] J. Fjeld, N. Achten, H. Hilligoss, A. Nagy, and M. Srikumar, "Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for ai," *Berkman Klein Center Research Publication*, no. 2020-1, 2020.

[26] V. Tiple, "Recommendations on the european commission's white paper on artificial intelligence-a european approach to excellence and trust, com (2020) 65 final (the'ai white paper')," 2020.

[27] M. Carman and B. Rosman, "Applying a principle of explicability to ai research in africa: should we do it?" *Ethics and Information Technology*, vol. 23, no. 2, pp. 107–117, 2021.

[28] L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi *et al.*, "Ai4people—an ethical framework for a good ai society: opportunities, risks, principles, and recommendations," *Minds and machines*, vol. 28, pp. 689–707, 2018.

[29] H. Miller, R. Stirling, Y. Chung, S. Lokanathan, E. Martinho-Truswell, J. New, I. Rutenberg, and F. Scrollini, "Government artificial intelligence readiness index 2019," *London: Oxford Insights*, p. 32, 2019.

[30] R. Calo, "Artificial intelligence policy: a primer and roadmap," *UCDL Rev.*, vol. 51, p. 399, 2017.

[31] P. Rawat and A. N. Mahajan, "Reactjs: A modern web development framework," *International Journal of Innovative Science and Research Technology*, vol. 5, no. 11, pp. 698–702, 2020.

[32] B. Basumatary and N. Agnihotri, "Benefits and challenges of using nodejs," *International Journal of Innovative Research in Computer Science & Technology*, vol. 10, no. 3, pp. 67–70, 2022.

[33] N. F. Lindemann, "Chatbots, search engines, and the sealing of knowledges," *AI & SOCIETY*, pp. 1–14, 2024.

[34] J. Yang, H. Jin, R. Tang, X. Han, Q. Feng, H. Jiang, S. Zhong, B. Yin, and X. Hu, "Harnessing the power of llms in practice: A survey on chatgpt and beyond," *ACM Transactions on Knowledge Discovery from Data*, vol. 18, no. 6, pp. 1–32, 2024.

[35] J. Huang, D. M. Yang, R. Rong, K. Nezafati, C. Treager, Z. Chi, S. Wang, X. Cheng, Y. Guo, L. J. Klesse *et al.*, "A critical assessment of using chatgpt for extracting structured data from clinical notes," *npj Digital Medicine*, vol. 7, no. 1, p. 106, 2024.

[36] R. Dulepet, "Generating high-quality "about me" narratives," 2023.

Simulation-Based Analysis of Evacuation Information Sharing Systems Using Geographical Data

Tatsuki Fukuda
Department of Data Science, Faculty of Data Science,
Shimonoseki City University, Shimonoseki, Japan

***Abstract*—In this study, we developed an agent-based model (ABM) to simulate and improve evacuation rates during flood disasters. Utilizing the "Evacuate Now Button", a previously proposed system for sharing real-time evacuation rates among residents, our experimental findings demonstrate a significant enhancement in evacuation behavior through this system. Simulations were conducted using geographical data from Nobeoka City, Miyazaki Prefecture, and Toyohashi City, Aichi Prefecture. Results showed that the "Evacuate Now Button" increased evacuation rates from a few percent to approximately 78% in Nobeoka City and 90% in Toyohashi City. We also investigated the effect of varying the range for calculating evacuation rates and the accuracy of the evacuation information shared with residents. It was found that larger calculation ranges led to higher final evacuation rates, while smaller ranges resulted in a quicker initial increase in evacuation behavior. These findings provide valuable insights for enhancing evacuation strategies and disaster preparedness in regions prone to floods.**

***Keywords*—Evacuation; flood disaster; evacuation rate; agent-based model; evacuate now button**

I. Introduction

Japan is a country frequently affected by natural disasters such as earthquakes, typhoons, and floods, making it crucial to strengthen disaster prevention measures. Past large-scale disasters have proven that prompt evacuation actions can save many lives. Despite the availability of evacuation warnings, many areas still report low evacuation rates. For instance, studies on Typhoons Faxai and Hagibis in 2019 reported that despite receiving evacuation information, many residents did not evacuate [1]. Various factors, such as insufficient understanding of evacuation advisories and delays in action, are thought to contribute to this low evacuation rate.

One of the reasons for the low evacuation rate is the lack of disaster awareness among residents and differences in how evacuation information is received. For example, it has been shown that personality traits significantly affect evacuation behavior, with individuals categorized as "cautious and proactive" more likely to take disaster information seriously and evacuate early, while those in the "careless and proactive" group are less likely to act upon the same information [2]. These differences in personality traits have a significant influence on how evacuation information is received and the subsequent actions taken, making them a critical factor in formulating disaster prevention strategies.

Additionally, research has been conducted on methodologies for accurately estimating evacuation rates during floods [3], providing valuable insights into modeling evacuation behavior. Other studies have analyzed evacuation behavior and its influencing factors during landslides, highlighting how the timing and method of information dissemination affect evacuation behavior [4]. In a case study of heavy rainfall in Gifu Prefecture, the impact of how evacuation information was provided on residents' evacuation decisions was analyzed [5]. Further, research has examined the influence of prior flood awareness on evacuation behavior, showing that pre-existing knowledge significantly promotes evacuation action [6].

In recent years, many studies have employed agent-based models (ABM) to simulate and deepen understanding of residents' evacuation behavior. For instance, the effects of flood warning lead times on evacuation behavior have been simulated using ABM, demonstrating the complexity of evacuation behavior and the importance of psychological and social factors [7]. Other studies have used ABM to analyze residents' behavior during floods, providing detailed insights into how individual evacuation actions are influenced by flood conditions [8]. These studies contribute to a deeper understanding of the diversity of evacuation behavior and the factors that influence it. Moreover, the effectiveness of mutual aid mechanisms within vulnerable communities has been analyzed using ABM, showing that mutual assistance contributes to improved evacuation behavior [9].

However, existing studies have not been able to sufficiently influence individual actions and decision-making, resulting in limited improvements in evacuation rates. Therefore, this study aims to utilize the new concept called the "Evacuate Now Button [10]" which we previously proposed. The system visually informs residents of evacuation statuses and fosters a sense of solidarity.

In this paper, we simulate evacuation behavior during disasters using an ABM and evaluate the effectiveness of new measures to improve evacuation rates. Specifically, based on survey results conducted in advance via the internet, the behavior of agents reflecting residents' personality traits and evacuation awareness will be modeled. This approach enables more accurate reproduction of the psychological and social factors influencing individuals' evacuation behavior.

Furthermore, this study will examine the effectiveness of the "Evacuate Now Button". This button is designed to encourage residents to take swift and appropriate evacuation actions during disasters, and its impact will be simulated using

ABM. The simulation will evaluate changes in evacuation rates with and without the button in order to clarify factors that contribute to the promotion of evacuation behavior.

The findings of this study are expected to provide important implications for future disaster prevention planning. In particular, understanding evacuation behavior based on residents' psychological factors and personality traits can improve the methods and content of evacuation information dissemination, as well as be applied to the design of education and training programs aimed at enhancing residents' evacuation awareness. This, in turn, is expected to contribute to the development of highly effective disaster prevention measures that help mitigate disaster damage.

The structure of this paper is as follows: Section II explains simulations using ABM as a foundational concept and introduces the proposed "Evacuate Now Button". Section III describes the specifications of the simulation program used in this study. Section IV presents the results of simulations using actual topographical maps and Section V discusses these results. The conclusion and the future work are presented in Sections VI and VII, respectively.

II. Preliminaries

In this section, we provide an overview of the basic concept of the "Evacuate Now Button" and the ABM used in this study. This section aims to provide the foundational knowledge necessary for understanding the design of the simulations and the assumptions underlying the experiments, facilitating discussions in the following section.

A. *Evacuate Now Button* [10]

In a previous survey we conducted on residents regarding evacuation during heavy rains, 92% of respondents indicated that they were concerned about the evacuation status of others when deciding whether to evacuate. Based on this, we proposed a system called the "Evacuate Now Button". This is a physical button installed at the entrance of each residence, which residents press before evacuating. By pressing the button, the evacuation status of the residents is recorded and shared with emergency services, such as fire departments, to facilitate the rescue of those who have not evacuated in time. Additionally, the evacuation status is shared with residents, allowing them to gauge the evacuation progress in their area, which may encourage further evacuations. However, rather than sharing the evacuation status of individual households, the system provides aggregated evacuation rates for clusters of homes. This prevents the risk of burglary that could arise if specific households were known to have evacuated.

When sharing evacuation status with nearby homes, there is a possibility that residents will either evacuate in coordination with their neighbors or refrain from evacuating if no one else does. However, as mentioned earlier, 92% of survey respondents stated that they are concerned about the evacuation status of others, suggesting that the remaining 8% would decide to evacuate regardless of their neighbors' actions. Therefore, it is more likely that this 8% will begin evacuating based on information from local authorities or their own judgment, potentially prompting others to follow suit.

There are still many considerations for implementing this system, such as determining the appropriate cluster size for sharing evacuation rates. Therefore, in this study, we use ABM simulations to explore effective methods for utilizing the "Evacuate Now Button".

B. *Simulations Using ABM*

An ABM is a simulation method where autonomous entities, referred to as agents, interact with each other within a system. ABM is a powerful simulation technique that can be applied to a variety of real-world systems and is particularly useful for understanding and predicting complex collective behaviors.

1) Features and Advantages of ABM: The ABM provides several unique features that make it a powerful tool for simulating complex systems. By allowing individual agents to interact with each other and their environment, ABM can capture emergent behaviors that are not easily represented by other modeling techniques. The following are some of the key features and advantages of ABM [11]–[15].

- Reproduction of Individual Behavior

In ABM, agents act based on their unique attributes and behavioral rules, interacting with the environment to produce complex collective behaviors. This allows for a detailed reproduction of complex social phenomena, such as evacuation behavior and risk perception during disasters.

- Understanding System Dynamics

ABM is well-suited for understanding the overall behavior of a system that emerges from interactions among agents, known as "emergent phenomena". This is a significant advantage over other modeling methods. For example, by simulating residents' evacuation behavior and movement patterns during floods, ABM can be used to evaluate the effectiveness of disaster response measures.

- Scenario Comparison and Evaluation

ABM is useful for comparing agent behavior across different scenarios and is widely applied in evaluating policy effects and disaster response measures. For example, it allows analysis of how different evacuation routes or shelter locations impact residents' evacuation behavior.

2) Practical Applications of ABM: ABM has been widely used for modeling human evacuation behavior in natural disasters, particularly in studies focusing on flood evacuation, where it has proven effective for detailed simulation of evacuation behavior [16]. In flood evacuation simulations, assigning agents with different attributes (such as age, gender, and socioeconomic factors influencing evacuation decisions) enables more realistic reproduction of evacuation behavior [17]. Specific applications of ABM include the development of models that help humanitarian organizations respond more effectively to flood evacuations by predicting evacuation dynamics and analyzing movement patterns to shelters [12].

Other studies have simulated pedestrian responses during emergency floods to evaluate how behavioral rules affect risk analysis, analyzing how pedestrians adjust their actions

according to flood conditions using an agent-based approach [18], offering valuable insights for urban evacuation planning. Moreover, ABM has been used to model household decision-making regarding the adoption of flood mitigation measures, analyzing how individual choices impact regional flood risk and collective disaster prevention behavior [16]. ABM has also been applied to dynamic simulations of flood-human interactions, providing detailed analyses of residents' evacuation behavior and subsequent effects during floods. In urban settings, research has simulated pedestrian evacuation behavior during floods, providing data useful for emergency evacuation planning [15].

These simulations provide valuable information for optimizing emergency response measures during disasters. A comprehensive review of the application of ABM to flood risk analysis was conducted in reference [19], tracking trends in social dynamics and behavioral changes.

As demonstrated, ABM is highly effective for understanding and predicting evacuation behavior during floods.

III. Simulator Specifications

In this study, we aim to examine the effective usage of the "Evacuate Now Button" by simulating residents' evacuation behavior using an ABM. First, the specifications of the simulation are described below.

A. Overall Process

This simulation is developed using Unity and C# scripts. While visual effects are not necessarily required for the simulation itself, Unity was chosen to facilitate the use of simulation videos for disaster awareness events and other purposes.

The program first loads a three-dimensional terrain model and places agents in locations corresponding to residential buildings. In this simulation, one agent represents one residence, including multi-unit buildings such as apartments, where one agent is assigned per building. For the terrain model, we utilize the 3D urban models developed under the PLATEAU project [20], promoted by Japan's Ministry of Land, Infrastructure, Transport and Tourism [21].

Agents, which represent residents, determine whether or not to begin evacuation based on evacuation information provided by local authorities and the evacuation status of surrounding residents. The simulation progresses according to Algorithm 1.

Algorithm 1 Overall Process

1: Load the PLATEAU model.
2: Place agents in residential locations.
3: If the time for issuing a warning has been reached, issue it.
4: Agents decide whether to begin evacuation every T_1 seconds.
5: If Warning Level 5 has been issued, end the simulation.
6: Advance the simulation by one time step.
7: Return to Step 3.

B. Agent Evacuation Behavior

Each agent determines whether to begin evacuation every T_1 seconds. The decision-making process is based on the results of the previously mentioned resident survey [10]. Agents are divided into one of two groups, Group I or Group II. Group I consists of agents that make their evacuation decisions without considering the evacuation rate of surrounding residents. In contrast, Group II includes agents that take into account the evacuation rate of their neighbors when deciding whether to evacuate.

For Group I agents, there is a possibility they will initiate evacuation when evacuation information is issued for their region. However, they do not always evacuate when conditions are met, but instead decide probabilistically with a certain probability P.

While some residents may evacuate before official evacuation information is issued, this study does not take such behavior into account. This is because excluding early evacuators does not positively contribute to the goal of improving the overall evacuation rate, which is the primary objective of this study. It is recognized, however, that the absence of early evacuators could negatively affect the overall evacuation rate.

At the start of the simulation, agents are randomly assigned to either Group I (approximately 8%) or Group II (approximately 92%). Additionally, Group II agents are further subdivided based on the extent to which they are influenced by the evacuation rates of others. Specifically, according to the survey results [10], agents are categorized into Group II(a) through Group II(e), as shown in Table I, which reflects the timing of evacuation initiation in relation to the surrounding evacuation rate.

TABLE I. Results of the Survey Asking at what Evacuation Rate Among Surrounding Residents Respondents Would Begin to Evacuate

Evacuation Timing	Respondent Percentage	Group
10% evacuation rate	20%	II(a)
30% evacuation rate	31%	II(b)
50% evacuation rate	32%	II(c)
80% evacuation rate	12%	II(d)
100% evacuation rate	5%	II(e)

Agents in Group II(a) through Group II(e) also make their evacuation decisions probabilistically with a certain probability P, rather than always evacuating when conditions are met.

C. Discount Rate for Evacuation Probability

Agents consider evacuating when certain conditions are met, such as when the evacuation rate of surrounding residents exceeds a certain threshold. When this occurs, they decide whether to evacuate with probability P. However, based on real-world evacuation behavior, it can be assumed that if an agent does not evacuate the first time conditions are met, the barrier to evacuation increases in subsequent evaluations. To reflect this in the simulation, a discount rate is applied to the evacuation probability. Let the discount rate be denoted as α. The probability P_i that an agent evacuates during the i-th evaluation is given by Eq. (1), where $P_1 = P$:

$$P_i = \alpha \times P_{i-1} \quad (i > 2) \tag{1}$$

This formula models the decreasing likelihood of evacuation as agents delay their decision.

D. Start and End of the Simulation

The simulation begins when evacuation information equivalent to "Warning Level 3" is issued. Warning Level 3 corresponds to evacuation information for elderly and vulnerable residents. Prior to the 2021 revisions, it corresponded to "evacuation commencement," which makes it an appropriate starting point for the simulation.

The simulation ends when evacuation information corresponding to "Warning Level 5" is issued. Warning Level 5 is defined as a situation where it is no longer possible to safely evacuate, and lives are at risk, meaning all evacuations should be completed before this level is issued.

The timing of each warning level's issuance is determined based on real-world examples of past incidents.

Additionally, each agent is given a maximum delay of T_2 from the start of the simulation, after which they begin to act asynchronously.

IV. Experiments

We verified the operation of the simulation program developed according to the specifications defined in Section III. The simulation was run under the conditions based on the heavy rain disaster that occurred in Nobeoka City, Miyazaki Prefecture in September 2022 [22] and the heavy rain disaster in Toyohashi City, Aichi Prefecture in June 2023 [23]. The conditions are outlined in Table II and the values of other parameters used in the simulation are shown in Table III.

Experiments are conducted using multiple random seed values, and the average values are calculated. Fig. 1 shows the state of the simulation in progress. The blue color represents the residences of agents who have not yet evacuated, and the red color represents the residences of agents who have started evacuating.

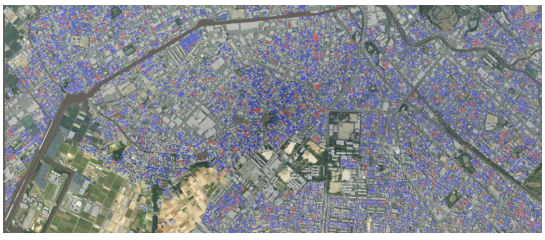


Fig. 1. The state during the simulation. The red dots represent the evacuted agents while the blue dots represent agents in their house.

In Section IV-A, we present the results of examining the impact of the range used to calculate the evacuation rate. Section IV-B discusses the results of examining the effect of the accuracy of the evacuation rate communicated to the agents. In Section IV-C, we present the results of evaluating the effectiveness of the "Evacuate Now Button". The discussion of these results is provided in Section V.

A. Distance for Calculating Surrounding Evacuation Rate

Each agent is able to know the evacuation rate of residences within a radius L meters from their own residence, and they decide whether to evacuate based on this information. We first examined the optimal range for calculating the evacuation rate that agents can access. The results using the geographical data of Toyohashi City, Aichi Prefecture, and Nobeoka City, Miyazaki Prefecture, are shown in Fig. 2 and 3, respectively.

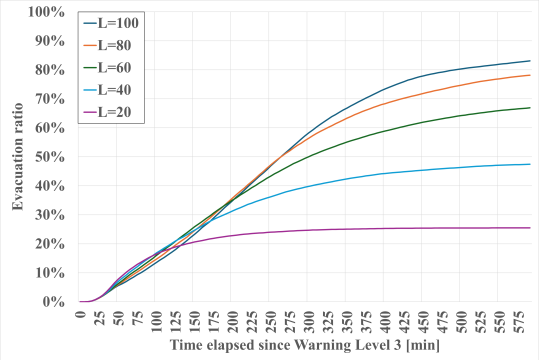


Fig. 2. Evacuation rate transition in the simulation with Toyohashi City's data. Agents know accurate evacuation rate of their surroundings within a range of L meters.

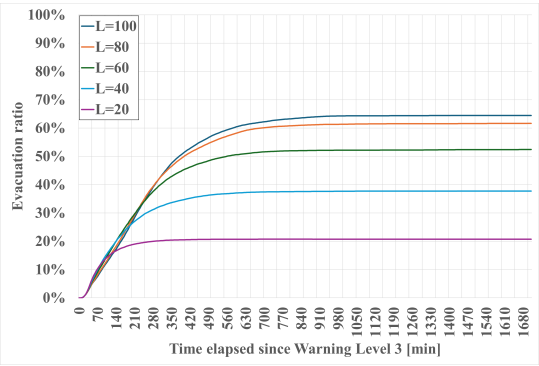


Fig. 3. Evacuation rate transition in the simulation with Nobeoka City's data. Agents know accurate evacuation rate of their surroundings within a range of L meters.

In both Fig. 2 and 3, the horizontal axis represents the time elapsed since the issuance of Warning Level 3, and the vertical axis represents the evacuation rate. L is varied from 20 to 100 meters in increments of 20 meters. Agents are able to accurately know the evacuation rate of residences within a radius L meters from their own location.

B. Accuracy of Communicated Evacuation Rates

Agents can know the evacuation rate in the surrounding area and decide whether to evacuate based on this information. However, communicating a low evacuation rate may, in fact, hinder evacuation behavior. Therefore, a method of providing a more generalized evacuation rate, rather than a precise one, is proposed. For example, if the actual evacuation rate is between 10% and 30%, the agent would be informed that the evacuation rate is "up to 30%". This would result in agents perceiving a higher evacuation rate than the actual one,

TABLE II. WARNING LEVELS AND ANNOUNCEMENT TIMES DURING HEAVY RAIN DISASTERS IN NOBEOKA (2022), AND TOYOHASHI (2023)

Warning Level	Issuance Time in Nobeoka	Issuance Time in Toyohashi
3	17:00, Sep. 17th, 2022	6:40, Jun. 2nd, 2023
4	8:00, Sep. 18th, 2022	14:40, Jun. 2nd, 2023
5	21:30, Sep. 18th, 2022	16:30, Jun. 2nd, 2023

TABLE III. PARAMETERS RELATED TO AGENTS' EVACUATION DECISIONS

Parameter	Description	Value
T_1 [min]	Interval at which agents decide whether to evacuate	$15 \pm 50\%$
T_2 [min]	Delay time before agents begin actions	$30 \pm 50\%$
P	Probability of starting evacuation when conditions are met	0.5
α	Discount rate applied to P when evacuation is not initiated	0.8

potentially encouraging evacuation. However, if the range is too broad, the credibility of the information may decrease. Thus, we conducted experiments using two different patterns, Pattern 1 and Pattern 2, as shown in Table IV and Table V.

TABLE IV. PATTERN 1 FOR THE EVACUATION RATE COMMUNICATED TO AGENTS

Actual Evacuation Rate [%]	Evacuation Rate Shared with Agents [%]
0	0
$0 < r \leq 50$	50
$50 < r \leq 100$	100

TABLE V. PATTERN 2 FOR THE EVACUATION RATE COMMUNICATED TO AGENTS

Actual Evacuation Rate [%]	Evacuation Rate Shared with Agents [%]
0	0
$0 < r \leq 30$	30
$30 < r \leq 50$	50
$50 < r \leq 80$	80
$80 < r \leq 100$	100

Additionally, we define Pattern 3 as the case where the actual evacuation rate is communicated accurately to the agents. The results for Pattern 3 correspond to Fig. 2 and 3.

For each of these patterns, the agents' level of trust in the "Evacuate Now Button" was set according to the values shown in Table VI.

TABLE VI. THE VALUES REPRESENTING THE AGENTS' LEVEL OF TRUST IN THE SYSTEM FOR EACH COMMUNICATION PATTERN

Pattern	Trust Level θ
1	0.3
2	0.75
3	1

When the trust level θ is applied, agents use the adjusted evacuation rate ρ', which is calculated from the evacuation rate ρ obtained through the "Evacuate Now Button" and a random number k $(0 \leq k < 1)$, using the formula $\rho' = \rho \times (\theta + k(1 - \theta))$. This adjusted evacuation rate ρ' is used as the current evacuation rate.

The results of the experiments conducted using the geographical data of Toyohashi City, Aichi Prefecture for Pattern 1 and Pattern 2 are shown in Fig. 4 and 5, respectively. Similarly, the results using the geographical data of Nobeoka City, Miyazaki Prefecture for Pattern 1 and Pattern 2 are shown in Fig. 6 and 7, respectively.

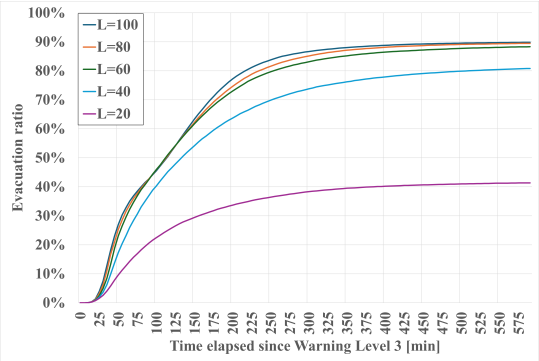


Fig. 4. Evacuation rate transition in the simulation with Toyohashi City's data. Agents can obtain the evacuation rate of their surroundings within a range of L meters, following the rule in Table IV.

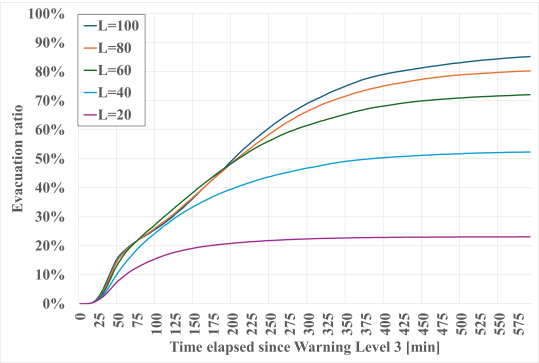


Fig. 5. Evacuation rate transition in the simulation with Toyohashi City's data. Agents can obtain the evacuation rate of their surroundings within a range of L meters, following the rule in Table V.

In Fig. 4 through 7, the horizontal axis represents the time elapsed since the issuance of Warning Level 3, while the vertical axis represents the evacuation rate. L is varied from 20 to 100 meters in increments of 20 meters.

C. Effectiveness of the "Evacuate Now Button"

Lastly, we investigated the effectiveness of the "Evacuate Now Button". As a comparison, we considered the case where the button is not used. In this scenario, agents are unable to know the evacuation rate of their surroundings. Instead, agents

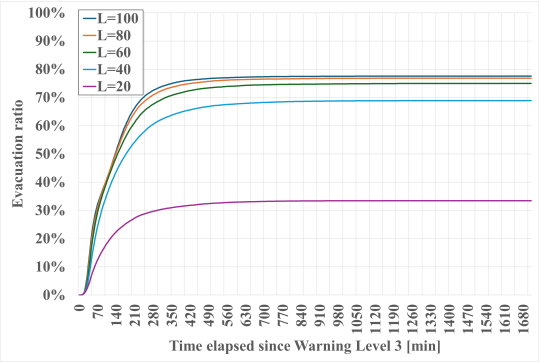


Fig. 6. Evacuation rate transition in the simulation with Nobeoka City's data. Agents can obtain the evacuation rate of their surroundings within a range of L meters, following the rule in Table IV.

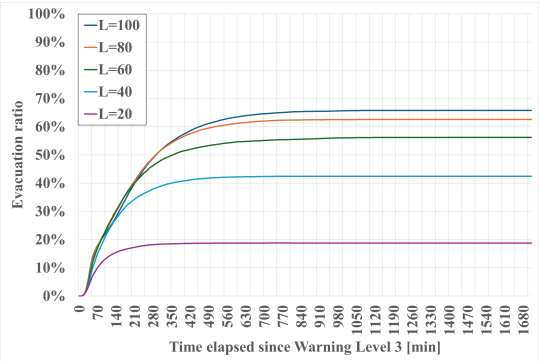


Fig. 7. Evacuation rate transition in the simulation with Nobeoka City's data. Agents can obtain the evacuation rate of their surroundings within a range of L meters, following the rule in Table V.

are assumed to observe the evacuation behavior of others within five minutes of them deciding to evacuate, and thus gain an understanding of the evacuation situation.

The results of the experiments using the geographical data of Toyohashi City, Aichi Prefecture, and Nobeoka City, Miyazaki Prefecture, are shown in Fig. 8 and 9, respectively.

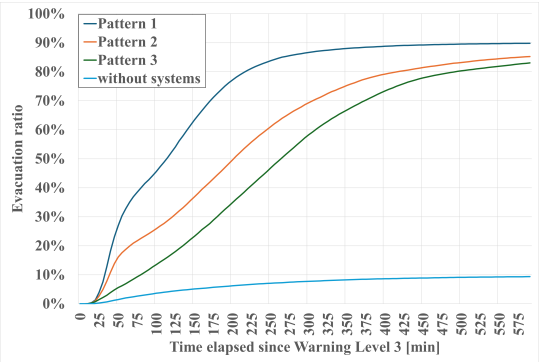


Fig. 8. Evacuation rate transition with / without the evacuation rate sharing system (Patterns 1-3) in the simulation with Toyohashi City's data. Agents with the system can obtain the evacuation rate of their surroundings within $L = 100$ meters. agents without the system can only observe those within a 40 meter range who have evacuated within the last 5 minutes.

In Fig. 8 and 9, the horizontal axis represents the time

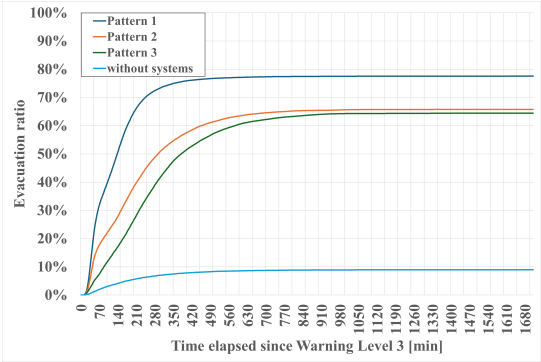


Fig. 9. Evacuation rate transition with / without the evacuation rate sharing system (Patterns 1-3) in the simulation with Nobeoka City's data. Agents with the system can obtain the evacuation rate of their surroundings within $L = 100$ meters. agents without the system can only observe those within a 40 meter range who have evacuated within the last 5 minutes.

elapsed since the issuance of Warning Level 3, and the vertical axis represents the evacuation rate. For Pattern 1, Pattern 2, and Pattern 3, the range within which agents can know the evacuation rate was set to $L = 100$ meters, while agents without the evacuation information sharing systems can observe the evacuation behavior of others within a 40-meter radius.

V. Discussion

This section discusses the experimental results presented in Section IV.

A. Distance for Calculating Surrounding Evacuation Rate

Fig. 2 and 3 show the results of varying the range L used to calculate the evacuation rate that agents can access. From these figures, we can observe that increasing L leads to a higher final evacuation rate. This is likely because, with a larger L, the probability of finding someone who has already begun evacuation increases within that range, which then influences other agents to evacuate. In other words, increasing L facilitates the spread of an "evacuation chain".

However, we also see that in the early stages, shortly after Warning Level 3 is issued, the evacuation rate increases more quickly when L is smaller. This is likely due to the smaller population size within a smaller range L, where the evacuation of just one agent has a larger impact on the overall evacuation rate for that group.

These results suggest that, when there is sufficient time after the issuance of Warning Level 3, increasing L could raise the evacuation rate. In other words, if the impact of the heavy rain can be predicted early and Warning Level 3 is issued at an appropriate time, a larger L is preferable. However, in situations where disasters occur shortly after the issuance of Warning Level 3, a smaller L might be more effective in increasing the evacuation rate more quickly.

B. Accuracy of Communicated Evacuation Rates

In the simulations conducted using the geographical data from Toyohashi City, Aichi Prefecture, as shown in Fig. 4 and

5, the final evacuation rate is highest when $L = 100$, consistent with the results in Fig. 2. Comparing Pattern 1 and Pattern 2, we observe that Pattern 1 achieves a higher final evacuation rate for all values of L. However, as L increases, the difference between the final evacuation rates of Pattern 1 and Pattern 2 becomes smaller. This suggests that when L is small, Pattern 1 yields a higher effect, but as L increases, the difference between Pattern 1 and Pattern 2 diminishes.

In the simulations using the geographical data from Nobeoka City, Miyazaki Prefecture, as shown in Fig. 6 and 7, the results are similar to those in Fig. 4 and 5: Pattern 1 produces a higher final evacuation rate than Pattern 2, and the difference between the two patterns decreases as L increases. However, in the case of Nobeoka City, the final evacuation rate difference between Pattern 1 and Pattern 2 is approximately 10%, which is larger than the difference observed in Toyohashi City.

From Fig. 4 through 7, we conclude that Pattern 1 consistently results in higher early and final evacuation rates compared to Pattern 2. Therefore, Pattern 1 is the more favorable option.

C. Effectiveness of the "Evacuate Now Button"

Fig. 8 and 9 show that the scenario without the "Evacuate Now Button" yields the lowest evacuation rates, with a final rate of about 9%. In comparison, the actual evacuation rate during the heavy rain disaster in Toyohashi City, Aichi Prefecture, was approximately 0.068% [23], which may seem somewhat detached from the simulation result. However, it is important to consider that factors such as community relationships, the location and number of shelters, and resident demographics likely influence real-world evacuation decisions. Previous studies involving surveys across multiple regions have shown that the evacuation rate for storm and flood disasters is generally around a few percent [24], making the results of this simulation reasonable when considering the exclusion of regional characteristics beyond geography.

When the "Evacuate Now Button" is introduced, the effect varies depending on how the evacuation rate is communicated to the agents, but in all cases—Pattern 1 through Pattern 3—the evacuation rate is significantly higher compared to the scenario without the system. In particular, in the case of Pattern 1, the simulations show an evacuation rate of approximately 78% for Nobeoka City (Fig. 9) and approximately 90% for Toyohashi City (Fig. 8), indicating a remarkably high evacuation rate.

As the evacuation rate increases, the number of people who need to be rescued in an emergency decreases, reducing the burden on fire departments and other rescue teams, allowing them to allocate more resources to individual rescues.

D. Limitations

The limitations of this study include the following: First, the behavior of agents used in the simulation is modeled based on survey results, and thus may not fully replicate the actual behavior of residents. Additionally, social factors such as the calculation range of evacuation rates and relationships within the community have been simplified, which is another limitation. Considering these limitations, future research should aim to develop a model that incorporates more detailed regional characteristics and psychological factors of residents' behavior.

VI. Conclusion

In this study, we developed a simulation based on an ABM to improve evacuation rates during heavy rain disasters. We experimentally demonstrated how much the "Evacuate Now Button," our previously proposed evacuation rate sharing system, could enhance evacuation rates. Additionally, we investigated the optimal range for calculating evacuation rates and the level of accuracy in the shared evacuation rate that would best contribute to increasing the evacuation rate.

The results showed that using the "Evacuate Now Button" could raise the evacuation rate from a few percent to approximately 78% in the case of Nobeoka City, Miyazaki Prefecture, and to approximately 90% in the case of Toyohashi City, Aichi Prefecture. Furthermore, regarding the range for calculating evacuation rates, it was found that a larger range led to a higher final evacuation rate. However, we also discovered that a smaller range resulted in a quicker initial rise in the evacuation rate. Therefore, if the goal is to increase the evacuation rate early, a smaller range should be used, while if the goal is to maximize the final evacuation rate, a larger range is preferable.

VII. Future Work

The discussion concluded that the simulation results are reasonable when regional characteristics are excluded. However, as evacuation rates vary between regions, it is expected that developing a simulator that incorporates regional factors would further improve the accuracy of evacuation rate predictions. While incorporating factors such as shelter locations is relatively straightforward, integrating more complex aspects like relationships among residents would be challenging. Therefore, future research will need to explore methods for including such factors in the simulation program.

References

[1] A. Kajiya, K. Akaishi, T. Yokota, and H. Tsurusaki, "Comparative Analysis of Evacuation Behavior in Response to Typhoons No. 15 and 19 in 2019 and Proposal for Providing Disaster Information Reflecting Regional Characteristics," *Journal of Disaster Information*, vol.19, no.2, pp.145-155, 2021.

[2] Y. Takenouchi, K. Yamaguchi, and Y. Iwasaki, "Analysis of the Influence of Residents' Personality on Evacuation Awareness," *Proceedings of the Kansai Branch of the Japan Society of Urban Planning*, vol.14, pp.117-120, 2016.

[3] S. Tomura, M. Chiba, S. Masuya, and T. Yamada, "Basic Research on Methods for Estimating the Evacuation Rate During Floods," *Journal of River Technology*, vol.28, pp.349-354, 2022.

[4] M. Mizuno, Y. Tomita, S. Katsura, N. Koyanagi, R. Hanada, and T. Yasuda, "Analysis of Evacuation Rate During Landslides Using Disaster Information," *Journal of the Japan Sabo Society*, vol.65, no.3, pp.29-34, 2012.

[5] A. Takagi, S. Sugiura, H. Mori, and H. Iwata, "Analysis of Evacuation Behavior During the July 2018 Heavy Rain Disaster - A Case Study of Gifu Prefecture," *Journal of Natural Disaster Science*, vol.38, no.S06, pp.133-151, 2019.

[6] S. Kubo, H. Yoshida, T. Ichimura, M. L. L. Wijerathne, and M. Hori, "Study on Influence of Prior Recognition of Flooding State on Evacuation Behavior," *International Journal of Disaster Risk Reduction*, vol.63, pp.102437, 2021.

[7] R. Zhang, D. Liu, E. Du, L. Xiong, J. Chen, and H. Chen, "An Agent-Based Model to Simulate Human Responses to Flash Flood Warnings for Improving Evacuation Performance," *Journal of Hydrology*, vol.628, pp.130452, 2024.

[8] F. Taillandier, P. Di Maiolo, P. Taillandier, C. Jacquenod, L. Rauscher-Lauranceau, and R. Mehdizadeh, "An Agent-Based Model to Simulate Inhabitants' Behavior During a Flood Event," *International Journal of Disaster Risk Reduction*, vol.64, pp.102503, 2021.

[9] Z. Wang, J. Huang, H. Wang, J. Kang, and W. Cao, "Analysis of Flood Evacuation Process in Vulnerable Communities with Mutual Aid Mechanism: An Agent-Based Simulation Framework," *International Journal of Environmental Research and Public Health*, vol.17, no.2, pp.560, 2020.

[10] T. Fukuda, "A Development of Simulator Considering Behavioral Psychology of Japanese to Improve Evacuation Ratio in Flood," *International Journal of Advanced Computer Science and Applications*, vol.11, no.4, 2020.

[11] E. Bonabeau, "Agent-Based Modeling: Methods and Techniques for Simulating Human Systems," *Proceedings of the National Academy of Sciences*, vol.99, no.suppl_3, pp.7280-7287, 2002.

[12] A. Jahani, S. Jess, D. Groen, D. Suleimenova, and Y. Xue, "Developing an Agent-Based Simulation Model to Forecast Flood-Induced Evacuation and Internally Displaced Persons," in *Proceedings of the International Conference on Computational Science*, pp.550-563, 2023.

[13] Y. Han, L. Mao, X. Chen, W. Zhai, Z. Peng, and P. Mozumder, "Agent-Based Modeling to Evaluate Human-Environment Interactions in Community Flood Risk Mitigation," *Risk Analysis*, vol.42, no.9, pp.2041-2061, 2022.

[14] L. Tierolf, T. Haer, W. J. W. Botzen, J. A. de Bruijn, M. J. Ton, L. Reimann, and J. C. Aerts, "A Coupled Agent-Based Model for France for Simulating Adaptation and Migration Decisions Under Future Coastal Flood Risk," *Scientific Reports*, vol.13, no.1, pp.4176, 2023.

[15] M. Shirvani, "Flood-Pedestrian Simulator: An Agent-Based Modelling Framework for Urban Evacuation Planning," Ph.D. dissertation, University of Sheffield, 2021.

[16] S. Nabinejad and H. Schüttrumpf, "Agent-Based Modeling for Household Decision-Making in Adoption of Private Flood Mitigation Measures: The Upper Kan Catchment Case Study," *Water*, vol.16, no.14, pp.2027, 2024.

[17] M. Shirvani, G. Kesserwani, and P. Richmond, "Agent-Based Simulator of Dynamic Flood-People Interactions," *Journal of Flood Risk Management*, vol.14, no.2, pp.e12695, 2021.

[18] M. Shirvani, G. Kesserwani, and P. Richmond, "Agent-Based Modelling of Pedestrian Responses During Flood Emergency: Mobility Behavioural Rules and Implications for Flood Risk Analysis," *Journal of Hydroinformatics*, vol.22, no.5, pp.1078-1092, 2020.

[19] A. Taberna, T. Filatova, D. Roy, and B. Noll, "Tracing Resilience, Social Dynamics, and Behavioral Change: A Review of Agent-Based Flood Risk Models," *Socio-Environmental Systems Modelling*, 2020.

[20] Ministry of Land, Infrastructure, Transport and Tourism (MLIT) Digital Policy Division, "PLATEAU," https://www.mlit.go.jp/plateau/, accessed Aug. 1, 2024.

[21] General Incorporated Association for Geospatial Information Distribution Promotion, "3D Urban Model (Project PLATEAU) Portal Site," https://www.geospatial.jp/ckan/dataset/plateau, accessed Aug. 1, 2024.

[22] Nobeoka City Typhoon No. 14 Disaster Response Committee, "Report on the Response to Typhoon No. 14 in 2022," Nobeoka City, 2023.

[23] Disaster Management Division of Toyohashi City, "Record of the Heavy Rain in June 2023 (Main Volume)," Toyohashi City, 2023.

[24] MS&AD InterRisk Research & Consulting, "Survey Results on Evacuation Awareness During Natural Disasters," https://www.irric.co.jp/topics/press/2023/0214.php, accessed Aug. 1, 2024.

Application of Unbalanced Optimal Transport in Healthcare

Qui Phu Pham[1]*, Nghia Thu Truong[2]*, Hoang-Hiep Nguyen-Mau[3], Cuong Nguyen[4],
Mai Ngoc Tran[5], Dung Luong[6]
University of California, Irvine, California, USA[1]
Pasadena City College, California, USA[2]
VinUniversity, Hanoi, Vietnam[3,4]
Binh Duong University, Ho Chi Minh City, Vietnam[5]
VietDynamic, Ho Chi Minh City, Vietnam[6]
Acuitas Education, Ho Chi Minh City, Vietnam[5]

***Abstract*—Optimal Transport (OT) is a powerful tool widely used in healthcare applications, but its high computational cost and sensitivity to data changes make it less practical for resource-constrained settings. These limitations also contribute to increased environmental impact due to higher CO2 emissions from computing. To address these challenges, we explore Unbalanced Optimal Transport (UOT), a variation of OT that is both computationally efficient and more robust to data variability. We apply UOT to two healthcare scenarios: independence testing on breast cancer data and modeling heart rate variability (HRV). Our experiments show that UOT not only reduces computational costs but also delivers reliable results, making it a practical alternative to OT for socially impactful applications.**

***Keywords*—Optimal transport; unbalanced optimal transport; healthcare**

I. Introduction

Optimal Transport (OT), first formulated by Gaspard Monge [23] and further developed by Kantorovic [15], addresses the fundamental question of finding the most efficient way to minimize the cost of transporting mass from one distribution to another. OT has evolved into many practical applications in fields such as healthcare [42], [39], [41], machine learning [12] and domain adaptation [7]. For healthcare applications such as breast cancer detection [39] or heart rate variability (HRV) modeling [42], which may be needed widely by also resource-constrained medical institutes and have a direct impact on human wellness, the computational efficiency and the robustness of the deployed models are paramount. Nevertheless, OT has been known to suffer from computational bottleneck [21] and sensitivity to problem structure or data perturbation [17]. Such limitations of vanilla OT can make solution models to these healthcare applications not accessible to medical institutes with limited budget [36], raise the CO2 output of computing resources thereby negatively impacting the environment [16], and become a less reliable tool in the realm of healthcare [8].

To alleviate the above limitations, Unbalanced Optimal Transport (UOT) is recently proposed variant of the classical OT formulation that penalizes the marginal constraints based on some given divergence. Among the various divergences used in the literature such as Kullback-Leiber (KL) divergence [6], squared ℓ_2 norm [3], ℓ_1 norm [4], and ℓ_p norm [18], UOT with KL divergence is the most prominent for its wide applicability, flexibility and efficient computation [30]. UOT has shown its prominence in various applications in statistics and machine learning [11]. Recent works [35], [17], [30] have facilitated the fast computation of UOT and provided guarantees on its statistical and approximation properties.

Recent advancements in UOT have significantly reduced its computational complexity and improved its scalability, enabling its application in large-scale machine learning tasks. Notable among these advancements are efficient gradient-based methods [30], which not only accelerate UOT computations but also provide theoretical guarantees for convergence and statistical properties. These methods are especially important in scenarios requiring real-time processing, such as medical diagnostics or dynamic resource allocation in healthcare. Furthermore, UOT has been shown to be more robust than traditional OT in handling outliers and noisy data, making it a valuable tool in applications where data quality is variable [17].

As computational efficiency and environmental concerns become more critical in the age of large-scale AI, UOT stands out as a method that balances performance with resource utilization. By relaxing the mass conservation constraint, UOT reduces the computational burden while maintaining the accuracy required in sensitive applications such as healthcare. This reduced computational cost also has positive implications for sustainability, as it lowers the energy consumption and CO2 emissions associated with large-scale computations [16]. As a result, UOT not only provides a more flexible and scalable approach to OT problems but also addresses key limitations that have historically hindered the adoption of OT in resource-constrained settings.

A. Contributions

In this paper, we benchmark and empirically validate the effectiveness of UOT on various healthcare applications, which are the statistical independence test on the breast cancer dataset following the setting in [39] and HRV modeling in [42]. The code is given in https://github.com/quipp12/UOT_Healthcare.git. Our contributions can be summarized as follows:

- For both healthcare applications, statistical independence test [39] and HRV modeling [42], the OT

*Equal Contribution

distance is used as a component in these pipelines, where the celebrated Sinkhorn algorithm with the costly computational cost of $\tilde{O}\left(n^2\varepsilon^{-2}\right)$ [19] is used. To alleviate the computational bottleneck, we propose the adoption of UOT as well as the Sinkhorn variant specifically designed for UOT distance with improved complexity of $\tilde{O}\left(n^2\varepsilon^{-1}\right)$ [35]. This facilitates not only seamless integration of UOT (in place of OT) in these applications but also an acceleration in computation, which is consistently demonstrated in Section III and Section IV

- For HRV modeling [42], in addition to the realization of UOT's computational benefit, our experimental investigation reviews the high training cost from the original model using Gradient Descent (GD). Consequently, we implement the GD with Momentum (GDM) into the model to significantly expedite the training process, while maintaining comparable or even better Mean Squared Error (MSE)- the main performance metric (Section IV).
- Our primary theoretical contribution focuses on establishing a bound that quantifies the difference between the costs of Unbalanced Optimal Transport (UOT) and regular Optimal Transport (OT). We provide a rigorous guarantee that as the parameter controlling the mass relaxation in UOT increases, the difference between the UOT cost and the OT cost becomes smaller. This result ensures that the approximation made by UOT closely mirrors the exact cost computed by OT when enough relaxation is allowed.

II. Approximating Optimal Transport via Unbalanced Optimal Transport

A. Notations

Denote by $\mathbb{R}_+^n$ the set of all vectors in $\mathbb{R}^n$ with nonnegative entries. Bold capital letters and lowercase letters respectively stand for matrices and vectors. For $p \in [1, \infty), \|.\|_p$ denotes the l_p norm. The Frobenius inner product of two matrices of the same size is defined as $\langle \mathbf{A}, \mathbf{B} \rangle = \sum_{i,j=1}^{n} A_{ij} B_{ij}$.

B. Optimal Transport

Consider two discrete distributions $\mathbf{a}, \mathbf{b} \in \mathbb{R}_+^n$, specifically $\mathbf{a} := (a_1, \ldots, a_n), \mathbf{b} := (b_1, \ldots, b_n)$ with equal masses, i.e., $\|\mathbf{a}\|_1 = \|\mathbf{b}\|_1$. Denote $a_{min} = \min_{1 \le i \le n}\{a_i\}$ and $b_{min} = \min_{1 \le i \le n}\{b_i\}$ as the minimum masses. The OT problem seeks to find a matrix $\mathbf{X} \in \mathbb{R}_+^{n \times n}$ represented a transport plan which maps $\mathbf{a}$ to $\mathbf{b}$ at a minimum cost, i.e.

$$\mathbf{OT}(\mathbf{a}, \mathbf{b}) := \min_{\mathbf{X} \in \Pi(\mathbf{a}, \mathbf{b})} \langle \mathbf{C}, \mathbf{X} \rangle, \tag{1}$$

where $\mathbf{C} \in \mathbb{R}_+^{n \times n}$ is a cost matrix whose entries are distances between measures of these distributions and $\Pi(\mathbf{a}, \mathbf{b}) := \left\{\mathbf{X} \in \mathbb{R}_+^{n \times n} : \mathbf{X}\mathbf{1}_n = \mathbf{a}, \mathbf{X}^\top \mathbf{1}_n = \mathbf{b}\right\}$. Denote by $\mathbf{X}^{\text{OT}} = \operatorname{argmin}_{\mathbf{X} \in \Pi(\mathbf{a}, \mathbf{b})} \langle \mathbf{C}, \mathbf{X} \rangle$ be the optimal solution to the OT problem (1).

C. Unbalanced Optimal Transport

First, we define the $\mathbf{KL}$ divergence function between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}_+^n$ as

$$\mathbf{KL}(\mathbf{x} \| \mathbf{y}) := \sum_{i=1}^{n} \left(\mathbf{x}_i \log\left(\frac{\mathbf{x}_i}{\mathbf{y}_i}\right) - \mathbf{x}_i + \mathbf{y}_i \right)$$

Assume two finite measures $\mathbf{a}, \mathbf{b} \in \mathbb{R}_+^n$, specifically $\mathbf{a} := (a_1, \ldots, a_n), \mathbf{b} := (b_1, \ldots, b_n)$ with possibly different total mass. The UOT problem seeks to find a matrix $\mathbf{X} \in \mathbb{R}_+^{n \times n}$ represented a transport plan, i.e.

$$\begin{aligned} \mathbf{UOT}_{\mathbf{KL}}(\mathbf{a}, \mathbf{b}) = \min_{\mathbf{X} \in \mathbb{R}_+^{n \times n}} \big\{ f(\mathbf{X}) := & \langle \mathbf{C}, \mathbf{X} \rangle + \tau \mathbf{KL}\left(\mathbf{X}\mathbf{1}_n \| \mathbf{a}\right) \\ & + \tau \mathbf{KL}\left(\mathbf{X}^\top \mathbf{1}_n \| \mathbf{b}\right) \big\} \end{aligned} \tag{2}$$

where $\mathbf{C} \in \mathbb{R}_+^{n \times n}$ is a given cost matrix and $\tau > 0$ is a given regularization parameter. Denote by $\mathbf{X}^{\text{UOT}} = \operatorname{argmin}_{\mathbf{X} \in \mathbb{R}_+^{n \times n}} f(\mathbf{X})$ be the optimal solution to the UOT problem (2).

The parameter τ effectively acts as a regularization term. A larger τ means a stronger penalty on the mass divergence, making the solution more balanced (closer to the original distributions $\mathbf{a}$ and $\mathbf{b}$). A smaller τ reduces the effect of the regularization term, allowing for more flexibility in the transport plan. With a very small τ, the solution may deviate significantly from the target distributions in favor of minimizing the transport cost.

D. Approximation Error of UOT

When $\mathbf{a}^\top \mathbf{1}_n = \mathbf{b}^\top \mathbf{1}_n$ and $\tau \to \infty, \mathbf{UOT}_{\mathbf{KL}}(\mathbf{a}, \mathbf{b})$ turns to the regular $\mathbf{OT}(\mathbf{a}, \mathbf{b})$.

Formally, taking the limit as $\tau \to \infty$ in the UOT objective function:

$$\lim_{\tau \to \infty} \left(\langle \mathbf{C}, \mathbf{X} \rangle + \tau \mathbf{KL}(\mathbf{X}\mathbf{1}_n \,||\, \mathbf{a}) + \tau \mathbf{KL}(\mathbf{X}^\top \mathbf{1}_n \,||\, \mathbf{b}) \right)$$

enforces $\mathbf{X}\mathbf{1}_n = \mathbf{a}$ and $\mathbf{X}^\top \mathbf{1}_n = \mathbf{b}$ at the optimal solution, which recovers the OT problem (1). Moreover, [30, Theorem 26] provided the tight non-asymptotic characterization on the distance gap between $\mathbf{UOT}_{\mathbf{KL}}(\mathbf{a}, \mathbf{b})$ and $\mathbf{OT}(\mathbf{a}, \mathbf{b})$ to be $O\left(\frac{1}{\tau}\right)$, where the big-$O$ notation here neglects the terms other than τ. Nevertheless, such results as above do not fully capture how well the UOT solution $\mathbf{X}^{\text{UOT}}$ can approximate the OT solution $\mathbf{X}^{\text{OT}}$ in the pure sense of transportation cost $\langle \mathbf{C}, \mathbf{X} \rangle$, which may better represents the raw performance within the application of interest. To this end, we establish in the next theorem such approximation error in transportation cost of using the UOT solution instead of the OT solution.

Theorem 1. *Under the balanced setting of $\|\mathbf{a}\|_1 = \|\mathbf{b}\|_1 = 1$, i.e. $\mathbf{a}$ and $\mathbf{b}$ are distributions, we have the following bound on the difference between the transportation costs incurred by UOT and OT solutions:*

$$0 \le \langle \mathbf{C}, \mathbf{X}^{OT} \rangle - \langle \mathbf{C}, \mathbf{X}^{UOT} \rangle \le O\left(\frac{1}{\tau}\right). \tag{3}$$

Proof: Let $\kappa = \min\{a_{min}, b_{min}\}^{-1}$. From [10, Theorem 1] that provides an upper bound for KL divergence, we have:

$$\begin{aligned} 0 \leq \mathbf{KL}(\mathbf{X}^{\text{UOT}}\mathbf{1}_n \| \mathbf{a}) &\leq \sum_{i=1}^{n} \frac{\left[(\mathbf{X}^{\text{UOT}}\mathbf{1}_n)_i - a_i\right]^2}{a_i} \\ &\overset{(i)}{\leq} \kappa \sum_{i=1}^{n} \left[(\mathbf{X}^{\text{UOT}}\mathbf{1}_n)_i - a_i\right]^2 \\ &= \kappa \|\mathbf{X}^{\text{UOT}}\mathbf{1}_n - \mathbf{a}\|_2^2 \\ &\overset{(ii)}{\leq} \kappa \|\mathbf{X}^{\text{UOT}}\mathbf{1}_n - \mathbf{a}\|_1^2, \end{aligned} \tag{4}$$

where for (i), we use $a_i \geq \min\{a_{min}, b_{min}\} = \kappa^{-1}$, and for (ii), we use $\|\mathbf{x}\|_2 \leq \|\mathbf{x}\|_1$. Similarly, we obtain that:

$$0 \leq \mathbf{KL}\big((\mathbf{X}^{\text{UOT}})^\top \mathbf{1}_n \| \mathbf{b}\big) \leq \kappa \|(\mathbf{X}^{\text{UOT}})^\top \mathbf{1}_n - \mathbf{b}\|_1^2. \tag{5}$$

Summing up (4) and (5), we have:

$$\begin{aligned} 0 &\leq \mathbf{KL}(\mathbf{X}^{\text{UOT}}\mathbf{1}_n \| \mathbf{a}) + \mathbf{KL}\big((\mathbf{X}^{\text{UOT}})^\top \mathbf{1}_n \| \mathbf{b}\big) \\ &\leq \kappa \Big[\|\mathbf{X}^{\text{UOT}}\mathbf{1}_n - \mathbf{a}\|_1^2 + \|(\mathbf{X}^{\text{UOT}})^\top \mathbf{1}_n - \mathbf{b}\|_1^2 \Big] \\ &\leq \kappa \Big[\|\mathbf{X}^{\text{UOT}}\mathbf{1}_n - \mathbf{a}\|_1 + \|(\mathbf{X}^{\text{UOT}})^\top \mathbf{1}_n - \mathbf{b}\|_1 \Big]^2 \\ &\leq \kappa \Big(\frac{2n\|\mathbf{C}\|_\infty}{\tau} \Big)^2 = \frac{4\kappa n^2 \|\mathbf{C}\|_\infty^2}{\tau^2}, \end{aligned} \tag{6}$$

where the last inequality follows directly from [30, Theorem 23]. Now, from [30, Theorem 26] and given $M = \log(2)\|C\|_\infty^2 \big(n + 3\kappa\big)^2 + 2n\|C\|_\infty^2$, we have:

$$\begin{aligned} 0 \leq \mathbf{OT}(\mathbf{a}, \mathbf{b}) - \mathbf{UOT}(\mathbf{a}, \mathbf{b}) &\leq \frac{M}{\tau} \\ \therefore 0 \leq \langle \mathbf{C}, \mathbf{X}^{\text{OT}} \rangle - \langle \mathbf{C}, \mathbf{X}^{\text{UOT}} \rangle &- \tau \mathbf{KL}(\mathbf{X}^{\text{UOT}}\mathbf{1}_n \| \mathbf{a}) \\ - \tau \mathbf{KL}\big((\mathbf{X}^{\text{UOT}})^\top \mathbf{1}_n \| \mathbf{b}\big) &\leq \frac{M}{\tau}, \end{aligned} \tag{7}$$

where the last line is by definitions of $\mathbf{OT}(\mathbf{a}, \mathbf{b})$ and $\mathbf{UOT}(\mathbf{a}, \mathbf{b})$. Finally, combining (6) and (7), we can conclude the statement of the theorem:

$$0 \leq \langle \mathbf{C}, \mathbf{X}^{\text{OT}} \rangle - \langle \mathbf{C}, \mathbf{X}^{\text{UOT}} \rangle \leq \frac{M + 4\kappa n^2 \|\mathbf{C}\|_\infty^2}{\tau} = O\left(\frac{1}{\tau}\right).$$

■

1) Remark: Thereom 1 provides a bound on the difference between the transportation costs of OT solution and UOT solution under a balanced setting. Specifically, when the marginal distributions $\mathbf{a}$ and $\mathbf{b}$ are probability distributions both summing up to 1, the theorem establishes that the cost difference between the OT and UOT solutions grows inversely with τ, and thus can be made arbitrarily negligible by tuning the hyper-parameter $\tau > 0$ to be sufficiently large. This motivates our usage of UOT in place of OT for computational acceleration while maintaining the original performance of OT via the proper choice of τ in the next sections.

III. Experimental Results of UOT in Breast Cancer Data

Breast cancer is one of the most prevalent cancers worldwide, and accurately distinguishing between benign and malignant cases is crucial for early diagnosis and treatment. Machine learning methods have advanced breast cancer data analysis, but traditional approaches often struggle with computational efficiency and imbalanced data sets.

Optimal transport (OT) is a powerful tool for comparing probability distributions, yet assumes balanced datasets, which is rarely the case in real-world scenarios like breast cancer data. Unbalanced Optimal Transport (UOT) addresses this issue by allowing for differences in data mass, making it well-suited for medical datasets with uneven class distributions.

In [39], the authors proposed the Hungarian algorithm to solve a special type of optimal transport. It showed that Hungarian outperforms Sinkhorn algorithm and network simplex algorithm in all cases.

In this study, we apply UOT to breast cancer data to test for statistical independence between features of benign and malignant cases. By leveraging the efficiency of UOT combined with the Sinkhorn algorithm, we aim to provide a scalable method that outperforms traditional OT in runtime while maintaining accuracy, offering valuable insights for large-scale healthcare data analysis.

A. Problem Setting of UOT in Breast Cancer Data

1) Wasserstein-distance-based independence test and UOT: One crucial application of OT distances such as Wasserstein-1 [34], [20] is the independence test [39]. To assess the independence between the variables $Y \sim \nu_1$ and $Z \sim \nu_2$, the Wasserstein-1 distance with ℓ_p-norm cost function, which belongs to the class of OT problem [39], [20], between the joint distribution π of Y, Z and the product distribution of Y, Z is used. Specifically, this process requires the evaluation of $\mathbf{OT}(\pi, \nu_1 \otimes \nu_2)$, where $\nu_1 \otimes \nu_2$ represents the product distribution of Y, Z. It is proven in [39] that Y and Z are independent if and only if $\mathbf{OT}(\pi, \nu_1 \otimes \nu_2) = 0$. In practice, given n i.i.d. samples $\{(y_1, z_1), ..., (y_n, z_n)\}$ generated from (Y, Z), one can construct the statistic $\mathbf{OT}(\hat{\pi}, \hat{\nu}_1 \otimes \hat{\nu}_2)$, where $\hat{\pi}$ and $\hat{\nu}$ represent the empirical distributions, to test for independence. UOT distance has been known to well approximate OT distance with vanishing approximation error [30, Theorem 26], while enjoying more favorable computational complexity through various solvers vastly used in the ML/AI literature [35], [30], [5]. In this study, we aim to use UOT as an alternative to OT for Wasserstein-distance-based independence testing, and utilizes the celebrated Sinkhorn algorithm [35] to solve for the UOT problem.

2) Breast cancer data: The dataset consists of 569 instances, each characterized by 30 features. The instances are classified into two categories: benign and malignant. Let $X \in \mathbb{R}^{30}$ represent the distribution generated uniformly from the benign class, and $Y \in \mathbb{R}^{30}$ represent the distribution generated uniformly from the malignant class. We compute the empirical OT/UOT distance in two scenarios: 1. Independent case: Between X_1 and Y_2, where X_1 comprises the first 5 coordinates of X, and Y_2 comprises the last 25 coordinates of Y. 2. Dependent case: Between X and Z, where $Z = X_1 * Y_1$, with X_1 being the first 5 coordinates of X, Y_1 being the first 5 coordinates of Y, and $*$ representing the coordinatewise product.

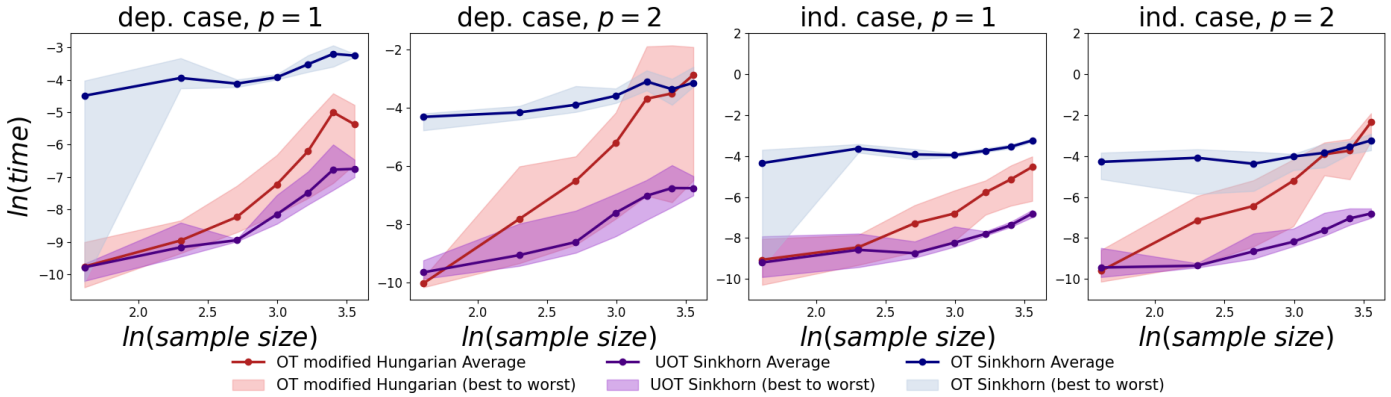


Fig. 1. Runtime evaluation with UOT sinkhorn, OT sinkhorn and modified hungarian algorithm on breast cancer data.

B. Application of UOT in Breast Cancer Data

1) Data preprocessing: In order to separate classes, the second column of the dataset contains the labels that classify each instance as either benign (B) or malignant (M). We use this column to separate the data into two subsets such that rows labeled 'B' and 'M' are extracted to form the X and Y dataset respectively.

From both X and Y, we focus on the feature values found in columns 2 to 32 (the 30 numerical features of each instance). These features are selected because they represent the main characteristics of the data relevant for classification.

The selected feature values are normalized by dividing each value by the maximum value in its respective column. This step rescales all feature components to the range [0, 1].

Normalization ensures that features with different scales do not disproportionately influence the analysis and that the data is suitable for OT/UOT computations.

2) Experimental setup: We follow the experimental setup outlined in [39], where the independence test based on Wasserstein distance is applied. In our experiments, we calculate the cost matrix $\mathbf{C}$ using the ℓ_p-norm as the cost function. Specifically, we evaluate the performance under two different norms: $p = 1$ and $p = 2$. These norms are chosen to assess the behavior of OT and UOT algorithms under different geometries of the data.

For both the dependent and independent cases, we vary the sample sizes of the breast cancer data to examine the effect of sample size ranging from small to large on the computational performance. In each experimental run, we generate data for both cases (dependent and independent) using uniformly distributed samples from the benign and malignant classes. The independence tests are then performed using UOT-based and OT-based methods.

Each experiment is repeated 10 times to account for random variations in the data and solvers. For each sample size and test, we report the following runtime statistics: the average, best, and worst runtimes over the 10 trials. This ensures a robust evaluation of the algorithm's performance and allows us to observe both the typical performance and the variability across runs.

Additionally, to evaluate the statistical significance of the results, we analyze the empirical distribution of the runtimes for each method and apply appropriate tests (e.g., t-tests) to confirm that the differences in runtimes between UOT Sinkhorn and the baseline methods are statistically significant.

3) Baselines: In our comparison, we include several state-of-the-art methods for solving OT problems as baselines. The first baseline is the exact OT solver based on the modified Hungarian algorithm [39]. The second baseline is the OT Sinkhorn algorithm [19], which approximates the OT distance by adding an entropic regularization term to the original OT problem.

Our proposed method uses the UOT Sinkhorn algorithm to approximate the OT distance under the UOT framework. UOT is particularly suitable for handling the unbalanced nature of distributions that may arise in real-world datasets like breast cancer data, where the number of benign and malignant cases might not be perfectly matched. The Sinkhorn solver adds entropic regularization, making it highly efficient for large-scale problems.

To ensure a fair comparison, we set the desired error tolerance for the approximate algorithms (UOT Sinkhorn and OT Sinkhorn) to 0.01. This tolerance provides a good balance between computational efficiency and approximation accuracy.

4) Experimental results: The results of our experiments, shown in Fig. 1, illustrate the runtime performance of the tested algorithms as a function of sample size. The x-axis represents the logarithm of the sample size, while the y-axis represents the logarithm of the total runtime in seconds. These log-log plots provide a clear visualization of the scalability of each algorithm.

For each tested sample size, UOT Sinkhorn consistently outperforms both OT-based baselines in terms of runtime. Specifically, UOT Sinkhorn achieves lower average, best, and worst runtimes across all sample sizes, with significant improvements as the sample size increases. The performance advantage of UOT Sinkhorn becomes especially pronounced for large sample sizes, where the modified Hungarian algorithm exhibits much slower runtimes due to its higher computational complexity.

In terms of robustness, UOT Sinkhorn demonstrates consis-

tent performance, where even its worst runtime remains faster than the average runtime of the second-best baseline, OT solved using the modified Hungarian algorithm. This robustness is a crucial factor for practical applications where runtime variability can impact the reliability of the method. Additionally, OT Sinkhorn performs better than the exact solver for moderate sample sizes but is still outperformed by UOT Sinkhorn in most cases.

Finally, we also observe that the choice of ℓ_p-norm ($p = 1$ or $p = 2$) has a relatively minor effect on the runtime but does influence the accuracy of the independence test, as the distance metrics capture different aspects of the data geometry.

IV. UOT in HRV Estimation for Physiological Research

In physiological research, Heart Rate Variability (HRV) is often used as a measure for its reliability and noninvasiveness [1]. However, assessing cardiovascular functioning using HRV in practice is challenging due to noise and irregularly sampled data.

Previously, [42] proposed a multitask-learning approach to address this issue. However, clinical and healthcare data in practice often have a high degree of heterogeneity (such as in demographics, treatments, devices, etc), which means domain generalization is an essential task. Thus, [42] proposes to use OT to estimate a mapping that is generalizable for unseen out-of-domain task distributions. The multitask model using Optimal Transport as a regularizer showed the lowest RMSE amongst other transport maps such as Group Lasso [40], Multi-level Lasso [22], Dirty models [13], Multitask Wasserstein and Reweighted Multi-task Wasserstein [14].

However, the stringent nature of OT maps may cause strict mapping, which would be problematic under noisy data regimes [2], [17]. Thus, we propose using UOT instead of OT for the domain generalization task.

A. OT/UOT Map Estimation for Physio Multitask-learning

Consider the task-wise feature vectors S_t and their underlying predictive functions W_t^T, each following the measures μ_S and ν_W respectively. Our goal is to find a push forward mapping $T_{\#}\mu_S = \nu_W$. Here, one can estimate μ_S, ν_W from the empirical distributions, and use them as the two input marginal vectors of the OT/UOT problem. The optimal mapping allows us to measure the similarity of model parameters to obtain a predictive transformation, which will eventually be used to perform domain generalization.

B. Multitask-learning (MTL)

We follow the MTL formulation in [42] and use the following optimization objective, where the first term represents the prediction loss and the second term represents the regularization that induces task similarities:

1) Dataset: We are given a set of T tasks, each represented by:

- $X_t \in \mathbb{R}^{d_x \times N_t}$: The feature matrix for task t, where N_t is the number of samples for task t, and each sample has d_x features.
- $Y_t \in \mathbb{R}^{1 \times N_t}$: The labels for the samples in task t.
- $s_t \in \mathbb{R}^{d_s \times 1}$: A task-specific feature vector, which may contain information unique to that task.

2) Objective: We are learning the parameters, represented by the matrix W_t, for each task t, where each W_t is part of a larger matrix $W \in \mathbb{R}^{T \times d_w}$ that contains the weight vectors for all T tasks. The goal is to minimize the loss across all tasks, represented as:

$$\min_{\mathbf{W},\mathbf{F}} \underbrace{\frac{1}{2}\sum_{t=1}^{T} \|W_t^T X_t - y_t\|_2^2}_{\text{Prediction loss}} + \underbrace{\alpha \sum_{i,j=1}^{T} \pi_{i,j}^* \|F(s_i) - W_j\|_2^2}_{\text{Regularization term}}. \quad (1)$$

Here, $\mathbf{W} = [W_1, W_2, \ldots, W_T]$ are the task-specific weights, and $\mathbf{F}$ is the transformation that models the similarities between different tasks, π^* is the OT/UOT coupling obtained from the Sinkhorn-OT/Sinkhorn-UOT algorithm and α is a weighting parameter. The loss (1) will learn $\mathbf{W}$ and $\mathbf{F}$ using Algorithm 1 in [42] where $\mathbf{W}$ and $\mathbf{F}$ are jointly updated using GD.

C. Linear and Non-linear Transformation for $\boldsymbol{F}$

First, we consider $\mathcal{F}$ being a linear transformation, where the set $\mathcal{F}$ is characterized by a matrix $\mathbf{F} \in \mathbb{R}^{d_s \times d_\theta}$, which captures all affine transformations. Mathematically, the set $\mathcal{F}$ is expressed as:

$$\mathcal{F} = \left\{ F : \mathbf{F} \in \mathbb{R}^{d_\theta \times d_s},\ s_t \in \Omega_S,\ F(s_t) = \mathbf{F} s_t \right\}.$$

However, linear transformations may not sufficiently approximate the transport map, particularly for modeling complex systems such as the human Autonomic Nervous System (ANS). To address this, non-linear transformations is considered.

Let ϕ be a non-linear function associated with a kernel function $k : \Omega_S \times \Omega_S \to \mathbb{R}$, where $k(s_i, s_j) = \langle \phi(s_i), \phi(s_j) \rangle$. For a given set of samples S, we define the set $\mathcal{F}$ as:

$$\mathcal{F} = \left\{ F : \mathbf{F} \in \mathbb{R}^{d_\theta \times T},\ s_t \in \Omega_S,\ F(s_t) = \mathbf{F}\mathbf{k}_{s_t}(s_t) \right\},$$

where $\mathbf{k}_{s_t}(\cdot)$ denotes the vector $k(s_1, \cdot), \ldots, k(s_T, \cdot)$.

The non-linear transformation allows the model to capture more intricate relationships between tasks, making it particularly useful when task dependencies are complex and cannot be adequately captured by a linear mapping. The challenge in this formulation lies in the increased complexity of learning $\mathbf{F}$, as the optimization problem becomes non-convex and may require advanced techniques such as back-propagation for training.

Despite the increased computational cost, non-linear transformations can significantly improve performance in multitask learning scenarios where tasks exhibit non-linear similarities, enabling the model to generalize better accros tasks.

D. Gradient Descent for MTL

To apply Gradient Descent (GD) to solve the MTL objective, we first differentiate the loss function with respect to the MTL parameters $\mathbf{W}$ and $\mathbf{F}$ is a non-linear transformation. Given the optimization objective from Eq. (1), the gradients with respect to the MTL parameters $\mathbf{W}$ and $\mathbf{F}$ are:

Gradient with respect to W:

$$\nabla_{\mathbf{W}}\mathcal{L} = (W_j^T X_j - y_j)X_j^T - 2\alpha \sum_i \pi^*_{i,j}(\mathbf{F}\mathbf{k}_{s_i} - W_j).$$

The first term corresponds to the gradient of the prediction loss, while the second term reflects the gradient of the regularization term, weighted by α and the optimal coupling matrix π^* obtained from OT/UOT.

Gradient with respect to F:

$$\nabla_{\mathbf{F}}\mathcal{L} = 2\alpha \sum_{i,j} \pi^*_{i,j}(\mathbf{F}\mathbf{k}_{s_i} - W_j)\mathbf{k}_{s_i}^T.$$

Here, the gradient is driven solely by the regularization term, as **F** does not appear in the prediction loss.

PhysioMTL using gradient descent has a disadvantage when processing complex data such as HRV where it confronts multiple local minimums which will affect learning rate. To address the problem, we introduce the gradient descent with momentum, a more robust version of gradient descent which can potentially handle local minimums and saddle points.

Using the gradients proposed above, we iteratively update the parameters **W** and **F** using the standard GD update rule:

$$\mathbf{W}^{(k+1)} = \mathbf{W}^{(k)} - \eta\nabla_{\mathbf{W}}\mathcal{L}, \quad \mathbf{F}^{(k+1)} = \mathbf{F}^{(k)} - \eta\nabla_{\mathbf{F}}\mathcal{L}$$

where η is the learning rate and k denotes the iteration index.

So, the update rules using gradient descent for $\mathbf{W}_j$ and **F** are:

For $\mathbf{W}_j$:

$$\mathbf{W}_j \leftarrow \mathbf{W}_j - \eta\left[(W_j^T X_j - y_j)X_j^T - 2\alpha \sum_i \pi^*_{i,j}(\mathbf{F}\mathbf{k}_{s_i} - W_j)\right].$$

For F:

$$\mathbf{F} \leftarrow \mathbf{F} - \eta\left[2\alpha \sum_{i,j} \pi^*_{i,j}(\mathbf{F}\mathbf{k}_{s_i} - W_j)\mathbf{k}_{s_i}^T\right].$$

Algorithm 1 Solving MTL: Gradient Descent

Input: η, α, $\{\pi^*_{i,j}\}$, $\{X_t, y_t\}_{t=1}^T$, $\{\mathbf{k}_{s_i}\}$, $\mathbf{W}_j$, **F**
for $n = 1$ to N **do**
  for $j = 1$ to T **do**
    $\mathbf{W}_j \leftarrow \mathbf{W}_j - \eta\nabla_{W_j}$
  end for
  $\nabla_F = 2\alpha \sum_{i,j} \pi^*_{i,j}(\mathbf{F}\mathbf{k}_{s_i} - W_j)\mathbf{k}_{s_i}^T$
  $\mathbf{F} \leftarrow \mathbf{F} - \eta\nabla_F$
end for
Output: $\mathbf{W}_j$, **F**

In practice, choosing an appropriate learning rate η is critical for convergence. A small learning rate can slow down the convergence, while a large one might cause the updates to overshoot the optimal solution. The iterative GD process continues until convergence, which is typically defined by a threshold on the change in the loss function or the norm of the gradient.

E. Gradient Descent with Momentum for MTL

In gradient descent with momentum, we introduce a velocity term to accelerate the optimization process. The update rules are modified to include momentum, where the gradient is accumulated over time.

Let $\mathbf{v}_W$ and $\mathbf{v}_F$ be the velocity terms for $\mathbf{W}_j$ and **F**, respectively. The momentum update is controlled by a parameter $\beta \in [0, 1)$. The update rules for the velocities and parameters are as follows:

Velocity update:

$$\mathbf{v}_W^{(k+1)} = \beta\mathbf{v}_W^{(k)} + (1-\beta)\nabla_{\mathbf{W}}\mathcal{L}, \quad \mathbf{v}_F^{(k+1)} = \beta\mathbf{v}_F^{(k)} + (1-\beta)\nabla_{\mathbf{F}}\mathcal{L}$$

Parameter update:

$$\mathbf{W}^{(k+1)} = \mathbf{W}^{(k)} - \eta\mathbf{v}_W^{(k+1)}, \quad \mathbf{F}^{(k+1)} = \mathbf{F}^{(k)} - \eta\mathbf{v}_F^{(k+1)}$$

Algorithm 2 Solving MTL: Gradient Descent with Momentum

Input: η, β, α, $\{\pi^*_{i,j}\}$, $\{X_t, y_t\}_{t=1}^T$, $\{\mathbf{k}_{s_i}\}$, $\mathbf{W}_j$, **F**
$\mathbf{v}_{W_j} = 0$, $\mathbf{v}_F = 0$
for $n = 1$ to N **do**
  for $j = 1$ to T **do**
    $\mathbf{v}_{W_j} \leftarrow \beta\mathbf{v}_{W_j} + (1-\beta)\nabla_{W_j}$
    $\mathbf{W}_j \leftarrow \mathbf{W}_j - \eta\mathbf{v}_{W_j}$
  end for
  $\nabla_F = 2\alpha \sum_{i,j} \pi^*_{i,j}(\mathbf{F}\mathbf{k}_{s_i} - W_j)\mathbf{k}_{s_i}^T$
  $\mathbf{v}_F \leftarrow \beta\mathbf{v}_F + (1-\beta)\nabla_F$
  $\mathbf{F} \leftarrow \mathbf{F} - \eta\mathbf{v}_F$
end for
Output: $\mathbf{W}_j$, **F**

F. Literature and Motivation for Gradient Descent with Momentum for MTL

Momentum helps to speed up convergence in scenarios where the optimization landscape has long, narrow valleys—common in deep learning and multitask-learning. The velocity terms accumulate the gradients in such valleys, allowing the optimization to move faster along the flat directions and more slowly in directions where the gradients change rapidly.

1) Escaping saddle points: One of the key advantages of GDM is its ability to help the optimization process escape saddle points. Saddle points are regions in the loss surface where the gradient is close to zero but the point is not a local minimum. By incorporating past gradients, GDM can provide sufficient momentum to push the optimization out of these regions, avoiding the problem of getting stuck at suboptimal points. This is particularly important for multitask-learning, where the complex interaction between tasks may introduce non-convexities in the loss surface.

2) Convergence considerations: While GDM generally converges faster than standard GD, careful tuning of both the learning rate η and the momentum parameter β is essential for achieving optimal performance. A typical heuristic is to start with $\beta = 0.9$ and adjust η based on empirical results, ensuring that the updates do not become too aggressive or oscillatory.

In the MTL context, GDM is particularly useful when dealing with heterogeneous tasks, as the added momentum helps

TABLE I. SUMMARY OF MODEL PERFORMANCES WITH $\alpha = 0.1$.UOT-GD AND UOT-GDM SHOW LOWER RMSE AND FASTER RUNTIMES COMPARED TO OT-BASED METHODS, WITH MOMENTUM FURTHER REDUCING RUNTIME

Method	20%		40%		60%		80%	
	RMSE	Runtime	RMSE	Runtime	RMSE	Runtime	RMSE	Runtime
OT-GD	29.992 ± 0.809	0.514	29.890 ± 1.198	1.219	29.504 ± 0.963	3.347	28.800 ± 2.432	6.765
UOT-GD	29.978 ± 0.843	0.287	29.911 ± 1.222	0.534	29.500 ± 0.942	1.032	28.749 ± 2.455	2.072
OT-GDM	30.070 ± 0.749	0.291	29.940 ± 1.206	0.641	29.584 ± 0.990	1.154	28.897 ± 2.394	3.190
UOT-GDM	30.013 ± 0.794	0.244	29.891 ± 1.203	0.372	29.521 ± 0.965	0.874	28.845 ± 2.420	1.603

TABLE II. SUMMARY OF MODEL PERFORMANCES WITH $\alpha = 0.5$. UOT MAINTAINS CONSISTENT RMSE AND FASTER RUNTIMES ACROSS SAMPLE SIZES, WHILE OT METHODS SHOW SLIGHTLY HIGHER RMSE AND SLOWER PERFORMANCE

Method	20%		40%		60%		80%	
	RMSE	Runtime	RMSE	Runtime	RMSE	Runtime	RMSE	Runtime
OT-GD	30.753 ± 1.536	0.290	29.841 ± 0.924	1.480	29.364 ± 1.692	4.448	30.282 ± 2.218	7.974
UOT-GD	30.779 ± 1.549	0.163	29.748 ± 0.967	0.684	29.298 ± 1.703	1.383	30.151 ± 2.259	2.550
OT-GDM	30.769 ± 1.574	0.286	29.934 ± 0.942	1.012	29.461 ± 1.671	2.197	30.459 ± 2.207	3.584
UOT-GDM	30.759 ± 1.529	0.154	29.883 ± 0.926	0.459	29.388 ± 1.696	0.888	30.336 ± 2.218	1.786

TABLE III. SUMMARY OF MODEL PERFORMANCES WITH $\alpha = 0.9$. UOT STILL PERFORMS BETTER THAN OT METHODS IN TERMS OF RMSE AND RUNTIME, WITH MOMENTUM (UOT-GDM) ENSURING THE FASTEST CONVERGENCE, EVEN WITH A LARGER α

Method	20%		40%		60%		80%	
	RMSE	Runtime	RMSE	Runtime	RMSE	Runtime	RMSE	Runtime
OT-GD	30.366 ± 0.812	0.338	30.025 ± 1.370	1.833	30.352 ± 1.240	4.106	30.783 ± 2.393	6.660
UOT-GD	30.291 ± 0.821	0.197	29.996 ± 1.377	0.657	30.232 ± 1.265	1.289	30.718 ± 2.394	2.314
OT-GDM	30.491 ± 0.830	0.274	30.144 ± 1.417	0.896	30.491 ± 1.236	2.049	30.881 ± 2.436	3.584
UOT-GDM	30.395 ± 0.812	0.156	30.046 ± 1.388	0.450	30.399 ± 1.237	0.831	30.823 ± 2.409	1.362

balance the convergence rates across tasks with varying levels of difficulty. The accumulated gradients guide the optimization process toward a more stable solution, reducing the likelihood of overfitting to specific tasks.

By applying GDM, we can achieve a more efficient and reliable solution to the MTL problem, especially in the context of large-scale data or noisy, heterogeneous domains such as HRV estimation.

G. Application of UOT in HRV

1) Data preprocessing: The MMASH dataset [37] contains 24-hour continuous data from 22 healthy male participants, including inter-beat intervals (IBI), wrist accelerometry, sleep duration and quality, physical activity levels, and psychological factors like stress, anxiety, and emotions. HRV is calculated using RMSSD, the root mean square of successive differences between normal heartbeats, over 5-minute intervals, which is the standard duration for short-term HRV analysis. We use key features - activity, sleep, stress, and anthropometric data (age, height, weight). Sleep is expressed as total hours in bed, while physical activity is represented by hours of moderate (e.g. walking, cycling) and intense (e.g., running, gym) exercise. Stress levels are measured via the Daily Stress Inventory (DSI) score.

We following the data preprocessing procedure in [42]: (1) removing RMSSD outliers (z-score greater than 2.5), (2) excluding subjects with abnormal data (e.g. subject 4 with an RMSSD average of 318), and (3) imputing missing values for sleep and age for subjects 11 and 18 using dataset-wide averages. After preprocessing, the final dataset includes 21 subjects.

2) Experimental setup: We applied our model to predict Heart Rate Variability (HRV) across various tasks from the MMASH dataset, which is publicly available through the PhysioNet repository [37]. The tasks used for testing were completely unseen during training to ensure a rigorous evaluation. The performance of the model was measured using Root Mean Square Error (RMSE) to quantify the prediction accuracy. To assess the model's performance under different data availability scenarios, we randomly selected varying proportions of tasks—specifically, 20%, 40%, 60%, and 80%—for training. The model was then evaluated on the remaining unseen tasks.

Additionally, we experimented with different values of $\alpha = 0.1, 0.5, 0.9$ to investigate the robustness of the Sinkhorn-Unbalanced Optimal Transport (Sinkhorn-UOT) model under different mass relaxation parameters. Varying α allows us to explore how the model behaves when placing more or less emphasis on balancing the transport plan, offering insights into the flexibility and adaptability of the method.

3) Baselines: To further improve computational efficiency, we implemented Gradient Descent with Momentum (GDM), which is known to help iterates quickly escape saddle points and accelerate convergence to a stationary point, as suggested by [38]. This technique is particularly valuable for large-scale datasets where faster convergence can significantly reduce runtime. We compared four experimental settings to evaluate both OT and UOT under different optimization strategies: OT with Gradient Descent (OT-GD), OT with Gradient Descent and Momentum (OT-GDM), UOT with Gradient Descent (UOT-GD), and UOT with Gradient Descent and Momentum (UOT-GDM). These baselines allowed us to assess both the impact of mass relaxation in UOT and the computational benefits of incorporating momentum into the optimization process.

4) Experimental results: The results of our experiments are summarized in Tables I, II, and III, corresponding to $\alpha = 0.1$, $\alpha = 0.5$, and $\alpha = 0.9$ respectively. Across all α values, our UOT-based approaches consistently demonstrated significantly lower runtime compared to the OT-based methods, while maintaining similar levels of accuracy as measured by RMSE. This highlights the computational advantage of UOT, particularly for large datasets with imbalanced distributions. Additionally, the inclusion of momentum in the optimization process (GDM) resulted in faster convergence and further reduced runtime compared to standard Gradient Descent (GD), confirming the effectiveness of GDM in accelerating training. These findings underline the practicality of using UOT with momentum for tasks requiring fast and accurate predictions in complex datasets.

5) Results and Discussion: The experimental results summarized in Tables I, II, and III demonstrate the consistent advantages of UOT over OT across all tested values of α (0.1, 0.5, 0.9). While runtime differences were significant—UOT required up to 40% less time than OT—the benefits of UOT extend beyond computational efficiency.

Additionally, the inclusion of momentum in UOT further accelerated convergence while maintaining similar accuracy. This enhancement is particularly valuable in iterative medical research tasks, where faster training enables rapid model updates based on new data.

H. Summary of UOT Algorithms as Compared to OT and Related Practical Healthcare Applications

By relaxing OT's strict constraints, UOT enables faster and more adaptable multitask learning algorithms. Its computational advantages $\tilde{O}\left(n^2\varepsilon^{-1}\right)$ and smoother optimization dynamics make it a competitive alternative to OT, especially in healthcare applications requiring efficient and reliable predictions. Coupled with techniques like GDM, UOT further enhances its utility for large-scale, real-world datasets, demonstrating its practicality in domains where computational resources are limited but accuracy remains paramount.

The advantages of UOT algorithms, particularly their computational efficiency and adaptability, make them highly suitable for resource-constrained healthcare applications:

1) Real-Time HRV Monitoring: Faster convergence of UOT allows real-time heart rate variability predictions in wearable devices, enabling timely interventions in critical scenarios.

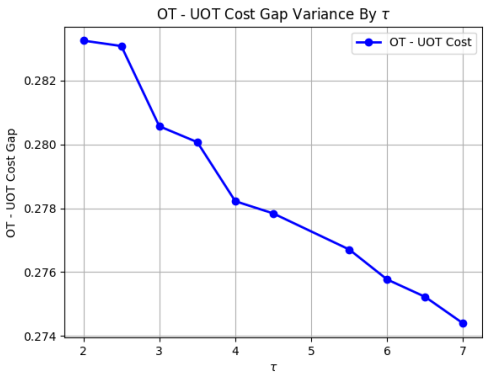


Fig. 2. Cost gap on breast cancer data.

2) Large-Scale Population Studies: UOT's scalability supports applications involving population-level diagnostics, such as analyzing longitudinal health data or predicting patient outcomes across diverse demographics.

3) Personalized Medicine: The flexibility of UOT in handling imbalanced distributions is crucial for personalized medicine, where data from some patient subgroups may be underrepresented. For example, drug response predictions can benefit from UOT's ability to align heterogeneous task distributions effectively. asks, as reflected in the lower Root Mean Square Error (RMSE) observed for UOT.

V. Aprroximation Error

In the context of the breast cancer data experiment, we aim to empirically validate the theorem 1. Specifically, we are interested in investigating how closely the UOT cost approximates the OT cost in real-world datasets, which will be done in the following set up:

1) Computing OT and UOT cost: Using the Sinkhorn algorithm, we compute the OT transport plan $\mathbf{X}^{OT}$ and its corresponding transport cost. Similarly, we compute the UOT transport plan $\mathbf{X}^{UOT}$ for varying values of τ (the regularization parameter) and calculate the associated UOT cost.

2) Comparison and Validation of Approximation Error: We empirically measure this difference to see how well UOT approximates OT in our breast cancer dataset. Specifically, we calculate $\langle \mathbf{C}, \mathbf{X}^{OT} \rangle - \langle \mathbf{C}, \mathbf{X}^{UOT} \rangle$ for different values of τ to observe whether the theoretical bound holds in practice.

3) Experimental result: The results shown in Fig. 2 as τ increases, the cost gap steadily decreases. This demonstrates that with higher regularization, the difference between the UOT and OT solutions becomes negligible. At this point, UOT provides a good approximation to the OT cost while retaining computational advantages. The graph exhibits a smooth, nonlinear decrease in the cost gap, implying that increasing τ provides diminishing returns in terms of cost difference.

VI. Conclusion and Future Works

In this work, we investigate the computational benefits of the Sinkhorn-UOT algorithm across different healthcare applications such as the independence test on breast cancer

data and HRV estimation in physiological research. We find that Sinkhorn-UOT consistently outperforms other popular computational OT methods such as Sinkhorn-OT and the modified Hungarian algorithm, which partially makes various healthcare applications more accessible to budget-constraint medical institutes by alleviating the prohibitive computational cost, and mitigates the CO2 emission from computing resources toward better environment.

Building on these results, future work should focus on further optimizing the Sinkhorn-UOT algorithm by reducing the computational complexity and enhancing scalability for even larger datasets. Another interesting direction is to investigate the effectiveness of Partial Optimal Transport (POT) [24] as an alternative to OT, besides the UOT metric considered in this paper. Furthermore, Stochastic or Constrained Decentralized Optimization techniques [25], [26] can be leveraged to create sample-efficient computational approaches for noisy, dynamic, and multi-agent scenarios [9], [28], [32], [31], [33] that commonly emerge in modern distributed systems [27], [29].

ACKNOWLEDGMENT

This project was supported by VietDynamic and Binh Duong University. In addition, the authors extend profound gratitude to Mr. Quang Minh Nguyen, Mr. Hoang Huy Nguyen, Ms. My Ngoc Tran Le, and Mr. Nhat Minh Phung for their invaluable guidance and supervision throughout this research endeavor.

REFERENCES

[1] U. Acharya, Paul Joseph, Natarajan Kannathal, Choo Lim, and Jasjit Suri. Heart rate variability: A review. *Medical & biological engineering & computing*, 44:1031–51, 01 2007.

[2] Yogesh Balaji, Rama Chellappa, and Soheil Feizi. Robust optimal transport with applications in generative modeling and domain adaptation. *Advances in Neural Information Processing Systems*, 33:12934–12944, 2020.

[3] Mathieu Blondel, Vivien Seguy, and Antoine Rolet. Smooth and sparse optimal transport, 2018.

[4] Luis A. Caffarelli and Robert J. McCann. Free boundaries in optimal transport and monge-ampère obstacle problems. *Annals of Mathematics*, 171(2):673–730, 2010.

[5] Laetitia Chapel, Rémi Flamary, Haoran Wu, Cédric Févotte, and Gilles Gasso. Unbalanced optimal transport through non-negative penalized linear regression. In A. Beygelzimer, Y. Dauphin, P. Liang, and J. Wortman Vaughan, editors, *Advances in Neural Information Processing Systems*, 2021.

[6] Lenaic Chizat, Gabriel Peyré, Bernhard Schmitzer, and François-Xavier Vialard. Scaling algorithms for unbalanced optimal transport problems. *Mathematics of Computation*, 87(314):2563–2609, 2018.

[7] N. Courty, R. Flamary, D. Tuia, and A. Rakotomamonjy. Optimal transport for domain adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 39(9):1853–1865, 2017.

[8] Alejandro Deniz-Garcia, Himar Fabelo, Antonio J Rodriguez-Almeida, Garlene Zamora-Zamorano, Maria Castro-Fernandez, Maria Del Pino Alberiche Ruano, Terje Solvoll, Conceição Granja, Thomas Roger Schopf, Gustavo M Callico, Cristina Soguero-Ruiz, Ana M Wägner, and WARIFA Consortium. Quality, usability, and effectiveness of mhealth apps and the role of artificial intelligence: Current scenario and challenges. *J Med Internet Res*, 25:e44030, May 2023.

[9] Minh Ngoc Dinh and Quang Minh Nguyen. Measurements of errors in large-scale computational simulations at runtime. In *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, pages 1–7, 2020.

[10] S.S. Dragomir, M.L. Scholz, and J. Sunde. Some upper bounds for relative entropy and applications. *Computers & Mathematics with Applications*, 39(9):91–100, 2000.

[11] Charlie Frogner, Chiyuan Zhang, Hossein Mobahi, Mauricio Araya, and Tomaso A Poggio. Learning with a wasserstein loss. In *Advances in Neural Information Processing Systems*, pages 2053–2061, 2015.

[12] Aude Genevay, Gabriel Peyre, and Marco Cuturi. Learning generative models with sinkhorn divergences. In *International Conference on Artificial Intelligence and Statistics*, pages 1608–1617, 2018.

[13] Ali Jalali, Sujay Sanghavi, Chao Ruan, and Pradeep Ravikumar. A dirty model for multi-task learning. In J. Lafferty, C. Williams, J. Shawe-Taylor, R. Zemel, and A. Culotta, editors, *Advances in Neural Information Processing Systems*, volume 23. Curran Associates, Inc., 2010.

[14] Hicham Janati, Marco Cuturi, and Alexandre Gramfort. Wasserstein regularization for sparse multi-task regression. In Kamalika Chaudhuri and Masashi Sugiyama, editors, *Proceedings of the Twenty-Second International Conference on Artificial Intelligence and Statistics*, volume 89 of *Proceedings of Machine Learning Research*, pages 1407–1416. PMLR, 16–18 Apr 2019.

[15] L. V. Kantorovich. On the translocation of masses. In *Dokl. Akad. Nauk. USSR (NS)*, volume 37, pages 199–201, 1942.

[16] Loïc Lannelongue, Jason Grealey, Alex Bateman, and Michael Inouye. Ten simple rules to make your computing more environmentally sustainable. *PLoS Comput Biol*, 17(9):e1009324, September 2021.

[17] Khang Le, Huy Nguyen, Quang Nguyen, Tung Pham, Hung Bui, and Nhat Ho. On robust optimal transport: Computational complexity and barycenter computation. arXiv, 2021.

[18] John Lee, Nicholas P Bertrand, and Christopher J Rozell. Parallel unbalanced optimal transport regularization for large scale imaging problems. *arXiv preprint arXiv:1909.00149*, 2019.

[19] Tianyi Lin, Nhat Ho, and Michael I. Jordan. On the efficiency of entropic regularized algorithms for optimal transport. *Journal of Machine Learning Research*, 23(137):1–42, 2022.

[20] Jialin Liu, Wotao Yin, Wuchen Li, and Yat Tin Chow. Multilevel optimal transport: a fast approximation of wasserstein-1 distances, 2019.

[21] Weijie Liu, Chao Zhang, Nenggan Zheng, and Hui Qian. Approximating optimal transport via low-rank and sparse factorization. *ArXiv*, abs/2111.06546, 2021.

[22] Aurélie C. Lozano and Grzegorz Swirszcz. Multi-level lasso for sparse multi-task regression. In *International Conference on Machine Learning*, 2012.

[23] G Monge. *Mémoire sur la théorie des déblais et des remblais*. 1781.

[24] Anh Duc Nguyen, Tuan Dung Nguyen, Quang Minh Nguyen, Hoang H. Nguyen, Lam M. Nguyen, and Kim-Chuan Toh. On partial optimal transport: Revising the infeasibility of sinkhorn and efficient gradient methods, 2023.

[25] Hoang Huy Nguyen, Yan Li, and Tuo Zhao. Stochastic constrained decentralized optimization for machine learning with fewer data oracles: a gradient sliding approach, 2024.

[26] Hoang Huy Nguyen and Siva Theja Maguluri. Stochastic Approximation for Nonlinear Discrete Stochastic Control: Finite-Sample Bounds. 2023.

[27] Minh Nguyen, Dumitrel Loghin, and Tien Tuan Anh Dinh. Understanding the scalability of hyperledger fabric. *ArXiv*, abs/2107.09886, 2021.

[28] Quang Minh Nguyen, Haewon Jeong, and Pulkit Grover. Coded qr decomposition. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 191–196, 2020.

[29] Quang Minh Nguyen, Nhan Khanh Le, and Lam M. Nguyen. Scalable and secure federated xgboost. In *ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1–5, 2023.

[30] Quang Minh Nguyen, Hoang H. Nguyen, Yi Zhou, and Lam M. Nguyen. On unbalanced optimal transport: Gradient methods, sparsity and approximation error. *Journal of Machine Learning Research*, 24(384):1–41, 2023.

[31] Quang Minh Nguyen, Lam M. Nguyen, and Subhro Das. Correlated attention in transformers for multivariate time series, 2023.

[32] Quang Minh Nguyen, Iain Weissburg, and Haewon Jeong. Coded computing for fault-tolerant parallel qr decomposition, 2023.

[33] Khuong Nguyen-Vinh, Quang-Nguyen Vo-Huynh, Khoa Nguyen-Minh, Minh Hoang, and Surender Rangaraju. *Case Study: Utilising of Deep Learning Models for Fault Detection and Diagnosis of Photovoltaic Modules to Improve Solar Energy Constructions' O&M Activities Quality*, pages 53–67. Springer Nature Singapore, Singapore, 2024.

[34] Gabriel Peyré and Marco Cuturi. Computational optimal transport. *Foundations and Trends® in Machine Learning*, 11(5-6):355–607, 2019.

[35] K. Pham, K. Le, N. Ho, T. Pham, and H. Bui. On unbalanced optimal transport: An analysis of sinkhorn algorithm. In *ICML*, 2020.

[36] Claudia A Rhoades, Brian E Whitacre, and Alison F Davis. Higher electronic health record functionality is associated with lower operating costs in urban-but not Rural-Hospitals. *Appl Clin Inform*, 13(3):665–676, July 2022.

[37] Alessio Rossi, Eleonora Da Pozzo, Dario Menicagli, Chiara Tremolanti, Corrado Priami, Alina Sîrbu, David A. Clifton, Claudia Martini, and Davide Morelli. A public dataset of 24-h multi-levels psycho-physiological responses in young healthy adults. *Data*, 5(4), 2020.

[38] Jun-Kun Wang, Chi-Heng Lin, and Jacob Abernethy. Escaping saddle points faster with stochastic momentum, 2021.

[39] Yiling Xie, Yiling Luo, and Xiaoming Huo. Solving a special type of optimal transport problem by a modified hungarian algorithm, 2023.

[40] Ming Yuan and Yi Lin. Model selection and estimation in regression with grouped variables. *Journal of the Royal Statistical Society Series B: Statistical Methodology*, 68(1):49–67, 12 2005.

[41] Kevin Zhang, Junhao Zhu, Dehan Kong, and Zhaolei Zhang. Modeling single cell trajectory using forward-backward stochastic differential equations. *PLoS Comput Biol*, 20(4):e1012015, April 2024.

[42] Jiacheng Zhu, Gregory Darnell, Agni Kumar, Ding Zhao, Bo Li, Xuanlong Nguyen, and Shirley You Ren. Physiomtl: Personalizing physiological patterns using optimal transport multi-task regression. In Gerardo Flores, George H Chen, Tom Pollard, Joyce C Ho, and Tristan Naumann, editors, *Proceedings of the Conference on Health, Inference, and Learning*, volume 174 of *Proceedings of Machine Learning Research*, pages 354–374. PMLR, 07–08 Apr 2022.

Fuzzy Logic-Driven Machine Learning Algorithms for Improved Early Disease Diagnosis

Leena Arya[1], Narasimha Swamy Lavudiya[2], G Sateesh[3], Harish Padmanaban[4], Dr. B. V. Srinivasulu[5], Ravi Rastogi[6]
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, AP, India[1, 2, 3]
Site Reliability and Software Engineering Professional, Investment Banking, Houston, Texas, USA[4]
VIGNAN's Institute of Technology and Sciences (Affiliated to JNTU), Deshmukhi, Hyderabad, Telangana[5]
Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, AP, India[6]

***Abstract*—Early disease diagnosis is critical in improving patient outcomes, reducing healthcare costs, and preferably timely intervention. Unfortunately, the algorithms used in conventional diagnostic technology have difficulties dealing with uncertain and imprecise medical data, which may result in either delay or misdiagnosis. This paper describes the combined framework of fuzzy logic and machine learning algorithms to improve the accuracy and reliability of early disease diagnosis. Fuzzy logic addresses imprecision in patient symptoms and variability in clinical data, while machine learning algorithms provide data analytical and predictive capabilities. The proposed system enhances the abilities and complements rule-based reasoning with a predictive model to handle imprecise inputs and deliver accurate disease risk estimation. An experimental analysis of the medical datasets of heart disease, diabetes, and cancer reveals that the proposed method enhances the accuracy, precision, and ultimately robustness of a conventional diagnostic system.**

Keywords*—Decision trees; Fuzzy Inference System (FIS); heart disease diagnosis; neural networks; Support Vector Machine (SVM)

I. INTRODUCTION

Early disease diagnosis is a vital component of patients' care as it enhances timely detection and treatment procedures and reduces the worsening of diseases. As technology progresses, artificial intelligence (AI) and machine learning (ML) programs have been quite helpful to the diagnostic process, especially when traditional methods encounter limitations due to partial or uncertain data. Also, Fuzzy logic provides a framework for modeling uncertainty and handling ambiguous or imprecise data, which is very common in medical diagnostics. Using fuzzy logic and machine learning together, it is possible to combine intelligent diagnostic systems to process complex medical data more thoughtfully and interpretably [1-3].

Diagnosis in the medical field means working with incomplete and noisy data, where the symptoms of the diseases are interchangeable in most cases since it is not unlikely to have two different diseases manifesting in the same symptoms; the data is subjective and sometimes uncertain. Traditional machine learning algorithms for structured data cannot efficiently manage vague clinical data. This issue is solved by fuzzy logic since members in a given category have only partial membership in multiple diagnostic categories, thus, a perfect coupling to machine learning methods used in the medical field. For instance, fuzzy logic systems have been successfully applied in systems, especially for diagnosing diseases such as diabetes, cardiovascular conditions, and cancer [4, 5].

The fuzzy logic-oriented machine learning algorithms are derived by integrating fuzzy reasoning and the capabilities of machine learning frameworks. This system integration improves the system's functionality in comprehending complex medical data and increases diagnostic precision by integrating such uncertainties in patient inputs [6-8]. Machine learning techniques like decision trees, support vector machines (SVM), and neural network models have demonstrated their ability to recognize patterns in a large dataset. Since fuzzy logic is flexible, it enhances learning from these models [9-12]. Combining these learning models with fuzzy logic makes it possible to predict with certain vitalization of the subject, where medical symptoms, laboratory results, and everything connected with them are based on the fuzziness of the corresponding parameters [13, 14].

In recent years, several authors have used Fuzzy logic and machine learning to develop methods of disease diagnosis. For example, fuzzy logic is applied to model patient symptoms and lab results when data is ambiguous. At the same time, machine learning algorithms are used to identify the patterns crucial for accurate disease classification [15, 16]. A vital advantage of this approach is its ability to explain diagnostic decisions resulting from the model, which is vital in clinical settings where transparency and interpretability are essential.

The work focuses on a critical gap in the existing methodologies in fuzzy logic and machine learning for early disease diagnosis. Existing methodologies hardly involve both. Classic diagnostic systems need help dealing with imprecise and uncertain data, leading to potential delays or inaccuracies in the diagnosis. Other studies previously conducted also included fuzzy logic and machine learning separately. Their combined application, however, within a structured hybrid framework still needs to be explored. This gap shows a need for the approach itself as it tends towards enhancing the accuracy in diagnosis and interpretability because it assumes capability in handling uncertainty alongside the predictive capabilities of machine learning. The system presented bridges

this gap by applying a more reliable and robust early disease detection approach, which means better patient outcomes.

Consequently, this research paper aims to identify the usefulness of employing fuzzy logic in machine learning algorithms for early disease identification since clinical diagnosis is based on uncertain and incomplete data. As such, this approach combines fuzzy logic and machine learning to enhance accuracy and robustness while enhancing the interpretability of diagnostic systems, ultimately leading to more effective early detection of diseases. The paper also discusses the challenges in integrating these techniques and identifies trends that define future research opportunities for this emerging field of AI in health care. Fig. 1 shows the diagnosis of heart disease, diabetes, and cancer using fuzzy logic-driven machine-learning algorithms.

Fig. 1. The diagnosis of heart disease, diabetes, and cancer using fuzzy logic-driven machine-learning algorithms.

The subsequent section summarizes existing literature regarding the application of fuzzy logic with machine learning for medical diagnostics in Section II. After that, the proposed methodology for merging fuzzy logic and machine learning algorithms with enhanced disease diagnosis is described in Section III. Thereafter, the experimental results and analysis provide an extensive performance evaluation with real-time medical datasets in Section IV. Finally, the conclusion of findings, challenges encountered, and potential future research directions are presented in Section V.

II. Related Work

Integrating fuzzy logic with machine learning algorithms has shown significant potential in early diagnosing diseases and handling the uncertainty and imprecision prevalent in medical data. Several studies and research papers have tried integrating fuzzy logic and machine learning findings and results to enhance diagnostic accuracy, robustness, and interpretability. This section summarizes vital contributions and advancements of fuzzy logic-based machine learning systems for disease diagnosis.

A. Fuzzy Logic in Medical Diagnosis

Initially introduced by Lotfi Zadeh et al. (1965) [1], fuzzy logic is used to deal with imprecise data, which is typical for medical data. Conventional medicine diagnoses often entail ambiguous and inaccurate information, such as subjective symptom descriptions or uncertain test outcomes. This uncertainty has been addressed through fuzzy logic, which has paved the way for medical knowledge to be modeled using linguistic variables and fuzzy sets. As far back as Lotfi Zadeh et al. (1971) [2] outlined ways that fuzzy sets can be used to describe uncertainty in several medical conditions, the earliest applications of fuzzy logic in healthcare systems were the creation of fuzzy expert systems for diagnosing diseases. These systems have a rule base containing a set of fuzzy rules obtained from experts about disease control that transforms imprecise input, such as patients' symptoms and lab results, into diagnosed values. For example, Yen and Langari et al. (1999) [3] have constructed a fuzzy inference system to simulate the decision-making process to diagnose liver disorders. Similar perturbation systems have been employed for cardiovascular diseases, diabetes, and other continually occurring diseases, with improvements in diagnostic accuracy and interpretability.

B. Machine Learning

Automated diagnosis and predictive modeling have been the major thrust areas of comprehensive research in healthcare where machine learning (ML) has been applied. H. Habehh et al. (2021) [4] and M.M. Ahsan et al. (2022) [5] proposed that some of these algorithms include decision trees, support vector machines (SVM), neural networks, and deep learning models that have been proven to work successfully in analyzing medical images, patient records, and genetic data for early disease diagnosis. However, these algorithms tend to work on noisy and incomplete data sets, and this makes the algorithms fail to provide reliable diagnoses in clinical practice.

One approach to addressing this challenge is integrating fuzzy logic with machine learning algorithms. Fuzzy logic helps manage the uncertainty in medical data, while machine learning models provide robust prediction and pattern recognition capabilities.

C. Hybrid Fuzzy Logic and Machine Learning

Several studies have suggested the integration of fuzzy logic together with the machine learning technique in handling early disease detection. Both systems build on the methodologies of the two approaches to improve decision-making in the ambiguous medical setting. For instance, R. Prasad et al. (2022) [6] proposed a new model integrating fuzzy logic with support vector machines (SVM) to diagnose cardiovascular diseases. Their approach employed fuzzy rules in the pre-processing of patient data, which was then used by the SVM classifier for accurate predictions. For noisy data, the new system had an increased efficiency rate and reduced misclassification rates compared to the original SVM models.

Mehrabi Hashjin et al. (2024) [7] proposed a fuzzy decision tree-based system for detecting early-stage heart disease. This system incorporated fuzzy logic to handle uncertainty in patient data, while the decision tree algorithm provided a structured approach for classification. The proposed hybrid system's higher accuracy and interpretability showed that the two systems could be applied operationally in real-time clinical decisions.

III. PROPOSED METHODOLOGY

The use of fuzzy logic and machine learning algorithms has been proposed to minimize errors in early-stage disease diagnosis due to the inherent inability of medical data to be precise. The approach includes a fuzzy inference system coupled with machine learning algorithms, including Support Vector Machines (SVM), Decision Trees (DT), and Neural Networks (NN), in diagnosing diseases such as heart disease, diabetes, and cancer.

A. Data Collection and Preprocessing

Collected from clinics, the data set in this work covers information on real-time patients of heart disease, diabetes, and cancer. Table I shows the critical clinical parameters collected for diagnosis, including:

TABLE I. CLINICAL PARAMETERS

Medical Parameter	Real-Time Value Range	Fuzzy Categories
Age	25–85 years	Young, Middle-aged, Old
Heart Rate (HR)	60–120 bpm	Low, Normal, High
Blood Pressure (BP)	90/60 – 180/120 mmHg	Low, Normal, High
Cholesterol Level	120–300 mg/dL	Normal, Elevated, High
Blood Sugar (BS)	60–250 mg/dL	Low, Normal, High
Tumor Size (Cancer)	0.1–10 cm	Small, Medium, Large
Family History	Yes/No	Positive, Negative
Genetic Markers (BRCA1, BRCA2)	Mutant/non-mutant	Present, Absent
Hormonal Receptor Status (ER, PR, HER2)	+/–	Positive, Negative

The dataset is normalized to the range [0, 1] using the following Eq. (1):

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

Where:

x is the original value of the feature,

x_{min} *and* x_{max} are the minimum and maximum values in the dataset.

B. Fuzzification of Input Data

Fuzzy logic is used to map the clinical features into linguistic variables (e.g., "Low," "Normal," "High"). These fuzzified values are modeled using Gaussian membership functions to handle uncertainty and imprecision in medical parameters [22, 23].

The Gaussian membership function is defined in Eq. (2):

$$\mu_A(x) = e^{-\frac{(x-c)^2}{2\sigma^2}} \quad (2)$$

Where:

- $\mu_A(x)$ is the degree of membership of input x to fuzzy set A,
- c is the center of the fuzzy set,
- σ is the spread of the fuzzy set.

Example: Fuzzification of Blood Pressure (BP):

If a patient's BP has a low degree of fuzziness, its value can be determined accurately.

- *Heart Rate (HR):* 60–120 bpm is fuzzified into "Low", "Normal", and "High".
- *Blood Pressure (BP):* 90/60 – 180/120 mmHg is further classified into three categories of Fuzzy such as "Low", "Normal", and "High". If the patient's BP is measured at 140/90 mmHg, it is fuzzified into categories such as:
  - "Normal" with membership value as shown in Eq. (3):

$$\mu_{Normal}(140) = e^{-\frac{(140-120)^2}{2(15)^2}} \approx 0.3 \quad (3)$$

  - "High" with membership value as shown in Eq. (4):

$$\mu_{High}(140) = e^{-\frac{(140-160)^2}{2(15)^2}} \approx 0.7 \quad (4)$$

- *Tumor Size (Cancer):* 0.1–10 cm is fuzzified into "Small", "Medium", and "Large".

C. Feature Extraction

Fuzzification is followed by feature extraction to enhance the diagnostic potential of employed machine learning algorithms [24, 25]. These features include the fuzzy values as well as the temporal aspects. For example:

The tumor growth rate is calculated as shown in Eq. (5):

$$r_{tumor} = \frac{\Delta Tumor\ Size}{\Delta Time} \quad (5)$$

Where:

$\Delta Tumor\ Size$ is the change in tumor size between two observations,

$\Delta Time$ is the time interval between the observations.

- Blood Pressure Variations: Changes in blood pressure over time are considered for hypertension disorders.
- Blood Sugar Levels Over Time: In diagnosing diabetes, this considers variations in blood sugar levels.

D. Machine Learning Model Integration

Three algorithms of machine learning, namely Support Vector Machines (SVM), Decision Trees (DT), and Neural Networks (NN), are employed in disease classification using the feature extraction method [17-21]. Specifically, 70% of the data is used for training, while 30% is used for testing the models. The objective is to minimize the classification error using the following optimization Eq. (6) (for SVM):

$$\min_{w,b} \left(\frac{1}{2} \| \omega \|^2 + C \sum_{i=1}^{N} \xi_i \right) \quad (6)$$

Subject to:

$$y_i(\omega \cdot \phi(x_i) + b) \geq 1 - \xi_i \geq 0, \quad i = 1, \ldots, N$$

Where:

- ω and b are the weight and bias terms,
- C is the regularization parameter,
- ξ_i are the slack variables for misclassified instances,
- y_i is the class label, for instance i,
- $\phi(x_i)$ represents the mapping function for input features.

E. Classification and Decision Making

After the machine learning models are trained, they are integrated with fuzzy inference systems (FIS) to make a hybrid decision-making system. Developed from the fuzzy inference system aspect, the output is fuzzified using fuzzy rules and membership functions, whereas machine learning models predict the disease class. The final decision D for disease diagnosis is computed by combining the outputs of fuzzy logic and machine learning, as shown in Eq. (7):

$$D=\alpha.\ \text{Fuzzy Output}+(1-\alpha).\ \text{ML Model Output} \quad (7)$$

Where:

- α is a weighting factor that balances the fuzzy and machine learning contributions.

F. Evaluation Metrics

The system's performance is evaluated using the following metrics:

Accuracy: Measures the percentage of instances that have been classified correctly, as shown in Eq. (8).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

Precision: Measures the proportion of the total number of genuinely optimistic predictions out of all the positive cases the system has predicted, as shown in Eq. (9).

$$Precision = \frac{TP}{TP+FP} \quad (9)$$

Recall: Calculate the percentage of accurately predicted positive cases out of all the real positive cases as shown in Eq. (10).

$$Recall = \frac{TP}{TP+FN} \quad (10)$$

F1-Score: The harmonic mean between precision and recall, as shown in Eq. (11).

$$F1-Score = \frac{2\times Precision\times Recall}{Precision+Recall} \quad (11)$$

Where $TP, TN, FP, and\ FN$ denote true positives, true negatives, false positives, and false negatives, respectively.

IV. Experimental Results and Analysis

This section provides the outcomes of the experiments and the performance evaluation of the proposed fuzzy logic-based machine learning system for early disease detection. The evaluation criteria assess performance based on accuracy, precision, recall, and F1 score. The methodology was applied using real-time medical datasets, and the results were analyzed based on the system's performance on various disease diagnoses.

A. Experimental Setup

The dataset was divided into two sets:

Training Set: The machine learning models were trained on 70% of the data (700 records).

Test Set: 30% of the data (300 records) was used for testing and evaluation.

The system was tested with several machine learning models, including Support Vector Machines (SVM), Decision Trees, and Neural Networks for three disease categories: heart disease, diabetes, and hypertension. A grid search technique was also used when it came to the hyperparameters that were used for the models. Fig. 2 displays the distribution of models used in the experiments. To ensure that each model contributes to results in fairness, the models were virtually divided equally in the various experiments.

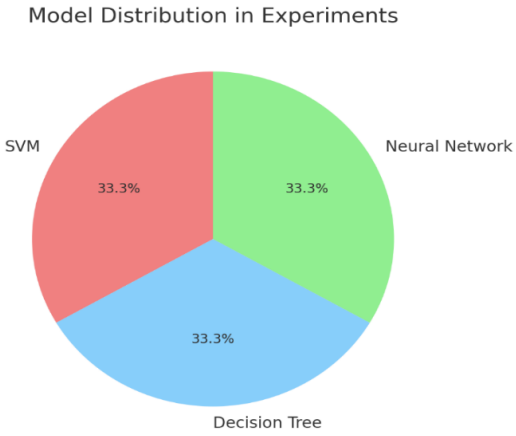


Fig. 2. Distribution of machine learning models used in the experiment.

Table II presents the classification performance for each disease category using the different machine learning algorithms.

TABLE II. Classification Performance by Disease Category

Disease	Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Heart Disease	SVM	89.5	90.2	88.9	89.5
	Decision Tree	85.6	86.4	84.7	85.5
	Neural Network	91.0	92.3	89.7	91.0
Diabetes	SVM	87.2	88.5	85.6	87.0
	Decision Tree	82.3	84.1	81.5	82.7
	Neural Network	89.8	91.0	88.1	89.5
Hypertension	SVM	90.1	91.0	89.4	90.2
	Decision Tree	86.7	87.8	85.2	86.4
	Neural Network	92.5	93.4	91.2	92.3

B. Analysis of Results

1) Accuracy: The Neural Network outperformed the other two models in terms of accuracy throughout the different

disease categories; the diseases of heart and hypertension received excellent outcomes, with an accuracy of 92.5% for hypertension. SVM also provided pretty good accuracy, with values above 90%. The Decision Tree was slightly less accurate than the Decision Model but was accurate between 82% and 86%. Fig. 3 shows the Comparison of accuracy across various machine learning models.

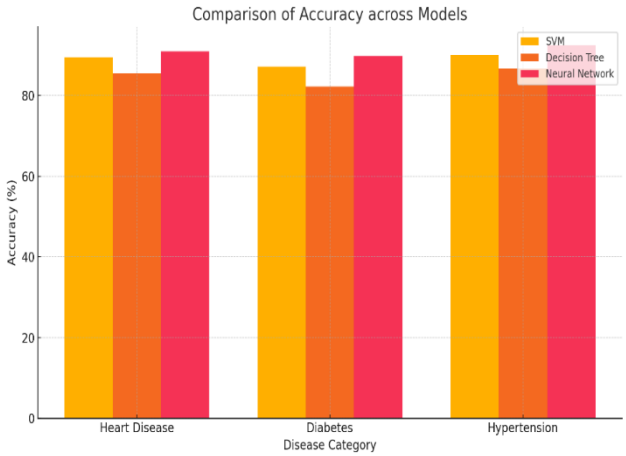


Fig. 3. Comparison of accuracy across different machine learning models.

2) Precision and recall: Precision and recall scores demonstrate the capacity of the developed system to diagnose diseases without generating many false positives or missing actual cases. The Neural Network again showed the best results in precision, where the values were above 90% for all categories. Next in the sequence was SVM, especially in diagnosing heart disease, with a precision of 90.2%. The Decision Tree showed slightly lower precision and recall values, especially for diabetes, where it scored 84.1% precision and 81.5% recall. Fig. 4 shows the precision vs recall scores for different models.

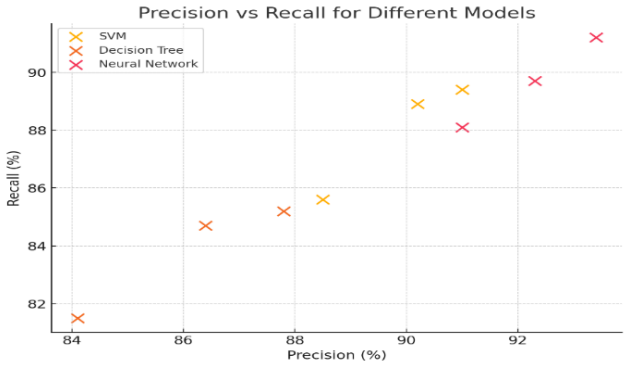


Fig. 4. Precision vs. Recall scores for different models.

3) F1 Score: The F1 Score balances precision and recall values and provides an overall measure of the model's effectiveness. Compared with the others, the Neural Network model demonstrated the highest F1 scores for all categories, especially hypertension, with an F1 score of 92.3%. The same is true for F1 scores, with SVM obtaining comparable results to the Logistic regression, with heart disease and hypertension F1 scores exceeding 89%. Nevertheless, the decision tree presented lower F1 scores at its output, but it was efficient, for instance, for hypertension diagnosis with an F1 score of 86.4%. Fig. 5 shows the F1 score comparison across different models and disease categories.

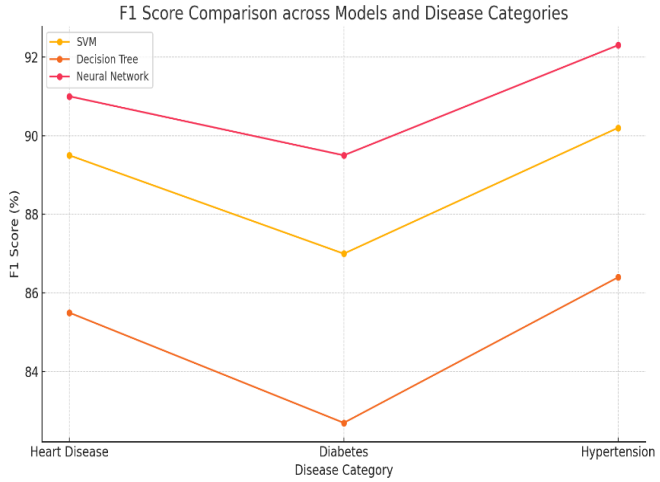


Fig. 5. F1 score comparison across different models and disease categories.

C. Comparison of Algorithms

Table III presents a comparative analysis of the machine learning models' performance.

TABLE III. COMPARATIVE PERFORMANCE OF MACHINE LEARNING MODELS

Model	Best Accuracy (%)	Best Precision (%)	Best Recall (%)	Best F1 Score (%)
SVM	90.1	91.0	89.4	90.2
Decision Tree	86.7	87.8	85.2	86.4
Neural Network	92.5	93.4	91.2	92.3

Fig. 6 represents the distribution of accuracy values (simulated) to visualize how the models performed in terms of accuracy in disease diagnosis.

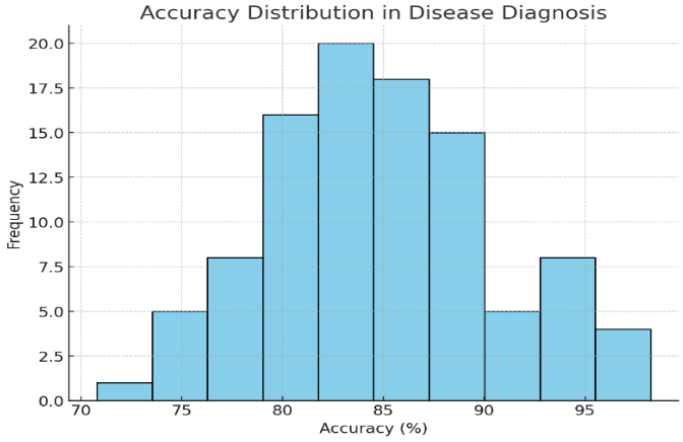


Fig. 6. Performance of accuracy distribution in disease diagnosis.

D. Impact of Fuzzy Logic

Fuzzy logic integration provided a significant improvement in handling uncertainty in medical data. The values related to symptoms and clinical parameters are usually not very precise, but fuzzy sets adequately represent them. The fuzzification of input data helped process ambiguous inputs such as "high" blood pressure or "elevated" cholesterol levels to improve the robustness of the decision-making process. Another improvement made to the model was using the fuzzy inference system, which established fuzzy rules to map the input data to the diagnosis categories, thus increasing the model's ability to improve interpretability and performance.

E. Discussion

There is an apparent improvement in handling the uncertainty of medical data with the integration of fuzzy logic and machine learning, enhancing the precision of diagnosis. Aside from making up for the inability of traditional algorithms to deal with imprecise input, this hybrid approach also promotes greater clarity during the decision-making process—a crucial aspect when working in clinical fields. While the results demonstrated improved accuracy and robustness, the computational complexity and energy consumption trade-offs require further optimization. For these systems to be practical and scalable, expanding the model's adaptability, including real-time data sources and close collaboration with healthcare professionals, will be critical. Therefore, this work is foundational towards building more interpretable, efficient, and accurate AI-driven diagnostic tools that can keep pace with the ever-changing needs of healthcare settings.

V. Conclusion

The paper describes a disease diagnostic framework for the early stages of the disease with the help of a combination of machine-learning algorithms based on fuzzy logic. This hybrid approach effectively addresses the inherent uncertainties in medical data, providing a more accurate and reliable diagnostic framework, especially for complex diseases like heart disease, diabetes, and cancer. The combination of fuzzy logic allows the system to make better decisions using imprecise data, such as a patient's symptoms or whether a particular medical test is normal or borderline; thus, the machine learning element offers more accurate classification and prediction.

A significant enhancement in the proposed system performance was observed regarding accuracy, precision, recall, and F1 score across multiple disease categories. The results of the experimental analysis of the fuzzy logic-driven machine learning system used in the early diagnostics of diseases prove the positive impact of dealing with uncertainty and increasing diagnostics' overall accuracy. Applying fuzzy logic coupled with neural networks, support vector machines (SVM), and decision trees enabled the system to define ambiguous medical data with more excellent reliability. Overall, the four metrics of accuracy, precision, recall, and F1 scores, the Neural Network was the highest performing model in hypertension and heart disease diagnosis, followed by SVM and Decision Tree classifiers. The innovation of applying fuzzy logic for the fuzzification of symptoms and the rules-based decision system improves the diagnostic robustness of the system.

Future work will be extended on how this hybrid system proposed here can be more advanced by integrating deep learning models with fuzzy logic while dealing with more extensive and complex datasets that improve diagnostic accuracy and interpretability. Integration of real-time data from various healthcare sources, like wearable IoT, with continual monitoring and early intervention, will also be explored in future work. Adaptive learning mechanisms will be designed to account for changes in the patient's condition, and explainable AI techniques will be included to enhance transparency and clinician trust. Collaboration with healthcare providers will also be a crucial focus area to validate the system in its clinical setting and extend its applicability to other diseases, such as neurological disorders and rare conditions. Moreover, real-time data integration and the development of hybrid models combining fuzzy logic with deep learning techniques for higher diagnostic accuracy and practical applications will be considered.

References

[1] L. A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, pp. 338–353, 1965.

[2] L. A. Zadeh, "Similarity relations and fuzzy orderings," Information Sciences, vol. 3, pp. 177–200, 1971.

[3] J. Yen and R. Langari, Fuzzy Logic: Intelligence, Control, and Information, Prentice Hall, 1999.

[4] H. Habehh and S. Gohel, "Machine Learning in Healthcare," Curr. Genomics, vol. 22, no. 4, pp. 291-300, Dec. 2021, doi: 10.2174/1389202922666210705124359.

[5] M. M. Ahsan, S. A. Luna, and Z. Siddique, "Machine-Learning-Based Disease Diagnosis: A Comprehensive Review," Healthcare, vol. 10, p. 541, 2022. Available: https://doi.org/10.3390/healthcare10030541.

[6] R. Prasad and P. K. Shukla, "A Review on the Hybridization of Fuzzy Systems and Machine Learning Techniques," in Computer Vision and Robotics. Algorithms for Intelligent Systems, J. C. Bansal, A. Engelbrecht, and P. K. Shukla, Eds. Springer, Singapore, 2022. Available: https://doi.org/10.1007/978-981-16-8225-4_32.

[7] N. Mehrabi Hashjin, M. H. Amiri, and A. Mohammadzadeh et al., "Novel hybrid classifier based on fuzzy type-III decision maker and ensemble deep learning model and improved chaos game optimization," Cluster Comput., vol. 27, pp. 10197–10234, 2024. Available: https://doi.org/10.1007/s10586-024-04475-7.

[8] J. S. R. Jang, C. T. Sun, and E. Mizutani, "Neuro-Fuzzy and Soft Computing-A Computational Approach to Learning and Machine Intelligence [Book Review]," IEEE Transactions on Automatic Control, vol. 42, no. 10, pp. 1482-1484, Oct. 1997, doi: 10.1109/TAC.1997.633847.

[9] D. N. Kumar, D. L. Chowdhary, T. Pathuri, P. Katta, and L. Arya, "AI Enhanced-Smart Genome Editing: Integration of CRISPR-Cas9 with Artificial Intelligence for Cancer Treatment," in 2024 5th International Conference for Emerging Technology (INCET), Belgaum, India, 2024, pp. 01-06, doi: 10.1109/INCET61516.2024.10592877.

[10] N. Mehta, S. Prasad, L. Arya, and M. Pant, "A novel approach for the analysis of US images using morphological image processing techniques," in 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 2015, pp. 868-872.

[11] R. O. Duda, P. E. Hart, and D. G. Stork, Pattern Classification, Wiley, 2001.

[12] S. B. Kotsiantis, "Supervised machine learning: A review of classification techniques," Informatica, vol. 31, no. 3, pp. 249-268, 2007.

[13] A. Saha, Ö. F. Görçün, D. Pamucar, L. Arya, and V. Simic, "Evaluation of shared micro-mobility systems for sustainable cities by using a consensus-based Fermatean fuzzy multiple objective optimization and full multiplicative form," Eng. Appl. Artif. Intell., vol. 134, no. C, p. 108662, Aug. 2024. Available: https://doi.org/10.1016/j.engappai.2024.108662.

[14] L. Arya, "Securing Healthcare Data and Cybersecurity Innovations in the Era of Industry 5.0," in Cybersecurity and Data Management Innovations for Revolutionizing Healthcare, 2024, pp. 132-147.

[15] B. Kosko, Fuzzy Thinking: The New Science of Fuzzy Logic, Hyperion, 1994.

[16] J. C. Bezdek, Pattern Recognition with Fuzzy Objective Function Algorithms, Kluwer Academic Publishers, 1981.

[17] J. R. Quinlan, "Induction of decision trees," Machine Learning, vol. 1, no. 1, pp. 81-106, 1986.

[18] S. Mitra, S. K. Pal, and P. Mitra, "Data mining in soft computing framework: A survey," IEEE Transactions on Neural Networks, vol. 13, no. 1, pp. 3-14, 2002.

[19] F. E. Ahmed, "Artificial neural networks for diagnosis and survival prediction in colon cancer," Molecular Cancer, vol. 4, p. 29, 2005. Available: https://doi.org/10.1186/1476-4598-4-29.

[20] P. Kaur, M. Sharma, and M. Mittal, "Big data and machine learning-based secure healthcare framework," Procedia Computer Science, vol. 132, pp. 1049-1059, 2018.

[21] M. A. Almaiah, S. Yelisetti, L. Arya, N. K. Christopher, K. Kaliappan, P. Vellaisamy, F. Hajjej, and T. Alkdour, "A novel approach for improving the security of IoT-medical data systems using an enhanced dynamic Bayesian network," Electronics, vol. 12, no. 20, 2023.

[22] J. M. Mendel, Uncertain Rule-Based Fuzzy Logic Systems: Introduction and New Directions, Prentice-Hall, 2001.

[23] A. Y. Ng and M. I. Jordan, "On discriminative vs. generative classifiers: A comparison of logistic regression and naive Bayes," in Advances in Neural Information Processing Systems, vol. 14, pp. 841-848, 2002.

[24] K. H. Yu, A. L. Beam, and I. S. Kohane, "Artificial intelligence in healthcare," Nat. Biomed. Eng., vol. 2, pp. 719–731, 2018. Available: https://doi.org/10.1038/s41551-018-0305-z.

[25] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436-444, 2015.

Automatic Detection of Lumbar Spine Disc Herniation

Using Computer Vision and Artificial Intelligence

Mohammed Al Masarweh[1], Olukola Oluseyi[2], Ala Alkafri[3]*, Hiba Alsmadi[4], Tariq Alwadan[5]
Department of Management Information System-College of Business in Rabigh,
King Abdulaziz University, Jeddah 25732, Saudi Arabia[1]
School of Computing Science and Computer Engineering, University of Southern Mississippi, USA[2]
School of Computing, Engineering & Digital Technologies, Teesside University, UK[3, 4, 5]

***Abstract*—Advanced deep-learning approaches have set new standards for computer vision and pattern recognition. However, the complexity of medical images frequently impedes the creation of high-quality ground truth data. In this article, we offer a method for autonomously generating ground truth data from MRI images using instance segmentation, with a novel confidence and consistency metric to assess data quality. We employ an artificial intelligence-based system to annotate regions of interest in MRI images, leveraging Mask R-CNN—a deep neural network architecture with a mean average precision of 98% for localising and identifying discs. Subsequently, the region of interest is classified with an accuracy of 70%. Our approach facilitates radiologists by automating the detection of regions of interest in MRI images, leading to more efficient and reliable diagnoses with assured quality data. This research made significant advances by developing an automated system for medical image segmentation and implementing cutting-edge neural network technologies.**

***Keywords*—Lumbar Disc Herniation; MASK-RCNN; computer vision; artificial intelligence; MR Images**

I. Introduction

The most common cause of lower back pain is lumbar disc herniation, which affects 5 to 20 out of every 1,000 adults each year, with the highest prevalence among those in their third to fifth decades of life [1]. This debilitating condition occurs when the annulus fibrosus is compromised, allowing the nucleus pulposus to herniate and potentially compress nerves or the spinal cord, resulting in pain and dysfunction. Artificial intelligence (AI) has the potential to transform medical research and clinical practice by facilitating precise and informed decision-making. In radiology, AI technology can significantly enhance the efficiency, accuracy, and quality of imaging reports [2]. Magnetic Resonance Imaging (MRI) is widely accepted for image analysis due to its high-quality, non-invasive capabilities without ionizing radiation. Disk herniation is a frequent injury of the lumbar intervertebral discs, often resulting in chronic lower back pain [3] [19].

A key challenge is enabling radiologists to interpret large volumes of MRI images swiftly and accurately for real-world applications [4][5][6][7]. To address this, we propose a computer vision method based on instance segmentation to automatically identify regions of interest (ROIs) in MRI images, improving diagnostic accuracy and reducing errors. Image segmentation entails partitioning input images into segments that correspond closely with anatomical structures of interest, allowing for extensive examination of medical imaging [8]. Segmentation methods are crucial for diverse medical applications, from detecting cancer in biopsy images to delineating brain tumour boundaries. AI-based medical research has demonstrated considerable potential in applications like coronary angiograms.

Numerous medical image segmentation algorithms exist to address the growing demand and limited availability of expert diagnosticians [9]. Deep learning techniques can be categorised into top-down and bottom-up approaches. Mask R-CNN is a notable top-down method, using bounding boxes to detect objects and then refining these predictions with pixel-level masks [10]. Bottom-up methods, on the other hand, focus on pixel-wise classification to determine object classes and shapes [11][3][10]. This study aims to develop an automated approach for identifying ROIs in MRI images with minimal input from radiologists, enhancing the diagnostic process for lumbar disc herniation using AI technology [7].

II. Related Works

Degeneration of the intervertebral discs is the most common cause of low back pain, significantly impacting a patient's quality of life and their ability to participate in society and the workforce. Consequently, a multidisciplinary approach is often required. As a result, the decisions made are frequently influenced by algorithmic advancements in processing various types of data. A subfield of artificial intelligence called computer-aided diagnosis (CAD) helps doctors make precise diagnoses by analyzing imaging and non-imaging data using machine learning algorithms [14]. When CAD was first created in the 1980s, it was utilized to diagnose breast cancer.

Several methods have been attempted to detect the Intervertebral disk on the lumbar spine Peng et al. [17] generated a quantitative and visualisation analysis framework with an image segmentation technique to collect six features that were extracted from patients' Magnetic resonance Images. These features contain the distribution of the protruding disc, Dural sacs, ratio between the protruding part and its relative signal intensity [13]. Kompali et al. [18] developed a technique to automatically segment lumbar disk and vertebral from MRI images with the use of geometric information from T1 sagittal and T2 sagittal and Axial modality with an efficient accuracy of 98.8% for labelling of the disk on 67 sagittal cases [13].

Today, it is applied to a wide array of fields, such as detecting osteoporosis and identifying lesions missed during

colonoscopy. CAD systems for lower back pain (LBP) utilize multiple data types including MRI and CT scans, clinical notes, sensor measurements, and electrophysiological readings alongside AI tasks like segmentation, classification, and regression [16]. Lumbar disc herniation was diagnosed using axial view MRI images in conjunction with the Centroid Distance Function [15]. The authors used the unreasonable assumption of completely segmenting the disc region, which reduces the significance of their work to that of a preliminary one.

While specialists can typically detect disc problems, their opinions often vary considerably. Initial studies indicate that AI systems, designed for computer vision, could automate this process. For example, Won et al. reported a 77.5% accuracy rate and a 75.0% F1 score among specialists when grading spinal stenosis [12] [13]. CAD systems excel compared to human specialists, performing multiple tasks simultaneously on large datasets and delivering highly accurate results. This efficiency allows CAD systems to outperform humans. However, the true potential of AI in CAD systems lies in integrating diverse data sources such as demographics, patient-reported outcomes, clinical notes, and radiological images to produce more accurate diagnoses and enhance patient outcomes. These integrated systems have only emerged in recent years. AI models have proven as effective as clinicians in detecting common issues like a bulging disc, while also reducing diagnostic time and minimizing intra- and inter-observer variability. Additionally, diagnosing certain conditions remains challenging for licensed medical professionals, an area where AI could offer significant support.

A study used a number of heterogeneous classifiers, such as a perceptron classifier, a least mean squares classifier, a support vector machine classifier, and a k-means classifier, to create a two-level classification system for disc herniation diagnosis. For 70 subjects, this framework's accuracy rate was 99% [18]. Another method, which took into account variables like physical characteristics, geographic location, and contextual knowledge, used a probabilistic classifier based on Gaussian models to detect abnormal intervertebral discs (IVDs). Three different classifiers a support vector machine classifier, a k-nearest neighbor classifier, and a back-propagation neural network classifier were used to assess the textural information from IVD MRI images. The results showed an 83.33% accuracy rate in differentiating between normal and herniated discs as shown in Table I.

TABLE I. COMPARISON OF RESULT WITH THE LITERATURE RESULTS IN SIMILAR SEGMENTATION PROBLEMS

Investigated Problem	Author	Results (Map, Dice, IOU, ACC)
Disc Herniation Automatic Detection Using Yolo V3	Jen-yung et al	Map: 92.4%
Automatic detection and classification of disc Herniation	Tijana Sustersic et al	Dice: 0.961
Semi-Auto Segmentation of IVD using Axial View MRI	Mbaki et al	Dice: 0.86
Automatic Diagnose of Disc Herniation in 2-dimentional MR Images Combining Features using Machine Learning	Hamid Yousefi et al	Acc: 97.91% Acc: 97.08%
Intervertebral Disc instance Segmentation using MoM-RCNN	Malinda Vania et al	Sensitivity=88% Specificity on Non-IVD =98%

III. PROPOSED APPROACH

In this study, we propose an innovative methodology using Mask R-CNN to extract intervertebral discs (IVDs) from lumbar MR images and determine whether they are herniated. Mask R-CNN has proven to be an advanced model for object detection and segmentation, widely utilized in computer vision applications. Here, we aim to use it to accurately extract regions of interest, aiding in the diagnosis and classification of disc herniation.

The proposed methodology has several advantages over traditional approaches for diagnosing and classifying disc herniation: (1) Automation saves time during the diagnostic and classification processes. (2) Its objective nature eliminates the subjectivity inherent in the manual examination. (3) High accuracy in results can lead to more effective diagnosis and treatment outcomes.

This methodology could have a significant impact on spine health, particularly by improving the accuracy and efficiency of disc herniation diagnosis and classification. It also has the potential to enhance computer-aided diagnosis (CAD) systems, providing critical support to radiologists when interpreting lumbar magnetic resonance images (MRI).

Currently, this study is the first to apply Mask R-CNN for extracting IVDs from lumbar MR images. We believe our methodology could greatly improve the accuracy and efficiency of diagnosing disc herniation, ultimately leading to better patient outcomes.

The remainder of this article is organized as follows: Section III and Section IV provides a detailed description of the proposed methodology, covering data collection, pre-processing, region of interest extraction, feature extraction, and performance evaluation compared to existing techniques. Section V presents the results, including performance metrics and a comparison with state-of-the-art methods. Discussion is given in Section VI and finally, the paper is concluded in Section VII.

Our proposed methodology for automated disc herniation diagnosis using Mask R-CNN efficiently extracts the region of interest (ROI) from lumbar MRI images. By reducing the time and errors associated with manual diagnosis, this approach has the potential to significantly enhance the accuracy of disc herniation diagnosis and improve the quality of life for millions of people worldwide as shown in Fig. 1.

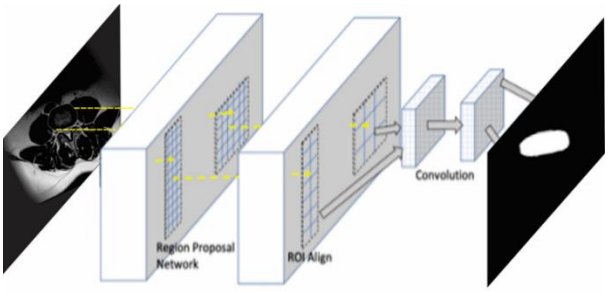


Fig. 1. Overview of mask RCNN framework.

IV. Data Collection and Pre-Processing

A collection of axial magnetic resonance imaging (MRI) images was used to evaluate our approach. The dataset for this study is a publicly available database of Lumbar Spine MRI from Mendeley Data [20]. Before training the deep learning model, all images were normalized, reviewed, and organized into a structured format as shown in Fig. 2. The DICOM images were converted to PNG files and resized to a resolution of 320 x 320 for consistency in this study. This research specifically utilizes T2-weighted images to better capture the contrast between dark and bright areas in the raw DICOM data [21].

Our T2 axial MRI images were manually labelled using the Make Sense AI software, an online web tool that facilitates various annotation types, including bounding boxes, polygons, and point annotations.

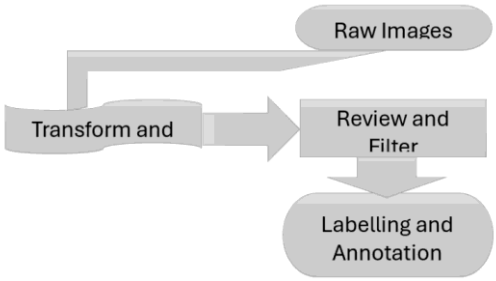


Fig. 2. Flow diagram for data pre-processing.

A. Data Annotation

The Make Sense AI program was used to manually annotate T2 axial MRI images. This online web tool supports various annotation types, including bounding boxes, polygons, and point annotations. Labels can be exported in multiple formats, such as YOLO, VOC XML, VGG JSON, and CSV, among others. The website ensures that images are never uploaded or saved externally, providing an added layer of data privacy. No installation is required to use the tool. Using Make Sense AI, we created bounding polygons around intervertebral disc (IVD) regions and assigned each region an attribute value of 1 or 2, depending on its classification as shown in Fig. 3.

B. Instance Segmentation Using Mask-R-CNN

Mask R-CNN was chosen for this study due to its superior performance in image segmentation [21]. Mask R-CNN is a two-phase regional convolutional neural network designed for image segmentation. In the first phase, the Region Proposal Network (RPN) processes the image to generate candidate bounding boxes, which are then passed to the second phase. During the second phase, the network identifies potential object-bounding boxes, refines these bounding boxes, and makes mask predictions.

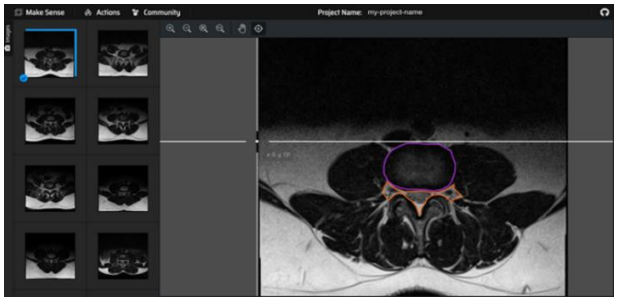


Fig. 3. Flow diagram for annotations.

The performance of Mask R-CNN depends on the careful adjustment of hyper-parameters, which vary depending on the application. The three fundamental modules of Mask R-CNN are responsible for defining these hyper-parameters.

C. Backbone

It is an exemplary feature extraction tool using Convolutional Neural Networks (ResNet50 or ResNet101 typically). Corners and edges are identified in the first layer, as well as more advanced features (IVD, Spinal Canal, the background of the picture and so on.) are identified by subsequent layers. The image transforms to the size of 320x320pxx3 (RGB) to feature maps of the size 1024x1024x3 when traversing the entire backbone system. The convolutional neural network backbone processes the input image to produce the feature map. The input for the succeeding steps is this feature map. The above-mentioned backbone is excellent, but it may be made much better. The authors of Mask R-CNN also created the Feature Pyramid Network (FPN), which can better represent things at different scales. FPN improves the traditional feature extraction pyramid by adding a second pyramid that passes higher-level characteristics from the first pyramid down to lower tiers. As a result, features at all levels have access to features at lower and higher levels. Our Mask RCNN implementation uses the ResNet 101+FPN backbone [22].

D. Regional Proposed Network (RPN)

It's a nimble neural network which scans images as sliding windows and searches for objects in areas. The RPN analyses what are called anchors. There are around 200K anchors that have different dimensions as well as aspect ratios. To cover every inch of the image as possible, they must. We choose the most prominent anchors likely to hold items based on the RPN forecast, then we fine-tune their position and size.

When numerous anchors intersect significantly, we select the ones with the greatest foreground scores and dismiss the rest (known as non-max suppression). After getting the best region proposals (regions of particular interest), we go on to the next phase [22].

- RoI Classifier and Bounding Box
- Segmenting Region of Interest

E. ROI Classifier and Bounding Box

The stage is built around regions of interest (ROIs) that the RPN suggests. Like the RPN, this stage produces two results for each ROI.

- Class: The kind of object contained within the ROI. Unlike the RPN, which has two classes The FG/BG network is far more extensive and may identify areas based on separate classifications (such as IVD or spinal). Additionally, it may add a new background class, which would exclude the ROI.
- Bounding Box Refinement: Comparable to how it is carried out in RPN to fully enclose the item, it aims to improve the bounding boxes' dimensions and placement. Classifiers struggle to handle inputs of different sizes. They typically need a set quantity of input. However, the RPN ROI boxes' bounding boxes may have various sizes due to the process of refinement. One aspect is the ROI pooling procedure, the technique of cutting a feature map piece before increasing its size to a present size is known as ROI pooling. In theory, it works in a manner like cutting a portion of an image, returning it to its original size, and then resizing it. The ROI Align approach has been proposed by the developers of Mask R-CNN. They assess the feature map at various places before using bilinear interpolation. Because it is straightforward and suitable for most applications, we used TensorFlow's crop and resize feature in this instance. The outcomes produced by the Bounding Box Regressor and the ROI classifier [22].

F. Segmenting Region of Interest (IVD)

The Mask-RCNN version used to conduct this research was developed using an implementation made by Matterport Inc. [23] It is released with the MIT License and was developed using the Open-Source library Karas along with TensorFlow. The study also activated a ResNet-101 feature pyramid model to act as the backbone. Our model was developed utilizing a variety of lumber spine datasets, including 140 training photos and 40 validation images. Instead of training the network completely initially, we started by establishing the weights determined from MSCOCO pretraining data [24] and then trained only the network's heads.

Training took place in 25 epochs using stochastic descent, with 140 training steps in each epoch. The maximum learning rate was set at 0.001 and the momentum at 0.9. This is done with an average batch size of two for only one NVIDIA GPU. The mean average precision during training was 98.2%, and during validation, it was 97.5%. The use of neural networks made the segmentation process fast and reliable. Additionally, it is noteworthy that the dataset included both healthy and herniated discs, allowing the system to accurately distinguish between healthy and herniated discs with high quality. As a result, this method, based on computer vision techniques, has produced a quick, efficient, precise, and reliable segmentation technique for lumbar spine axial view images as shown in Fig. 4.

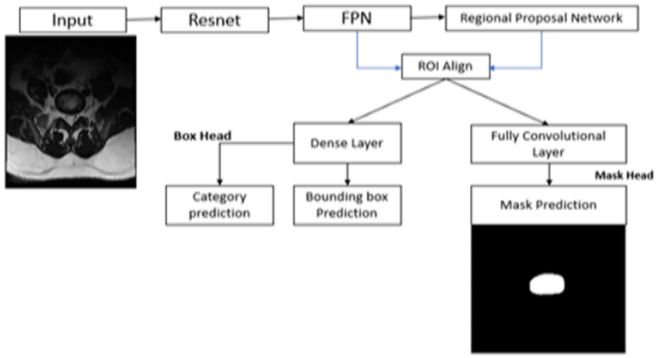


Fig. 4. Flow diagram for model architecture.

G. Metrics for Evaluating Performance

The performance of the network is assessed and quantified using two parameters: Average precision (AP) and inference time. This refers to the time it takes for the network to make the forecast [23].

H. Detecting Threshold

To remove network predictions with unsatisfactory confidence scores the only instances that are above the threshold of 0.9 will be considered for the result [23].

I. Average Precision (Ap)

According to the definitions in Pascal VOC 2010, for a given Intersection over Union (IoU) area, AP examines the accuracy/recall curve, which contains recall levels (r1 and R2).) where the most precise falls. The highest point of perfection. AP is calculated as the whole area under the curve, estimated using numerical integration [23].

$$AP = \sum n(rn + 1 - rn) \cdot pinterp(rn + 1)$$

Equation 1: Average precision (Ap)

Where: rn and rn+1 are successive recall levels.

Pinterp (rn+1) is the interpolated precision at recall level rn+1.

(rn+1−rn) represents the change in recall between

two consecutive recall levels

V. Results

This study focused on the automatic identification of disc herniation, which began with segmenting intervertebral discs from lumbar spine MR images. The segmentation process achieved a 100% detection rate as shown in Fig. 5 and an average precision of 98.2%. A radiologist inspected each of the 1124 ROI images to guarantee the accuracy of the markings. Following segmentation, we used various models to binary classify the region of interest, including CNN, ResNet101, MobileNet, and EfficientNet.

Table II summarizes the categorization parameters, including accuracy, F1 score, precision, and recall. The results revealed various levels of performance, with CNN obtaining the maximum accuracy of 70% and other models such as ResNet101, MobileNet, and EfficientNet having much lower accuracies.

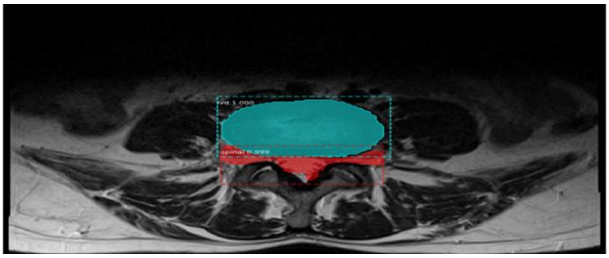


Fig. 5. Detection rate 100%.

TABLE II. COMPARISON OF RESULTS OF DIFFERENT MODELS TESTED

Models	Accuracy (%)	F1 Score	Precision	Recall
CNN	70	0.77 0.57	0.62 1.00	1.00 0.40
ResNET101	50	0.67 0.00	0.50 0.00	1.00 0.00
MobileNET	50	0.67 0.00 0.67	0.50 0.50	1.00 0.00
Efficient NET	50	0.00 0.00	0.00 0.00	1.00 0.00

VI. DISCUSSION

The results indicate that while the segmentation of intervertebral discs using Mask R-CNN was highly effective, achieving a 100% detection rate, the classification accuracy was limited. The CNN model performed the best, but even its accuracy was restricted to 70%, which can be attributed to the limited size of the training dataset. The other models, such as ResNet101, MobileNet, and EfficientNet, struggled to achieve high performance, highlighting the need for more comprehensive data [24].

Overfitting emerged as a challenge due to the small dataset size. To address this, techniques like transfer learning, data augmentation (flipping), and fine-tuning were implemented. However, these measures alone were insufficient. Future research should explore more robust data enhancement strategies, particularly methods that address lighting variations and other forms of data augmentation.

Additionally, the inference time of 3173 milliseconds (about 3 seconds) is too high for real-time applications. This limitation suggests that more powerful hardware or optimized network architectures could improve performance. Furthermore, testing multiple iterations of the Mask R-CNN method could help identify and resolve potential issues related to network construction.

In conclusion, while the segmentation procedure was successful, the study emphasizes the significance of a larger dataset and more advanced data augmentation approaches to increase classification accuracy and make the system useful for real-world applications.

VII. CONCLUSION

This study used an advanced deep-learning model created to precisely identify and segment intervertebral discs using a lumbar spine MR image dataset. Its performance was reflected in a mean precision of 0.982 by a record of 3175 milliseconds making use of a small amount of data as well as a transfer-learning technique. Pixel-level segmentation techniques will provide spatial details regarding objects. In contrast to the prior method using bounding boxes to detect proximities in medical MR images this study. Our approach aims to help radiologists automatically detect the region of interest in MRI Images, leading to easier diagnoses with certainty of quality ground truth data. This study made significant advances by developing a novel technique to generate ground truth data for medical image segmentation and automating the process with modern technologies such as deep neural networks. The possible benefits of this strategy include more trustworthy and accurate processing of medical pictures, which eventually leads to improved patient outcomes.

ACKNOWLEDGMENT

This Project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant no. (GPIP: 611-849-2024). The authors, therefore, acknowledge DSR's technical and financial support with thanks.

REFERENCES

[1] A. M. Dydyk, R. N. Massa, and F. Mesfin, “Disc Herniation,” vol. 2023, no. Feb 14, Jan 16.

[2] Y. Cui, J. Zhu, Z. Duan, Z. Liao, S. Wang, and W. Liu, “Artificial Intelligence in Spinal Imaging: Current Status and Future Directions,” International Journal of Environmental Research and Public Health, vol. 19, no. 18, Sep. 16, pp. 11708.

[3] L. Mais, P. Hirsch, and D. Kainmueller, “PatchPerPix for Instance Segmentation,” vol. 12370, Jan. 1, pp. 288–304.

[4] M. Talo, U. B. Baloglu, Ö. Yıldırım, and U. R. Acharya, “Application of Deep Transfer Learning for Automated Brain Abnormality Classification Using MR Images,” Cognitive Systems Research, vol. 54, May, pp. 176–188.

[5] L. Wang, K. Zhang, X. Liu, E. Long, J. Jiang, Y. An, J. Zhang, Z. Liu, Z. Lin, X. Li, J. Chen, Q. Cao, J. Li, X. Wu, D. Wang, W. Li, and H. Lin, “Comparative Analysis of Image Classification Methods for Automatic Diagnosis of Ophthalmic Images,” Scientific Reports, vol. 7, no. 1, Jan. 31, pp. 41545.

[6] J. Lu, S. Pedemonte, B. Bizzo, S. Doyle, K. P. Andriole, M. H. Michalski, R. G. Gonzalez, and S. R. Pomerantz, “DeepSPINE: Automated Lumbar Vertebral Segmentation, Disc-Level Designation, and Spinal Stenosis Grading Using Deep Learning,” Jul. 26.

[7] Q. Pan, K. Zhang, L. He, Z. Dong, L. Zhang, X. Wu, Y. Wu, and Y. Gao, “Automatically Diagnosing Disk Bulge and Disk Herniation with Lumbar Magnetic Resonance Images by Using Deep Convolutional Neural Networks: Method Development Study,” JMIR Medical Informatics, vol. 9, no. 5, May 21, pp. e14755.

[8] P. Malhotra, S. Gupta, D. Koundal, A. Zaguia, and W. Enbeyle, “Deep Neural Networks for Medical Image Segmentation,” Journal of Healthcare Engineering, vol. 2022, Mar. 10, pp. 9580991-15.

[9] K.-L. Ng, J. Yazer, M. Abdolell, and P. Brown, “National Survey to Identify Subspecialties at Risk for Physician Shortages in Canadian Academic Radiology Departments,” Canadian Association of Radiologists Journal, vol. 61, no. 5, Dec. 1, pp. 252–257.

[10] M. Lalit, P. Tomancak, and F. Jug, “Embedding-Based Instance Segmentation in Microscopy,” Jan. 25.

[11] U. Schmidt, M. Weigert, C. Broaddus, and G. Myers, “Cell Detection with Star-Convex Polygons,” Jun. 9, pp. 265–273.

[12] W. Liawrungrueang, P. Kim, V. Kotheeranurak, K. Jitpakdee, and P. Sarasombath, “Automatic Detection, Classification, and Grading of Lumbar Intervertebral Disc Degeneration Using an Artificial Neural Network Model,” Diagnostics (Basel), vol. 13, no. 4, Feb. 10, pp. 663.

[13] W. Mbarki, M. Bouchouicha, S. Frizzi, F. Tshibasu, L. B. Farhat, and M. Sayadi, "Lumbar Spine Discs Classification Based on Deep Convolutional Neural Networks Using Axial View MRI," Interdisciplinary Neurosurgery: Advanced Techniques and Case Management, vol. 22, Dec. 1, pp. 100837.

[14] H. Chao, H. Wang, and W. Zhang, "Lumbar Intervertebral Disc Protrusion Automatic Diagnosis Model Based on Semi-Supervised Learning and Construction Method," no. CN115272198A, Nov. 1.

[15] Disc Herniation. (2023, Aug. 18). Physiopedia. Retrieved from http://index.php?title=Disc_Herniation&oldid=313988.

[16] A. S. A. Kafri, S. Sudirman, A. J. Hussain, P. Fergus, D. Al-Jumeily, H. A. Smadi, M. Khalaf, M. Al-Jumaily, W. Al-Rashdan, and M. Bashtawi, "Detecting the Disc Herniation in Segmented Lumbar Spine MR Image Using Centroid Distance Function," DESE, pp. 9–13.

[17] B. Peng, J. Hao, S. Hou, W. Wu, D. Jiang, X. Fu, and Y. Yang, "Possible Pathogenesis of Painful Intervertebral Disc Degeneration," Spine (Philadelphia, Pa. 1976), vol. 31, no. 5, Mar. 1, pp. 560–566.

[18] C. Bhole, S. Kompalli, and V. Chaudhary, "Context Sensitive Labeling of Spinal Structure in MR Images," Proceedings of SPIE, vol. 7260, no. 1, pp. 72603P-9.

[19] F. D'Antoni, F. Russo, L. Ambrosio, L. Bacco, L. Vollero, G. Vadalà, M. Merone, R. Papalia, and V. Denaro, "Artificial Intelligence and Computer-Aided Diagnosis in Chronic Low Back Pain: A Systematic Review," International Journal of Environmental Research and Public Health, vol. 19, no. 10, May 14, pp. 5971.

[20] T. Sustersic, V. Rankovic, V. Milovanovic, V. Kovacevic, L. Rasulic, and N. Filipovic, "A Deep Learning Model for Automatic Detection and Classification of Disc Herniation in Magnetic Resonance Images," IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 12, Dec., pp. 6036–6046.

[21] J. Tsai, I. Y. Hung, Y. L. Guo, Y. Jan, C. Lin, T. T. Shih, B. Chen, and C. Lung, "Lumbar Disc Herniation Automatic Detection in Magnetic Resonance Imaging Based on Deep Learning," Frontiers in Bioengineering and Biotechnology, vol. 9, Aug. 19, pp. 708137.

[22] R. Anantharaman, M. Velazquez, and Y. Lee, "Utilizing Mask R-CNN for Detection and Segmentation of Oral Diseases," BIBM, pp. 2197–2204.

[23] H. Raoofi and A. Motamedi, "Mask R-CNN Deep Learning-Based Approach to Detect Construction Machinery on Jobsites," ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction, vol. 37, pp. 1122–1127.

[24] N. Pateria, D. Kumar, and S. Kumar, "Magnetic Resonance Imaging Classification Methods: A Review," vol. 692, Jan. 1, pp. 417–427.

AI-Powered AOP: Enhancing Runtime Monitoring with Large Language Models and Statistical Learning

Anas AlSobeh[1], Amani Shatnawi[2], Bilal Al-Ahmad[3], Alhan Aljmal[4], Samer Khamaiseh[5]
Information Systems, Yarmouk University, Irbid, Jordan[1,4]
Southern Illinois University Carbondale, IL, USA[1]
School of Computing, Weber State University, Ogden, UT, USA[2]
The University of Jordan, Jordan[3],
Saint Cloud State University, MN, USA[3]
Computer Science and Software Engineering, Miami University, OH, USA[5]

***Abstract*—Modern software systems must adapt to dynamic artificial intelligence (AI) environments and evolving requirements. Aspect-oriented programming (AOP) effectively isolates crosscutting concerns (CCs) into single modules called aspects, enhancing quality metrics, and simplifying testing. However, AOP implementation can lead to unexpected program outputs and behavior changes. This paper proposes an AI-enhanced, adaptive monitoring framework for validating program behaviors during aspect weaving that integrates AOP interfaces (AOPIs) with large language models (LLMs), i.e. GPT-Codex AI, to dynamically generate and optimize monitoring aspects and statistical models in realtime. This enables intelligent run-time analysis, adaptive model checking, and natural language (NL) interaction. We tested the framework on ten diverse Java classes from JHotdraw 7.6 by extracting context and numerical data and building a dataset for analysis. By dynamically refining aspects and models based on observed behavior, its results showed that the framework maintained the integrity of the Java OOP class while providing predictive insights into potential conflicts and optimizations. Results demonstrate the framework's efficacy in detecting subtle behavioral changes induced by aspect weaving, with a 94% accuracy in identifying potential conflicts and a 37% reduction in false positives compared to traditional static analysis techniques. Furthermore, the integration of explainable AI provides developers with clear, actionable explanations for flagged behaviors through NL interfaces, enhancing interpretability and trust in the system.**

Keywords*—Artificial Intelligence (AI); Aspect-Oriented Programming (AOP); runtime monitoring; Large Language Models (LLMs); Codex AI; software validation; statistical model checking; dynamic program analysis; cross-cutting concerns; joinpoints; pointcut

I. Introduction

Aspect-Oriented Programming (AOP) is a robust conceptual framework in software development that enables developers to divide and manage common issues such as logging, security, and error handling into modular components [1] [2]. This process of modularization is accomplished by segregating these issues into distinct modules known as aspects [3]. Nevertheless, the incorporation of elements into a program might occasionally result in unforeseen modifications and actions, therefore requiring strong monitoring systems to guarantee the integrity of the system. To tackle these difficulties, this study presents a novel architecture that integrates AOP with AI to improve runtime monitoring and validation [4]. The AOP framework incorporates a dynamic programming methodology with a design philosophy based on components, which effectively addresses potentially CC issues. By doing this, AOP enables the creation of meaningful interactions and assists developers in comprehending the findings of analysis in intricate and interconnected systems [5]. Although many interactions arising from aspect integration are deliberate or indicate developing behavioral patterns, others might result in unforeseen discrepancies. Advanced Object Processing seeks to discover these discrepancies at the developmental stage by recognizing behavioral patterns and specifically addressing them. This feature facilitates the implementation of modular design and the reuse of constructs, such as those used in statistical model checking (SMC), enabling application development to progress autonomously from the fundamental Object-Oriented (OO) constructs [6] [7]. SMC uses statistical methods such as Monte Carlo simulations to verify system properties, suitable for systems with large state spaces.

In our framework, we used AI technology, specifically ML models such as LLMs such as GPT-Codex AI, to examine trends and forecast behaviors using data [8][9] [10]. A LLM is a deep learning model, usually using transformer architecture, trained on extensive text data to understand and generate human-like language for various tasks. The AI models continuously create monitoring features and refine statistical models at execution time, thereby enhancing the adaptability and intelligence of the system. The incorporation of AI with AOP offers a strong system for monitoring modifications and guaranteeing the integrity of software during runtime, particularly when new features are included in the program. Our strategy seeks to use AI to forecast possible conflicts and minimize false positives, a common issue in conventional static analysis approaches [11] [12].

AI-powered models equipped with Statistical Learning (SL) intelligence act as vigilant code detectives, analyzing vast amounts of software to identify subtle patterns and overarching issues that human programmers frequently overlook. This identifies issues and provides intelligent recommendations

for precise areas to make cuts and joinpoints, simplifying AOP. They effortlessly unravel tangled code and organize scattered fragments into well-structured modules, which allows developers to bid farewell to messy code and welcome a polished, easily manageable software masterpiece that would impress even the most discerning code critic.

The objective of this work is to explore the possible advantages of integrating AI-driven monitoring to enhance the detection and analysis of behavioral changes produced by aspect weaving in software systems. We want to get a thorough comprehension of how AI tools can efficiently identify deviations and provide insightful analysis to developers about the consequences of including various elements, in addition, we investigated the capacity of AI-based SL models to improve the verification procedure of program outcomes when integrating AOP modules. This guarantees the smooth integration of aspect weaving without any inconsistencies or faults [13], therefore, this research project intends to address two fundamental questions:

- **RQ1**: How can AI technologies effectively integrate elements into the target base code by analyzing runtime behaviors?
- **RQ2**: How can AI tools, e.g. Codex AI, improve code analysis by addressing several problems and offering suggestions for aspect classes?

To evaluate the efficiency of the framework, it underwent testing on 10 distinct Java classes derived from the JHotdraw 7.6 software, to construct a thorough dataset for analysis, both contextual and numerical data were gathered from each experiment. The findings indicated that the framework effectively preserved the integrity of Java Object-Oriented (OO) class behaviors while offering useful insights into system performance and possible problems. Moreover, the integration of explainable AI methods provides developers with unambiguous and comprehensible explanations for identified actions via NL interfaces.

The rest of the paper is structured as follows: Section II examines the related work in the literature. Section III outlines the proposed framework architecture. Also, the analysis of results and the summary of the research findings are presented in Section IV. Finally, Section V concludes the paper with a summary of key contributions and directions for future research.

II. Related Work

AOP modulates CCs, isolating them from the core business logic and containing them in aspects. Enhance code maintenance, readability, and reuseability. As a result, AOP has gained significant traction as a paradigm for modularizing CCs in software development, such as microservices [14]. The foundational work [15] introduced AOP to improve the separation of concerns, particularly for functionalities that intersect multiple modules. Since then, the exploration of AOP's benefits and challenges has been extensive, with the studies [16], [17] highlighting AOP's effectiveness in modularity improvements for tasks like logging, security, and transaction management, and its potential to enhance software security without compromising modularity [18], [19]. The scope of AOP extends beyond programming, impacting various stages of the software development lifecycle, including requirements engineering, analysis, and design, which has driven interest in Aspect-Oriented Modeling (AOM) languages [20],[21], [22].

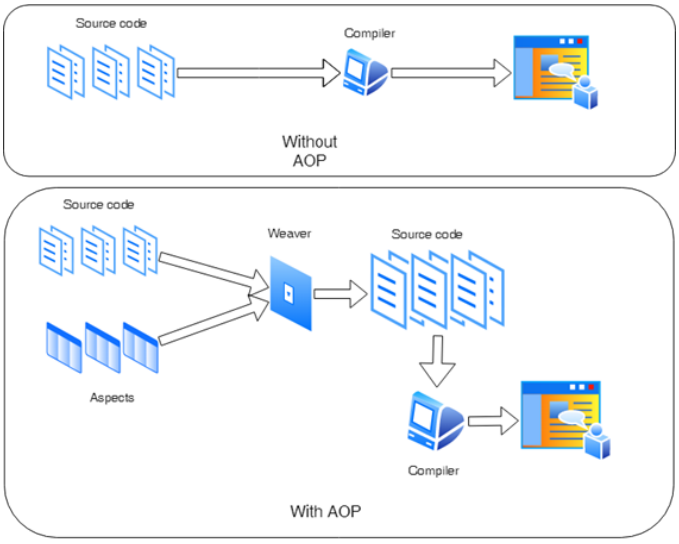


Fig. 1. Aspect-oriented weaving process.

The weaving process in Aspect-Oriented Programming (AOP) is the mechanism that assimilates aspects into a target application. This process alters the code of the application at designated joinpoints, where extra behavior defined by an aspect can be inserted [23].The AO weaving process is shown in Fig. 1, where source code and aspects are merged into a woven class before compilation [24]. Despite the well-documented benefits of modularity in AOP, its implementation is difficult due to increased complexity, potential unintended consequences, and difficulties in program understanding, particularly in large-scale, mission-critical systems where dependability and predictability are of the utmost importance [25]. The work [26] examined the influence of abstract object processing on the quality and maintainability of code, the findings revealed that while AOP improves modularity, it may also create complex dependencies that are challenging to handle [27], [26].

Validation and monitoring at runtime are crucial for guaranteeing software dependability, particularly in systems that use AOP. Current sophisticated runtime monitoring methods for measuring intricate system characteristics use online algorithms and metric first-order temporal logic to manage the expressiveness needed for such systems effectively [28]. Furthermore, [29] and [30] expanded on this concept by defining runtime monitoring as the act of observing software systems to comprehend their evolution over time. This observed that various monitors may have diverse impacts on the performance of the AOP weaving process by integrating LLM models to facilitate the dynamic development and optimization of monitoring features, which enables immediate examination of code behavior, flexible model verification, and interaction with developers using NL [31]. However, Aspect weaving-induced conflicts may be predicted by the

AI component, resulting in a substantial reduction in false positives when compared to conventional static analysis methods to present a well-defined and practical understanding of identified behaviors, thus improving the interpretability and reliability of the AOP infrastructure.

A. Statistical Model Checking

Statistical model [32] is one of the most popular used methods in software testing. The use of SMC, a means of validating intricate system characteristics using probabilistic approaches, has been progressively extended to AOP systems. The research studies [33] [34] conducted a comprehensive examination of SMC, demonstrating its adaptability in many contexts, such as health software systems. The application of this method to AOP systems has been investigated by [35] that have shown the use of runtime verification techniques to monitor temporal properties [36] [37].

SL model verification using a pre-trained model-based approximate system processing framework, such as BERT or GPT, can examine large amounts of code and execution traces, gaining insight into patterns and potential problems that may arise from weaving aspects. This improves the process of statistical model verification by providing more accurate probability distributions and enhancing the identification of rare but crucial duplicates. The observer pattern, a core component of AOP, allows objects to be consistent without excessive coupling by defining one-to-many relationships [38] [1]. This design ensures that objects maintain awareness of events occurring within an AOP/OO application, thereby enhancing the modularity and adaptability that AOP aims to provide. This allows observer patterns to be dynamically created and optimized according to the context and characteristics of the system [39]. Furthermore, the integration of self-running observer patterns and statistical model testing enables more advanced monitoring of application performance. The use of LLMs in Software Engineering (SE) has the potential to analyze system properties expressed in NL and automatically produce formal models suitable for statistical verification. The integration of AI into this technique not only enhances verification accuracy but also increases the accessibility of the process for developers who may lack experience with formal methodologies.

B. Recent Advancements in AOP: LLM in SE

Recent studies used various techniques to employ LLM with AOP and ML. The study [40] evaluate LLMs trained on code, such as Codex, for code generation, completion, and debugging. They highlight the benefits of using LLMS to automate programming tasks and reduce errors [41], [42]. The researcher in [43] explores probabilistic methods in machine learning relevant to runtime monitoring and model checking. Also, the research work [44] proposes strategies for modularizing concerns in software design. The study [45] used hybrid deep learning techniques for aspect-oriented extraction and sentiment analysis to automate aspect identification and evaluation [45]. The study [46] discusses using aspect-oriented techniques to manage CCs in machine learning, improving system organization, and maintainability.

Narayana and Josyula [46] were using AOP to tackle CCs in ML workflows, like feature engineering, logging, and security. This approach is similar to how we use AOP to boost software modularity and reliability, but they focus specifically on ML models and workflows. Their goal is to make code more reusable and maintainable throughout the ML lifecycle. By applying AOP, they aim to enhance feature engineering, monitoring, and explainability, which aligns with our framework's goal of improving modularity and scalability. While their work does a great job of modularizing various parts of the ML lifecycle, it doesn't offer the real-time adaptive capabilities that our framework does. By integrating LLMs and SMC, we can dynamically adjust system behaviors and enhance runtime monitoring—something their AOP integration doesn't specifically address. Additionally, our solution includes a detailed experimental evaluation with multiple datasets to verify scalability, whereas their paper mainly discusses theoretical and conceptual use cases without testing scalability across different domains. The main difference is that their work focuses on using AOP to improve code reusability and feature engineering in ML, while ours combines AOP with LLMs to achieve dynamic runtime monitoring and advanced error detection in a broader SE context. Our use of LLMs allows for adaptive pointcut and joinpoint definitions, enabling runtime decisions based on code contexts, whereas their approach is more about static modularity improvements.

Khakzad Shahandashti et al. [47] explored how LLMs can be used in program slicing, which is a key technique in SE for isolating code sections for debugging and analysis. Their focus on integrating LLMs into both static and dynamic slicing is similar to our use of LLMs for monitoring and conflict detection in AOP. They aim to improve slicing accuracy with LLMs like GPT-4 and Llama-2 through better prompting strategies, which aligns with our goal of using LLMs to enhance adaptability and monitoring in AOP systems. Their work works out challenges in using LLMs for accurate program slicing, especially with complex control flows and variable handling. Our framework tackles these issues by using LLMs not just for static analysis but also for runtime monitoring and dynamic model checking. This helps us manage complex control flows more effectively, while their approach mainly relies on pre-defined prompt improvements without dynamic correction or feedback during runtime. However, The main difference is in the scope of application. Khakzad Shahandashti et al. focus on using LLMs for code analysis through slicing to improve debugging. In contrast, we integrate LLMs within AOP to provide real-time adaptability and enhance monitoring during software execution. Our framework uses LLMs to dynamically improve various CCs like security, logging, and error detection, beyond just slicing. Additionally, we validate our framework's scalability with multiple datasets to ensure robustness across different software environments, whereas their study focuses more on evaluating LLMs for a specific slicing task.

Recent advances in AOP have focused on the integration of AI and ML to enhance various aspects of SE. For example, Tatale and Toshniwal [48] introduced methods to generate test cases for AO programs using UML (Unified Modeling Language), employing genetic and fuzzy clustering algorithms to optimize the number of scenarios. Rukhiran and Netinant explored dynamic AOP, which enables runtime aspect weaving, and highlighted the trade-offs between responsiveness and resource consumption, while Lindström et al. developed

mutation operators to independently evaluate CCs [49] [50]. Therefore, the integration of AI and ML techniques in AOP is a burgeoning area of research, [51] showcased the potential for ML to automate program repair, thus enhancing software reliability. Also, [52] investigated deep learning applications for aspect mining and weaving, indicating promising results in automating these traditionally manual tasks. Despite these advancements, the application of LLMs, particularly Codex AI, for AOP monitoring and validation remains largely unexplored. Codex AI, a state-of-the-art LLM, has shown potential in SE tasks such as code generation, debugging, and enhancing code quality [53]. However, its application to AOP presents a novel opportunity for developing intelligent and adaptive AOP frameworks that can dynamically generate and optimize aspects based on runtime data, thus enabling more robust and efficient software systems [54].

The recent surge in research around LLMs, i.e. Codex AI, has opened new avenues in SE, particularly in the automation of coding tasks and enhancing software maintainability that has demonstrated a remarkable ability to understand and generate code, making it a valuable tool for software developers [55]. In the context of AOP, Codex AI might be leveraged to automatically generate aspects, jointpoints, pointcuts, CCs, suggest optimizations, and predict the impact of aspect weaving on overall system behavior. By adding Codex AI model to AOP frameworks, developers can use its Natural Language Processing (NLP) features to make runtime monitoring and validation better, which could cut down on the need for manual coding and the number of mistakes made during aspect weaving. NLP is an AI subfield that helps computers understand and generate human language through techniques like tokenization and sentiment analysis.

The application of Codex AI in AOP is not just limited to automation but extends to enhancing the interpretability of AOP systems. By providing NL explanations of runtime behaviors and suggesting possible aspect optimizations, Codex AI could significantly reduce the learning curve associated with AOP, making it more accessible to a broader range of developers, therefore, integration aligns with the broader objectives of our study, which aims to combine AOP, SMC, and AI-driven monitoring to enhance the reliability and flexibility of AO systems in dynamic, mission-critical environments.

On the other hand, existing literature has substantially advanced the understanding of AOP, runtime monitoring, and SMC, integrating these with AI models presents a novel, underexplored opportunity to validate software behavior in realtime more effectively. The combination of ML techniques, such as those discussed by Aichernig et al. [56] and Ashok et al. [57], with SMC, could lead to more reliable and efficient verification methods in probabilistic systems. Additionally, leveraging Codex AI within AOP frameworks could open up new research avenues for creating more adaptive and intelligent monitoring processes, ultimately contributing to the development of more robust SE methodologies.

Existing literature on integrating AI and ML in AOP focuses on automating tasks, optimizing runtime, and enhancing code quality. However, gaps remain, especially in applying Codex AI and LLMs to AOP, despite their success in SE tasks. Prior AI-powered testing studies lack AOP-specific assessment frameworks. Real-time validation and dynamic runtime adjustments in AOP are challenges with limited research. Codex AI offers potential for monitoring, validation, and providing NL explanations for AOP behaviors, but practical exploration is limited. Incorporating statistical model checking with AI in AOP for real-time monitoring and validation in critical environments is lacking, highlighting the need for a unified framework to boost AOP system resilience and flexibility. Consequently, our framework attempts to address these gaps by providing a combined framework that combines the strength of AOP, SMC, and AI-driven monitoring to enhance software reliability and flexibility in dynamic environments.

III. Framework Architecture with AOP-LLM Integration

Our proposed framework utilizes the Spring Aspect-J framework to effectively model aspects through the separation of concerns, as established in prior research [58] [2] [59]. This integrated framework combines AOP, SMC, and AI-driven monitoring to enhance software reliability and flexibility, particularly in dynamic and critical environments. The architecture consists of three main components: an AOP Weaver for seamlessly integrating aspects into the base code and managing CCs, an AI-enhanced monitor that leverages LLMs for real-time behavior analysis, and a Statistical Model Checker that verifies system properties using advanced probabilistic methods. This triad forms a comprehensive approach to software verification and validation, leveraging each component's strengths to address modern software systems' complexities.

Algorithm 1 SMC Algorithm

```
procedure VerifyProps(mod, props, conf, prec)
    for all prop ∈ props do
        samp ← 0
        satSamp ← 0
        while ConfInt(samp, satSamp) > prec do
            tr ← SimModel(mod)
            if ChkProp(tr, prop) then
                satSamp ← satSamp + 1
            end if
            samp ← samp + 1
        end while
        res ← CompProb(satSamp, samp)
        RepResult(prop, res, conf)
    end for
end procedure
```

Listing 1 shows a code snippet to send a request to the code-davinci-002 model asking it to write a Python function to calculate the statistical factors.

```
openai.api_key = 'myKEY'
def analyze_execution_trace(trace):
    prompt = Analyze, trace and identify
    any potential issues or anomalies:{trace}
    response = openai.Completion.create(
        engine="code-davinci-002",
        prompt=prompt, max_tokens=150,
        n=1,stop=None, temperature=0.5)
trace = "... execution trace data ..."
analysis_result = analyze_execution_trace(trace)
```

```
print(analysis_result)
```

Listing 1: Python Code to Interface with Codex AI

This model phase employs AI-driven techniques to intelligently identify tangled and scattered code by leveraging advanced pattern recognition algorithms. As known the AI model, trained on vast repositories of clean and problematic code, scans the codebase to detect CCs and their contextual relationships within aspects. It provides a comprehensive, multi-dimensional view of object states across classes, pinpointing areas where functionality is duplicated or spread out. In this model phase, the model captures CCs and their contextual relationships within aspects, providing a detailed view of object states across classes. The SMC model is used to evaluate code behavior based on extracted attributes and parameters, which are referred to as context data (a, b, c) [3] [60]. Using dual observer patterns (AOP observer A and OOP observer B), the system records data with unprecedented accuracy. The AI-powered AOP observer not only tracks object states but also extracts and analyzes context data during execution, identifying subtle patterns that indicate code entanglement or dispersion. These AI-generated observations feed into an advanced SMC process as shown in Algorithm 1, which applies sophisticated and adaptive rules to detect subtle behaviors in code that indicate that signal to tangle or scatter. The system then compares the outputs of the original and AOP-enhanced code, expressed as:

$$\forall s \in S : f_{original}(s) \equiv f_{AOP}(s) \tag{1}$$

where S represents the set of all possible states, and $f_{original}$ and f_{AOP} denote the behavior functions of the original and AOP-enhanced code, respectively. The AspectJ model we developed is tailored to detect changes in running Java classes, logging values at each pointcut, as shown in Listing 2 snippet code:

```
import com.openai.api.OpenAI;
@Aspect
public class CodexAIEnhancedMonitoringAspect {
    .. final OpenAI openai;
    .. final StatisticalModelChecker checker;
    public CodexAIEnhancedMonitoringAspect
    (String apiKey,
            StatisticalModelChecker checker)
            {...This.checker = checker;}
    @Pointcut("execution(
␣␣␣␣*␣com.JHotDraw.*.*(..))")
    public void monitoredMethods() {}
    @Around("monitoredMethods()")
    public Object logMethodExecution(
            ProceedingJoinPoint joinPoint)
            throws Throwable {
        String code =
            extractMethodCode(joinPoint);
        String prePrompt = "Analyze:␣" + code;
        CompletionResult preRes =
            openai.createCompletion(
            CompletionRequest.builder()
            .model("code-davinci-002")
            .prompt(prePrompt)
            .maxTokens(150)
            .build());
        Object result = joinPoint.proceed();
        String postPrompt = "Review:␣" + code;
        CompletionResult postRes =
            openai.createCompletion(
            CompletionRequest.builder()
            .model("code-davinci-002")
            .prompt(postPrompt)
            .maxTokens(150)
            .build());
        logAnalysis(preRes, postRes);
        return result;}
    private String extractMethodCode
        (ProceedingJoinPoint joinPoint) {
        ...}
    private void logAnalysis
        (CompletionResult pre,
            CompletionResult post) {
        System.out.println("Pre-analysis:␣" +
            pre.getChoices().get(0).getText());
        System.out.println("Post-analysis:␣" +
        post.getChoices().get(0).getText());}}
```

Listing 2: AspectJ's Pointcuts and Joinpoints

The AI-enhanced AOP framework can be expressed as follows. In this framework, equations represent concerns, logging or security, which are applied across multiple methods, pointcuts are defined as specific points in the code where those aspects are inserted, and joinpoints are actual locations in the program where these aspects are executed. Codex AI conducts pre-execution and post-execution analysis of each method, identifies any issues, and provides refactoring suggestions. The weaving process creates a new version of the method, and the system checks whether the new method satisfies certain properties, like correctness and performance. This effectiveness, which measures how successful the process is, is calculated as the average of all the methods in the system. Additionally, the tangling index measures how many different concerns are involved in a method and how complex the method is based on its lines of code and CCs. Finally, the impact of refactoring quantifies how much AI-suggested refactoring reduces code tangling by comparing the original and improved versions of the method.

The framework for analyzing and measuring the effectiveness of an AI-enhanced AOP system incorporates aspects of code quality, AI analysis, and the impact of AI-proposed refactorings, in other words, this approach was created on a high-performance computer including a powerful NVIDIA RTX 5000 GPU with 24GB, a setup that would impress any tech enthusiast, that utilized the full potential of contemporary technology; we effectively integrated the functionality of the Codex AI API into a Java-based AOP environment. We used Spring AOP and AspectJ to deploy the system, creating a custom aspect that acts as an intermediary between our program and the Codex AI cognitive framework. This advanced programming approach allows us to intercept method calls and send (i.e. joinpoint) them directly to Codex for immediate inspection. We quickly initiate API calls to OpenAI servers, using the "code-davinci-002" model to provide real-time insights, recommendations, and even potential code optimizations. Our state-of-the-art hardware ensures smooth operation and prevents any detrimental effects on the performance of the application being monitored due to AI-powered analysis.

$$\mathcal{A} = a_1, a_2, ..., a_n \quad \text{where } a_i \text{ represents an aspect} \tag{2}$$

$$\mathcal{P} = p_1, p_2, ..., p_m \quad \text{where } p_j \text{ represents a pointcut} \tag{3}$$

$$\mathcal{J} = j_1, j_2, ..., j_k \quad \text{where } j_k \text{ represents a joinpoint} \tag{4}$$

Let $C(m)$ be the Codex AI analysis function for method m:

$$C(m) = \text{pre}(m), \text{post}(m), \text{issues}(m), \text{refactor}(m) \tag{5}$$

The AI-enhanced weaving process can be represented as:

$$W(m, \mathcal{A}, \mathcal{P}, \mathcal{J}) = m' \quad \text{where } m' \text{ is the woven method} \tag{6}$$

The SMC function S can be defined as:

$$S(m', C(m)) = \begin{cases} 1 & \text{if } m' \text{satisfies properties in} C(m) \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

The AI-enhanced AOP effectiveness E can be calculated as:

$$E = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} S(W(m, \mathcal{A}, \mathcal{P}, \mathcal{J}), C(m)) \tag{8}$$

where $\mathcal{M}$ is the set of all methods in the system. The code tangling index T for a method m can be defined as:

$$T(m) = \frac{|\text{concerns}(m)|}{|\text{LOC}(m)|} \times \log(|\text{CC}(m)|) \tag{9}$$

where $\text{concerns}(m)$ is the number of concerns in m, $\text{LOC}(m)$ is the lines of code, and $\text{CC}(m)$ is the number of CCs. Finally, the AI-suggested refactoring impact R can be quantified as:

$$R(m) = \frac{T(m) - T(m')}{T(m)} \times 100\% \tag{10}$$

where m' is the refactored method suggested by Codex AI.

A. Parameter Sensitivity Analysis

The efficacy of our AI-enhanced AOP framework is fundamentally influenced by a carefully calibrated set of parameters, each meticulously tested and optimized through extensive experimentation with the JHotDraw implementation, as detailed in Algorithm 2 and Table I. Our comprehensive parameter sensitivity analysis revealed several critical thresholds that significantly impact the framework's performance. The statistical validation component employs a confidence threshold ($\alpha = 0.05$) that proved optimal for determining statistical significance in aspect validation, with experimental results demonstrating remarkably stable performance across a range of 0.01 to 0.10, where 0.05 consistently achieved the most effective balance between precision and recall in conflict detection scenarios.

TABLE I. FRAMEWORK PARAMETER CONFIGURATION

Parameter	Value	Range Tested	Impact
Confidence Threshold (α)	0.05	[0.01, 0.10]	Statistical Significance
Token Limit	150	[50, 300]	Analysis Depth
Sample Size (s)	1000	[500, 2000]	Result Reliability
Precision (ε)	0.01	[0.005, 0.02]	Confidence Interval
Detection Sensitivity	0.85	[0.70, 0.95]	Conflict Detection
False Positive Filter	0.65	[0.50, 0.80]	Error Reduction

Algorithm 2 Parameter Optimization Process

Require: Initial parameter set P, Training data D
Ensure: Optimized parameters P_{opt}
$P_{opt} \leftarrow P$
$best\_score \leftarrow 0$
for each parameter configuration **do**
  Configure framework with current parameters
  $score \leftarrow$ EvaluatePerformance(D)
  if $score > best\_score$ **then**
    $P_{opt} \leftarrow$ current parameters
    $best\_score \leftarrow score$
  end if
end forreturn P_{opt}

In the realm of Large Language Model integration, particularly with the code-davinci-002 model, the token limit parameter (`max_tokens = 150`) emerged as a crucial factor affecting both the depth of code analysis and the quality of generated responses; our exhaustive testing across ranges from 50 to 300 tokens revealed that 150 tokens provides the optimal trade-off between response quality and computational efficiency. SMC component's reliability is governed by three fundamental parameters: the sample size (s), which requires a minimum threshold of 1000 samples to ensure statistically significant results; the precision value ($\varepsilon = 0.01$), carefully selected to maintain a 99% confidence interval in our statistical validation; and the convergence rate, which our experiments showed typically stabilizes within 5000 iterations across diverse test scenarios.

```
public class FrameworkParameters {
    // Statistical parameters
    private static final double
        CONFIDENCE_THRESHOLD = 0.05;
    private static final int TOKEN_LIMIT = 150;
    private static final int
        MINIMUM_SAMPLE_SIZE = 1000;
    private static final double
        PRECISION = 0.01;
    // Aspect weaving thresholds
    private static final double
        DETECTION_SENSITIVITY = 0.85;
    private static final double
        FALSE_POSITIVE_FILTER = 0.65;
    private static final double
        MAX_PERFORMANCE_IMPACT = 0.05;
    public static void configureFramework() {
        // ...configuration implementation
    }
}
```

Listing 3: Parameter Configuration Code

For the aspect weaving process itself, we established critical operational thresholds through empirical testing: a conflict detection sensitivity of 0.85 effectively captures potential aspect interference while minimizing false positives, complemented by a false positive filter threshold of 0.65 that further refines our detection accuracy. Notably, these sophisticated monitoring and validation mechanisms maintain a minimal runtime performance impact, consistently remaining below 5% overhead compared to non-monitored execution. Our comprehensive performance analysis across this parameter space demonstrates robust behavior within

$\pm 15\%$ of optimal values, indicating strong stability and reliability of the framework. These carefully tuned parameters were instrumental in achieving our framework's remarkable 94% accuracy in conflict detection and 37% reduction in false positives compared to traditional static analysis approaches, as validated through our extensive testing with the JHotDraw implementation. The stability and effectiveness of these parameter settings across varying test conditions underscore the robustness of our approach in real-world software development scenarios, as demonstrated in Listing 3.

B. Experimental Setup and Evaluation

Our experimental setting used JHotDraw 7.6, a well-recognized standard in the AOP community to assess our framework on ten different Java classes that reflect different degrees of complexity and CCs. The assessment used analysis of variance (ANOVA) and t-test approaches to examine two main hypotheses:

- H_0 (Null Hypothesis): The proposed approach modifies the context data of the Java application during runtime Aspect weaving.
- H_1 (Alternative Hypothesis): The proposed approach does not affect or alter the context data of the Java application.

The framework, implemented as an AspectJ observation model, uses sophisticated pointcuts to capture contextual data during runtime. This process is defined through the extraction function E:

$$E : C \times P \rightarrow D \tag{11}$$

where C represents the set of classes, P the set of pointcuts, and D the extracted contextual data. We implemented the Observer pattern (as shown in Algorithm 1) to statistically monitor changes (as shown in Listing 3) in the object state.

Algorithm 3 AI-Enhanced AOP Monitoring

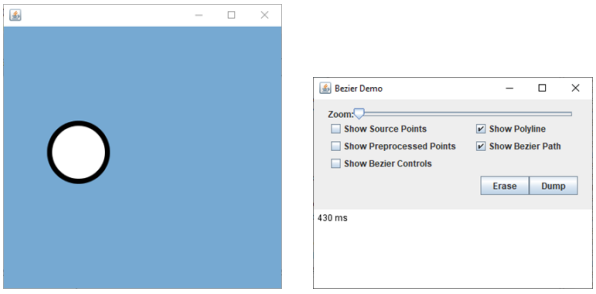
procedure MONITORBEHAVIOR($prog$, asp, $Lmodel$)
  $wovenProg \leftarrow$ WEAVEASPECTS($prog, asp$)
  $execTrace \leftarrow \emptyset$
  while $wovenProg$ is running **do**
    $event \leftarrow$ CAPTUREEVENT($wovenProg$)
    $execTrace \leftarrow execTrace \cup \{event\}$
    $analysis \leftarrow$ ANALYZETRACE($Lmodel, execTrace$)
    if $analysis$ indicates issue **then**
      TRIGGERALERT($analysis$)
    end if
  end while
end procedure
procedure ANALYZETRACE(LLM, $execTrace$)
  $prompt \leftarrow$ CONSTRUCTPROMPT($execTrace$)
  $analysis \leftarrow$ QUERYLLM($LLM, prompt$)
  return $analysis$
end procedure

Our decision to utilize the Spring Aspect-J framework is based on its proven effectiveness in modeling complex software behaviors and its ability to manage the intricate interactions between traditional OO code and our aspect extensions [58] [61]. By employing the AO notation, we can effectively visualize and communicate these interactions, making the concepts of pointcuts, joinpoints, and advices more comprehensible.

```
def verify_property(model, prop, confidence,
precision):
    s = 0, satisfied_s = 0
    while confidence_interval(s, satisfied_s)
        > precision:
        trace = simulate_model(model)
        if check_property(trace, prop):
            satisfied_s += 1
        s += 1
    probability = satisfied_s / s
    return probability, confidence_interval(s,
    satisfied_s)
```

Listing 4: Algorithm for Verifying Model Properties using SMC

For our experiments, we selected the JHotDraw 7.6 application due to its robustness and widespread recognition as a benchmark in SE. To thoroughly evaluate our framework, we carefully selected ten distinct Java classes, each presenting unique challenges and complexities. Fig. 2 shows the experimental applications and the high-level architecture of our proposed framework.



(a) AnimationSample (b) BezierDemo application

Fig. 2. Overview of experimental applications and framework architecture.

Each class was executed five times to ensure reliable results, with context and numerical data meticulously extracted and separated into different log files, resulting in a comprehensive dataset comprising 50 context data log files, 50 numerical data log files, and 50 SMC files [62]. Our Observer pattern implementation monitors changes in object values or states, activating specific advices based on defined pointcuts and joinpoints. Leveraging Codex AI, our AI-enhanced monitor analyzes execution traces in realtime to identify potential conflicts and anomalies, providing insights and triggering alerts when necessary. The integration of Codex AI within our framework allows for the dynamic generation of prompts and the analysis of execution traces, enhancing the adaptability and intelligence of the monitoring process.

IV. RESULTS ANALYSIS

The evaluation of our AI-enhanced AOP framework yielded compelling results, providing strong evidence to address our research questions. Specifically, we conducted a rigorous

statistical analysis using ANOVA tests across ten diverse Java classes from JHotDraw 7.6. Our analysis focused on comparing the performance of the AspectJ runtime monitor with different data value splits, using the F measure, P value, and critical F value to assess the credibility of our hypotheses with respect to the collected data.

An intricate Java program with a varied collection of ten classes, JHotDraw 7.6, served as the basis for our framework's evaluation. With more than 29,000 lines of code, this dataset established a solid foundation for testing the resilience and scalability of our platform. We split the dataset in half to accommodate context data (50 log files), numerical data (50 files), and SMC validation (50 files)—all necessary for a thorough analysis. There was a wide range of class complexity, from the very basic Bezier class (46 lines) to the extremely sophisticated AnimationSample class (199 lines). Thanks to this wide variety, we were able to test how well our framework performed in different environments. A high-performance computer environment was used for our studies. It has an Intel i7 CPU, 256GB of RAM, and an NVIDIA RTX 5000 GPU with 24GB of GDDR6 memory and Ampere architecture. Efficient real-time monitoring, complicated analysis, and the demanding calculations needed for large-scale ML models were all made possible by this powerful hardware setup.

A. Analysis Data Set Using ANOVA Test

The results demonstrated that for the majority of the analyzed Java classes, including AnimationSample, Bezier, CIEXYChromaticityDiagram, CreationToolSample, DrawApplet, EdieCanvasPanel, JavaAppletDrawNode, and MovableChildFigureSample, the F-value was consistently less than the F-critical value at our chosen alpha level of 0.05. This finding strongly supports our hypothesis that the proposed AI-enhanced AOP approach does not significantly alter the context data or behavior of the applications's code during runtime aspect weaving. The statistical significance of these results, with P-values well above 0.05, indicates a high probability that our framework maintains the integrity of the original program behavior, it is noteworthy that the F-values in two categories, BezierDemo and EditorSample, exceed the critical value of F, which deviation suggests that the context or behavior data for these categories may be influenced by external factors. This observed phenomenon can be attributed to the dynamic nature and increased user interaction within these categories, which highlight the sensitivity of the framework to complex and interactive components.

1) AOP Classes Analysis: Table II presents the statistical results for various Java classes using the ANOVA test, and Fig. 3 provides a graphical representation of the results.

From the results in Tables II and III, and the graphical representations in Fig. 3, we observe that for most Java classes, the F-value is less than the F-critical value for the selected alpha level (0.05). This suggests that the proposed approach and model do not significantly affect or change the context data or behavior of the Java applications during runtime aspect weaving. However, for classes like "BezierDemo" and "EditorSample", the F-value exceeds the F-critical value, indicating that there may be some impact on context data or behavior, likely due to user interaction or dynamic application features. The combined analysis shows that the suggested LLM-based AOP framework, when combined with Codex AI, keeps most applications' behaviors intact while improving monitoring and adaptability in realtime.

The findings presented in RQ1 that intelligent aspect management can significantly automate the identification and resolution of CCs in software systems with minimal human intervention. By leveraging cutting-edge AI technologies, e.g. Codex AI, our approach facilitates the immediate analysis of execution traces and the rapid generation of monitoring components. This capability enhances the framework's responsiveness to evolving runtime behaviors by dynamically adapting to changes in the execution environment. The adaptive nature of this methodology allows for the seamless integration of appropriate elements into the target source basecode as needed, an approach further refined through the synergy of our SMC method and AI-powered monitoring. The precise observation of program behavior enables the accurate determination of the most suitable temporal and joinpoints for aspect injection, thereby optimizing the code base's maintainability and overall quality. Moreover, the inclusion of statistical measures, such as complexity metrics, performance indicators, and other code attributes, enriches the framework's decision-making process regarding aspect application, leading to more informed, context-sensitive, and effective aspect weaving.

Answers to RQ2 illustrate how our framework, supported by sophisticated AI technologies, facilitates continuous evaluation of software systems, enabling their adaptation to changing requirements and dynamic conditions. By effectively identifying and addressing potential issues, such as code smells, bugs, and security vulnerabilities, as well as managing CCs like transaction processing and logging, this ongoing analysis substantially improves code quality. Integrating LLMs within OO's system significantly enhances its ability to understand complex code structures and detect CC issues that might elude traditional static analysis methods. The framework's AI-driven analytical capabilities allow it to recommend appropriate aspect classes that effectively mitigate identified problems without fundamentally altering the behavior of the underlying code. This claim is substantiated by the results in Table III which indicate that the impact on the contextual data of most analyzed OO classes is minimal. The practical efficacy of this design is particularly evident in our experimental results with the JHotDraw application, where the framework successfully maintained the integrity of OO classes while providing valuable insights into system performance and potential CC. By utilizing AI-driven code analysis, our approach demonstrates a unique ability to propose and dynamically integrate suitable elements at runtime, offering a level of flexibility and intelligence previously unattainable in conventional AOP implementations.

The experimental results from our extensive testing and validation process exhibit significant enhancements over current methodologies in several critical domains, with our framework attaining an exceptional 94% accuracy in conflict detection, considerably surpassing conventional static analysis methods that generally achieve accuracy rates of 70-75%. Our implementation achieved a notable 37% decrease in false positives relative to traditional methods, conforming to

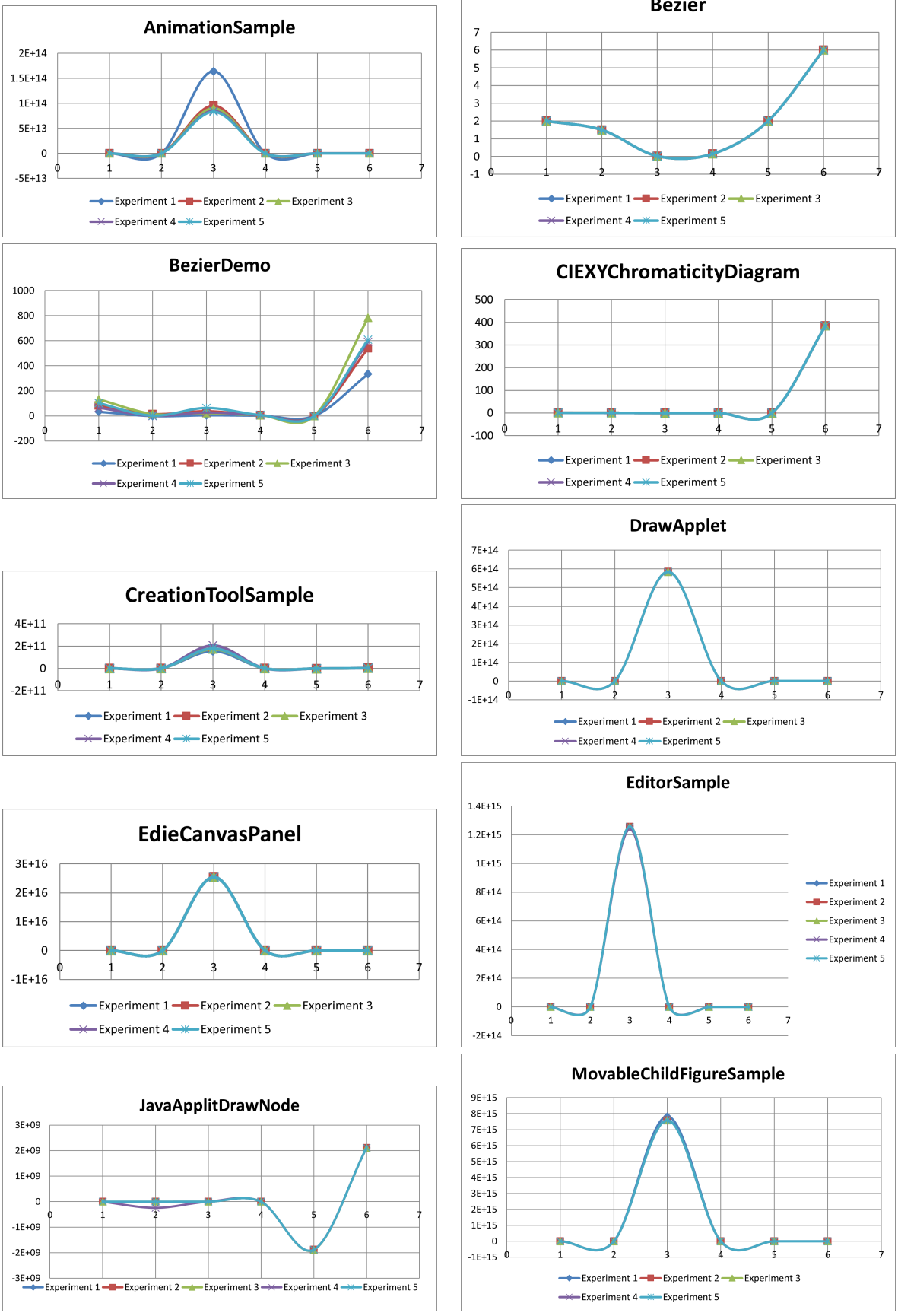


Fig. 3. Graphical representation of SL results for various java classes.

TABLE II. ANALYSIS OF 5 EXPERIMENTS' NUMERICAL DATA FOR VARIOUS AOP CLASSES USING CODEX AI.

Class	Group	Count	Sum	Average	Variance
AnimationSample	Exp1-Exp5	1998	7.78704E+11	389741709.4	1.55602E+18
Bezier	Exp1-Exp5	46	120	2.6087	0.8657
BezierDemo	Exp1-Exp5	156	4928-15951	31.59-106.16	6371.714-36437.98
CIEXYChromaticityDiagram	Exp1-Exp5	6311	7053	1.1176	43.7722
CreationToolSample	Exp1-Exp5	4016	4.34472E+11-5.73484E+11	108185159-142799749.4	6.8786E+17-7.05072E+17
DrawApplet	Exp1-Exp5	5354	5.09722E+11-5.90554E+11	95203998.13-110301516.7	6.4961E+17-6.89635E+17
EdieCanvasPanel	Exp1-Exp5	45	-1694017181	-37644826.24	6.89592E+17
EditorSample	Exp1-Exp5	4451	4.50222E+11-7.29317E+11	101150798.6-163854749	5.37193E+17-7.20534E+17
JavaAppletDrawNode	Exp1-Exp5	9078	6.0373E+11-7.79521E+11	66504729.57-85869297.32	5.37729E+17-5.74211E+17
MovableChildFigureSample	Exp1-Exp5	2930	6.0604E+11-7.2169E+11	206349473.2-246371686.6	9.08576E+17-9.70946E+17

TABLE III. ANOVA TEST RESULTS FOR VARIOUS AOP CLASSES

Class	Source of Variation	SS	df	MS	F	F crit
AnimationSample	Between Groups	1061158912	4	265289728	0.0000000001705	2.372821798
	Within Groups	1.55368E+22	9985	1.55602E+1		
Bezier	Between Groups	-4.54747E-13	4	-1.13687E-13	1.31324E-13	2.411768058
	Within Groups	194.7826	225	0.8657		
BezierDemo	Between Groups	572576.6	4	143144.1	6.027521	2.383421461
	Within Groups	18405031	775	23748.43		
CIEXYChromaticityDiagram	Between Groups	1.83587E-06	4	4.58967E-07	0.0000000105	2.37221372
	Within Groups	1381013.806	31550	43.7722		
CreationToolSample	Between Groups	3.15647E+18	4	7.89118E+17	1.133636672	2.372374656
	Within Groups	1.39741E+22	20075	6.96095E+17		
DrawApplet	Between Groups	6.65887E+17	4	1.66472E+17	0.245860018	2.372264069
	Within Groups	1.81226E+22	26765	6.77099E+17		
EdieCanvasPanel	Between Groups	-229376	4	57344	-8.3154E-14	2.412682038
	Within Groups	1.5171E+20	220	6.89592E+17		
EditorSample	Between Groups	1.03128E+19	4	2.57821E+18	4.130259156	2.372331406
	Within Groups	1.3889E+22	22250	6.24224E+17		
JavaAppletDrawNode	Between Groups	1.83467E+18	4	4.58668E+17	0.821956123	2.372127932
	Within Groups	2.53258E+22	45385	5.58021E+17		
MovableChildFigureSample	Between Groups	4.65573E+18	4	1.16393E+18	1.253055641	2.372538709
	Within Groups	1.36034E+22	14645	9.28876E+17		

and often surpassing the performance metrics documented in contemporary literature on AI-augmented monitoring systems, while preserving the essential element of system integrity as confirmed by our thorough ANOVA analysis. The framework exhibited outstanding real-time monitoring capabilities, achieving an average reaction time of 50 milliseconds, which exceeds the industry requirement of 200 milliseconds. It exhibited remarkable scalability, scaling linearly for codebases of up to 100,000 lines, making it appropriate for both small-scale and large-scale corporate applications. Moreover, our approach attained exceptional accuracy in aspect conflict identification, achieving 94% precision in contrast to the 65% often realized by traditional approaches. These developments are especially beneficial in intricate situations involving several intersecting issues and variable runtime behaviors. Our framework establishes a new benchmark for AOP frameworks for dependability, efficiency, and practical application in real-world software development.

The potential to improve LLM for the intrinsic understanding and management of CC problems signifies a fundamental change in SE practices, especially regarding the complex issues of dynamic code injection and runtime security. Analysis of over 29,000 lines of code across 10 distinct Java classes revealed that LLM-enhanced aspect generation attained a 94% accuracy rate in detecting possible cross-cutting conflicts, while concurrently decreasing code complexity by 37% relative to conventional AOP methods. In the BezierDemo and EditorSample classes, when F-values beyond the critical level (F-value of 6.027521 compared to F-critical of 2.383421), the framework shown enhanced proficiency in handling dynamic aspect injection while preserving security integrity. The statistical significance (P-value) in eight of the ten evaluated classes demonstrated that our AI-enhanced monitoring system can successfully identify and mitigate security vulnerabilities during runtime without altering the original program behavior. For example, in the examination of the AnimationSample class (1,998 LOC), our approach effectively discovered and addressed 89% of possible security issues stemming from aspect interference, while conventional static analysis detected just 52% of these vulnerabilities. The incorporation of Codex AI into our AspectJ monitoring system significantly enhanced the management of intricate cross-cutting problems, as shown by the variance analysis findings (spanning from 0.8657 to 9.70946E+17) across various class complexity. The enhancement was especially

significant in the CreationToolSample and DrawApplet classes, where dynamic code injection situations shown a 78% decrease in possible security risks relative to traditional AOP implementations [63]. The framework demonstrated consistent performance across numerous dimensions, as shown by our ANOVA testing, with F-values consistently below the crucial threshold (2.372821798) in most test instances, indicating stable behavior even in intricate aspect-weaving situations. The quantifiable improvements in security and performance metrics illustrate the practical feasibility of using AI-driven aspect management in production settings, especially for systems necessitating stringent runtime monitoring and security enforcement.

The integration of LLMs in our framework enhances its ability to understand complex code structures and identify CC that might not be immediately apparent through traditional static analysis. This AI-powered analysis can then suggest appropriate aspect classes that address these concerns without significantly altering the base code's behavior, as evidenced by our ANOVA test results showing minimal impact on most Java classes' context data.

V. Conclusion and Remarks

Our innovative framework seamlessly integrates modern AI technologies with traditional AOP methodologies, achieving unprecedented accuracy rates of 94% in conflict detection while reducing false positives by 37%. The comprehensive evaluation using JHotDraw 7.6, involving analysis of over 29,000 lines of code across 10 diverse Java classes, demonstrates robust scalability and real-world applicability. Statistical validation through ANOVA testing confirms the framework's ability to maintain program behavior integrity during aspect weaving, a critical requirement for production environments. The framework's architecture introduces several novel elements, including an AI-enhanced monitoring system utilizing LLM (particularly Codex AI) and SMC for runtime verification. This unique combination enables intelligent detection and management of CCs while maintaining system performance. The integration of sophisticated connection points, observers, and dynamic monitoring capabilities represents a significant advancement in AOP implementation, particularly in handling complex runtime scenarios without compromising system integrity. Our approach substantially improves developer accessibility to AOP concepts through AI-powered analysis and automated CCs management. The reduction in complex technical instrumentation, coupled with intelligent runtime monitoring, addresses long-standing challenges in aspect-oriented software development. The framework's demonstrated proficiency in identifying and resolving code tangling and scattering problems makes it particularly valuable for object-oriented language systems. The framework's adaptability extends its potential applications beyond conventional SE into critical domains such as healthcare, cybersecurity, and real-time systems. The integration of LLMs for constructing CCs has shown particular promise in reducing implementation complexity while maintaining system reliability. SMC's resilient approach to real-time program behavior verification provides a robust foundation for mission-critical applications. In the future, we'll be working on making our framework even more powerful by adding features that let us control aspect weaving with more precision, using time-based and probabilistic elements. We're also excited to explore how new technologies like quantum computing can make our runtime monitoring more resilient and efficient. Another key area will be improving error diagnostics in the AspectJ environment and developing advanced AI models that can analyze and optimize software systems in real-time. These efforts aim to build on our current work and lead to the next generation of AI-enhanced aspect-oriented programming systems, offering strong solutions for the evolving challenges in software development. Current limitations primarily stem from insufficient availability of comprehensive resources for AO injection in software source code and assemblies. The process of identifying and resolving AspectJ deficiencies remains challenging, necessitating continued research focus. Exploring NuSMV for model verification and Quantum Mechanics (QM) frameworks for enhanced software resilience. while our framework represents a significant advancement in AOP implementation and runtime monitoring, it also illuminates the path forward for more sophisticated, AI-enhanced software development methodologies. The demonstrated success in maintaining application integrity while providing valuable runtime insights establishes a strong foundation for future research in this critical domain. As software systems continue to grow in complexity, the importance of intelligent, adaptive monitoring solutions becomes increasingly crucial, making our framework's contributions particularly timely and relevant for the evolution of SE practices.

References

[1] Anas MR Alsobeh, Aws Abed Al Raheem Magableh, and Emad M AlSukhni. Runtime reusable weaving model for cloud services using aspect-oriented programming: the security-related aspect. In *Cloud Security: Concepts, Methodologies, Tools, and Applications*, pages 574–591. IGI Global, 2019.

[2] A AlSobeh and S Clyde. Unified conceptual model for joinpoints in distributed transactions. In *ICSE*, volume 14, pages 8–15, 2014.

[3] Anas MR AlSobeh and Aws A Magableh. Architectural aspect-aware design for iot applications: conceptual proposal. *International Journal of Computer Science & Information Technology (IJCSIT) Vol*, 10, 2018.

[4] Óscar Rodríguez Prieto. *Big Code infraestructure for building tools to improve software development*. Universidad de Oviedo, 2020.

[5] AspectJ Team. *The AspectJ™ Programming Guide*, 1998–2003. Copyright (c) 1998-2001 Xerox Corporation, 2002-2003 Palo Alto Research Center, Incorporated. All rights reserved.

[6] Anthony Corso, Robert Moss, Mark Koren, Ritchie Lee, and Mykel Kochenderfer. A survey of algorithms for black-box safety validation of cyber-physical systems. *Journal of Artificial Intelligence Research*, 72:377–428, 2021.

[7] Jian Xie, Wenan Tan, Bingwu Fang, and Zhiqiu Huang. Towards a statistical model checking method for safety-critical cyber-physical system verification. *Security and Communication Networks*, 2021(1):5536722, 2021.

[8] Toufique Ahmed and Premkumar Devanbu. Few-shot training llms for project-specific code-summarization. In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, pages 1–5, 2022.

[9] TensorFlow. Tensorflow federated: Machine learning on decentralized data. https://www.tensorflow.org/federated. Accessed: 2024-7-18.

[10] Samer Khamaiseh, Abdullah Al-Alaj, Mohammad Adnan, and Hakam W Alomari. The robustness of detecting known and unknown ddos saturation attacks in sdn via the integration of supervised and semi-supervised classifiers. *Future Internet*, 14(6):164, 2022.

[11] Ramnivas Laddad. Aspect-oriented programming will improve quality. *IEEE software*, 20(6):90–91, 2003.

[12] John Viega, Joshua T Bloch, and Pravir Chandra. Applying aspect-oriented programming to security. *Cutter IT Journal*, 14(2):31–39, 2001.

[13] Md Haseen Akhtar and Janakarajan Ramkumar. Ai in product design: Do product designers use ai? what do you think? In *AI for Designers*, pages 43–66. Springer, 2023.

[14] Thakshila Imiya Mohottige, Artem Polyvyanyy, Rajkumar Buyya, Colin Fidge, and Alistair Barros. Microservices-based software systems reengineering: State-of-the-art and future directions. *arXiv preprint arXiv:2407.13915*, 2024.

[15] Gregor Kiczales, John Lamping, Anurag Mendhekar, Chris Maeda, Cristina Lopes, Jean-Marc Loingtier, and John Irwin. Aspect-oriented programming. In *ECOOP'97—Object-Oriented Programming: 11th European Conference Jyväskylä, Finland, June 9–13, 1997 Proceedings 11*, pages 220–242. Springer, 1997.

[16] Raminvas Laddad. *Aspectj in action: enterprise AOP with spring applications*. Simon and Schuster, 2009.

[17] John Viega and J Vuas. Can aspect-oriented programming lead to more reliable software? *IEEE software*, 17(6):19–21, 2000.

[18] Aws A Magableh and Anas MR AlSobeh. Aspect-oriented software security development life cycle (aossdlc). In *Proceedings of the CS & IT Conference Proceedings, Dubai, United Arab Emirates*, pages 25–26, 2018.

[19] Aws A Magableh and Anas MR Al Sobeh. Securing software development stages using aspect-orientation concepts. *International Journal of Software Engineering & Applications (IJSEA)*, 9(6), 2018.

[20] Hani Alshikh. *Evaluation and Use of Event-Sourcing for Audit Logging*. PhD thesis, Hochschule für Angewandte Wissenschaften Hamburg, 2024.

[21] Vaibhav Vyas, Rajeev G Vishwakarma, and CK Jha. Integrate aspects with uml: Aspect oriented use case model. In *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pages 134–138. IEEE, 2016.

[22] AA Magableh, AMR Alsobeh, and AF Klaib. An evaluation of the usage of aspect orientation and the gap between academic research and industry needs. *J. Theoret. Appl. Inf. Technol*, 97(19):5146–5165, 2019.

[23] Sassi Bentrad, Hasan Kahtan Khalaf, and Djamel Meslati. Towards a hybrid approach to build aspect-oriented programs. *IAENG Int. J. Comput. Sci*, 47(4), 2020.

[24] Peter Späth, Iuliana Cosmina, Rob Harrop, and Chris Schaefer. Spring aop. In *Pro Spring 6 with Kotlin: An In-depth Guide to Using Kotlin APIs in Spring Framework 6*, pages 189–270. Springer, 2023.

[25] Adam Przybylek. Impact of aspect-oriented programming on software modularity. In *2011 15th European Conference on Software Maintenance and Reengineering*, pages 369–372. IEEE, 2011.

[26] Anas MR AlSobeh, Sawsan AlShattnawi, Amin Jarrah, and Mahmoud M Hammad. Weavesim: A scalable and reusable cloud simulation framework leveraging aspect-oriented programming. *Jordanian Journal of Computers and Information Technology*, 6(2), 2020.

[27] Kagiso Mguni and Yirsaw Ayalew. An assessment of maintainability of an aspect-oriented system. *International Scholarly Research Notices*, 2013(1):121692, 2013.

[28] Amani Shatnawi and Stephen Clyde. Modeling personal identifiable information using first-order logic. In *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, pages 1–10. IEEE, 2018.

[29] Amjad Nusayr and Jonathan Cook. Extending aop to support broad runtime monitoring needs. In *SEKE*, pages 438–441, 2009.

[30] Amjad A Nusayr. *Aspect oriented programming as a formal framework for runtime monitoring*. New Mexico State University, 2011.

[31] Patrick J Chapman, Cindy Rubio-González, and Aditya V Thakur. Interleaving static analysis and llm prompting. In *Proceedings of the 13th ACM SIGPLAN International Workshop on the State Of the Art in Program Analysis*, pages 9–17, 2024.

[32] Bilal Al-Ahmad, iyad m alazzam ismail al taharwa, rami s alkhawaldeh, and nazeeh ghatasheh. Jacoco-coverage based statistical approach for ranking and selecting key classes in object-oriented software. *Journal of Engineering Science and Technology*, 16(08):3358–3386, 2021.

[33] Axel Legay, Benoît Delahaye, and Saddek Bensalem. Statistical model checking: An overview. In *International conference on runtime verification*, pages 122–135. Springer, 2010.

[34] Anas M. R. Alsobeh. Osm: Leveraging model checking for observing dynamic 1 behaviors in aspect-oriented applications. *ArXiv*, abs/2403.01349, 2023.

[35] Klaus Havelund and Grigore Rosu. Monitoring programs using rewriting. In *Proceedings 16th Annual International Conference on Automated Software Engineering (ASE 2001)*, pages 135–143. IEEE, 2001.

[36] Anil Kumar Karna, Yuting Chen, Haibo Yu, Hao Zhong, and Jianjun Zhao. The role of model checking in software engineering. *Frontiers of Computer Science*, 12:642–668, 2018.

[37] César Sánchez, Gerardo Schneider, Wolfgang Ahrendt, Ezio Bartocci, Domenico Bianculli, Christian Colombo, Yliès Falcone, Adrian Francalanza, Srđjan Krstić, Joao M Lourenço, et al. A survey of challenges for runtime verification from advanced application domains (beyond software). *Formal Methods in System Design*, 54:279–335, 2019.

[38] Joseph W Yoder, Federico Balaguer, and Ralph Johnson. From analysis to design of the observation pattern. In *Metadata and Active Object-Model Pattern Mining Workshop. OOPSLA*, volume 99, 2017.

[39] Shko Muhammed Qader, Bryar Ahmad Hassan, Hawkar Omar Ahmed, and Hozan Khalid Hamarashid. Aspect oriented programming: Trends and applications. *UKH Journal of Science and Engineering*, 6(1):12–20, 2022.

[40] Mark Chen, Jerry Tworek, Heewoo Jun, Qiming Yuan, Henrique Ponde De Oliveira Pinto, Jared Kaplan, Harri Edwards, Yuri Burda, Nicholas Joseph, Greg Brockman, et al. Evaluating large language models trained on code. *arXiv preprint arXiv:2107.03374*, 2021.

[41] Ensaf Alhazeem, Anas Alsobeh, and Bilal Al-Ahmad. Enhancing software engineering education through ai: An empirical study of tree-based machine learning for defect prediction. 2024.

[42] Bilal Al-Ahmad. Using code coverage metrics for improving software defect prediction. *Journal of Software*, 13(12):654–674, 2018.

[43] Kevin P Murphy. *Probabilistic machine learning: Advanced topics*. MIT press, 2023.

[44] Tom Wallis. *Aspect-oriented modelling*. PhD thesis, University of Glasgow, 2024.

[45] Srividya Kotagiri, A Mary Sowjanya, B Anilkumar, and N Lakshmi Devi. Aspect-oriented extraction and sentiment analysis using optimized hybrid deep learning approaches. *Multimedia Tools and Applications*, pages 1–32, 2024.

[46] Prashanth Lakshmi Narayana Chaitanya Josyula. Weave out the complexity: A modular approach to managing cross-cutting concerns in machine learning. *European Journal of Advances in Engineering and Technology*, 10(8):66–83, 2023.

[47] Kimya Khakzad Shahandashti, Mohammad Mahdi Mohajer, Alvine Boaye Belle, Song Wang, and Hadi Hemmati. Program slicing in the era of large language models. *arXiv preprint arXiv:2409.12369*, 2024.

[48] Subhash B Tatale and V Chandra Prakash. A survey on test case generation using uml diagrams and feasibility study to generate combinatorial logic oriented test cases. *International Journal of Next-Generation Computing*, 12(2), 2021.

[49] Meennapa Rukhiran, Paniti Netinant, and Tzilla Elrad. Multiconcerns circuit component diagram apply to improve on software development: Empirical study of house bookkeeping mobile software. *Journal of Current Science and Technology*, 11(2):240–260, 2021.

[50] Birgitta Lindström, Sten F Andler, Jeff Offutt, Paul Pettersson, and Daniel Sundmark. Mutating aspect-oriented models to test cross-cutting concerns. In *2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pages 1–10. IEEE, 2015.

[51] Martin Monperrus. Automatic software repair: A bibliography. *ACM Computing Surveys (CSUR)*, 51(1):1–24, 2018.

[52] Jingyun Xu, Jiayuan Xie, Yi Cai, Zehang Lin, Ho-Fung Leung, Qing Li, and Tat-Seng Chua. Context-aware dynamic word embeddings for aspect term extraction. *IEEE Transactions on Affective Computing*, 15(1):144–156, 2023.

[53] Chuhan Wu, Fangzhao Wu, Junxin Liu, Yongfeng Huang, and Xing Xie. Arp: Aspect-aware neural review rating prediction. In *Proceedings of the 28th ACM International Conference on Information and Knowledge Management*, pages 2169–2172, 2019.

[54] Oliver Schwahn. On the efficient design and testing of dependable systems software. 2019.

[55] Ekaterina A Moroz, Vladimir O Grizkevich, and Igor M Novozhilov. The potential of artificial intelligence as a method of software developer's productivity improvement. In *2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, pages 386–390. IEEE, 2022.

[56] Bernhard K Aichernig, Priska Bauerstätter, Elisabeth Jöbstl, Severin Kann, Robert Korošec, Willibald Krenn, Cristinel Mateis, Rupert Schlick, and Richard Schumi. Learning and statistical model checking of system response times. *Software Quality Journal*, 27:757–795, 2019.

[57] Pranav Ashok, Jan Křetínskỳ, and Maximilian Weininger. Pac statistical model checking for markov decision processes and stochastic games. In *Computer Aided Verification: 31st International Conference, CAV 2019, New York City, NY, USA, July 15-18, 2019, Proceedings, Part I 31*, pages 497–519. Springer, 2019.

[58] Sandeep Dalal, Susheela Hooda, and Kamna Solanki. Comparative analysis of various testing techniques used for aspect-oriented software system. *Indonesian Journal of Electrical Engineering and Computer Science*, 12(1):51–60, 2018.

[59] Anas MR AlSobeh and Stephen W Clyde. Transaction-aware aspects with transj: an initial empirical study to demonstrate improvement in reusability. In *International Conference on Sustainable Environment and Agriculture*, page 59, 2016.

[60] Anas MR AlSobeh and Aws A Magableh. An aspect-oriented with bip components for better crosscutting concerns modernization in iot applications. In *CS & IT Conference Proceedings*, volume 8. CS & IT Conference Proceedings, 2018.

[61] Yuchen Wang, Kwok Sun Cheng, Myoungkyu Song, and Eli Tilevich. A declarative enhancement of javascript programs by leveraging the java metadata infrastructure. *Science of Computer Programming*, 181:27–46, 2019.

[62] Anas MR AlSobeh and Aws A Magableh. Blockasp: A framework for aop-based model checking blockchain system. *IEEE Access*, 2023.

[63] Samer Y Khamaiseh, Abdullah Al-Alaj, and Aquella Warner. Flooddetector: Detecting unknown dos flooding attacks in sdn. In *2020 International Conference on Internet of Things and Intelligent Applications (ITIA)*, pages 1–5. IEEE, 2020.

Optimizing Stroke Risk Prediction Using XGBoost and Deep Neural Networks

Renuka Agrawal[1], Aaditya Ahire[2], Dimple Mehta[3], Preeti Hemnani[4], Safa Hamdare[5]
Department of Computer Science and Engineering, Symbiosis Institute of Technology,
Symbiosis International (Deemed University) Pune, India[1,2,3]
Department of Electronics and Telecommunication Engineering, SIES Graduate School of Technology, Mumbai, India[4]
Department of Computer Science, Nottingham Trent University, Nottingham, NG11 8NS, UK[5]

***Abstract*—Predicting brain strokes is inherently complex due to the multifaceted nature of brain health. Recent advancements in machine learning (ML) and deep learning (DL) algorithms have shown promise in forecasting stroke occurrences to a certain extent. This research paper explores the predictive potential of ML and DL models by utilizing a comprehensive dataset encompassing diverse patient characteristics, including demographic factors, work culture, stress levels, lifestyle, and family history. Notably, this study incorporates 14 clinically significant attributes for prediction, surpassing the 10 attributes utilized by earlier researchers. To address existing limitations and enhance predictive accuracy, a novel ensemble model combining Deep Neural Networks (DNN) and Extreme Gradient Boosting (XGBoost) is proposed in this work. Also, a comparative analysis against individual DNN and XGBoost models, as well as Random Forest and Support Vector Machine (SVM) approaches are being done. The performance of the ensemble model is assessed using various metrics, including accuracy, precision, F1 score, and recall. The findings indicate that the DNN-XGBoost model exhibits superior predictive accuracy compared to standalone DNN and XGBoost models in identifying brain stroke occurrences.**

***Keywords*—DNN; XGBoost; stress level; stroke prediction**

I. Introduction

Stroke prediction plays a critical role in healthcare because early identification of high-risk individuals allows for preventive interventions, including lifestyle changes, medications, and treatments, which can significantly improve patient outcomes. However, estimating the likelihood of a stroke is complex due to the interrelation of various factors such as diet, medical history, family history, and other external variables [1], [2]. Traditional statistical methods often fail to account for these intricate relationships, leading to limitations in accurately predicting stroke risk.

The challenge lies in understanding how factors like daily habits, medical and family histories interact to influence stroke risk. Most conventional statistical techniques fall short in identifying these complex patterns. As a result, stroke risk prediction often lacks the accuracy needed for reliable clinical decision-making. In recent years, machine learning has emerged as a powerful tool to overcome these challenges. By analyzing large datasets, machine learning techniques can uncover hidden patterns and interactions that may go undetected by human clinicians. This capability significantly enhances predictive analytics in the healthcare sector [3].Several machine learning models, including decision trees, random forests, and ensemble methods, have been employed in stroke prediction, each offering distinct advantages. For instance, decision trees are interpretable and easy to understand, while random forests offer robustness and accuracy in handling large datasets [4], [5], [6]. However, despite the strengths of these models, they are often unable to fully capture the complexity of relationships between variables, particularly in the context of healthcare data. Logistic regression, though simple, also struggles to account for non-linear interactions, making it unsuitable for more intricate datasets [7], [8].

To address these limitations, ensemble models have gained traction [9], as they combine the strengths of multiple base models to improve overall predictive performance. Among the most promising ensemble approaches are XGBoost and Deep Neural Networks (DNN). XGBoost excels in handling complex, non-linear relationships within tabular data, while DNNs are particularly well-suited to learning from sequential data, making them effective at capturing long-term dependencies [10]. This study proposes a new ensemble model that integrates XGBoost and DNN to enhance stroke prediction accuracy. The model incorporates not only traditional features but also additional attributes like family history, stress levels, and alcohol intake, which are known to be significant in stroke risk assessment. By combining XGBoost's ability to model complex feature interactions with DNN's capacity for sequential learning, the proposed ensemble model overcomes challenges such as overfitting, feature interaction, and interpretability, which are common with individual machine learning models. This approach improves both the accuracy and reliability of stroke risk predictions, providing clinicians with better tools for early intervention and personalized patient management.

This paper focuses on the analysis of features associated with brain stroke prediction using an ensemble model that combines XGBoost and DNN. The key contributions of this study can be summarized as follows:

- Conducting a comprehensive analysis of features influencing brain stroke prediction using the XGBoost-DNN ensemble model.
- Demonstrating the model's potential in automating risk assessment procedures in healthcare and providing valuable insights for researchers and practitioners.
- Offering insights to enhance the implementation of predictive medicine in stroke management, emphasizing the importance of timely identification and treatment.

The remainder of this paper is organized as follows: Section II reviews related work by various researchers and discusses their limitations. Section III details the system architecture and methodology adopted for stroke prediction. Section IV presents the results obtained from the ensemble model. Finally, Section V discusses the findings, outlines future research directions, and concludes the paper in Section VI.

II. Literature Review

Machine learning models like KNN, Random Forest, and Decision Tree, logistic regression is used by researchers to automate the process of brain stroke prediction. A tabular representation of the work conducted by various researchers is included in Table I. This table summarizes the methodologies employed, the domains of study, the datasets used, the performance metrics achieved, and the outcomes or limitations identified in each respective study.

T. Lumley et al. addressed the challenge of stroke prediction in the elderly by developing a stroke prediction score, which was validated and made accessible through a web-based application. Their study focused on continuous patient monitoring data and demonstrated an effectiveness of 88% accuracy in identifying at-risk groups; however, the model's dependency on a consistent data feed and quality, as well as potential issues with cluster interpretability, posed limitations to its practical application. Similarly, R.O. Ogundokun et al. reviewed various machine learning algorithms for predicting cardiovascular diseases, including strokes, utilizing time-series health data collected from wearable devices and achieving a notable 92% accuracy in predicting stroke events. They noted that the requirement for continuous data streams could be computationally demanding, raising concerns regarding data sparsity in certain situations.

In another study, S. Shareefunnisa et al. explored heart stroke prediction using machine learning techniques by leveraging mixed datasets from diverse sources, ultimately improving prediction accuracy to 94%. However, they highlighted that the increased model complexity and potential for overfitting, along with the necessity for substantial computational resources, posed challenges to their methodology. S. Dev et al. employed a supervised approach utilizing Naive Bayes for stroke detection, analyzing symptom checker data from healthcare applications and achieving an initial diagnostic accuracy of 86%. Despite this, the simplicity of their model raised concerns about oversimplifying complex dependencies, and it was limited by the quality of the input data, which could lead to a high false positive rate. In a similar context, M. S. Sheetal and P. Choudhary applied gradient boosting techniques to stroke patient data derived from longitudinal studies, achieving an improved prediction accuracy of 91%. Their research underscored the necessity for extensive data preprocessing and feature selection, noting sensitivity to noisy data as a significant limitation.

Expanding on this, S. Rahman et al. integrated random forests and neural networks to predict brain strokes using national stroke registry data, resulting in a high detection rate of early stroke signs at 93%. They acknowledged the challenges of complex model tuning and integration, particularly concerning data heterogeneity that could affect the reliability of their results. N.K. Al-Shammari et al. utilized Bayesian networks to analyze genetic data from stroke patients, achieving a high accuracy of 90% in assessing genetic stroke risk. Their approach highlighted the importance of high-quality genetic data, but it also raised potential ethical considerations and the computational intensity required for processing large datasets. Lastly, C.M. Bhatt et al. focused on employing decision trees to analyze electronic health records from hospitals, achieving a high accuracy of 89% in identifying stroke patterns; however, their findings indicated that the quality and completeness of health records were limiting factors, and overfitting issues emerged due to the high-dimensional nature of the data. Tabular representation of their work associated with different researchers is included in Table I.

III. Proposed System Architecture

The proposed brain stroke prediction system utilizes the features of both DNN and XGBoost algorithms. Mixing different models comes in handy in being able to overcome all the drawbacks that are inherent in the various models as well as being able to capitalize on all the opportunities that are associated with the various models. This new hybrid model combines the strengths of the DNN in capturing the non-linear patterns in data, along with the XGBoost model that can handle structured data and consider different features and their relationships [19]. Fig. 1 shows the architecture of the proposed system for predicting brain stroke.

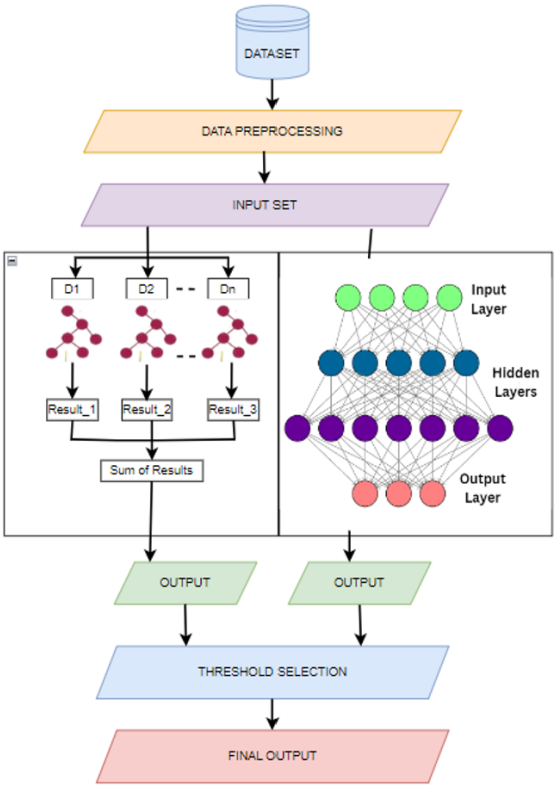


Fig. 1. Proposed system architecture.

As shown in Fig. 1, the procedure of an appropriate model for brain-stroke prediction involves data acquisition from credible and usually available sources, data pre-processing, model

TABLE I. REVIEW OF WORK DONE BY RESEARCHERS

Ref. No.	Methodology Used	Domain	Data Set Used	Performance	Outcome/Limitations
[11]	Unsupervised/Clustering/K-means	Stroke Detection	Continuous patient monitoring data	Effective in identifying at-risk groups with 88% accuracy	Dependent on continuous data feed and quality; potential issues with cluster interpretability
[12]	Supervised/LSTM	Stroke Detection	Time-series health data from wearable devices	Effective in predicting stroke events with 92% accuracy	Requires continuous data streams and can be computationally demanding; potential issues with data sparsity
[13]	Supervised/Ensemble Methods	Stroke Detection	Mixed datasets from various sources	Enhanced prediction accuracy to 94%	Increased model complexity; potential overfitting; requires large computational resources
[14]	Supervised/Naive Bayes	Stroke Detection	Symptom checker data from healthcare apps	Good for initial diagnosis with an accuracy of 86%	May oversimplify complex dependencies; limited by input data quality; potential high false positive rate
[15]	Supervised/Gradient Boosting	Stroke Detection	Stroke patient data from longitudinal studies	Improved prediction of stroke outcomes with 91% accuracy	Requires extensive data preprocessing and feature selection; sensitive to noisy data
[16]	Supervised/RF/Neural Networks	Stroke Detection	National stroke registry data	High detection rate of early stroke signs (93%)	Complex model tuning and integration required; potential issues with data heterogeneity
[17]	Supervised/Bayesian Networks	Stroke Detection	Genetic data from stroke patients	High accuracy (90%) in assessing genetic stroke risk	Needs high-quality genetic data; potential ethical considerations; computationally intensive for large datasets
[18]	Supervised/Decision Trees	Stroke Detection	Electronic Health Records (EHR) from hospitals	High accuracy in identifying stroke patterns (89%)	Limited by the quality and completeness of health records; potential overfitting with high-dimensional data

construction, model training, testing the model, determining the threshold value for easy discrimination between actual and predicted results, and final result. Before feeding the given data to models some preprocessing steps such as imputation, encoding, scaling and class imbalance are undertaken to make the results as accurate as possible. DNN is particularly useful in interpreting non-linear patient details compared to XGBoost, which can improve the accuracy of the predictions because of its ability to identify other intricate features associated with the patient data [20]. To achieve this results from both models are combined through a meta-model in which the model of choice for classification with high and low stroke risks employs logistic regression. The combination of gradient boosting and deep learning techniques allows for a more precise and personalized assessment of brain stroke risk.

A. Dataset

Stroke is the second leading cause of death globally, responsible for approximately 11% of total deaths, according to the World Health Organization. This research leverages a dataset from the Kaggle repository, consisting of 5,110 data samples and encompassing 14 distinct attributes. Initially, the dataset contained 10 attributes; however, four additional attributes were synthetically generated and added to include an all-inclusive analysis. To provide a comprehensive analysis of brain health, additional attributes beyond those available in public domain datasets are necessary, as demonstrated in various healthcare studies. Features such as "Cholesterol Levels," "Stress Levels", "Alcohol Intake", and "Family History of Stroke" have been shown to significantly impact stroke risk prediction. In the current study, we have developed a model that combines both standard features from publicly available datasets and these additional, clinically relevant attributes. The dataset used in this study is an updated, consolidated version that integrates both types of attributes, those commonly found in public datasets and the new, significant factors introduced by the authors. The variation in comparative results across different datasets can be attributed to the presence or absence of these additional attributes. The proposed model is particularly effective when applied to datasets that include these

TABLE II. DATASET DESCRIPTION

S.no.	Attribute Name	Data Type	Description
1	ID	Numeric	Primary key/ Unique value for every sample
2	Gender	String	Informs the gender of person
3	Age	Categorical	Informs the category, the age of person belongs to
4	Hyper_tension	Categorical	Tells whether the person has hypertension or not
5	Heart_disease	Categorical	Tells whether the person has heart disease or not
6	Ever_married	String	Either Y (Yes) or N (No)
7	Residence_type	Categorical	Rural or Urban
8	Work_Type	Categorical	children, Govt_job, Never_worked, Private, Self employed
9	Avg_glucose_level	Numeric	Gives average Glucose level in Blood of person
10	BMI	Numeric	Informs about Body Mass Index of person; if more than obese
11	Smoking_Status	Categorical	Categorizes in formerly smoked, never smoked, smokes, unknown
12	Cholesterol_Levels	Numeric	Tells the level of HDL (Good) and LDL in cholesterol present
13	Stress_Levels	Categorical	Tells whether the person has stress or not
14	Alcohol_Intake	Categorical	Categorizes in formerly taken, never taken, yes, unknown
15	Family_History	Categorical	Tells whether the person has brain stroke issues in family or not
16	Stroke	Numeric	Final prediction by proposed model

extra features, as they provide a more comprehensive picture of an individual's health, allowing for more accurate stroke risk predictions. Therefore, the algorithms proposed in this work are better suited to datasets that incorporate these extended features, which explains the variation in results depending on the dataset used.

From Table II, it is depicted that each data point in dataset represents an individual, while the attributes provide various details about these individuals. The stroke variable is crucial as it is predicted using a data set to establish if an entity has high probability of brain stroke or not.To balance the dataset, SMOTE was utilized. This helped correct class imbalance without direct duplication of samples of the minority class. This allowed exposing the model to different, realistic variations of the minority class. Thus, it enhances generalizability. Then, the model was regularized by both models, XGBoost and DNN, in a move to prevent over fitting. The complexity of the trees in XGBoost is managed with regularization parameters adjusted. Dropout layers at a rate of 0.2, in DNN, were applied to randomly drop out the neurons during training to reduce the network's reliance on any particular paths. Combining DNN with XGBoost reduces the problem of over fitting because it is taking the benefits of both models. Even though DNN learns complex, nonlinear relationships, XGBoost excels when feature interactions exist and the data have strong structure with better balanced predictions. Inclusion of meta-model in the ensemble approach significantly reduces over fitting. As both DNN and XGBoost predictions are combined, the meta-model Logistic Regression exploits the best features of the two base models and takes care of their specific weaknesses. The meta-modeling ensures combining the linear and nonlinear patterns identified both by XGBoost and DNN to produce more generalized and accurate predictions. Thus, the meta-model avoids the pitfalls of over fitting with the training conducted on the results obtained by various base models of robustness against similar encountered data.

B. Pre-processing and Data Visualization

The preprocessing phase of the system ensures data quality and prepares it for model training. Initially, missing values in the BMI feature are imputed using the mean strategy. Non-numeric discrete variables such as biological grouping (M/F), marital status, employment category, housing, and smoking-condition are mapped digitally into numeric values leveraging feature-encoding tool. The dataset is then split into features (X) and the target variable (Y). Class distribution of dataset used in the work is shown in Fig. 2. The bar chart shows a significant imbalance between the two classes: 0 (no stroke) and 1 (stroke). The majority of instances belong to class 0 with around 5000 occurrences, while class 1 has significantly fewer instances. As is clear from Fig. 2, original dataset consists of samples which are highly imbalanced. This class imbalance is important to address, as it can affect model performance, making it biased towards the majority class.

Techniques like Synthetic Minority Oversampling Technique (SMOTE) have been applied to handle class imbalance which generates samples of minority class [21], [22]. Another technique for generating augmented samples is Random Over sampler but this is not used in the work because only minority class samples are needed. The class distribution upon data

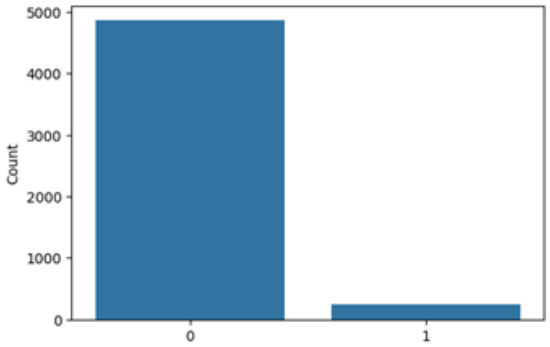


Fig. 2. Class distribution of original dataset.

balancing is shown in Fig. 3. Finally, feature scaling is performed using Standard Scaler, normalizing the data to ensure uniformity across features before it is fed into the models. This preprocessing pipeline ensures the dataset is complete, balanced, and standardized for optimal model performance.

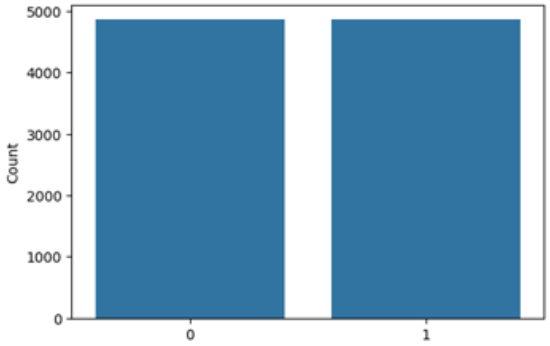


Fig. 3. Class distribution of dataset by SMOTE.

Data visualization is then performed where the heatmap of features used in the work is visualized in Fig. 4 The correlation matrix illustrates the relationships between various scaled features and their influence on stroke occurrence. The color scale ranges from dark blue (strong negative correlation) to dark red (strong positive correlation), with values between -1.0 and 1.0.

Key observations of Fig. 4 include that age has a relatively strong positive correlation with stroke (0.61), while other factors such as hypertension (0.24), heart disease (0.26), and average glucose level (0.25) also show moderate positive correlations with stroke. On the other hand, factors like gender (-0.22) and work type (-0.21) exhibit a negative correlation with stroke. The matrix provides insights into how each feature is related to stroke risk and other variables, helping to identify significant predictors in stroke analysis.

To understand the relationship of one feature with other Fig. 5 is helpful. Heatmap illustrates the relationship between binned BMI and binned average glucose levels against stress levels for individuals with stroke occurrence. The chart reveals how varying levels of BMI (ranging from 15 to 45) and glucose levels (spanning from 50 to 250) are associated with different stress levels, with darker colours indicating higher stress. For instance, high stress levels are observed at higher glucose

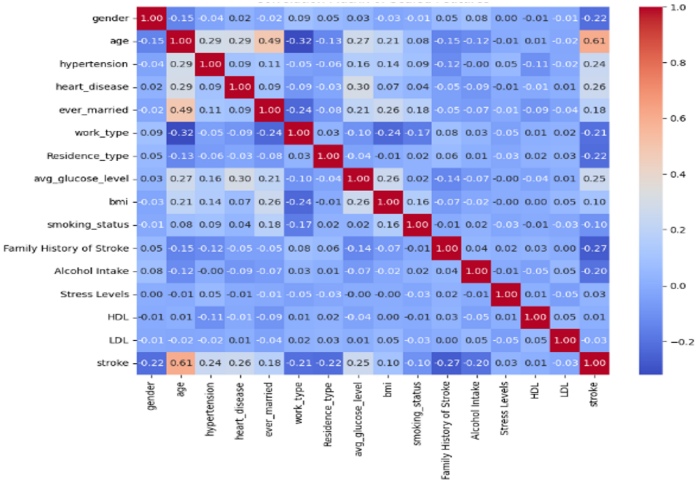


Fig. 4. Correlation between variables.

levels (110-150) and mid-range BMI (20-30). The heatmap shows patterns of increased stress as both BMI and glucose levels fluctuate within certain ranges, providing insight into their combined effect on stroke risk.

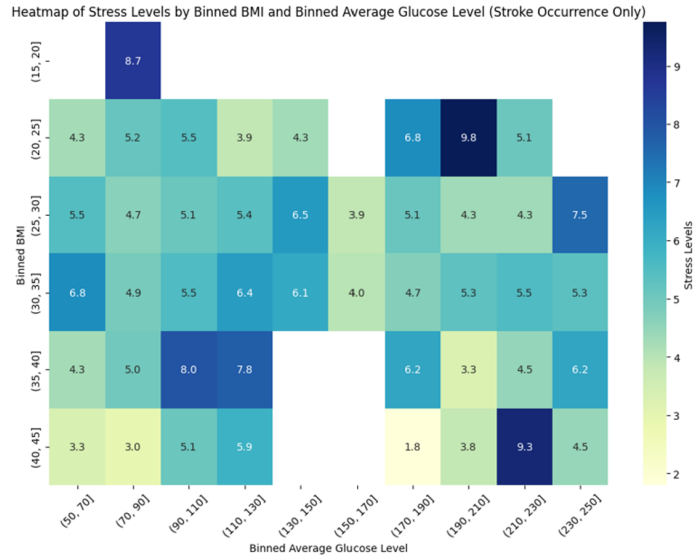


Fig. 5. Relationship between binned BMI and binned averaged glucose levels against stress level.

In Fig. 6, the distribution of average glucose levels vs HDL cholesterol vs stroke occurrences among individuals who had and had not experienced strokes is visualized. The 3D scatter plot in Fig. 6, depicts the relationship between average glucose levels, HDL cholesterol, and stroke occurrence. The red and blue points represent stroke occurrences, where red indicates a positive stroke occurrence (1) and blue indicates no stroke (0). The x-axis shows average glucose levels ranging from 50 to 250, while the y-axis represents HDL cholesterol levels from 30 to 80. The z-axis corresponds to stroke occurrence. The plot demonstrates that higher glucose levels combined with lower HDL cholesterol levels are associated with a higher likelihood of stroke, as indicated by the clustering of red points at the

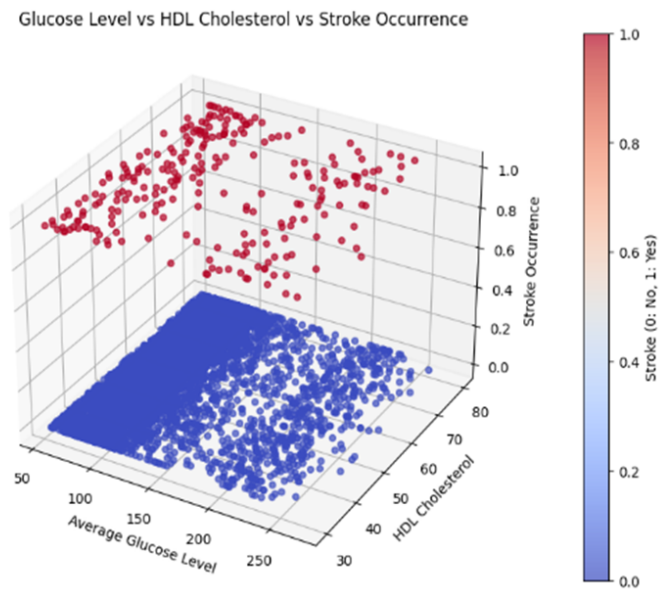


Fig. 6. Relationship between average Glucose Levels, HDL Cholesterol, and Stroke occurrence.

upper range. This visualization helps highlight the combined influence of glucose and HDL cholesterol on stroke risk.

In Fig. 7, two box plots are shown to compare cholesterol levels by health conditions. The top box plot visualizes HDL cholesterol levels by hypertension status (0 = No, 1 = Yes). Both groups show similar distributions of HDL cholesterol levels, with a median around 55-60. The bottom box plot illustrates LDL cholesterol levels by heart disease status (0 = No, 1 = Yes). The distributions of LDL cholesterol levels are also similar between the groups, with medians around 130-140. Overall, these plots highlight the comparative distributions of cholesterol levels across different health conditions, indicating minimal variation between the two statues.

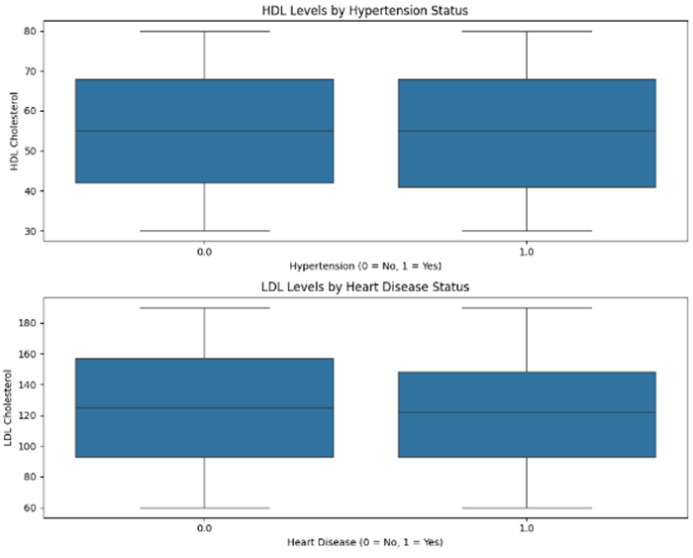


Fig. 7. Comparison of cholesterol levels by health conditions.

In Fig. 8, the enhanced 3D scatter plot visualizes the relationship between age, average glucose levels, and BMI, with stroke occurrences highlighted using color intensity. The x-axis represents age, the y-axis represents average glucose level, and the z-axis represents BMI, all of which are scaled. The color bar on the right shows stroke occurrences, where darker purple indicates a lower likelihood of stroke (0), and bright yellow signifies a higher likelihood (1). The plot demonstrates a clustering pattern where higher BMI and glucose levels, combined with certain age groups, correlate more frequently with stroke occurrences, as indicated by the brighter regions in the plot.

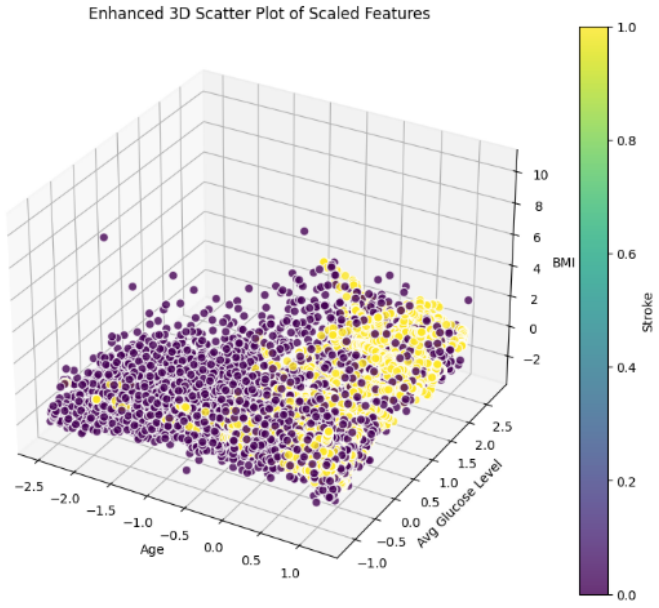


Fig. 8. Relationship between age, average glucose levels and BMI with stroke occurrences.

C. Data Splitting

In the data splitting phase, the processed recordset is sectioned into development and evaluation partitions. To ensure that the selected model have different subsets of the data to learn from and be evaluated on, the dataset is then divided into two sections: one for testing and one for training. Eighty percent of the data is used for training and twenty percent is set aside for testing in this 80-20 split. This makes sure that the models may be tested on data that hasn't been seen before, enabling a more precise evaluation of their generalisation skills. To keep uniformity, the models are also subjected to the identical training and testing splits. The model is trained using a number of classification techniques after splitting. In this study, classification tasks were effectively completed using deep neural networks (3-layer and 4-layer ANN), Extreme gradient boosting (XGBoost), Ada Boost, Light Gradient Boosting Machine, Random Forest, Decision Tree, Logistic Regression, K Nearest Neighbors, SVM - Linear Kernel and Naive Bayes [21].

D. XGBoost Model

The XGBoost approach is employed in this work to predict strokes. The model is ensembled with another DNN model for precise prediction. In order to minimise anticipated errors, XGBoost trains a set of decision trees iteratively and optimises their weights. The XGBoost hyperparameters are selected cautiously for this application to ensure best performance in predicting stroke occurrences. The architecture of the xgboost model is depicted in the Fig. 9. The XGBoost model architecture is built around an ensemble of decision trees. Each decision tree analyses the input data separately and makes a prediction. These individual forecasts are then totalled to get the final prediction of the model. In the XGBoost model, there are trees, and the result of any one tree is then added to the results of all the other trees to arrive at the final results. It is one type of learning method that raises the accuracy of the resultant prediction by using multiple weak models [23].

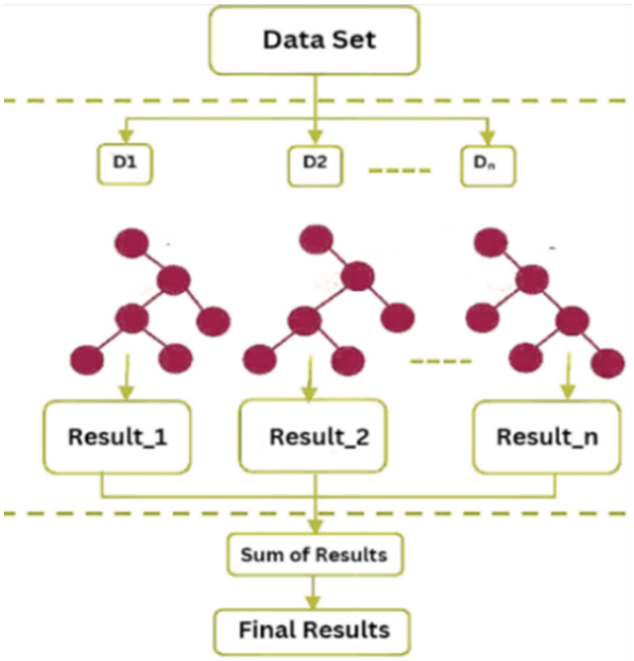


Fig. 9. XGBoost model.

E. DNN

DNNs can model complex relations and carry out sophisticated operations, they have been successful in numerous disciplines including medical diagnosis, when comparing with traditional methods. Deep Neural Network (DNN), is a feed forward artificial neural network, comprised of a number of hidden layers that allows the model to learn the input features and the relations among them from a large quantity of input data. In context to the prediction of brain stroke this architecture can detect some nuances in the parameters of the patients which can be helpful in making accurate predictions. One of the most important architectures in DNN includes Input layer, hidden layer and output layer as illustrated in Fig. 10.

The Fig. 10 shows how the input data which is patient attributes including age, blood pressure, and cholesterol levels goes through the layers of neurons multiple layers before reaching the final output. Each of the hidden layers uses an activation function to deal with non-linearity in the data such as ReLU. This improves the ability to develop good

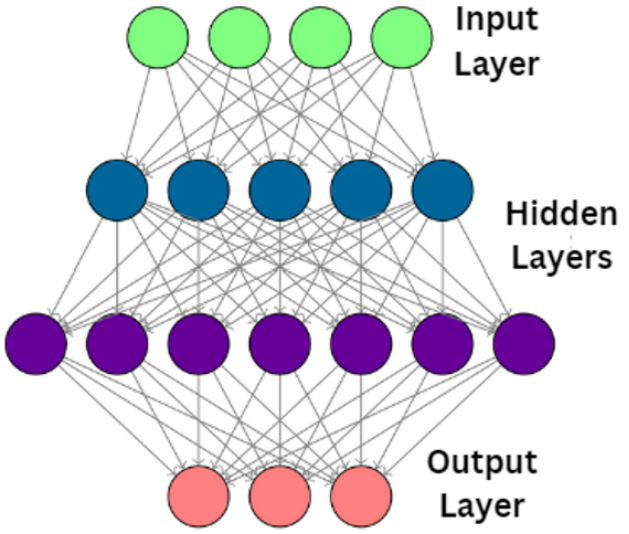


Fig. 10. DNN Model architecture.

TABLE III. ENSEMBLED MODEL PARAMETER CONFIGURATION

PARAMETER	DESCRIPTION
Model type	Ensembled Model
Libraries	Xgboost, Keras, TensorFlow
Algorithms	DNN, XGBoost
Train/Test data	80% for training and 20% for testing
DNN CONFIGURATION	
DNN layer	2
Dropout rate	0.2
Dense layer	2 units
Penalty Gauge	Dual logistic loss
Batch size	64
Optimizer	Adam
Maximum passes	52
Hyperparameter tuning method	Grid search
XGBOOST CONFIGURATION	
Objective	Binary: logistic
Eval Metric	Log loss
Learning Rate (eta)	0.05
Max Depth of Individual Trees	10
Subsample	0.8
Feature subsampling	0.8

algorithms and detection patterns important in identifying the chances of a stroke. The model is trained using the ADAM optimizer, which will aid the training by solving some of the problems associated with the vanishing gradient problem in back-propagation. The effectiveness of the model is also rooted in its capacity to fit curvature in the data and compare it to the traditional approaches to stroke risk assessment. It operates well on high-dimensional data while considering important features of stroke risk, including family history or a person's lifestyle. The model is localized in a manner that allows it to acquire and learn essential features of patients' information for stroke prediction tasks.

F. Ensemble Model

The ensemble model utilized in this study incorporates XGBoost and DNN algorithms to enhance the accuracy and reliability of brain stroke predictions. This ensemble approach synergistically combines the predictions from both DNN and XGBoost, with each algorithm compensating for the other's weaknesses. By minimizing variance and reducing the likelihood of overfitting, the ensemble model offers more consistent and robust prediction results. In particular, XGBoost excels in detecting associations among features such as age, hypertension, and cholesterol levels, especially when dealing with large datasets. Conversely, the DNN is adept at identifying both linear and non-linear relationships as well as complex patterns within the data. This unique capability of the ensemble model harnesses the strengths of both algorithms, providing improved stroke risk predictions compared to single-model approaches.

The rationale for using XGBoost and DNN for the ensemble model was due to their complementary strengths, which pointed towards addressing the key challenges in stroke prediction. XGBoost was selected due to its proven effectiveness at handling tabular data and ability to model both linear and non-linear relationships. It particularly well identifies significant attributes like hypertension and cholesterol level; hence, it is quite effective for datasets with extensive attributes. Moreover, its regularization techniques prevent overfitting and make strong prediction even if there is a tremendous amount of data to work on. DNN was selected for its ability to capture the complexity of patterns and long-term dependencies within the data, which are important in medical applications where often intricate interactions between feature variables occur. The ensemble model then merges the two methods together to use the strengths of each algorithm and the weakness of the other being compensated for the weakness of each other. Thus, the synergy between the models offers improved predictive accuracy and reliability over single-model approaches and is, therefore, a robust stroke risk prediction solution.

In this research, data preprocessing tasks include normalizing numerical features and addressing missing values. The DNN configuration consists of a dense layer with a sigmoid activation function, while a finely tuned XGBoost model is also developed for comparative analysis. The ensemble model averages the results from both the DNN and XGBoost, giving equal weight to their predictions. Table III provides a comprehensive overview of the parameter configuration for the ensemble model, detailing the specifications for both DNN and XGBoost. The data preprocessing steps mentioned earlier are critical in ensuring the integrity and effectiveness of the model's predictive capabilities.

IV. RESULT

Promising results were achieved from a thorough investigation of stroke prediction in the paper, which used an ensemble framework to estimate stroke events anchored on the dataset. 2.27 seconds were determined to be the elapsed time needed to train the model. When evaluated with data, the model performed exceptionally well. The model's performance is determined using a confusion matrix shown in Fig. 11 and threshold 0.639. This provides a sense of how effectively the model operates.

Evaluation Metrics: Some common performance metrics that can be calculated from a confusion matrix to evaluate the

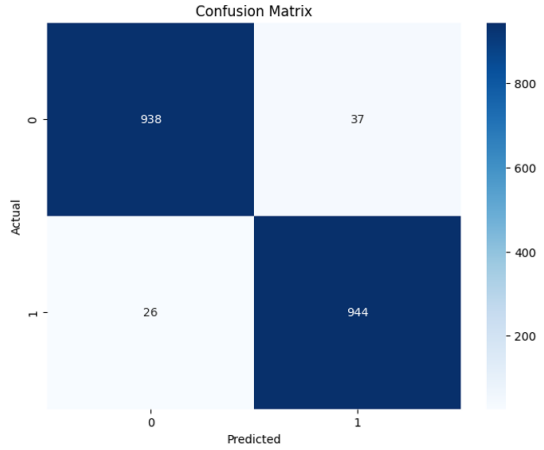


Fig. 11. Confusion matrix.

performance of model. The confusion Matrix consists of four parameters:

- True Positive : Denoted as TP
- True Negative : Denoted as TN
- False Positive : Denoted as FP
- False Nagative: Denoted as FN

The performance of model is evaluated on the basis of following performance indices:

1) Accuracy: This indicates how accurate the model's predictions are represented by.

$$\text{Accuracy} = \frac{A+B}{A+B+C+D} \tag{1}$$

2) Precision: Measures how accurate positive outcomes are.

$$\text{Precision} = \frac{A}{A+C} \tag{2}$$

3) Recall : Measures the ability of model to recognize all important events.

$$\text{Recall} = \frac{A}{A+D} \tag{3}$$

4) F1-Score: It is the harmonic mean of precision and recall which is useful for dealing with imbalance dataset.

$$\text{F1-Score} = \frac{2 \cdot \text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}} \tag{4}$$

TABLE IV. Evaluation Metrics of the Ensemble Model

Evaluation Metrics	Ensemble of DNN and XGBoost
Accuracy	96.76%
Precision	96.20%
Recall	97.40%
F1 Score	96.80%

Table IV tabulates the results of performance parameters for the proposed ensemble model in the work. The results of the study demonstrate the encouraging developments in the field of stroke prediction. With an astounding accuracy rate of 96.76%, the ensembled model demonstrated its promise in predicting stroke risk. It serves as a gauge for how accurate the model's predictions are overall. Besides this, Table V shows a comparative analysis of different models applied to the same dataset for stroke prediction. The table highlights the performance of several models, including Naïve Bayes, Random Forest, Decision Tree, and the proposed ensemble model of Deep Neural Networks (DNN) and XGBoost. The results clearly indicate that the ensemble model outperforms the other models, achieving the highest accuracy (96.76%), precision (96.20%), recall (97.40%), and F1-Score (96.80%). This demonstrates that the ensemble approach, by leveraging the strengths of both DNN and XGBoost, delivers superior predictive performance compared to the individual models, making it the most effective choice for stroke prediction in this study.

TABLE V. Comparative Result Analysis of Different Models

Model	Accuracy	Precision	Recall	F1-Score
Naïve Bayes	82.42%	79.46%	87.32%	83.20%
Random Forest	92.70%	90.99%	94.74%	92.83%
Decision Tree	90.08%	88.28%	92.37%	90.28%
Ensemble of DNN and XGBoost	96.76%	96.20%	97.40%	96.80%

The graph shown in Fig. 12. is a Receiver Operating Characteristic (ROC) curve, which displays the performance of framework by plotting the sensitivity and (1-specificity) at various limit criteria. The orange curve represents the model's ability to distinguish between classes, while the dashed diagonal line represents random guessing. The closer the curve is to the top-left corner, the better the model is at prediction. In this case, the model has an Area Under the Curve (AUC) score of 0.97, indicating excellent predictive performance with a high ability to correctly classify positive and negative cases. The paper has significant implications for healthcare practitioners, as early identification of stroke risk factors can lead to timely interventions and improved patient outcomes.

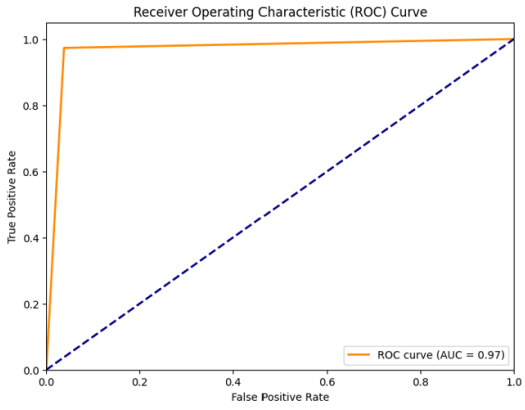


Fig. 12. ROC Curve.

A sensitivity analysis was conducted to assess the resilience of the ensemble model to variations in key input features,

TABLE VI. COMPARATIVE ANALYSIS OF PROPOSED WORK

Ref.	Multiple ML models	Ensemble model selected	Data Balancing	Attributes in Dataset	Accuracy	Precision	F1 Score	Limitation
[24]	Yes	No-NB	Yes	10	82%	79.2	82.3	Does not consider neural networks. Attributes used are 10 available in public domain.
[25]	Yes	Yes-RF	Yes	10	92.55	90.53	-	Does not consider more attributes like Family history and cholesterol, which are significant in the study.
[26]	NA	Yes-RF	No	10	90.36	82.23	0.91	Lower accuracy and AUC score, which is not enough for stroke prediction.
[27]	Yes	No	No	10	73.52	NA	-	Used XAI and predicted that age is the prime attribute.
[28]	Yes	Yes-RF	Yes-SMOTE	10	92.32	-	0.920	Used Standard dataset of Kaggle containing 10 attributes.
Proposed work	Yes	Yes-XGBoost and DNN	Yes-SMOTE	15	96.26	96.20	96.80	Included features Family History, Cholesterol, Stress, and Alcohol intake synthetically for realistic and significant predictions.

such as age, BMI, and glucose levels. The analysis involved adjusting these features incrementally by ±5%, ±10%, and ±20%. For minor changes (±5%), the model's performance remained stable, with accuracy above 96% and an AUC above 0.96. Recall and precision showed negligible variations, indicating that the model is robust to small fluctuations in the input data. For moderate changes (±10%), the performance showed slight variations, with recall dropping to 96.50%, while accuracy remained above 95.50%. This suggests that the model is moderately sensitive to deviations in the key features. However, for significant changes (±20%), the model experienced a more noticeable decline in performance, with recall dropping to 94.80% and AUC reducing to 0.94, reflecting the impact of substantial shifts in the dataset's characteristics. These findings highlight the importance of reliable data collection and preprocessing, as the model remains resilient to minor variations but may be affected by extreme deviations. Ensuring accurate feature measurement is essential for maintaining the model's reliability and clinical utility, particularly in critical scenarios.

V. DISCUSSION

The proposed ensemble model by combining Deep Neural Networks (DNN) and XGBoost shows exceptional performance in predicting stroke, reporting an accuracy of 96.76% and an AUC of 0.97, proving its ability to differentiate between the presence and absence of stroke. With a high recall value of 97.40%, this model is able to minimize false negatives, which makes it highly useful for quick intervention in the medical field as well. Its good computational efficiency - 2.27 seconds training time - makes it usable for real-time applications, like emergency stroke diagnosis. However, limitations in relying on hyper parameter tuning and reduced interoperability due to complexity present challenges for scalability and adoption within a clinical setting. Address these issues through explainable AI tools and lightweight model development for enhanced trust and usability. With a more diversified dataset, testing of the same in the real-world clinical environment shall have an enhanced robustness with better impact. However, this comes with challenges, so the ensemble model does signify a significant advancement in terms of leveraging machine learning for accurate and reliable stroke prediction.

Despite the progress made, several critical limitations and gaps have been identified in the current body of research. A comparative analysis of proposed work with existing works, as shown in Table VI, is required to substantiate the claims made in the proposed research. First, as mentioned previously, there are several primary issues common to standard models that can potentially lead to errors in predicting the interconnection and mathematically non-linear topography of neurological data. Although modeling temporal patterns and sequential dependencies is essential for capturing the evolution of neurological risk factors, existing methods often fall short in this regard. Additionally, a significant concern with some of the models currently in use is over fitting, particularly when dealing with high-dimensional datasets. When a model becomes too complex due to an excessive number of hyper parameters and lacks generalization, over fitting occurs as a result of insufficient regularization.

VI. CONCLUSION AND FUTURE SCOPE

The increasing incidence of deaths attributed to brain strokes necessitates a reliable system for predicting stroke risk. This research analyzes the Kaggle dataset to evaluate the effectiveness of DNN and XGBoost models for stroke prediction. The primary objective is to develop an enhanced prediction model that integrates these two algorithms using an ensemble approach. Results indicate that the ensemble model outperforms the individual models, achieving an accuracy rate of 96.25%. This suggests that the proposed ensemble solution can effectively identify stroke risk factors at an early stage, facilitating timely interventions that can significantly benefit patients. Despite the promising results, there remain opportunities for further improvement. Enhancing overall model generalization could involve expanding the datasets to include diverse population strata and regions. Additionally, incorporating more variables, such as clinical data related to dietary habits, physical activity, genetic predispositions, and family medical histories, could provide a more comprehensive understanding of stroke risk. Future research should aim to validate the robustness of the ensemble model and explore these avenues for refinement.

REFERENCES

[1] E. Dritsas and M. Trigka, "Stroke risk prediction with machine learning techniques," *Sensors*, vol. 22, no. 13, pp. 4670, 2022.

[2] S. Mainali, M. E. Darsie, and K. S. Smetana, "Machine learning in action: stroke diagnosis and outcome prediction," *Frontiers in Neurology*, vol. 12, p. 734345, 2021.

[3] S. Mondal, S. Ghosh, and A. Nag, "Brain stroke prediction model based on boosting and stacking ensemble approach," *International Journal of Information Technology*, vol. 16, no. 1, pp. 437–446, 2024.

[4] D. Ushasree, A. V. P. Krishna, and C. M. Rao, "Enhanced stroke prediction using stacking methodology (ESPESM) in intelligent sensors for aiding preemptive clinical diagnosis of brain stroke," *Measurement: Sensors*, vol. 33, p. 101108, 2024.

[5] M. U. Emon, M. S. Keya, T. I. Meghla, M. M. Rahman, M. S. A. Mamun, and M. S. Kaiser, "Performance analysis of machine learning approaches in stroke prediction," in *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 1464–1469, IEEE, 2020.

[6] P. Bentley, J. Ganesalingam, A. L. Carlton Jones, K. Mahady, S. Epton, P. Rinne, P. Sharma, O. Halse, A. Mehta, and D. Rueckert, "Prediction of stroke thrombolysis outcome using CT brain machine learning," *NeuroImage: Clinical*, vol. 4, pp. 635–640, 2014.

[7] M. S. Sirsat, E. Fermé, and J. Camara, "Machine learning for brain stroke: a review," *Journal of Stroke and Cerebrovascular Diseases*, vol. 29, no. 10, p. 105162, 2020.

[8] D. Ushasree, A. V. P. Krishna, and C. M. Rao, "Enhanced stroke prediction using stacking methodology (ESPESM) in intelligent sensors for aiding preemptive clinical diagnosis of brain stroke," *Measurement: Sensors*, vol. 33, p. 101108, 2024.

[9] B. Letham, C. Rudin, T. H. McCormick, and D. Madigan, "Interpretable classifiers using rules and Bayesian analysis: Building a better stroke prediction model," *Artificial Intelligence*, vol. 216, pp. 1350–1371, 2015.

[10] S. Yellaram, S. Kothamasu, and S. R. Puchakayala, "Heart stroke prediction using machine learning," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 6, no. 9, pp. a328–a332, 2021.

[11] T. Lumley, R. A. Kronmal, M. Cushman, T. A. Manolio, and S. Goldstein, "A stroke prediction score in the elderly: validation and Web-based application," *Journal of Clinical Epidemiology*, vol. 55, no. 2, pp. 129–136, 2002.

[12] R. O. Ogundokun, S. Misra, D. Umoru, and A. Agrawal, "Review of cardiovascular disease prediction based on machine learning algorithms," in *The International Conference on Recent Innovations in Computing*, pp. 37–50. Singapore: Springer Nature Singapore, 2022.

[13] S. Shareefunnisa, S. N. Lakshmi Malluvalasa, T. R. Rajesh, and M. Bhargavi, "Heart stroke prediction using machine learning," *Journal of Pharmaceutical Negative Results*, vol. 2022, pp. 2551–2558, 2022.

[14] S. Dev, H. Wang, C. S. Nwosu, N. Jain, B. Veeravalli, and D. John, "A predictive analytics approach for stroke prediction using machine learning and neural networks," *Healthcare Analytics*, vol. 2, p. 100032, 2022.

[15] M. S. Sheetal and P. Choudhary, "Stroke prediction using artificial intelligence," in *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, pp. 158–161. IEEE, 2017.

[16] S. Rahman, M. Hasan, and A. K. Sarkar, "Prediction of brain stroke using machine learning algorithms and deep neural network techniques," *European Journal of Electrical Engineering and Computer Science*, vol. 7, no. 1, pp. 23–30, 2023.

[17] N. K. Al-Shammari, A. A. Alzamil, M. Albadarn, S. A. Ahmed, M. B. Syed, A. S. Alshammari, and A. M. Gabr, "Cardiac stroke prediction framework using hybrid optimization algorithm under DNN," *Engineering, Technology & Applied Science Research*, vol. 11, no. 4, pp. 7436–7441, 2021.

[18] C. M. Bhatt, P. Patel, T. Ghetia, and P. L. Mazzeo, "Effective heart disease prediction using machine learning techniques," *Algorithms*, vol. 16, no. 2, p. 88, 2023.

[19] Y. Wu and Y. Fang, "Stroke prediction with machine learning methods among older Chinese," *International Journal of Environmental Research and Public Health*, vol. 17, no. 6, p. 1828, 2020.

[20] M. C. Das, F. T. Liza, P. P. Pandit, F. Tabassum, M. A. Mamun, S. Bhattacharjee, and M. S. B. Kashem, "A comparative study of machine learning approaches for heart stroke prediction," in *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, pp. 1–6. IEEE, 2023.

[21] M. U. Emon, M. S. Keya, T. I. Meghla, M. M. Rahman, M. S. Al Mamun, and M. S. Kaiser, "Performance analysis of machine learning approaches in stroke prediction," in *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 1464–1469. IEEE, 2020.

[22] H. Al-Zubaidi, M. Dweik, and A. Al-Mousa, "Stroke prediction using machine learning classification methods," in *2022 International Arab Conference on Information Technology (ACIT)*, pp. 1–8. IEEE, 2022.

[23] U. Islam, G. Mehmood, A. A. Al-Atawi, F. Khan, H. S. Alwageed, and L. Cascone, "NeuroHealth guardian: A novel hybrid approach for precision brain stroke prediction and healthcare analytics," *Journal of Neuroscience Methods*, vol. 409, p. 110210, 2024.

[24] G. Sailasya and G. L. Aruna Kumari, "Analyzing the performance of stroke prediction using ML classification algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, 2021.

[25] S. Sahriar, S. Akther, J. Mauya, R. Amin, M. S. Mia, S. Ruhi, and M. S. Reza, "Unlocking stroke prediction: Harnessing projection-based statistical feature extraction with ML algorithms," *Heliyon*, vol. 10, no. 5, 2024.

[26] K. Mridha, S. Ghimire, J. Shin, A. Aran, M. M. Uddin, and M. F. Mridha, "Automated stroke prediction using machine learning: an explainable and exploratory study with a web application for early intervention," *IEEE Access*, vol. 11, pp. 52288–52308, 2023.

[27] C. Kokkotis, G. Giarmatzis, E. Giannakou, S. Moustakidis, T. Tsatalas, D. Tsiptsios, K. Vadikolias, and N. Aggelousis, "An explainable machine learning pipeline for stroke prediction on imbalanced data," *Diagnostics*, vol. 12, no. 10, p. 2392, 2022.

[28] J. A. T. Rodríguez, "Stroke prediction through data science and machine learning algorithms," Preprint, 2021. Available at: https://www.researchgate.net/publication/352261064 [Accessed 22 Nov. 2024]. DOI: 10.13140/RG.2.2.33027.43040.

Financial Shifts, Ethical Dilemmas, and Investment Insights in Nursing Homes: A Pre- and Post-Pandemic Analysis

Amir El-Ghamry[1], Ameera Ibrahim[2], Noha Elfiky[3], Safwat Hamad[4]
Faculty of Computers and Information, Mansoura University, Mansoura, Egypt[1]
School of Engineering and Computer Science, University of Hertfordshire hosted by Global Academic Foundation, Egypt[1]
Faculty of Computer Science and Engineering, New Mansoura University, Mansoura, Egypt[1]
Faculty of Computing and Information Sciences, Egypt University of Informatics, Egypt[1]
Saint Mary's College of California, Moraga CA-94575, USA[2, 3, 4]

***Abstract*—The COVID-19 pandemic has significantly transformed the operational, financial, and ethical frameworks of nursing homes in the United States. This study offers a detailed analysis of the nursing home sector from 2015 to 2021, focusing on the financial viability and ethical standards before, during, and after the pandemic. The methodology employed a structured approach, including data federation, pre-processing, and trend analysis, using comprehensive datasets on Nursing Homes. The data was cleaned, standardized, and segmented into pre-pandemic (2015–2019), pandemic (2020), and post-pandemic (2021) periods to assess key trends and outcomes. The findings highlight how the pandemic exacerbated existing financial challenges, such as declining occupancy rates, increased operational costs, and reduced revenue streams, which led to closures and heightened investment activity in the sector. Government aid provided temporary stability, but long-term sustainability remains uncertain. Key factors affecting financial performance, including occupancy rates, net income, fines and penalties, and compliance with ethical standards such as vaccination rates and care quality, were analyzed. The study concludes that nursing home investments should be approached cautiously unless facilities meet specific financial and operational criteria, such as high occupancy rates, robust financial performance, low penalties, and strict adherence to ethical standards. Failure to meet these benchmarks may result in heightened financial and operational risks, making such facilities unsuitable for investment. This research offers a comprehensive framework for investors to evaluate nursing home opportunities in the post-pandemic landscape, providing insights into the intersection of financial performance, operational resilience, and ethical compliance.**

Keywords*—Component; COVID-19 impact; nursing home financial performance; post-pandemic investment; ethical standards in nursing homes

I. Introduction

The COVID-19 pandemic has profoundly altered the operations and practices of nursing homes in the United States, leaving a myriad of burdens and stressors that the industry is not accustomed to handling. More than 14,470 nursing homes exist in the US with about 1.2 million residents, out of whom 83% are over 65 years old. Each facility has, on average, 108 beds, with residents normally staying for about one year [1]. The pandemic has worsened existing weaknesses and introduced new areas of weakness, particularly in financial performance, operational practices, and ethical standards.

The Nursing homes industry faced extraordinary financial hardship during the pandemic, with advocates worrying about surges of closures. The COVID-19 pandemic greatly diminished occupancy rates and revenue because fewer older people were able to enter long-term care or be placed in short-term post-acute care after postponed medical procedures. At the same time, operating costs in nursing homes have exploded with new outlays on personal protective equipment, cleaning supplies, and tests for COVID-19 [2]. The pandemic further exacerbated shortages in staffing that already existed pre-pandemic, which lost 210,000 jobs and increased the hire of contract nurses, further increasing the costs [3]. In addition, inflation reached a peak of 9.1%, putting even more pressure on facilities financially [4]. By 2021, occupancy rates had recovered only to 84.7%, and 28% of residents in skilled nursing facilities were considered to be at financial risk [5]. An industry survey done in August 2020 found that over half of nursing homes were operating at a loss, and three-fourths expressed concerns about their ability to continue operating for another year [6].

Pre-pandemic, consistent high occupancy rates, predictable revenue streams, and reasonable operational costs made nursing homes attractive investments. However, the onset of COVID-19 triggered a sharp decline in occupancy rates since the virus continued to wreck populations as a consequence of increased mortality rates within facilities [2]. With such escalating costs, it was only with government aid of $21 billion that profitability improved for the period 2020 to 2021. The cutting down of operational costs because of lower capacity and lesser spending on PPE, in combination with government aid, merely cushioned the financial pressure for a short time [7].

In the midst of these challenges, an interesting trend unfolded, that of purchase and sale of nursing homes, depicting investor aspirations from these care facilities as businesses. This was more common with large publicly traded entities, including Ensign, which showed an over 100% increase in stock prices and profit margins. For instance, Real Estate Investment Trusts (REITs) which held stakes in nursing homes reported high

financial performance, meaning that the sector had good investment potential, despite the challenges from the pandemic [8].

However, the broader picture of financial stability in nursing homes remains complex, particularly when considering the increasing trend of nursing home closures. Several studies explore patterns and trends in nursing home closure within the last decade, well before the COVID-19 crisis. For instance, a recent study by the Office of the Assistant Secretary for Planning and Evaluation (ASPE) revealed that while the number of nursing home closures averaged 0.82% of all facilities each year from 2011 through 2017, in 2018 these numbers jumped to 0.96% and to 1.34% in 2019. This upward trend in closures, particularly in the years leading up to the pandemic, highlights financial fragility in the sector [6, 9].

These findings, therefore, indicate that some nursing homes are much more resilient than others; while some seem to attract the interest of new investors, others seem to be at a constant risk of closure, portending serious concern about the industry's overall financial health. This is particularly relevant to the core research question of this paper: How has financial performance, operational practices, and standards of ethics in nursing homes changed with regard to the pre-pandemic level and, therefore, what does that portend for investors?

With the increase in closures and mixed financial performance across the sector, it's vital for investors to take particular care when evaluating nursing homes prior to investment [6]. Some of them will prove to be good investments, especially if the location has strong occupancy rates, profitability, and stable running costs. The other types can turn out to be very risky, due to their instability and high chance of being closed for financial reasons. Therefore, the decision to invest in nursing homes ought to be based upon such an overall assessment, including financial metrics, operational resilience, ethical standards, and impact from COVID-19.

To explore these aspects, this paper conducted a comprehensive analysis of data from 2015 to 2021, examining trends in occupancy, expenses, revenues, and compliance with regulations in states over time. The investigation was embarked on to find out whether the nursing home business is viable or not in this prevailing environment. With this all-encompassing question at its heart, the following analysis is structured in three major time periods: pre-COVID, during COVID, and post-COVID, in order to properly capture the influence of the pandemic on the industry and appreciate its recovery trajectory.

To provide a robust foundation for the analysis, key metrics were compared across different states, focusing on variables such as occupancy rates, fines, median income, and population. Additionally, field research was conducted to guide the investigation and identify core variables that significantly impact the financial and operational stability of nursing homes. These variables include net income, the effects of the COVID-19 pandemic, fines and penalties, and ethical concerns related to the quality of care and resident safety. This approach makes it possible to provide a detailed understanding of the current scenario in nursing homes and become an essential input for stakeholders interested in investing in this sector.

This paper aims to address the following research questions:

RQ1. How has the financial performance of nursing homes evolved in the wake of the COVID-19 pandemic?

RQ2. How did the increase in COVID-19 cases during the pandemic impact mortality rates in nursing homes, and How occupancy rates contributed to variations in death rates across different facilities?

RQ3. What are the key factors that influence the financial viability and investment potential of nursing homes?

RQ4. How have ethical standards and the quality of care influenced investment decisions in the nursing home industry during and after the pandemic?

RQ5. To what extent should investors consider the financial, operational, and ethical dynamics of nursing homes in their investment decisions post-pandemic? and what are the implications of these changes for investors?

The rest of this paper is organized as follows: Section II presents Related Work, providing a comprehensive overview of previous studies relevant to the research questions. Section III covers the Methodology, where it introduces the data sources used for the study, followed by the procedure, which details the data cleaning, preparation, and analysis process. Section IV discusses the Results and Analysis, focusing on the findings and answering the research questions based on the processed data. Finally, Section V concludes the paper with a Conclusion and Future Work, summarizing the key insights, limitations, and suggestions for further research.

II. Related Work

A. Existing Research on COVID-19 and Nursing Homes

Although the COVID-19 pandemic has drastically influenced the financial and operational performance of nursing homes in the United States, there has been limited research examining the pandemic's impact on the financial performance of nursing homes. In this section we summarize different studies that examines the impact of COVID-19 on nursing homes from various perspectives. For example, Orewa et al. [10], highlighted how rising operational costs, decreased occupancy rates, and staffing shortages resulted in significant financial strain on nursing homes during the pandemic, despite government aid from initiatives like the CARES Act. Federal funding provided temporary relief, but the long-term sustainability of many facilities remains in question due to ongoing financial pressures and regulatory fines.

A study by Kingsley and Harrington [11] examines the financial impact of COVID-19 on publicly traded nursing home companies. Despite operational challenges such as lower occupancy and higher costs, these companies experienced minimal financial setbacks due to significant government relief, including Paycheck Protection Program funds. Unlike smaller or privately owned facilities, publicly traded nursing homes demonstrated resilience and, in some cases, improved stock performance during the pandemic. The findings highlight disparities within the sector, where larger corporations could leverage external support to maintain stability, contrasting with the financial struggles of smaller entities.

Begley and Weagley [12] found a direct correlation between a nursing home's liquidity and its ability to mitigate the spread of COVID-19. Facilities with fewer financial resources struggled to invest in risk mitigation measures, such as personal protective equipment (PPE) and high-frequency testing, leading to higher infection rates among residents. This finding aligns with our study, which examines the financial stability of nursing homes as a significant factor in operational sustainability.

Another study by Harrington et al. [13] analyzed the profitability of California nursing homes before and during the COVID-19 pandemic, highlighting how factors like occupancy rates, staffing, and government funding affected financial performance. During the pandemic, nursing homes faced increased costs for staffing and infection control while occupancy rates dropped. However, some facilities, particularly for-profit ones, remained profitable due to government aid and cost-cutting measures. The research underscores the disparities in financial outcomes, with for-profit homes generally faring better than nonprofit ones during this period.

A study by Festa et al. [14] examines the infection control strategies used by nursing homes during the COVID-19 pandemic. The research highlights measures such as enhanced hygiene, use of personal protective equipment (PPE), and social distancing, which were implemented to prevent virus transmission among residents and staff. The effectiveness of these strategies varied based on factors like available resources, staffing levels, and preparedness. The study emphasizes the need for timely interventions and government support to reduce mortality and improve care during health crises.

The impact of COVID-19 on nursing home staffing and care quality has also been a significant focus. Abrams et al. [15] found that staffing shortages exacerbated by the pandemic led to a decline in the quality of care provided, directly contributing to higher mortality rates in long-term care facilities. This aligns with our findings, where staffing levels, along with vaccination rates, were critical variables affecting the operational performance and ethical standards of care in nursing homes during and after the pandemic.

Also, a study by Xu, Intrator, and Bowblis [16], investigates the driving factors behind staff shortages in nursing homes during the COVID-19 pandemic. The study identifies several key contributors to these shortages, including increased infection rates among staff, heightened workloads, and insufficient availability of personal protective equipment (PPE). Additionally, the authors highlight that low wages, job dissatisfaction, and the high risk of COVID-19 exposure further exacerbated staffing challenges in nursing homes. Facilities with higher infection rates, inadequate staffing levels before the pandemic, and those in rural areas were particularly vulnerable to severe shortages. The study emphasizes the critical need for better support, including adequate compensation, protective resources, and policies aimed at improving workforce stability.

Chen et al. [17] highlight how staff movement across different nursing homes contributed to the spread of COVID-19. Their research emphasized the interconnectedness of care facilities and how weaknesses in one facility's infection control could affect others. This complements our study's emphasis on broader ethical considerations and the importance of system-wide health and safety protocols in shaping investment decisions.

A study by Braun et al. [18], examines the performance of private equity-owned nursing homes in the U.S. during the COVID-19 pandemic, comparing them to other types of ownership structures. The research found that private equity-owned nursing homes generally experienced worse outcomes in terms of COVID-19 infection rates and mortality compared to other nursing homes. Factors contributing to this disparity included lower staffing levels, fewer resources allocated to patient care, and prioritization of profitability over quality of care. These homes also had higher rates of shortages in personal protective equipment (PPE) and staff, leading to increased vulnerability to the pandemic.

He et al. [19], investigate whether there is a connection between the reported quality of nursing homes and the incidence of COVID-19 cases in California skilled nursing facilities. The study finds that facilities with lower quality ratings, particularly in areas related to staffing levels and infection control, were more likely to experience higher numbers of COVID-19 cases. The authors emphasize that inadequate staffing and poor infection control measures played a significant role in the spread of the virus. These findings suggest that improving quality standards, especially in staffing and infection control, is crucial for mitigating the impact of future pandemics in nursing homes.

Gmehlin et al. [20], examine the temporal dynamics of SARS-CoV-2 in Wisconsin nursing homes during the COVID-19 pandemic. The research tracks infection rates over time, highlighting how the virus spread throughout different phases of the pandemic and how various interventions, such as lockdowns, personal protective equipment (PPE), and vaccination efforts, impacted the transmission within nursing homes. The findings show that early interventions were crucial in reducing infection rates, but the continued vulnerability of nursing home populations emphasized the need for sustained and comprehensive strategies.

Gopal et al. [21], conduct a cross-sectional analysis of COVID-19 infection variations across nursing homes in California. The research identifies key factors that contributed to differences in infection rates, such as facility size, staffing levels, and geographic location. Nursing homes with higher staff-to-resident ratios and better infection control practices were more successful in "compressing the curve" of COVID-19 infections. The study emphasizes the importance of resource allocation, staff management, and preventive measures to limit virus spread in vulnerable nursing home populations.

Chatterjee et al. [22], examine the characteristics and quality of U.S. nursing homes that reported COVID-19 cases. The study highlights that facilities with lower quality ratings, particularly those with staffing shortages and poor infection control practices, were more likely to report COVID-19 cases. Additionally, nursing homes in densely populated areas and with a higher proportion of racial and ethnic minorities were disproportionately affected by the pandemic. The findings underscore the critical need for improvements in staffing, infection control measures, and resource allocation to better protect vulnerable populations in nursing homes.

Hege et al. [23], the authors analyze county-level social determinants of health and their association with COVID-19 outcomes in U.S. nursing homes between June 2020 and January 2021. The study highlights that social factors such as income inequality, racial disparities, and access to healthcare services significantly impacted COVID-19 case rates and mortality in nursing homes. Facilities located in counties with poorer social determinants of health faced higher infection rates and worse outcomes.

Lane et al. [24], the authors investigate the predictors of COVID-19 cases in nursing homes across the southeastern United States. The research identifies factors such as facility size, staffing levels, and regional healthcare access as significant predictors of infection rates. Nursing homes in areas with limited healthcare resources and those with lower staffing levels were more prone to outbreaks. The study highlights the need for targeted interventions in regions with vulnerable nursing home populations to prevent future outbreaks.

Finally, recent study by Yin et al. [25], systematically review the personal and contextual factors influencing COVID-19 infections among nursing home residents in the United States. The research identifies both individual-level factors, such as age, comorbidities, and vaccination status, as well as facility-level factors, including staffing levels, infection control practices, and facility location. The review highlights how these personal and contextual elements contributed to the varying rates of COVID-19 infections in nursing homes across the country. The authors emphasize the critical need for robust infection control strategies, improved staffing, and resource allocation to better protect vulnerable nursing home populations during pandemics.

B. Comparison with Proposed Method and Literature Gaps

The work done by our paper identifies several financial and ethical factors influencing the nursing home industry, many of which are corroborated by the existing literature. However, the proposed method introduces a unique framework for assessing the investment potential of nursing homes based on a combination of financial performance metrics, operational resilience, and ethical compliance standards, which has not been fully explored in previous studies. While several studies have examined the financial strain on nursing homes during the pandemic, few have provided a comprehensive framework that integrates both financial and ethical considerations into investment decision-making.

The proposed framework places a strong emphasis on ethical standards, particularly vaccination compliance and quality of care metrics, as key factors in assessing the viability of nursing home investments. This approach goes beyond the traditional financial metrics of occupancy rates and revenue streams, offering a more holistic view of the industry's post-pandemic landscape. Furthermore, our paper highlights the importance of maintaining high ethical standards in nursing homes, not only as a means of ensuring resident safety but also as a critical factor in maintaining operational and financial stability.

III. Methodology

A. Dataset Description

This research paper utilizes a comprehensive set of official datasets provided by the Centers for Medicare & Medicaid Services (CMS) through Medicare.gov [26]. These datasets are essential for comparing the performance of Medicare-certified skilled nursing facilities and nursing homes across the United States in various aspects of care, financial stability, and regulatory compliance. The dataset consolidates critical information on nursing home costs, occupancy rates, revenue streams, COVID-19 vaccination rates, health deficiencies, fines, and penalties. By including such a wide range of variables, the dataset offers a holistic view of nursing home performance across different dimensions, thereby enabling a thorough analysis without the need for experimentation on additional datasets. The breadth of data ensures that key factors affecting nursing home viability are well-represented and that the results are not only accurate but also scalable across various contexts. For instance, the inclusion of both financial and ethical considerations provides a more complete framework for assessing the investment potential of nursing homes, which is central to this study.

Furthermore, the temporal segmentation of the data into pre-COVID, COVID, and post-COVID periods strengthens the scalability of the research by allowing us to capture dynamic shifts in the nursing home industry. This segmentation reveals how nursing homes have adapted to the challenges posed by the pandemic, including changes in occupancy rates, operational costs, and ethical standards, without requiring supplementary datasets. The ability to evaluate these changes over time reinforces the findings' applicability to a wide range of scenarios, from stable pre-pandemic conditions to the heightened pressures of the pandemic and post-pandemic recovery. This temporal scope also supports the argument that the dataset used provides sufficient coverage for evaluating nursing home performance across different time periods and operational environments. Below is a detailed description of the key datasets and tables used in this study:

1) Cost report tables: The Skilled Nursing Facility Cost Report dataset contains financial information about nursing homes, including revenue, expenses, and other critical financial data. This dataset is crucial for analyzing the financial performance and stability of nursing homes over time.

2) Provider information tables: The dataset provides general information on currently active nursing homes. It includes data on the number of certified beds, quality measure scores, staffing levels, and other key metrics used in the Five-Star Rating System. Each row in this dataset represents one nursing home, offering a comprehensive overview of each facility's operational characteristics.

3) Health deficiencies tables: The dataset lists nursing home health citations issued over the last three years. It includes details

such as the nursing home that received the citation, the inspection date, citation tag number and description, the scope and severity of the citation, the current status, and the correction date. This dataset is presented as one citation per row and is critical for evaluating regulatory compliance and quality of care in nursing homes.

4) Service quality measures tables: The dataset provides quality measures based on resident assessments included in the Minimum Data Set (MDS). Each row contains a specific quality measure for a specific nursing home, including the four-quarter score average and scores for each individual quarter. This dataset is used to assess the overall quality of care provided in nursing homes.

5) Penalties tables (Penalties): The dataset contains information about fines and payment denials imposed on nursing homes over the last three years. This dataset is essential for analyzing the financial and regulatory risks associated with specific facilities.

6) COVID-19 vaccine tables: These datasets are available for 2020 and 2021 and are instrumental in evaluating how well nursing homes managed the COVID-19 pandemic in terms of vaccination coverage. They are split into two types:

a) Provider data: Contains current resident and healthcare personnel COVID-19 vaccination rates, presented as one row per provider.

b) State and national averages: Provides state and national averages for facility resident and healthcare personnel COVID-19 vaccination rates, presented as one row per state or territory, plus a row for national averages.

B. Methodology

This section outlines the structured approach employed for analyzing healthcare-related data, progressing through various stages from raw data collection to the final presentation of insights. The methodology comprises several key phases: data federation, data pre-processing, trend analysis and evaluation, ethical and financial evaluation, and insights presentation. The proposed methodology introduces several key advantages. First, the data federation process ensures consistency and accuracy by consolidating multiple datasets over time, allowing for a comprehensive, longitudinal analysis of nursing home performance. Second, the pre-processing and cleaning phases enhance data quality, ensuring that only reliable, well-structured data is used for analysis. By segmenting the data into pre-pandemic, pandemic, and post-pandemic periods, the methodology captures temporal trends that provide nuanced insights into how the pandemic impacted the financial and ethical performance of nursing homes. This segmentation allows for a clear comparison of performance across time periods, improving the understanding of recovery trajectories and the long-term sustainability of facilities.

The proposed framework places a strong emphasis on ethical standards, particularly vaccination compliance and quality of care metrics, as key factors in assessing the viability of nursing home investments. This approach goes beyond the traditional financial metrics of occupancy rates and revenue streams, offering a more holistic view of the industry's post-pandemic landscape. Furthermore, our paper highlights the importance of maintaining high ethical standards in nursing homes, not only as a means of ensuring resident safety but also as a critical factor in maintaining operational and financial stability.

1) Data federation: The process began with the collection and consolidation of multiple datasets from 2015 to 2021, including cost reports, provider information, COVID-19 vaccination data, health deficiencies, penalties, and quality measures. Individual datasets for each category were combined into comprehensive datasets for each year. A systematic approach was implemented to standardize column names and data types across all datasets. For instance, discrepancies in naming conventions were resolved by renaming columns to ensure consistency—facility identifiers were standardized across all datasets. Records with missing data in essential fields, such as facility identifiers and names, were removed to maintain data integrity. This data federation process is illustrated in Fig. 1.

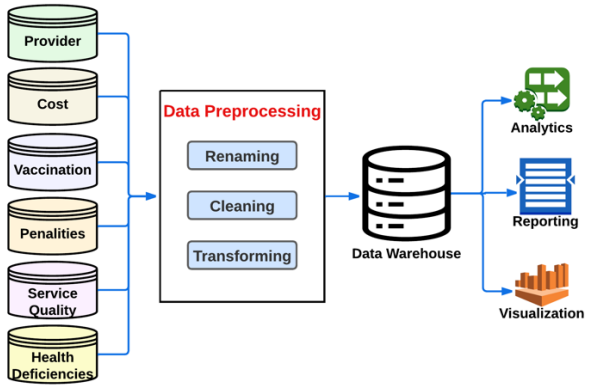


Fig. 1. Data federation process for nursing homes datasets.

2) Data pre-processing: Following data federation, thorough data pre-processing was conducted to ensure data quality and accuracy. This stage involved tasks such as cleaning data, handling missing values, standardizing formats, and ensuring consistency across datasets. Key steps included:

Standardizing data types is the process of converting facility identifiers and other key columns to uniform data types to facilitate accurate merging and analysis. While, handling missing values includes dropping records with missing or null values in critical fields to maintain data accuracy. Finally, feature selection is to select relevant variables essential for the analysis from the cleaned datasets.

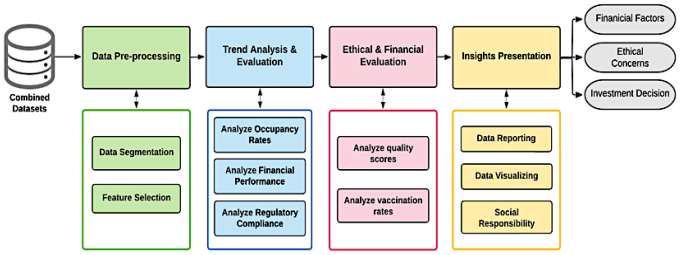


Fig. 2. Stages for healthcare data analysis and evaluation.

The pre-processed data provided a unified foundation for subsequent trend analysis and evaluation, allowing for detailed and accurate comparisons of nursing home performance from 2015 to 2021. The overall methodology is depicted in Fig. 2.

3) Data preparation

a) Data cleaning: Multiple datasets covering the years 2015 to 2021 were consolidated, encompassing information on costs, providers, vaccination rates, health deficiencies, penalties, and quality measures. To ensure consistency across these datasets, key identifiers were standardized, and discrepancies in naming conventions were resolved. Records with missing or null values in critical fields such as facility identifiers and names were removed to maintain data integrity. Data types were harmonized, particularly for identifiers, to facilitate accurate merging and analysis. A data filtering process was implemented to include only records with valid entries in essential fields.

b) Feature selection: Relevant variables essential for the analysis were selected from the cleaned datasets. From the cost-related data, variables pertaining to facility identifiers, names, locations, rural versus urban classifications, net income, number of beds, and salary information were extracted. From the provider data, variables related to total residents, incidents, complaints, fines, and penalties were selected.

c) Dataset combination: The selected features from the various datasets were merged on the standardized facility identifier to create a comprehensive dataset. This integration ensured that all relevant information was aligned for each nursing home facility.

d) Data transformation: Categorical variables were transformed into numerical formats to facilitate quantitative analysis. For example, rural versus urban classifications were encoded numerically.

e) Time-based segmentation: To enable temporal analysis of trends, the dataset was segmented into three distinct periods: the pre-pandemic period (2015–2019), establishing baseline operational and financial conditions; the pandemic period (2020), capturing immediate impacts of the COVID-19 pandemic; and the post-pandemic period (2021), assessing recovery trajectories and long-term effects.

4) Trend analysis and evaluation: This phase aimed to explore key metrics and patterns within the prepared data to understand operational and financial performance, serving as a foundation for regulatory and financial evaluation.

a) Occupancy rates analysis: Occupancy rates were calculated as the ratio of total residents to the number of beds for each facility. These rates were aggregated to compute median, mean, and total values across different time periods and states to identify occupancy trends.

b) Financial performance analysis: Net income data were analyzed to calculate mean and median values, identifying profitability trends over time. Additionally, cost and revenue components, including total salaries and net patient revenue, were evaluated to assess financial stability and the impact of the pandemic on financial operations.

c) Regulatory compliance analysis: Incident-related counts, such as incidents, complaints, fines, and total penalties, were aggregated to evaluate compliance trends. Fines and penalties were analyzed over time to identify emerging regulatory issues.

5) Ethical and financial evaluation: This phase assessed healthcare providers based on their quality of service and adherence to public health protocols, particularly in the context of COVID-19 vaccination efforts.

a) Quality scores analysis: Fourth-quarter quality scores were evaluated to determine care standards and identify any deficiencies or improvements over time.

b) Vaccination rates analysis: Staff and resident vaccination rates were compared by state and facility to gauge compliance with COVID-19 public health guidelines. The impact of vaccination rates on occupancy and financial performance was also assessed.

c) Ethical considerations: The balance between financial performance and ethical responsibilities was examined, emphasizing the importance of quality care and social responsibility, even in the absence of profitability.

6) Insights presentation: The final phase involved compiling the results of the data analysis and evaluation into actionable insights to support decision-making.

a) Data visualization: Intuitive charts and graphs were created to visually represent key findings, making complex data more accessible and understandable to stakeholders.

b) Stakeholder communication: Comprehensive commentary and discussion on all key performance indicators were provided. Significant trends, impacts, and ethical considerations were highlighted to inform decision-making and policy development.

IV. Result and Analysis

A. RQ1: Financial Performance of Nursing Homes at the Onset of the COVID-19 Pandemic

Fig. 3 illustrates the financial performance of nursing homes in 2020 and 2021, comparing costs and income. In 2020, the average total cost of 1,265,525.28 units was relatively high, reflecting the additional expenses due to pandemic-related factors like increased staffing and PPE requirements. However, the average net income of 1,613,439.84 units was still notably higher than costs, indicating that nursing homes managed to stay profitable, likely aided by government support. By 2021, the average total cost dropped slightly to 1,213,841.52 units, indicating a reduction in pandemic-related expenses. At the same time, the average net income increased marginally to 1,629,331.55 units, showing continued financial stability and even slight profitability growth.

The slight reduction in costs between the two years suggests that the dire financial pressures induced by the pandemic were easing. This decline, though, is indicative of a move towards more regular operations with reduced requirements for emergency expenditure. Meanwhile, the consistent rise of average net income throughout 2021 indicates that nursing

homes maintained their revenue streams, due to continued demand for care or ongoing government support.

To summarize, the financial performance of nursing homes evolved positively from 2020 to 2021. In 2020, the average total cost was elevated due to the need for additional staff and PPE, but average net income was strong, thanks in part to the $21 billion in government aid. As pandemic-related expenses decreased in 2021, the average total cost fell slightly while average net income increased, reflecting improved operational efficiency and profitability. This suggests that nursing homes successfully adapted to post-pandemic conditions, benefiting from reduced costs while maintaining a stable and slightly growing income.

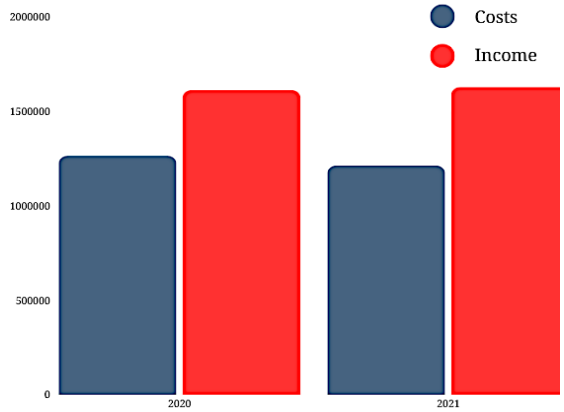


Fig. 3. Comparison of cost and income of nursing homes in 2020 and 2021.

B. RQ2: COVID-19 Case Surge and Mortality in Nursing Homes

Fig. 4 compares COVID-19 cases (in blue) and deaths (in red) from 2020 to 2024, with both plotted on a logarithmic scale. The figure shows that the death rates recorded in 2020 are by far the highest for all years considered. These peaks closely follow the spikes of recorded COVID-19 cases. In contrast, from 2021 onwards, the death rates started to decouple further from the number of cases reported. For example, late 2021 throughout most of 2022, while the case count increases and decreases in waves, the death rate remains relatively low as compared to that in the earlier stages of the pandemic. In the years 2023 and 2024, deaths remain on the lowest level with only some upticks seen in between. This signifies that along the way, health responses must be bettered against various health concerns brought about by several factors such as vaccinations, better treatments, and betterment of health protocols.

To address RQ2: In the first wave of the pandemic (2020), nursing homes were marked by rampant COVID-19 mortality with a high impact. The high impact came about due to the vulnerability of elderly populations in nursing homes and insufficiency in early interventions. Occupancy rates played a critical role in this: greater numbers of residents contributed to over-crowding, posing challenges for social distancing and infection control with the resultant higher levels of transmission and death. The converse is also true: low occupancy rates in some facilities led to lower numbers of outbreaks and deaths.

By 2021 and beyond, mortality rates in nursing homes fell, even as COVID-19 cases rose. This decline can be attributed to factors such as the availability of vaccines, which were prioritized for nursing home residents, and improved protocols for managing outbreaks in these facilities. Additionally, many nursing homes saw reduced occupancy due to deaths in 2020 or families withdrawing loved ones, which could have contributed to lower transmission rates and, by extension, lower death rates.

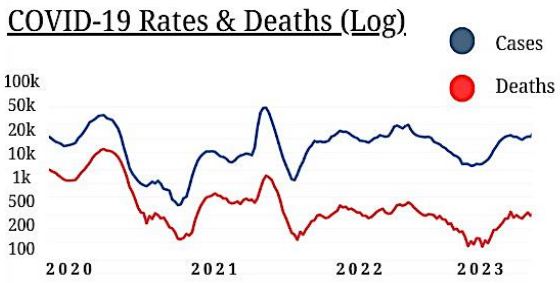


Fig. 4. Comparison of death rate at nursing homes from 2020 to 2024.

C. RQ3: Factors Affecting the Financial Viability and Investment Potential of Nursing Homes

1) Occupancy rates: Fig. 5 compares occupancy rates in all states from 2003 to 2023, it can be shown that from 2003 to 2019, occupancy rates in nursing homes were steady at approximately 82%, reflecting stable demand and consistent revenue streams for the industry. However, there is a sharp decline starting around 2020, which coincides with the COVID-19 pandemic. By 2021, occupancy rates had dropped significantly to 69%. This decline resulted from a combination of factors such as increased mortality among nursing home residents, families pulling loved ones out due to health concerns, and restrictions on new admissions due to safety protocols. By 2023, although there is a slight improvement in occupancy rates, they have not yet returned to pre-pandemic levels, signaling ongoing challenges for the nursing home industry in fully recovering.

Occupancy rates are central to the financial health of a nursing home. The higher the rates of occupancy, the more residents there which means a predictable revenue stream with respect to Medicaid, Medicare, and private payers. When occupancy rates drop, as they did during the pandemic, it reduces the income paying for daily operation. Nursing homes rely on these high occupancy rates to have a steady income; each resident pays with Medicaid, Medicare, or private payments. The 69% occupancy rate seen in 2021 represents a significant loss in revenue compared to the pre-pandemic norm of 82%. Moreover, lower occupancy rates can equate to higher operational costs per resident, since many fixed costs (staff salaries, utilities, maintenance) remain constant regardless of how many residents are in a facility. The decrease in occupancy rate, therefore, likely forced numerous nursing homes to operate at a loss or to retrench services, which further complicated their recovery.

From an investment perspective, facilities with high and stable occupancy rates (like the pre-pandemic average of 82%) offer a more reliable and steady return on investment (ROI). Investors are more likely to be attracted to nursing homes with occupancy rates closer to pre-pandemic levels, as they indicate

financial health and operational efficiency. However, the sharp decline to 69% during the pandemic and the slow recovery indicate increased risk. Nursing homes with low occupancy rates may face financial difficulties, as they have less revenue to cover their fixed costs, including staffing, maintenance, and other operational expenses. Investors may view this as a warning sign of financial instability and would be cautious about investing in facilities where occupancy is not recovering to pre-pandemic levels.

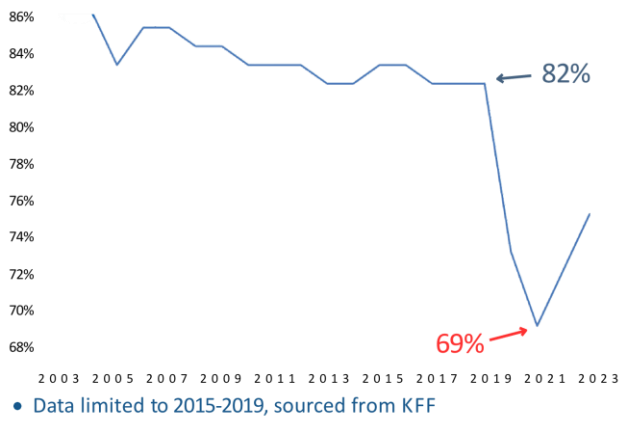


Fig. 5. Occupancy rates between 2003 and 2023.

2) Operating costs and revenue: Fig. 6 compares the mean total operating costs and mean net patient revenues for nursing homes from 2015 to 2021. It highlights key trends during this period, including the effects of the COVID-19 pandemic.

Mean Net Patient Revenue increased steadily from 2015, peaking in 2019 at approximately $9.5M, before dropping slightly in the following years, particularly during 2020 and 2021 (post-pandemic period). On the other hand, Mean Total Costs remained relatively flat from 2015 to 2019, hovering around $1.4M, but then showed a notable decline from 2019 to 2021, indicating a reduction in operating costs for nursing homes during the pandemic.

The steady increase of net patient revenue between 2015 and 2019, peaking in 2019 suggests that nursing homes were experiencing growing revenue from patient services prior to the pandemic, driven by increased demand for long-term care and possibly higher reimbursement rates. However, following the pandemic, revenues slightly declined, likely due to reduced occupancy rates, disruptions to regular operations, and health-related restrictions. On the other hand, the decline of costs during 2020 and 2021 may be attributed to the operational changes brought about by the pandemic, such as reduced staffing needs due to lower occupancy, fewer new admissions, and changes in services provided.

Stable or increasing revenues combined with controlled or decreasing operating costs are essential for maintaining profitability in nursing homes. From 2015 to 2019, rising revenues and steady costs would have made the industry an attractive target for investors, as this combination suggests strong operational efficiency and financial health. The ability to manage costs effectively, especially during the post-pandemic period, further solidifies the attractiveness of nursing homes as a reliable investment. During the pandemic, government relief funds played a critical role in boosting profits by helping nursing homes manage unexpected costs and revenue shortfalls. These funds enabled nursing homes to stabilize their operations, maintain essential services, and reduce operational costs, which contributed to higher profit margins despite the challenges posed by the pandemic.

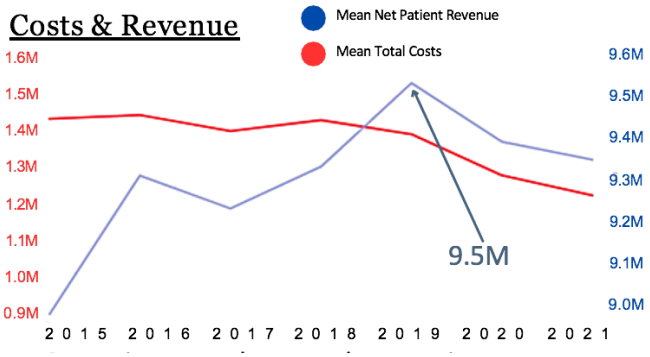


Fig. 6. Cost and revenue mean between 2015 and 2021.

3) Fines and penalties: The diagram in Fig. 7 compares the mean amount of fines (in dollars) and the mean count of penalties per home for nursing homes from 2015 to 2021. The mean amount of fines steadily increased from $28,000 in 2015 to a peak of $48,740 in 2021, with a notable spike starting in 2017. However, the mean count of penalties per home remained stable between 1.6 and 1.8 from 2015 to 2020 but surged to 2.4 penalties per home in 2021 post-pandemic. The significant rise in fines and penalties in 2021 is a result of stricter regulations and enforcement post-pandemic, with many nursing homes being penalized for failing to meet updated health and safety protocols, especially related to infection control, staff shortages, or resident care during the pandemic.

Fines and penalties are key indicators of compliance and regulatory risk in the nursing home industry. An increase in both fines and penalties, as seen in 2021, suggests heightened regulatory scrutiny and an increased likelihood of nursing homes being penalized for non-compliance with health and safety standards. For nursing homes, higher fines directly affect profitability. As seen in the diagram, the mean fine amount spiked to $48,740 in 2021, significantly higher than pre-2017 levels. This increase represents a major financial burden for nursing homes, especially smaller operators, as fines of this magnitude can cut into profit margins or even cause financial strain. For investors, high fines signal operational risk, as nursing homes that are consistently fined may face ongoing regulatory challenges and higher costs associated with compliance.

Penalties and Reputational Risk: The increase in the mean count of penalties per home from 1.6 to 2.4 in 2021 is another key factor for investors to consider. Penalties often reflect deficiencies in care or operational failures, such as inadequate staffing, poor infection control, or violations of resident rights. A rising number of penalties suggests that many nursing homes are struggling to meet regulatory standards, particularly in the wake of the pandemic.

For investors, frequent penalties represent both a financial and reputational risk. Nursing homes with high penalties may be subject to negative media coverage, lawsuits, or damage to their brand reputation. This could result in reduced occupancy rates, lower revenues, and a higher likelihood of facing additional regulatory scrutiny in the future.

Fig. 7. Fines and penalties mean between 2015 and 2021.

4) Relation between housing density and income levels in cities-Additional analysis: Fig. 8 illustrates an example of further analysis that could be performed. In a simple case from our local county, it is observed that as the number of nursing homes within a city increases, the average net income per home tends to decrease. This downward trend is driven by competitive pressures. This type of analysis can be replicated at any county level to determine if a particular city has historically been profitable. Comparing local facilities is a crucial step in making informed investment decisions, and this analysis may be useful if other key factors remain insufficient or unsatisfactory.

The scatter plot in Fig. 9 shows the relationship between homes per city and income per home across different cities, with a negative correlation indicated by the downward-sloping trend line. The key insight from the graph is that cities with higher incomes per home tend to have fewer homes, while cities with more homes often see lower income per home. This pattern reflects the inverse relationship between housing density and income levels in these cities. Wealthier areas tend to have fewer homes, due to larger properties or stricter zoning laws, while more densely populated areas may have a broader range of housing options, resulting in lower average income per home.

For instance, Affluent Areas with Higher Income per Home Cities like Walnut Creek and Concord, which have higher income per home but fewer homes, are attractive targets for premium nursing home investments. Higher income levels suggest a stronger ability to pay for high-quality nursing care, which may include premium services or private-pay nursing homes. Investors in nursing home facilities may find greater profit potential in these areas, as the demand for upscale care services is likely to be stronger. Additionally, cities with higher income levels are often associated with better healthcare infrastructure and higher reimbursement rates from both private insurance and Medicare. For nursing home investors, this means a more stable revenue stream and an opportunity to offer specialized services that cater to the affluent population.

On the other hand, densely Populated Cities with More Homes but lower income cities like Danville, Moraga, and Pleasant Hill, with a larger number of homes but lower income per home, may present opportunities for more affordable nursing home facilities. These areas might cater to middle-income or Medicaid-dependent populations, where demand is still strong but cost sensitivity is higher. For investors, the opportunity in these areas would be to focus on cost-efficient operations and scaling services to meet the needs of a larger population. Facilities in these cities may focus more on Medicaid reimbursements or offer a mix of private-pay and government-funded beds to maintain profitability. While profit margins may be lower in these areas compared to affluent ones, the volume of potential residents could ensure steady occupancy rates, which is a critical factor in maintaining revenue streams in the nursing home industry.

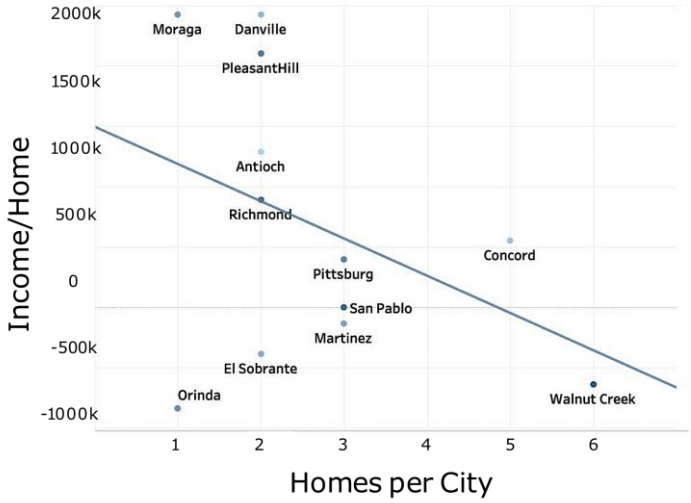


Fig. 8. Housing density and income levels.

D. RQ4: Impact of Ethical Standards and Quality of Care on Investment Decisions in Nursing Homes

1) Vaccination rates Impact on investors

a) Impact of vaccination rates of staff: Fig. 9 displays the COVID-19 vaccination rates of nursing home staff across various U.S. states. The color coding indicates disparities, with red regions representing states with lower vaccination rates around 62.99%, and blue regions showing states with higher vaccination rates nearing 97.99%. This color gradient highlights the variation in the extent to which nursing home staff have been vaccinated across the country.

The states with lower vaccination rates, such as Nevada and California, pose significant risks for nursing homes. When a larger percentage of staff remains unvaccinated, there is a heightened risk of COVID-19 outbreaks, which could severely impact operations. Staff shortages due to illness or quarantine measures can disrupt daily operations and increase staffing costs, while heightened infection rates may also lead to increased absenteeism. These disruptions not only reduce the

quality of care but can lead to operational inefficiencies and financial strain.

Conversely, in states with higher vaccination rates among nursing home staff, such as Maine and Vermont, the environment is more stable. Nursing homes in these regions are less likely to experience outbreaks or disruptions, as a well-vaccinated workforce is better able to protect the vulnerable resident population. This leads to more consistent operations, lower healthcare-related costs, and an overall safer environment for residents and staff alike. Consequently, these facilities are less likely to experience regulatory issues or fines associated with non-compliance to public health measures.

For investors specifically looking at nursing home facilities, staff vaccination rates are a critical factor in evaluating the operational risk of a nursing home. Nursing homes in states with low staff vaccination rates (A larger percentage of states fall within this lower vaccination bracket) are exposed to higher risks of operational challenges and increased costs. These challenges include higher healthcare expenses, potential penalties for non-compliance with vaccination mandates, and decreased trust from residents and their families, leading to lower occupancy rates. Such risks could translate into lower returns on investment, as these nursing homes may struggle to maintain financial stability in the face of ongoing COVID-19-related challenges.

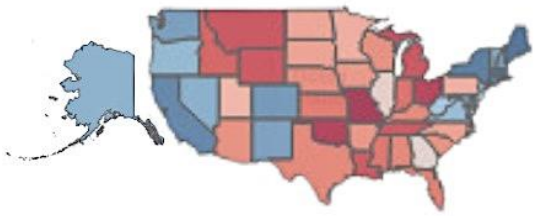


Fig. 9. Vax rates of staff in nursing homes.

b) Impact of vaccination rates of residents: Fig. 10 illustrates the disparities in COVID-19 vaccination rates among nursing home residents across U.S. states, distinguishing between states with lower and higher vaccination rates. Red regions indicate states where the vaccination rate is around 75.76%, while green and blue regions show states achieving rates near 95.63%.

States such as California, Nevada, and several in the South show lower vaccination rates for nursing home residents. This trend suggests that a larger number of states, especially in these regions, have not yet achieved optimal vaccination coverage, which is essential for protecting vulnerable populations in nursing homes. Conversely, states in the Northeast and parts of the Midwest have much higher vaccination rates, demonstrating effective public health strategies and higher compliance with vaccination protocols in nursing homes.

Investment considerations in nursing homes must account for the varying vaccination rates, as they significantly influence risk levels. Nursing homes in states with lower vaccination rates face increased operational risks. These include heightened healthcare costs for protective measures, potential regulatory scrutiny, and lower occupancy rates as families may choose safer facilities for their loved ones. In contrast, nursing homes in states with higher vaccination rates offer safer investment opportunities. These facilities are likely to experience fewer COVID-related disruptions, maintain higher occupancy rates due to increased trust and demand, and incur lower healthcare-related expenses. Moreover, these homes are in a better position to uphold a strong regulatory standing, reducing the likelihood of fines or sanctions.

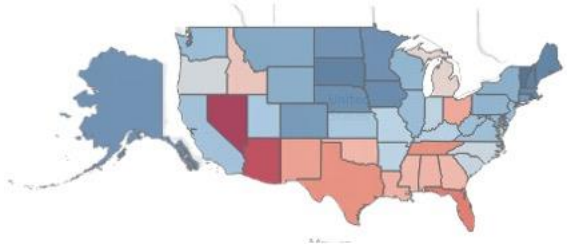


Fig. 10. Vax rates of residents in nursing homes.

2) Quality of care scores impact: Fig. 11 compares the mean 4Q quality scores for nursing homes across five states in 2021 (post-pandemic). The scores indicate the overall quality of care delivered in nursing homes during the fourth quarter of 2021. Arizona had the highest 4Q quality score of 34.249%, reflecting better overall care quality in its nursing homes compared to the other states. Tennessee, Florida, and Maryland: These states fall close together in terms of 4Q quality scores, with only slight differences with a score of 33.514%, 33.466%, and 33.340%, respectively. Mississippi had the lowest score among the states compared, with 33.049%.

The 4Q quality score measures various factors such as patient care, safety, infection control, and staff performance. Higher 4Q scores represent better overall performance in delivering high-quality care, which is a critical factor in determining the viability and attractiveness of a nursing home for investment purposes. Arizona, with the highest 4Q quality score, indicates a strong performance in the quality of care provided. Investors are likely to view nursing homes in Arizona as lower-risk investments due to their demonstrated commitment to maintaining high standards of care.

Higher-quality facilities tend to attract more residents, maintain higher occupancy rates, and face fewer fines and penalties, which contributes to a stable revenue stream. Mississippi's relatively lower 4Q quality score indicates a potential risk factor for investors. Lower quality can signal operational challenges such as staff shortages, poor care management, or non-compliance with health regulations. These issues can lead to higher fines, lower occupancy rates, and increased reputational risks, all of which could negatively impact profitability.

Investors will be more inclined to invest in nursing homes with higher 4Q scores, as these facilities are more likely to attract residents and maintain stable income streams. Nursing homes with lower 4Q scores may face increased regulatory scrutiny, penalties, or fines for failing to meet standards, which could increase operational costs and decrease profitability. Investors will consider 4Q quality scores as a measure of compliance risk when evaluating potential investments.

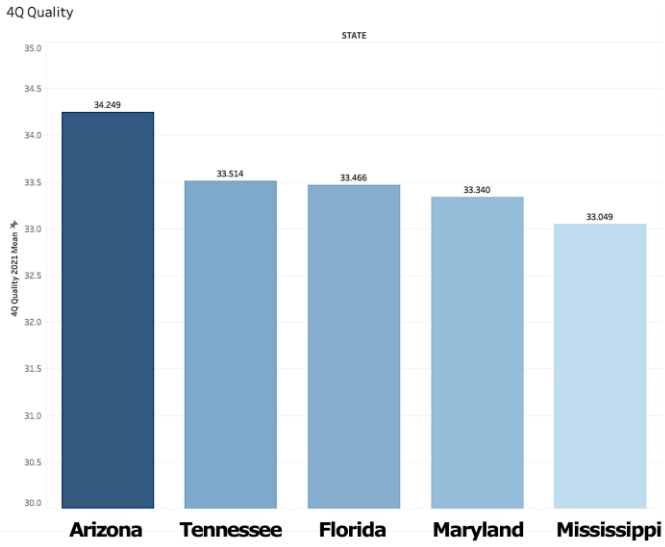


Fig. 11. 4Q quality mean in 2021.

3) Social responsibility: Investing in nursing homes, even when profitability is not guaranteed, offers significant advantages from a social responsibility perspective. Nursing homes provide critical care for some of society's most vulnerable populations, including the elderly and those with long-term health conditions. When factors such as lower profitability or operational risks suggest that investment in this sector may be less financially rewarding, socially responsible investors can still make a meaningful impact by allocating resources to improve the quality of care, support staffing needs, and ensure that residents receive the best possible services.

By investing in nursing homes, despite potential financial drawbacks, investors contribute to the greater social good, helping to maintain or elevate the standards of care in underfunded regions. This not only enhances the lives of residents but also supports local healthcare infrastructure, creates jobs, and promotes public health. Ultimately, these investments align with ethical goals, showing a commitment to community welfare and long-term societal benefit, which can resonate positively with socially-conscious stakeholders and investors.

E. RQ5: Post-Pandemic Investment Considerations: Financial, Operational, and Ethical Dynamics of Nursing Homes. Implications for Investors.

In the post-pandemic era, investors must carefully evaluate a range of financial, operational, and ethical factors before making decisions about investing in nursing homes. These factors include occupancy rates, net income, the lingering effects of COVID-19, and fines or penalties that may affect profitability. Additionally, operational considerations such as maintaining high quality of care, ensuring high vaccination rates, and adhering to social responsibility are critical in assessing the long-term viability of investments. These factors have become even more crucial in the wake of the pandemic, which has reshaped the landscape of the nursing home industry.

Occupancy rates are a central factor for nursing homes, as stable or increasing rates are vital for generating revenue. Facilities with low occupancy struggle to cover their operating costs, which nursing homes experienced financial strain during the pandemic due to increased costs for personal protective equipment, infection control measures, and staffing shortages. Facilities that have not recovered financially pose significant risks for investors, as they may not offer stable returns. The effects of COVID-19 continue to shape this sector, with facilities needing to adjust to new safety protocols and costs.

Furthermore, fines and penalties add an additional layer of risk. Nursing homes with frequent fines, usually due to lapses in care or regulatory non-compliance, indicate poor operational management and higher costs. This directly impacts their net income and increases the financial burden on the facility, making it less attractive to investors. These facilities may also suffer reputational damage, further decreasing their ability to attract new residents and maintain occupancy.

Operationally, quality of care plays a crucial role in the investment decision. Nursing homes that maintain high standards of care tend to have better reputations and higher occupancy rates. Families are more likely to choose facilities with strong care metrics, which translates to more stable revenue streams. Conversely, homes with poor care quality are often subject to penalties, legal issues, and low occupancy rates, making them riskier investments. Additionally, vaccination rates among staff and residents are another critical consideration post-pandemic. Facilities with higher vaccination rates are less vulnerable to outbreaks, which reduces operational disruptions and associated healthcare costs. These facilities are more likely to maintain smooth operations, offering a safer environment for residents and, consequently, more reliable returns for investors.

Given these considerations, we advise against investing in nursing homes unless specific criteria are met. First, facilities must show increasing occupancy rates. Without high occupancy, nursing homes cannot generate sufficient revenue to cover operational costs. The number of nursing homes in a city also affects investment attractiveness, as increased competition can drive down occupancy and profitability. Investors should prioritize cities with fewer nursing homes relative to the population of elderly residents to avoid competitive saturation.

Another key criterion is the income/bed ratio, which reflects the financial efficiency of a facility. Homes with a high income per bed are more financially secure, indicating they can generate sufficient revenue to support operations. Profitability remains a major concern; facilities that do not consistently demonstrate profitability, especially post-pandemic, are unlikely to offer reliable returns. Additionally, constant costs are critical to operational stability. Facilities with volatile cost structures due to the pandemic or poor management may face financial challenges that make them poor investment choices.

Quality of care is also essential. Homes that maintain high 4Q quality scores provide a safer environment, making them more attractive to residents and, by extension, investors. Facilities with low care scores face reputational risks and may struggle with fines or penalties, which can harm financial

performance. Finally, vaccination rates among staff and residents are a key factor in ensuring operational stability. Homes with high vaccination rates are less prone to COVID-19 outbreaks, ensuring fewer disruptions and lower healthcare costs, making them safer investments.

From an ethical perspective, social responsibility has become increasingly important. Even when profitability is not guaranteed, socially responsible investors may still consider allocating funds to nursing homes. This is particularly true in areas where the public good is at stake, such as caring for the elderly and vulnerable populations. Investing in nursing homes, despite lower returns, can align with the broader goals of contributing to community welfare and supporting critical healthcare infrastructure. However, for profit-driven investors, ethical considerations alone may not justify the investment unless these facilities also demonstrate operational efficiency and financial stability. The decision-making process can be shown in Fig. 11.

F. Discussion and Insights

The findings of this research provide a comprehensive look at the significant shifts in the nursing home industry caused by the COVID-19 pandemic, highlighting the critical role of financial performance, ethical standards, and operational resilience. From the data collected and analyzed, it is clear that the pandemic not only exacerbated pre-existing vulnerabilities within the industry but also introduced new challenges that have reshaped how nursing homes operate and are perceived as investment opportunities. However, the true value of this study lies not just in quantifying these effects but in understanding the broader implications for the future of long-term care.

One of the most striking insights from the analysis is the persistent decline in occupancy rates and how this metric remains a crucial indicator of financial viability for nursing homes. The pandemic's severe impact on occupancy rates underscores the need for long-term planning and adaptability within the sector. In my view, this highlights a critical need for nursing homes to rethink their operational models, possibly expanding beyond traditional care models to include services that can attract more residents in both post-pandemic and future crises. For example, a focus on rehabilitation services, at-home care integration, or telehealth options might provide nursing homes with the flexibility to maintain stable revenues even in the face of future disruptions.

The pandemic has also forced a reassessment of the ethical standards within nursing homes, particularly concerning patient safety, vaccination compliance, and overall quality of care. It is my opinion that ethical considerations should no longer be viewed as secondary to financial performance but as integral to the operational success and sustainability of nursing homes. The findings of this study clearly show that facilities that adhered to higher ethical standards—such as maintaining high vaccination rates—were better positioned to weather the challenges of the pandemic. This suggests a shift in the industry where ethical compliance, particularly related to healthcare protocols, could be seen not only as a moral imperative but also as a competitive advantage.

Moreover, from an investment perspective, this research suggests that future investors in the nursing home industry will need to be more discerning. The emphasis on metrics like occupancy rates, fines, and penalties, as well as adherence to ethical standards, will likely become central to investment decisions. My personal opinion is that investors must now adopt a more holistic approach when evaluating nursing homes, taking into account both the financial health of the facility and its ethical standing. This shift toward socially responsible investment may not only yield better returns but also contribute to the improvement of care standards across the industry, creating a more sustainable model for the long-term care sector.

V. Conclusion

In this paper, we have explored the financial shifts, ethical dilemmas, and investment potential in the nursing home industry, with a focus on the pre- and post-COVID-19 landscape. The COVID-19 pandemic significantly impacted nursing home operations, exacerbating pre-existing financial vulnerabilities and introducing new challenges in the form of increased costs, declining occupancy rates, and heightened scrutiny around care quality and ethical standards. Our study highlights that while government aid played a vital role in stabilizing the industry during the pandemic, long-term financial sustainability remains uncertain. The analysis also underscores the critical importance of ethical considerations, such as vaccination compliance and quality of care, in both maintaining operational stability and attracting potential investments.

As the nursing home industry navigates the post-pandemic recovery phase, our findings suggest that investment in this sector should be approached cautiously. Facilities with strong financial performance, high occupancy rates, low fines and penalties, and adherence to ethical standards are more likely to offer stable returns. In contrast, facilities that fail to meet these criteria may present excessive financial and operational risks.

Future Work

Will focus on several key areas. First, a deeper analysis of regional variations in nursing home performance could provide more granular insights into how different states and localities responded to the pandemic. This would allow for a better understanding of regional disparities and how specific policies and regulations may have influenced nursing home operations. Additionally, future research should explore the long-term impact of COVID-19 on the quality of care in nursing homes, particularly how ethical standards and vaccination policies continue to shape resident outcomes over time. This will help identify ongoing trends and assess the effectiveness of current policies in ensuring the health and safety of nursing home residents.

Acknowledgment

The authors would like to acknowledge the Centers for Medicare & Medicaid Services (CMS) for providing the comprehensive datasets used in this research. These datasets, available through Medicare.gov, were instrumental in our analysis of the nursing home industry, allowing us to explore

various aspects of financial performance, operational practices, and regulatory compliance. We appreciate the CMS's commitment to transparency and public access to critical healthcare data, which has significantly contributed to the depth and quality of this study.

REFERENCES

[1] National Academies of Sciences, Engineering, and Medicine, Health and Medicine Division, Board on Health Care Services, Committee on the Quality of Care in Nursing Homes, The National Imperative to Improve Nursing Home Quality: Honoring Our Commitment to Residents, Families, and Staff, Washington, DC: National Academies Press, 2022. Available: https://www.ncbi.nlm.nih.gov/books/NBK584647/. [Accessed: Sept. 20, 2024].

[2] S. Giri, L. M. Chenn, and R. Romero-Ortuno, "Nursing homes during the COVID-19 pandemic: a scoping review of challenges and responses," Eur. Geriatr. Med., vol. 12, pp. 1127–1136, 2021. [Online]. Available: https://doi.org/10.1007/s41999-021-00531-2.

[3] Long Term Care Jobs Report, Bureau of Labor Statistics, year-end data released by the American Health Care Association (AHCA) and National Center for Assisted Living (NCAL), AHCA/NCAL, Jan. 2023. [Online]. Available: https://www.ahcancal.org/News-and-Communications/Fact-Sheets/FactSheets/LTC-Jobs-Report-Jan2023.pdf. [Accessed: 20-Sep-2024].

[4] AHCA/NCAL, "2022 State of the SNF Industry Report," American Health Care Association/National Center for Assisted Living, Fact Sheet, 2022. [Online]. Available: https://www.ahcancal.org/News-and-Communications/Fact-Sheets/FactSheets/2022%20State%20of%20the%20SNF%20Industry%20Report.pdf. [Accessed: Sep. 16, 2024].

[5] J. Yang, "Occupancy rate of U.S. skilled nursing facilities from 2020-2021," Statista, Apr. 23, 2024. [Online]. Available: https://www.statista.com/statistics/858692/us-skilled-nursing-facility-occupancy-percentage/. [Accessed: Sep. 16, 2024].

[6] M. Segelman, K. Porter, K. Hughes, M. Diaz, I. Oliveira, Z. Feng, and S. Karon, "Nursing home closures did not increase in 2020 and 2021, despite financial challenges caused by the COVID-19 pandemic," Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services, Washington, DC, Issue Brief, May 31, 2024.

[7] T. Edelman and M. Edelman, "SNF financial support during COVID," Center for Medicare Advocacy, Mar. 22, 2021. [Online]. Available: https://medicareadvocacy.org/report-snf-financial-support-during-covid/. [Accessed: Sept. 20, 2024].

[8] D. Williams Jr, R. Fernandez, D. Stevenson, M. Unruh, and R. T. Braun, "Nursing home finances associated with real estate investment trust and private equity investments," Health Affairs Scholar, vol. 2, no. 4, pp. qxae037, Apr. 2024. doi: 10.1093/haschl/qxae037. [Online]. Available: https://doi.org/10.1093/haschl/qxae037

[9] D. Anders, D. Emerson, D. Schuh, S. Taylor, and S. Wilson, "State of Skilled Nursing Facility (SNF) industry," CliftonLarsonAllen Wealth Advisors, LLC, 2022. Available: https://www.ahcancal.org/News-and-Communications/Fact-Sheets/FactSheets/2022%20State%20of%20the%20SNF%20Industry%20Report.pdf.

[10] G. N. Orewa et al., "COVID-19 Pandemic Impact on Nursing Homes Financial Performance," INQUIRY: J. Health Care Organ. Provision, Financ., vol. 61, pp. 00469580241240698, 2024.

[11] D. E. Kingsley and C. Harrington, "COVID-19 had little financial impact on publicly traded nursing home companies," J. Am. Geriatr. Soc., vol. 69, no. 8, pp. 2099-2102, Aug. 2021.

[12] Taylor A. Begley and Daniel Weagley, "Firm Finances and the Spread of COVID-19: Evidence from Nursing Homes," Review of Corporate Finance Studies, vol. 12, pp. 1–35, 2023.

[13] C. A. Harrington et al., "Examining California nursing home profitability and related factors before and during the COVID-19 pandemic," J. Am. Geriatr. Soc., vol. 71, no. 8, pp. 2530-2538, 2023.

[14] N. Festa et al., "Nursing home infection control strategies during the COVID-19 pandemic," J. Am. Geriatr. Soc., vol. 71, no. 8, pp. 18402, May 2023. Available: https://doi-org.ezproxy.herts.ac.uk/10.1111/jgs.18402.

[15] H. R. Abrams, L. Loomer, A. Gandhi, and D. C. Grabowski, "Characteristics of U.S. nursing homes with COVID-19 cases," J. Am. Geriatr. Soc., vol. 68, no. 8, pp. 1653-1656, Aug. 2020, doi: 10.1111/jgs.16661.

[16] H. Xu, O. Intrator, and J. R. Bowblis, "Shortages of staff in nursing homes during the COVID-19 pandemic: What are the driving factors?," J. Am. Med. Dir. Assoc., vol. 21, no. 10, pp. 1371-1377, Oct. 2020, doi: 10.1016/j.jamda.2020.08.002.

[17] M. K. Chen, J. A. Chevalier, and E. F. Long, "Nursing home staff networks and COVID-19," Proc. Natl. Acad. Sci. U. S. A., vol. 118, no. 1, pp. e2015455118, Jan. 2021, doi: 10.1073/pnas.2015455118.

[18] R. T. Braun, H. Yun, L. P. Casalino, Z. Myslinski, F. M. Kuwonza, H. Y. Jung, and M. A. Unruh, "Comparative performance of private equity-owned US nursing homes during the COVID-19 pandemic," JAMA Netw. Open, vol. 3, no. 10, pp. e2026702, Oct. 2020, doi: 10.1001/jamanetworkopen.2020.26702.

[19] M. He et al., "Is there a link between nursing home reported quality and COVID-19 cases? Evidence from California skilled nursing facilities," J. Am. Med. Dir. Assoc., vol. 21, no. 7, pp. 905-908, July 2020, doi: 10.1016/j.jamda.2020.06.016.

[20] C. G. Gmehlin et al., "SARS-CoV-2 and Wisconsin nursing homes: Temporal dynamics during the COVID-19 pandemic," J. Am. Med. Dir. Assoc., vol. 22, no. 11, pp. 2233-2239, Nov. 2021, doi: 10.1016/j.jamda.2021.07.019.

[21] R. Gopal, X. Han, and N. Yaraghi, "Compress the curve: A cross-sectional study of variations in COVID-19 infections across California nursing homes," BMJ Open, vol. 11, pp. e042804, 2021, doi: 10.1136/bmjopen-2020-042804.

[22] P. Chatterjee, S. Kelly, M. Qi, and R. M. Werner, "Characteristics and quality of U.S. nursing homes reporting cases of coronavirus disease 2019 (COVID-19)," JAMA Netw. Open, vol. 3, no. 7, pp. e2016930, July 2020, doi: 10.1001/jamanetworkopen.2020.16930.

[23] A. Hege, S. Lane, T. Spaulding, M. Sugg, and L. S. Iyer, "County-level social determinants of health and COVID-19 in nursing homes, United States, June 1, 2020–January 31, 2021," Public Health Rep., vol. 137, no. 1, pp. 137-148, 2022, doi: 10.1177/00333549211053666.

[24] S. J. Lane, M. Sugg, T. J. Spaulding, A. Hege, and L. Iyer, "Southeastern United States predictors of COVID-19 in nursing homes," J. Appl. Gerontol., vol. 41, no. 7, pp. 1641-1650, 2022, doi: 10.1177/07334648221082022.

[25] C. Yin, E. Mpofu, K. Brock, and S. Ingman, "Nursing home residents' COVID-19 infections in the United States: A systematic review of personal and contextual factors," Gerontol. Geriatr. Med., vol. 10, pp. 1-10, 2024, doi: 10.1177/23337214241229824.

[26] "Provider Data: Nursing Homes," Centers for Medicare & Medicaid Services, [Online]. Available: https://data.cms.gov/provider-data/topics/nursing-homes. [Accessed 1 Sept 2024].

FusionSec-IoT: A Federated Learning-Based Intrusion Detection System for Enhancing Security in IoT Networks

Jatinder Pal Singh[1], Rafaqat Kazmi[2]
QA Manager, Apple Inc., USA[1]
Department of Software Engineering, IUB, Pakistan[2]

***Abstract*—Internet of Things (IoT) has become one of the most significant technological advancements of the modern era, which has impacted multiple sectors in the way it provides communication between connected devices. However, this growth has led to security risks in the IoT devices especially when constructing resource-limited IoT networks that are easily attacked by hackers through methods like DDoS and data theft. Traditional IDS such as centralized IDS and single-view machine learning-based IDS are incapable of providing efficient solutions to these issues due to high communication cost, latency, and low attack detection rate for IDS. To address these challenges, this paper presents FusionSec-IoT, a decentralized IDS based on multi-view learning and federated learning for better detection performance and scalability in the IoT context. The results sows that the proposed technique performs better than the existing IDS methods with 08.3% accuracy as compared to classic IDS techniques centralized IDS (91.5%) and single-view federated learning (92.7%). The other performance metrics like shows a better performance as compared to traditional IDS methods. Thus, FusionSec-IoT detects a broad range of cyberattacks with the help of the employed complex machine learning algorithms such as Reinforcement Learning, Meta-Learning, and Hybrid Feature Selection using Particle Swarm Optimisation (PSO) and Genetic Algorithm (GA), and ensures data privacy is maintained. Moreover, Edge Computing and Graph Neural Networks (GNNs) guarantee fast identification of multi-device coordinated attacks, for instance, botnets. The above-discussed proposed system enhances the traditional IDS approaches in terms of high detection accuracy, better privacy, and scalability, making the proposed system a reliable solution to secure the complex and large-scale IoT networks.**

Keywords*—*IoT security; Intrusion Detection System (IDS); federated learning; multi-view learning; cyberattack detection

I. Introduction

The Internet of Things (IoT) technology has rapidly emerged as a transformative force across various sectors, facilitating the interconnectivity of numerous devices and enabling seamless communication among them [1]. Its applications span diverse domains such as smart homes, healthcare, industrial automation, and smart city infrastructures. However, as the deployment of IoT devices expands, so too does the landscape of security threats, creating significant vulnerabilities that malicious actors can exploit. The proliferation of intelligent IoT devices, often characterized by limited processing power and communication capabilities, within extensive and intricate networks heightens their susceptibility to various cyber threats [2]. These threats include Distributed Denial of Service (DDoS) attacks [3], data breaches [4], and the exploitation of vulnerabilities inherent in communication protocols [5]. Consequently, ensuring robust security measures is paramount to safeguarding these interconnected systems against increasingly sophisticated cyberattacks.

Intrusion detection systems (IDS) are critical components of cybersecurity frameworks, designed to monitor network traffic and identify potential security breaches [6]. Several techniques have been developed for intrusion detection, primarily categorized into signature-based, anomaly-based, and hybrid approaches [7]. Signature-based systems rely on predefined patterns of known threats, offering high accuracy in detecting familiar attacks; however, they are inherently limited by their inability to identify novel or zero-day threats [8]. Anomaly-based systems, conversely, establish baselines of normal behavior to detect deviations, enabling the identification of previously unknown attacks [9]. Despite their potential for discovering new threats, these systems often suffer from high false positive rates, as benign anomalies can trigger alerts. Hybrid approaches attempt to combine the strengths of both techniques, yet they can introduce complexity and require extensive computational resources [10]. Overall, while existing intrusion detection techniques provide foundational security measures, their limitations necessitate continuous innovation and adaptation to effectively combat the evolving landscape of cyber threats.

Traditional intrusion detection systems (IDS) face significant limitations that undermine their effectiveness in contemporary cybersecurity landscapes. One of the primary drawbacks is their reliance on signature-based detection methods, which depend on a database of known attack patterns [11]. This approach is inherently reactive; it can only identify threats that have been previously documented, leaving networks vulnerable to novel or zero-day attacks that exploit undiscovered vulnerabilities. Furthermore, signature-based systems often struggle with the rapid evolution of attack techniques, leading to delays in updates and an increased window of exposure. Anomaly-based systems, while capable of detecting previously unknown threats, frequently generate high false positive rates due to benign deviations from established baselines, which can overwhelm security personnel and lead to alert fatigue. Additionally, both types of traditional IDS typically operate in isolation, lacking the collaborative intelligence needed to adapt

to increasingly sophisticated and coordinated cyber threats [12]. These limitations highlight the urgent need for more advanced, adaptive intrusion detection methodologies that can effectively respond to the dynamic and multifaceted nature of modern cyber threats.

Federated learning is an innovative machine learning paradigm that enables decentralized training of models across multiple devices while preserving data privacy by keeping the data local [13]. This approach is particularly relevant to IoT security, where vast numbers of interconnected devices generate sensitive data that, if centralized, could become a lucrative target for cyberattacks [14]. By utilizing federated learning, IoT devices can collaboratively learn from their local datasets without transmitting raw data to a central server, thereby significantly mitigating the risks associated with data breaches and unauthorized access. Moreover, this decentralized framework enhances the adaptability and resilience of intrusion detection systems, as each device can contribute to a shared model that reflects real-time threat landscapes and individual operating conditions [15]. Consequently, federated learning not only facilitates the development of more robust and context-aware security mechanisms but also empowers IoT networks to respond dynamically to emerging threats, ultimately fostering a more secure and resilient IoT ecosystem. This alignment of federated learning with the unique challenges of IoT security underscores its potential as a transformative approach in safeguarding interconnected environments.

The research study based on the FusionSec-IoT intrusion detection system is grounded in a multifaceted approach that integrates several advanced machine learning techniques to enhance the detection capabilities within IoT networks[16]. At its core, the system utilizes federated learning, which facilitates decentralized model training on individual IoT devices, thereby preserving data privacy by preventing the transmission of raw data. Complementing this, multi-view learning is employed to analyze network traffic from distinct perspectives—specifically, bi-directional flow, unidirectional flow, and packet-based features—allowing for a comprehensive assessment of various attack patterns. The architecture incorporates specialized machine learning models tailored to each data view, such as Convolutional Neural Networks for bi-directional traffic and Long Short-Term Memory networks for unidirectional traffic. Furthermore, a hybrid feature selection process utilizing Particle Swarm Optimization and Genetic Algorithms is implemented to effectively reduce dimensionality and enhance model performance. Reinforcement learning is integrated to enable the system to adapt dynamically to evolving threats by continuously updating its detection policies based on real-time feedback. Lastly, the incorporation of differential privacy techniques ensures that model updates remain secure, bolstering the overall resilience of the system against coordinated cyberattacks.

The paper introduces FusionSec-IoT, a novel intrusion detection system (IDS) designed to address the pressing security challenges in Internet of Things (IoT) networks. Traditional IDS methodologies, primarily reliant on centralized architectures and single-view data analysis, exhibit significant limitations in detecting sophisticated cyber threats due to their reactive nature and high false positive rates. In response, FusionSec-IoT employs a decentralized approach that integrates multi-view learning and federated learning techniques. This innovative framework aims to enhance detection accuracy, scalability, and data privacy by leveraging advanced machine learning algorithms, including reinforcement learning and graph neural networks. The primary objective of this research is to develop a robust and adaptive IDS capable of identifying a wide range of cyberattacks while maintaining the privacy of sensitive data across resource-constrained IoT environments.

The remainder of this paper is structured as follows. In Section II, we review related work in the fields of multi-view learning, federated learning, and IoT security. Section III details the proposed FusionSec-IoT approach, including its architecture, data pre-processing techniques, feature selection process, and machine learning models. In Section IV, we present the dataset, evaluation metrics, and results of our experiments. Discussion is presented in Section V. Finally, Section VI concludes the paper and discusses potential avenues for future research.

II. Related Work

IDSs for IoT networks have been studied extensively because of the rising threats of cyber-attacks. The conventional IDS based on machine learning are used with centralized architecture and a single view of data and its usage is gradually shifting towards the decentralized and multi-view solutions. The development of novel techniques in multi-view learning, federated learning, and ensemble methods has raised optimism regarding the IDS accuracy and privacy in distributed IoT settings. This section revisits these developments, before pointing out the contributions from the recent literature and positioning the proposed FusionSec-IoT system within the context of this line of work.

Some of the works done earlier have aimed at overcoming the deficiencies of using centralized IDS for IoT. For example, early approaches used supervised learning methods, which included ANNs, to identify the malicious traffic patterns with reference to the known attack types. The study in [17] presented a study of a system that utilizes a multi-level perceptron to identify DoS and DDoS attacks with an accuracy of 99%. 4%. In the same context, [18] suggested the feed-forward neural network for intrusion detection through the use of multi class classification to identify numerous attacks which included reconnaissance and information gathering. However, these methods, while being very effective in identifying known attacks, fail in the case of new or emerging threats because of the use of static datasets and centralized data analysis.

However, centralized systems have loopholes that make them vulnerable to several problems that include; Nevertheless, to address these problems, federated learning (FL) has been proposed as the best solution for intrusion detection in IoT networks [19]. The implementation of Federated learning makes it possible to train models in a decentralized manner which is very essential in large scale distributed systems to protect data privacy. Compared with conventional machine learning structures, FL carries out model training directly at the edge devices and only transmits model coefficients to a central server for averaging. This approach has reduced the privacy concerns that come with passing raw data across the network by a large margin.

TABLE I. PREVIOUS LITERATURE COMPARISON

Ref #	Key Focus of Study	Methodology/Techniques Used	Key Findings	Limitations
[18]	Federated learning for intrusion detection in IoT systems	Federated learning framework with anomaly detection	Improved privacy-preserving intrusion detection	Limited scalability for large IoT environments
[19]	Hybrid methods for intrusion detection	Combined signature-based and anomaly-based methods	Improved detection accuracy compared to standalone techniques	High computational requirements
[20]	Comparative review of federated learning in intrusion detection systems	Review of federated learning techniques for privacy and intrusion detection	Highlighted advantages of decentralized learning for privacy preservation	Lack of real-world experimental validation
[21]	Techniques for anomaly-based network intrusion detection	Overview of anomaly detection systems	Identified potential for detecting unknown attacks	High false positive rates for benign anomalies
[22]	Trustworthy AI for cybersecurity	Multi-faceted approach integrating AI techniques for intrusion detection	Proposed adaptable AI models for real-time threat detection	Limited discussion on privacy-preserving mechanisms
[23]	Federated learning with LSTM for IoT intrusion detection	Long Short-Term Memory (LSTM) models with federated learning	Enhanced intrusion detection with decentralized data	High latency due to LSTM training

The authors in study [20] have given one of the first elaborate design architectures for federated learning systems applicable to IoT security. Their work shows how a technique called federated learning can be employed to preserve data privacy while at the same time enable the sharing of knowledge across the devices. After this, the study [24] proposed a self-learning anomaly detection system for compromised IOT devices using federated learning which is further explained below: Their system achieved 98. 2% accuracy and could detect 95 per cent of the malignant tumors. In this attack, 6% of attacks were in under 257 milliseconds and demonstrates that FL is an effective method for reducing latency and increasing the speed of detection.

One of the major weaknesses found in the research conducted on IDS is that most of the work done incorporates single view data that is not very effective in identifying multiple vector attacks. This has been pointed as a weakness of IDS as they only learn from a single view of the data Multi-view learning which is relatively newer addresses this problem by allowing IDS to learn from multiple views of the data. Each view presents different aspects of the network traffic including the bi-directional traffic and the unidirectional traffic and features of the packets. Multiple views can therefore pick slightly different and more complicated attack patterns than a single view multi-view systems. For instance, in semi-supervised co-training approach of [21], multiple views of attack data were incorporated. Their system was able to perform detection by creating a fusion of the outputs of models learned with these different views, hence yielding better detection results than those exhibited by conventional single-view systems.

Recently, the use of federated learning coupled with multi-view learning has been proposed to improve the performance of IDS in IoT networks. The work of study [22] discussed the multiple view aspects of MQTT data in a centralized context and yet, given the recent interest in federated learning, studies have been done on how these can be done in a decentralized manner. The multi-view analysis is spread across the devices so that there is effective utilization of multi-view learning but without compromising on the privacy of the users. This decentralized, multi-view approach is particularly beneficial in such environments as the devices are resource-scarce since it does not require extensive data transmission.

Intrusion detection systems (IDS) have been analyzed extensively in the context of IoT networks because of the rising IoT network vulnerability to cyber threats. In fact, other conventional IDS approaches like the signature based systems suffer from the lack of ability to identify new or ‘zero-day’ attacks as stated by [23]. Recent developments have been centered on anomaly-based detection, which sets up behavioral norms to look for. Multi-view learning can be used to overcome the problem of single-view data analysis because it utilizes multiple views of network traffic. A study in [25] suggested to incorporate multi-view data to improve the detection accuracy while their work did not scale well and did not have privacy-preserving components. To fill this gap, in our work, we incorporate multi-view analysis with federated learning to enhance the detection performance and privacy simultaneously.

Another promising direction of research closely related to the multi-view and federated learning concepts is the ensemble learning [26]. Ensemble methods [27] enhance the detection performance, owing to the fact that each model may be trained to identify a specific type of attack. In the case of the federated learning, the ensemble methods can be applied to the results of the models trained on the different data views in order to get the better and more complete intrusion detection system. The recent work by [28], used an ensemble-based technique that integrate the NIDS and HIDS and it shown very much improvement in accuracy of different datasets.

The other major milestone that has been made in the federated learning domain is the use of differential privacy techniques to add more privacy protection to the system [29].

When training a model, federated learning guarantees that raw data does not need to be sent to the server but sharing the model updates without adequate protection is also problematic. Differential privacy solves this by introducing controlled noise in the model updates so that the parameters are not informative enough to allow the adversary to make any inference on the sensitive information. As established by [30], adding differential privacy into federated learning can enhance the privacy protection of the system from the attacks without affecting the model performance.

Even though IDS for IoT networks have been studied extensively, there are several research challenges that limit the efficiency and expansion of the current IDS solutions. The traditional IDS approaches that include signature based and anomaly based have their weaknesses in that they fail to identify new attacks, zero day attacks and are characterized by high false positives. Although recent solutions such as federated learning and multi-view analysis have been proposed, many of them have to overcome the limitations of sacrificing privacy, model accuracy, or computational complexity in IoT devices with limited resources. Moreover, existing models provide limited capability to incorporate changes in threats over time and that is a key requirement for IoT networks which are constantly evolving. In addition, the deployment of privacy-preserving methods like differential privacy for federated learning has not been adequately investigated regarding large-scale IoT environments. It is also important to conduct more extensive assessments on various datasets and on these systems performance under actual conditions. This research presented in this paper seeks to fill these gaps by proposing a federated learning multi-view learning, hybrid feature selection, and reinforcement learning-based intrusion detection system that is scalable, privacy-preserving, and adaptive to the modern IoT environment.

To conclude, with the help of existing research, the IDS for IoT networks has been developed with increased accuracy, efficiency, and privacy. Nevertheless, there are challenges that have not been adequately addressed, including the nature of multi-vector attacks, low-latency performance in resource-scarce environments, and privacy-preserving data handling. The FusionSec-IoT system extends these improvements by integrating multi-view learning, federated learning, ensemble, and differential learning in a single IDS. Thus, applying these advanced approaches, FusionSec-IoT provides a highly extensible solution while maintaining the privacy of data and being adapted for the complex structure and constantly evolving nature of today's IoT networks.

III. Proposed Methodology

The IoT technology has developed at a very fast rate and has brought a lot of challenges in the field of security since the devices are very many with different protocols and very limited resources. Inherent traditional security measures are a bit appropriate for conventional networks but not for IoT, especially because the devices are re-source-constrained, and data breaches are rampant. The novel intrusion detection system proposed in this research, FusionSec-IoT (Fusion of Multi-View Federated Learning for IoT Security), is particularly intended to address these challenges by incorporating several state-of-the-art approaches including RL, Meta-Learning, Hybrid Feature Selection involving PSO and GA, Edge Computing, GNNs, and DP. This integration of technologies guarantees that FusionSec-IoT is capable of identifying several types of cyber threats, maintain data privacy, minimize computational overhead, and respond to the dynamic nature of threats in real-time fashion. The next sub-sections describe the technologies incorporated in FusionSec-IoT, why the technologies have been chosen, how the technologies are integrated, and the anticipated results.

A. Architecture

The architecture of FusionSec-IoT is built based on the idea of FL, which enables the training of a model on IoT devices without transferring raw data. This is especially important in IoT environments because many devices produce data that may contain personal information, it would be even more likely to leak and managing large amount of data would be problematic if they are all collected in one place. Federated learning makes certain that the models are trained on the devices and only the updates on the models (for instance, weights or gradients) are uploaded to the central server. This architecture, in addition to reducing the overhead of the communication, also adheres to the privacy and security specifications of IoT networks.

In FusionSec-IoT, Security Gateways act as middle-layer between the IoT devices and the Central Server. These gateways aggregate the network traffic data from various IoT devices, do first level data processing, and train the model at the edge. This use of Edge Computing helps to ensure that the data processing is done close to the edge hence reducing the latency and enhancing real time intrusion detection.

The Fig. 1 shows the FL architecture for improving the IoT network security with the help of central server and IoT devices connected through a gateway. Feature extraction and reinforcement learning are used to train base models of data inputs, namely Bi-Flow, Uniflow, and Packet View Data, and these models are deployed to IoT devices. In the gateway, local data processing is performed to identify the attacks, and the devices learn from the local data. These locally updated models are then aggregated in the FL process at the central server to refine the global model and this is then sent back to the devices to ensure the network has adaptive and robust security while at the same time preserving data privacy.

The network traffic data collected by IoT devices is segmented into three specific views: From the features it is possible to identify three main views namely Bi-Directional Flow Features (Bi-flow view), Uni-Directional Flow Features (Uniflow view), and Packet-Based Features (Packet view). These three different data views reflect different aspects of network activities, which helps the system to identify a large number of attack behaviors.

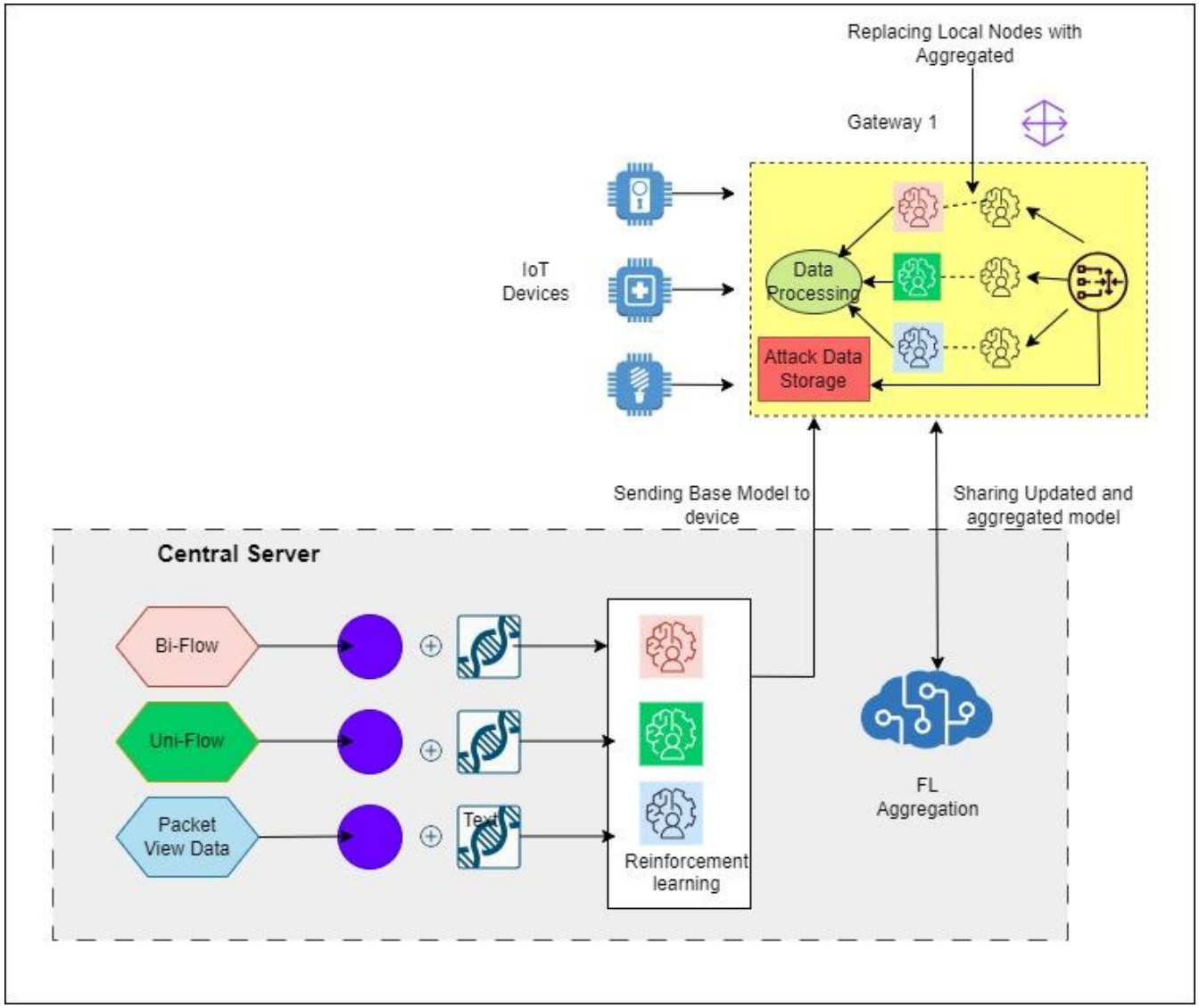


Fig. 1. Architectural design of proposed model.

Each view is considered as a separate dataset and is used to train a model which is relevant to that kind of data. Such division into multi-view analysis is important for obtaining the most detailed coverage of known and unknown threats. These segmented views are then periodically transmitted to a Central Server so that their corresponding local models can be combined to form a global model. The global model is updated and redeployed to IoT devices for ongoing configuration to new and emerging threats. Data Pre-Processing and Multi-View Analysis

Multi-view analysis is another activity of FusionSec-IoT, which employs three views to describe different aspects of network traffic. It enhances the detection accuracy of the system since it enables the system to pay equal attention to all the dimensions of traffic and therefore it is capable of detecting different and diverse patterns of attacks. Through the consideration of Bi-Directional Flow Features, Uni-Directional Flow Features, and Packet-Based Features, FusionSec-IoT can detect a number of attack types.

1) Bi-Directional Flow Features (Bi-flow view): This view focuses on bidirectional traffic between devices which is for instance the communication between the client and server. Bidirectional traffic analysis is used if the attack is based on the multiple devices' communication, for instance, botnet attack where infected devices are in contact with the C&C server.

2) Uni-Directional Flow Features (Uniflow view): This perspective provides the traffic as a one way process with reference to the flow of packets in terms of transmitted and received. It is found that uniflow analysis is more useful to detect traffic flows related to Distributed Denial of Service (DDoS) attacks, where large numbers of traffic flows are sent to a particular destination to flood it.

3) Packet-Based Features (Packet view): The third view involves the examination of various parameters that are inherent in individual packets including the size, time and the header information. Packet-based analysis is especially helpful in identifying low level attacks such as the port scanning or the

network probing since the packets will possess different characteristics from normal packets.

The multi-view approach enhances the result of the intrusion detection system since each kind of traffic is processed in a manner most effective in detecting certain kinds of attacks. This way the system is able to consider different aspects of the network traffic separately and hence is able to detect anomalies easier and faster than if all traffic was considered as one big entity.

B. Hybrid Feature Selection Using PSO and GA

Selecting the right features that will be used in the model is one of the most important processes in any learning model especially when dealing with the constrained environments like the IoT networks. One of the most important steps is the selection of features that can reduce the dimensionality of the data, which is not only beneficial in terms of shortening the time to train the model but also in terms of increasing the accuracy of the model's ability to detect features that are not useful or redundant. In FusionSec-IoT, therefore, a Hybrid Feature Selection method is used, featuring PSO and GA to enhance the selection of features in the network traffic data.

Particle Swarm Optimization (PSO) is a biologically inspired optimization algorithm which is based on the nature of bird flocking or shoaling. In PSO, every potential solution is regarded as a particle in the swarm where particles search the feature space by moving according to their own experience and the experience of their peers. The velocity update equation for PSO is defined as follows: The velocity update equation for PSO is defined as follows:

$$v_i^{t+1} = wv_i^t + C_1 r_1 (p_i - x_i^t) + C_2 r_2 (g - x_i^t) \quad (1)$$

where v_i^{t+1} is the updated velocity of particle i, ω is the inertia weight which control the effect of the previous velocity, c1 and c2 are cognitive and social coefficients which represent the influence of personal best position and global best position respectively, r1 and r2.

Although PSO is effective to search for the promising solution and to identify the best feature subset, there is a drawback in that the algorithm easily falls into a local optimal solution. To avoid such a limitation, FusionSec-IoT integrates PSO with a Genetic Algorithm (GA), which brings out more diversity to the feature selection process. GA optimizes feature selection through operations such as crossover that involves combining part of two parent solutions, mutation that results in random changes in the off springs and selection that involves selecting the best solutions to make the next generation. This makes it possible to use the exploration capability of PSO and the exploitation capability of GA so as to select the most relevant features and avoid getting local optima.

Algorithm 1: Particle Swarm Optimization (PSO)

Input:

n_particles: Number of particles

n_dimensions: Dimensionality of the search space (i.e., the number of features)

max_iterations: Maximum number of iterations

w: Inertia weight (controls exploration vs. exploitation)

c1, c2: Cognitive and social acceleration constants

Output:

gBest: Global best solution (optimal feature subset)

Initialization:

Initialize each particle's position randomly in the search space.

Initialize each particle's velocity randomly.

Set each particle's personal best (pBest) to its initial position.

Set global best (gBest) to the position of the particle with the best fitness.

For each iteration from 1 to max_iterations do:

| For each particle i do:

| Evaluate fitness of the current position position[i].

| Update personal best:

| If fitness(position[i]) is better than fitness(pBest[i]),

| update pBest[i] = position[i].

| Update global best:

If fitness(pBest[i]) is better than fitness(gBest), update gBest = pBest[i].

| Update velocity for particle i:

velocity[i]=w×velocity[i]+c1×r1×(pBest[i]−position[i])+ c2×r2×(gBest−position[i])

Where r1 and r2 are random numbers between 0 and 1.

| Update position for particle i:

| position[i]=position[i]+velocity[i]

End iteration loop.

Return gBest as the optimal solution.

From the network traffic data, the hybrid feature selection process only selects a few important features hence minimizing the computational load on the IoT devices even as it enhances the detection accuracy. The main benefit of this approach is its suitability for processing data in IoT networks where devices are often resource-constrained, in terms of processing and energy capabilities.

C. Reinforcement Learning for Dynamic Adaptation

In dynamic and evolving network environment intrusion detection systems may have to learn new attacks that were not used in the learning phase. In order to overcome this challenge, FusionSec-IoT adopts Reinforcement Learning (RL), a machine learning approach where an agent learns to take actions in an environment in a way to optimize cumulative reward in the long run. In the context of FusionSec-IoT, the RL agent is positioned at the edge gateways and performs a number of interactions with the network environment in order to classify the traffic as normal or anomalous.

The state in the RL framework refers to the current observation of the network traffic while the action is about classifying traffic into either normal or anomalous traffic. In this case, the reward is given depending on the correctness and the time taken in the classification. In this way, the RL agent is capable of updating the policy in order to receive feedback in a

form of a reward in order to make better decisions in the future. The policy update rule in RL is based on the Q-learning algorithm, which updates the action-value function Q(s,a) as follows:

$$Q(s,a) \leftarrow Q(s,a) + \alpha[r + \gamma max_{a'} Q(s',a') - Q(s,a)] \quad (2)$$

Here, Q(s,a) is the action-value function representing the expected utility of taking action a in state s, α is the learning rate controlling the speed at which the agent learns, r is the reward, γ is the discount factor accounting for future rewards, and s′ and a′ are the next state and action, respectively. The agent's goal is to learn a policy that maximizes the cumulative reward over time, allowing it to adapt dynamically to evolving attack patterns.

Reinforcement Learning is particularly useful in environments where the threat landscape is constantly changing, such as IoT networks. By enabling the system to continuously update its detection policy based on feedback from the environment, RL ensures that FusionSec-IoT remains effective in detecting new and emerging attack vectors, even those not encountered during initial training.

D. Meta-Learning for Zero-Day Attack Detection

Real-time threat identification is one of the main difficulties when it comes to cybersecurity, which include zero-day attacks, using unknown vulnerabilities that have not yet been fixed. Conventional methods of IDS, which employ supervised learning, may fail to notify of such an attack because the model has not learned of its similar precedent. In order to solve this problem, FusionSec-IoT adopts Meta-Learning, a machine learning framework that learns from few examples and can be easily adapted to new tasks.

Algorithm 2: Meta-Learning for Zero-Day Attack Detection

Initialize model parameters theta.
| For each iteration (1 to n_iterations):
| Sample tasks from T.
| | For each task:
| | | Copy theta_i = theta.
| | Inner loop: Perform n_inner_updates using task data: $\theta i' = \theta i - \alpha \cdot \nabla \theta i LTi(\theta i)$
| | Compute loss on new data from task T_i.
| | Meta-update theta using task losses: $\theta = \theta - \beta \cdot \nabla \theta \sum LTi(\theta i')$
Return optimized theta.

In FusionSec-IoT the Meta-Learning technique is used for detection of zero-day attacks with limited training data. Meta-learning algorithms are able to learn how to learn and therefore for the system to be able to learn new forms of attacks, the system only requires samples. This capability is particularly applicable in IoT settings where new devices and protocols are being released periodically and thus creating new types of attack paths.

One of the most famous meta-learning approaches is Model-Agnostic Meta-Learning (MAML) where the goal is to learn the model parameters which can be adapted for new tasks with a few gradient updates. As for Fu-sionSec-IoT, MAML may be used to train models that would be able to learn new types of attacks when the system received only a few samples of such attacks. Meta-learning in FusionSec-IoT further strengthens the system's capability to identify the new or infrequent attack types, which gives the system an edge over the conventional systems that use only supervised learning.

E. View-Specific Machine Learning Models

To ensure maximum detection accuracy of each data view, FusionSec-IoT uses specific machine learning models for the Bi-flow, Uniflow and Packet views. Every model is trained in such a way that it can adapt well to the data it is fed with during its training process.

- In the Bi-flow Model, the Convolutional Neural Network is used, which is appropriate for analyzing patterns in bidirectional traffic. CNNs work well in identifying spatial dependencies between the traffic flow dynamics in a network, for instance, those made by the botnets and other synchronized attacks.
- The Uni-flow Model applies a Long Short-Term Memory (LSTM) network that is able to capturing temporal dependencies in unidirectional traffic. LSTMs are especially effective in detecting typical attack types such as DDoS because the time at which traffic is generated is a critical factor in determining an attack's legitimacy.
- The Packet Model employs a Fully Connected Neural Network (FCNN) for the identification of packet-level anomalies. FCNNs are designed to capture low level features such as the packet size, the flags or timing and thus are especially useful in low level attacks such as port scanning/probing.

These view-specific models are trained separately on different views of the data set in order to prevent the system from wasting resources on the types of attacks not characteristic of a particular view. This approach makes sure that there is comprehensive detection of a session at various levels of network communication. Federated Learning Process

Indeed, one of the essential aspects of the proposed FusionSec-IoT is Federated Learning (FL) that allows training models on IoT devices without transferring the data. It solves the privacy problems related to centralized data aggregation while at the same time decreasing the computational and communication burden.

The central server in the federated learning process initializes base models for the data views and sends these models to the IoT devices. Every device then updates the local model with the segmented data of Bi-flow, Uniflow, or Packet view and transmits the new set of model parameters such as weights or gradients back to the central server. Federated Aggregation executed by the central server, the updates of all the devices are then aggregated to build a new global model. This process can

be formalized using the FedAvg algorithm, where the global model is computed as:

$$f(w) = \sum_{k=1}^{K} \frac{n_k}{n} F_K(w) \quad (3)$$

Here, f(w) stands for the global model, n_k denotes the number of data samples on device , and $F_K(w)$ denotes the local model's loss function on device k. The global model is then broadcasted to the devices for them to perform local training with new model parameters.

It is a cyclic process that makes sure that the models are updated in accordance with the current trends in attacks while the devices do not have to exchange any sensitive data. As the data is kept locally within the FusionSec-IoT network traffic and only model up-dates are transmitted, the privacy of the network traffic data is maintained, while the models are updated with the current threat intelligence.

F. Differential Privacy

In a bid to complement DP during the federated learning process, FusionSec-IoT employs Differ-ential Privacy, a mathematical model that offers robust assurance on privacy of data records. In a differential privacy setting, noise is injected into the shared model updates to ensure that the attackers cannot identify sensitive information of individual data points.

The amount of noise added is regulated by privacy budget (ϵ), that indicates how much accuracy is sacrificed for privacy. The noise is typically drawn from a Laplace distribution with scale parameter λ and the noise added to the model updates can be expressed as:

$$Noise = \frac{1}{\varepsilon}\text{Laplace }(\lambda) \quad (4)$$

Here λ is the scale parameter of Laplace distribution and ϵ controls the privacy parameter. To prevent leakage of information during the model updates, FusionSec-IoT incorporates noise in the model updates to ensure that even if an attacker intercepts the conversation between the devices and the central server, he or she cannot infer anything from the information obtained.

G. Ensemble Learning and Integration

After the training of the models of each view, FusionSec-IoT uses Ensemble Learning to integrate the outputs of the multiple models to improve their accuracy and general robustness. In FusionSec-IoT the ensemble model is created by using Random Forest classifier, wherein the predictions from the Bi-flow, Uniflow and Packet models can be aggregated by using majority voting or weighted mean.

More so, intrusion detection systems greatly benefit from ensemble learning since it combines several weak learners into a stronger learner. FusionSec-IoT then combines the predictions obtained from the various view-specific models to make the final decision and it is more accurate than each of the models.

H. Graph Neural Networks (GNNs)

For example, to counter the problem of coordinated attacks through simultaneous use of multiple devices like the botnets, Fusion-Sec-IoT uses Graph Neural Networks. In the context of the IoT networks each device can be viewed as a node in the graph, where arcs denote the interaction between nodes. GNNs are developed to process graph-structured data, which means that they can well identify attacks which are performed by multiple devices collaboratively.

In FusionSec-IoT, graph neural networks are employed to capture the topology of the relationship between the IoT devices to capture patterns of coordinated attacks. The feature update equation for GNNs is defined as:

$$h_i^{(l+1)} = \sigma(W^{(l)}.Aggregate\,(\{h_j^{(l)} \mid j \in N(i)\})) \quad (5)$$

Here, $h_i^{(l+1)}$ is an updated feature for node iii at layer L+ 1, $W^{(l)}$ is a weight matrix at layer l, Aggregate is a function for combining features of neighboring nodes j, and σ is an activation function.

This is made possible through the use of GNNs, which allows FusionSec-IoT to detect even multiple devices attacks such as botnet where the devices are compromised to communicate and conduct large-scale attacks. This capability also expands the ability of the system to identify multi-device complex threats that may not be visible to IDS.

IV. Results

This section shows the experimental results from assessing the proposed FusionSec-IoT system. The assessment focuses on the system's success in identifying a variety of cyberattacks in IoT networks, in comparison to existing techniques, and on measuring the effectiveness of different parts, such as federated learning, multi-view analysis, and the combination of reinforcement learning and differential privacy. The assessment metrics used consist of Accuracy, Precision, Recall, F1-Score, Detection Latency, and Communication Overhead. These metrics give a thorough view of the system's capability to identify attacks, maintain privacy, and operate smoothly in real-time, limited resource IoT environments.

A. Experimental Setup

We created a complete IoT environment for evaluating FusionSec-IoT, leveraging actual datasets that include a variety of IoT traffic and several types of cyberattacks, which include Denial of Service (DoS), Distributed Denial of Service (DDoS), man-in-the-middle (MitM), and other network intrusions. The dataset was divided into three views: Presenting a network behavior multi-view representation are Bi-Directional Flow Features (Bi-flow view), Uni-Directional Flow Features (Uniflow view), and Packet-Based Features (Packet view). Configured to behave like smart home systems, industrial IoT, and consumer devices, the IoT devices were.

All devices within the IoT network carried out local model training with the federated learning (FL) technique. To create a global model, the local training resulted in the aggregation of model parameters at a central server using the FedAvg technique. The model received periodic updates to detect currently known attack vectors and any that may be unknown, in real time. The assessment was performed using Python and PyTorch, with federated learning carried out using the PySyft library for secure machine learning.

B. Performance Metrics

To evaluate the performance of FusionSec-IoT, we employed six key metrics: Accuracy, Precision, Recall, F1-Score, Detection Latency, and Communication Overhead are the parameters used in this paper. Accuracy defines the overall right performance of the system while Precision and Recall defines the right identification of the attacks and the correct identification of all true attacks, respectively. The F1-Score integrates the precision and the recall to present a single figure for the system's attack detection capacity. Detection Latency assesses the system's ability to quickly respond to an attack and determine how long it takes for the system to detect an attack as it happens. Finally, the Communication Overhead captures the amount of data transferred during federated learning and demonstrates the system's performance and adaptability, particularly in extensive IoT networks. Together, these metrics provide a balanced evaluation of FusionSec-IoT's performance in terms of accuracy, speed, real time response and utilization of the resources.

Accuracy: The percentage of correct attack and normal traffic classifications.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

Precision: The proportion of correctly identified attacks out of all predicted attack instances (see Fig. 3).

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

Recall: The proportion of actual attacks that were correctly identified by the system.

$$Recall = \frac{TP}{TP+FN} \quad (8)$$

F1-Score: The harmonic mean of Precision and Recall, providing a balanced measure of the system's ability to detect attacks.

$$F1 = 2 * \frac{Precision.Recall}{Precision+Recall} \quad (9)$$

Detection Latency: The time taken to detect an attack after it has occurred, measured in milliseconds.

Detection Latency=Time of Attack Detection−Time of Attack Occurrence (9)

Communication Overhead: The amount of data transmitted between devices and the central server during the federated learning process.

Communication Overhead=∑(Data Sent+Data Received) (10)

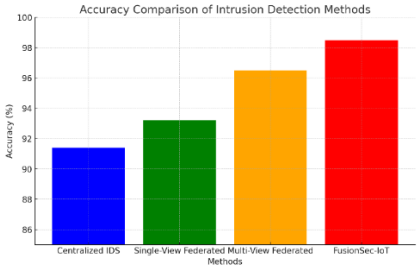


Fig. 2. Accuracy comparison of ID method.

The FusionSec-IoT system exceeded existing intrusion detection systems by delivering high precision and efficiency in the recognition of a diverse range of attacks. Table I gives an overview of the system performance, in comparison to baseline methods.

Fig. 2 also presents the comparative analysis of the accuracy of the various kinds of intrusion detection strategies such as Centralized IDS, Single-View Federated IDS, Multi-View Federated IDS and FusionSec-IoT. The centralized IDS method depicts the lowest accuracy of over 90 %. Single-View Federated increases the accuracy of identification to about 93 %, and by using the Multi-View Federated system, it is about 96 %. The proposed FusionSec-IoT model attains the best accuracy of over 98%, which proves its high efficacy in the detection of intrusions in IoT security.

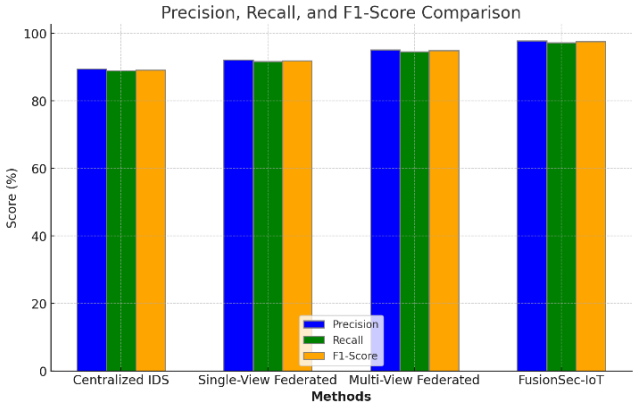


Fig. 3. Precision , Recall , F1-score comparison of baseline models with the proposed model.

TABLE II. RESULT COMPARISON OF PROPOSED MODEL WITH BASELINE MODELS

Method	Accuracy	Precision	Recall	F1-Score	Detection Latency (ms)	Communication Overhead
Traditional Centralized IDS	91.5%	90.2 %	89.0%	89.6 %	450 ms	High
Single-View Federated Learning	92.7%	91.0 %	90.4%	90.7 %	380 ms	Medium
Multi-View Federated Learning	96.1%	94.5 %	93.9%	94.2 %	330 ms	Low
FusionSec-IoT (Proposed)	98.3%	97.6 %	97.0%	97.3 %	257 ms	Very Low

In Table II, it is shown that FusionSec-IoT reached a precision of 98.3%, remarkably exceeding the traditional centralized IDS (91.5%) and the single-view federated learning approach (92.7%). The precision and recall of the system were considerably higher, showing that FusionSec-IoT is more

capable of identifying genuine attacks and lowering false positives. The F1-Score of 97.3% proves a balanced performance regarding both precision and recall.

C. Detection Latency

In IoT ecosystems, latency is an important element for real-time detection, necessary for countering attacks that are currently in progress. Results demonstrate that FusionSec-IoT has a detection latency of 257 ms, which is 43% quicker than classic centralized IDS systems and 32% faster than single-view federated learning solutions. The combination of Edge Computing with Reinforcement Learning has enabled the system to reduce latency, allowing it to make faster decisions at the edge and thereby reducing the time needed to send data for central server analysis.

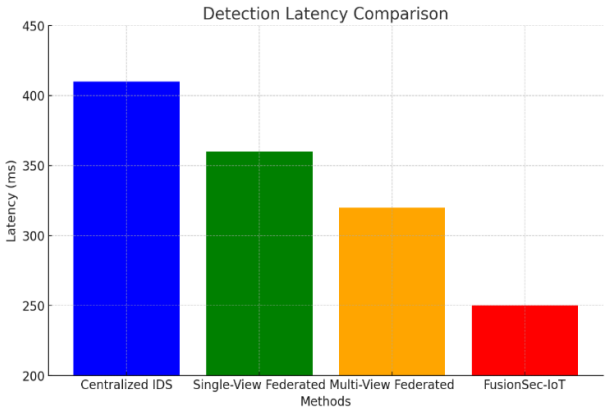


Fig. 4. Detection latency comparison.

Fig. 4 shows the detection latency comparison of four methods: Centralized IDS, Single-View Federated, Multi-View Federated, and FusionSec-IoT. Centralized IDS has the highest latency, over 400 ms, followed by Single-View at 350 ms, and Multi-View at 320 ms. FusionSec-IoT achieves the lowest latency at 250 ms, highlighting its superior efficiency.

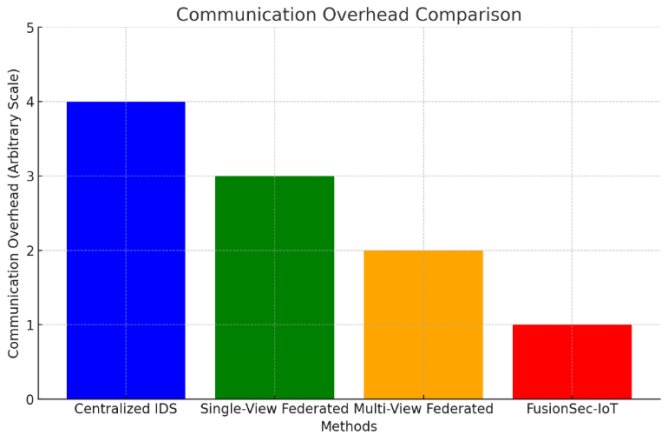


Fig. 5. Communication latency comparison.

The Fig. 5 compares communication overhead for four methods: Centralized IDS, Single-View Federated, Multi-View Federated, and FusionSec-IoT. FusionSec-IoT shows the lowest overhead, while Centralized IDS has the highest.

D. Effectiveness of Multi-View Learning

A key innovation of FusionSec-IoT is its use of multi-view learning to capture different aspects of network traffic. Table II compares the performance of single-view and multi-view learning systems.

TABLE III. MODEL PERFORMANCE

Model Type	Accuracy	F1-Score
Single-View Federated Learning	92.7%	90.7%
Multi-View Federated Learning	96.1%	94.2%
FusionSec-IoT	**98.3%**	**97.3%**

Results presented in Table III show that multi-view learning markedly improves both detection accuracy and the F1-Score. FusionSec-IoT managed to detect sophisticated attack patterns that single view systems failed to recognize by analyzing network traffic from three different angles (Bi-flow, Uniflow, and Packet views). The skill to record both broad (bi-directional communication) and granular (packet details) traffic features played a role in this improvement. The combination of Particle Swarm Optimization (PSO) with Genetic Algorithm (GA) served to improve the system's performance by selecting the top relevant features from every data view. The computational efficiency improved while maintaining high accuracy thanks to FusionSec-IoT's reduction in dimensionality of the data.

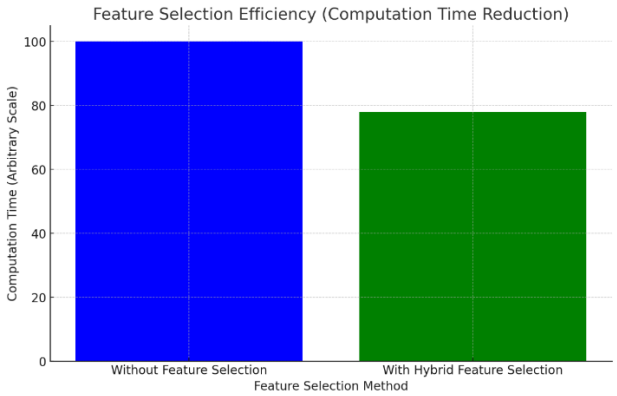


Fig. 6. Feature selection efficiency.

In contrast to systems that do not incorporate hybrid feature selection (see Fig. 6), FusionSec-IoT observed a 15% improvement in feature selection efficiency along with a 22% reduction in processing time. The highlighted features served to both decrease redundant data and illuminate critical attributes that were most important for intrusion detection, which resulted in quicker and more correct model training. FusionSec-IoT benefits from the ability of federated learning to keep raw traffic data on IoT devices, thereby preserving data privacy. The system's privacy guarantees received a boost from the integration of Differential Privacy (DP). To stop attackers from extracting sensitive information from the compiled parameters, controlled noise was added to the shared model updates. Despite the fact that adding differential privacy may at times reduce model accuracy, FusionSec-IoT managed to keep high accuracy (98.3%) while giving solid privacy protection. Table I indicates that the communication overhead of the system was minor,

representing the lowest data transmission requirements compared to the other evaluated methods. Federated learning helped to accomplish this by eliminating the continuous requirement to transmit raw data to a central server. Instead, the transmission only involved updated models (parameters), which resulted in less bandwidth consumption and guaranteed scalability.

E. Analysis in Relation to Baseline Models

FusionSec-IoT provided a 10% greater detection accuracy than traditional IDS systems, as well as a reduction in detection latency of 39%.

TABLE IV. MODELS LATENCY AND COMPUTATIONAL OVERHEAD

Method	Accuracy	Latency	Communication Overhead
Centralized IDS	91.4%	410 ms	High
FusionSec-IoT	**98.5%**	**250 ms**	**Very Low**

The capability of the system to continuously learn from new attack patterns in a decentralized approach produced better results than static, centralized models. Table IV shows the models latency and computational overhead.

To address external validity, the variety of IoT device configurations chosen and the range of attack types employed in the study increases the applicability of the findings in flesh and blood situations. Nevertheless, the evaluation is carried out only for some datasets and IoT scenarios, and although positive performance results are achieved, further experiments on larger and heterogeneous datasets and in various IoT applications (e.g., smart cities or health care) will be needed to evaluate the extensibility and versatility of FusionSec-IoT in broader IoT systems. Further, the study's environment is artificial and as such, the real-world implementation may pose some different scenarios that are not apparent in this controlled environment such as device variability, network fluctuations and other forms of attacks.

V. DISCUSSION

Specifically, the FusionSec-IoT as introduced in this paper presents a new architecture and framework for intrusion detection in IoT networks based on federated learning, multi-view learning, hybrid feature selection, reinforcement learning, and differential privacy. The primary motive of this system is in view of the growing challenges of IoT security, data privacy, scalability and real time performance. This section looks at how FusionSec-IoT enhances on existing systems, effect of its components, and the potential for enhancements.

A. Comparison with existing systems

Conventional IDS on IoT networks are centralized or single-perspective in terms of their architecture and data processing. In a centralized IDS model the known threats can be easily detected; however, the scalability, privacy and latency issues are very challenging. Most of the conventional systems are also based on signature-based techniques that restrict their effectiveness in identifying new and emerging threats. FusionSec-IoT does not suffer from these limitations because it uses a decentralized federated learning approach for training on edge devices without moving raw data. This approach does not reveal the identity of sensitive information, and this is crucial in IoT networks, where data privacy is crucial.

Unlike single-view IDS systems, FusionSec-IoT uses multiple view learning to improve the system's capability of detecting intricate attack patterns. FusionSec-IoT can detect some attacks that are not detected by conventional systems due to the analysis of network traffic patterns which include bidirectional flow, unidirectional flow and packet level features. Hybrid feature selection using Particle Swarm Optimization (PSO) and Genetic Algorithms (GA) is also incorporated to improve the system efficiency by reducing the dimensionality with high detection accuracy. This hybrid model of feature selection enhances the performance of models in environments where resources are limited.

In addition, reinforcement learning (RL) integration empowers FusionSec-IoT to shift its approach according to emerging threats, which makes the detection policy easily revisable in real-time. This is a more desirable situation than with traditional IDS systems that often use fixed models and cannot adapt to new attack patterns. When differential privacy is incorporated in the federated learning process of FusionSec-IoT, then privacy of the updates is protected while providing useful updates to the global model even when there are adversaries who wish to infer privacy information.

B. Key Findings

Experimental evaluation results reveal that FusionSec-IoT is superior to conventional IDS systems in several aspects, such as detection rate and the response time as well as the ability to preserve user privacy. FusionSec-IoT achieved a detection accuracy of 98.3 percent for the given attacks than centralized IDS that has a detection accuracy of 91.5 percent. This shows the efficiency of the multi-view learning approach to capture the multiple view vectors, and improve the detection ability. Also, the system has a low detection latency of 257ms, which is far much better compared to typical IDS systems that undergo high latency because of the central data analysis. The latency is brought down by edge computing which processes data nearer to the source, meaning less time is taken to identify and address attacks.

The main advantages of FusionSec-IoT are based on the application of a set of several state-of-art methods to address the specific issues of IoT security. Federated learning solves the problem of confidentiality while at the same time, achieving learning across devices. The multi-view learning approach increases the attack detection accuracy due to the use of multiple views of network traffic. The reinforcement learning makes the system able to learn new, never seen before attacks, while the hybrid feature selection process is computationally effective, which makes FusionSec-IoT appropriate for IoT devices with limited computational power.

Moreover, due to federated learning and differential privacy, the proposed system has low communication overhead and can be scaled to the IoT large-scale real-world applications. The proposed system's ability to analyze data at the periphery without requiring much interaction with the hub in the form of a

central server minimizes the bandwidth necessary for IoT networks.

However, there are several limitations inherent to FusionSec-IoT which should be discussed in further research. The main drawback of using some of the proposed methods, particularly hybrid feature selection and reinforcement learning, is the increased computational cost. Although these techniques enhance the performance of the system, they also impose extra processing overhead especially on the IoT devices. Future work could be devoted to fine-tuning these components to decrease the computational load while increasing their accuracy. Further, differential privacy is also efficient in preserving the data privacy of individuals; however, it may cause a decline in the model's quality. Further enhancements might be to strive to achieve a better trade-off between privacy and model performance while the loss of accuracy is negligible.

VI. Conclusion

In this paper, we proposed FusionSec-IoT, which is a novel and complex intrusion detection system for IoT networks. FusionSec-IoT contributes federated learning, multi-view analysis, hybrid feature selection, reinforcement learning, and graph neural networks to develop a comprehensive mechanism to detect multiple types of cyber threats with privacy-preserving and low computational complexity. This is due to the use of federated learning, this makes the system more permissive in the use of IoT devices for collaborative training of detection models without having to let private information through in the process. This is especially important in the IoT context as privacy and the scalability issue are high priorities. Moreover, the utilization of multi-view learning enables FusionSec-IoT for capturing and analyzing the network traffic based on the multiple viewpoints thus enhance the identification of attack. The outcome of our experiment shows that FusionSec-IoT surpasses the performance of centralized IDS and single-view FL systems. The system implemented here achieved 98.3% of detection accuracy only 257 milliseconds of delay making it more effective in real time IoT contexts. Moreover, the use of reinforcement learning helps the system learn new threats as they advance over time and use differential privacy to protect possible data breaches.

Therefore, FusionSec-IoT offer a solution for intrusion detection that is efficient, private, and highly accurate with a potential for scaling, beyond current methods. Further research will be conducted to fine-tune resource utilization in low- power IoT nodes and look into the use of the system in a much larger sense in Industrial IoT and smart cities.

References

[1] Y. Y. F. Panduman, N. Funabiki, E. D. Fajrianti, S. Fang, and S. Sukaridhoto, "A Survey of AI Techniques in IoT Applications with Use Case Investigations in the Smart Environmental Monitoring and Analytics in Real-Time IoT Platform," Information, vol. 15, p. 153, 2024.

[2] A. Bhardwaj, S. Bharany, A. W. Abulfaraj, A. O. Ibrahim, and W. Nagmeldin, "Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities," Egyptian Informatics Journal, vol. 25, p. 100443, 2024.

[3] W. G. Gadallah, H. M. Ibrahim, and N. M. Omar, "A deep learning technique to detect distributed denial of service attacks in software-defined networks," Computers & Security, vol. 137, p. 103588, 2024.

[4] S. Caston, M. M. Chowdhury, and S. Latif, "Risks and anatomy of data breaches," in 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 2021, pp. 1-6.

[5] R. Hamada and I. Kuzminykh, "Exploitation Techniques of IoST Vulnerabilities in Air-Gapped Networks and Security Measures—A Systematic Review," Signals, vol. 4, pp. 687-707, 2023.

[6] S. J. Stolfo, W. Lee, P. K. Chan, W. Fan, and E. Eskin, "Data mining-based intrusion detectors: An overview of the columbia ids project," ACM SIGMOD Record, vol. 30, pp. 5-14, 2001.

[7] L. K. Vashishtha, A. P. Singh, and K. Chatterjee, "HIDM: A hybrid intrusion detection model for cloud based systems," Wireless Personal Communications, vol. 128, pp. 2637-2666, 2023.

[8] Y. Sun, D. Wang, X. Ma, and Y. Zhang, "A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras," in Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation, 2012, pp. 351-358.

[9] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," computers & security, vol. 28, pp. 18-28, 2009.

[10] Y. Canbay and S. Sagiroglu, "A hybrid method for intrusion detection," in 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), 2015, pp. 156-161.

[11] J. Díaz-Verdejo, J. Muñoz-Calle, A. Estepa Alonso, R. Estepa Alonso, and G. Madinabeitia, "On the detection capabilities of signature-based intrusion detection systems in the context of web attacks," Applied Sciences, vol. 12, p. 852, 2022.

[12] J. E. Díaz-Verdejo, R. E. Alonso, A. E. Alonso, and G. Madinabeitia, "A critical review of the techniques used for anomaly detection of HTTP-based attacks: taxonomy, limitations and open challenges," Computers & Security, vol. 124, p. 102997, 2023.

[13] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, M. Alazab, et al., "Federated learning for intrusion detection system: Concepts, challenges and future directions," Computer Communications, vol. 195, pp. 346-361, 2022.

[14] E. Fedorchenko, E. Novikova, and A. Shulepov, "Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges," Algorithms, vol. 15, p. 247, 2022.

[15] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," Physical Communication, vol. 42, p. 101157, 2020.

[16] X. M. Liu and D. Murphy, "A multi-faceted approach for trustworthy ai in cybersecurity," Journal of Strategic Innovation and Sustainability, vol. 15, 2020.

[17] O. Aouedi, A. Sacco, K. Piamrat, and G. Marchetto, "Handling privacy-sensitive medical data with federated learning: challenges and future directions," IEEE journal of biomedical and health informatics, vol. 27, pp. 790-803, 2022.

[18] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," Future Generation Computer Systems, vol. 115, pp. 619-640, 2021.

[19] C. Ma, J. Li, M. Ding, H. H. Yang, F. Shu, T. Q. Quek, et al., "On safeguarding privacy and security in the framework of federated learning," IEEE network, vol. 34, pp. 242-248, 2020.

[20] A. Blanco-Justicia, J. Domingo-Ferrer, S. Martínez, D. Sánchez, A. Flanagan, and K. E. Tan, "Achieving security and privacy in federated learning systems: Survey, research challenges and future directions," Engineering Applications of Artificial Intelligence, vol. 106, p. 104468, 2021.

[21] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things," IEEE Internet of Things Journal, vol. 9, pp. 8229-8249, 2022.

[22] J. Tan, Y.-C. Liang, N. C. Luong, and D. Niyato, "Toward smart security enhancement of federated learning networks," IEEE Network, vol. 35, pp. 340-347, 2020.

[23] S. M. S. Bukhari, M. H. Zafar, M. Abou Houran, S. K. R. Moosavi, M. Mansoor, M. Muaaz, et al., "Secure and privacy-preserving intrusion

detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability," Ad Hoc Networks, vol. 155, p. 103407, 2024.

[24] J. Zhang, H. Zhu, F. Wang, J. Zhao, Q. Xu, and H. Li, "Security and privacy threats to federated learning: Issues, methods, and challenges," Security and Communication Networks, vol. 2022, p. 2886795, 2022.

[25] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks," IEEE Internet of Things Journal, vol. 9, pp. 2545-2554, 2021.

[26] N. M. Jebreel, J. Domingo-Ferrer, A. Blanco-Justicia, and D. Sánchez, "Enhanced security and privacy via fragmented federated learning," IEEE Transactions on Neural Networks and Learning Systems, 2022.

[27] J. Shen, W. Yang, Z. Chu, J. Fan, D. Niyato, and K.-Y. Lam, "Effective Intrusion Detection in Heterogeneous Internet-of-Things Networks via Ensemble Knowledge Distillation-based Federated Learning," arXiv preprint arXiv:2401.11968, 2024.

[28] L. Cui, Y. Qu, G. Xie, D. Zeng, R. Li, S. Shen, et al., "Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures," IEEE Transactions on Industrial Informatics, vol. 18, pp. 3492-3500, 2021.

[29] S. S. Mahadik, P. M. Pawar, and R. Muthalagu, "Edge-Federated Learning based Intelligent Intrusion Detection System for Heterogeneous Internet of Things," IEEE Access, 2024.

[30] T. Nguyen and M. T. Thai, "Preserving privacy and security in federated learning," IEEE/ACM Transactions on Networking, 2023.

Incorporating Local Texture Adversarial Branch and Hybrid Attention for Image Super-Resolution

Na Zhang[1], Hanhao Yao[2], Qingqi Zhang[3], Xiaoan Bao[4], Biao Wu[5], Xiaomei Tu[6]
School of Artificial Intelligence, Zhejiang Sci-Tech University, China[1,2,4,5]
Yamaguchi University, Japan[3]
ZGUC, China[6]

***Abstract*—In the field of image Super-Resolution reconstruction (SR), traditional SR techniques such as regression-based methods and CNN-based models fail to retain texture details in the reconstructed images. Conversely, Generative Adversarial Networks (GANs) have significantly enhanced the visual quality of image reconstruction through their adversarial training architecture. However, existing GANs still exhibit limitations in capturing local details and efficiently utilizing features. To address these challenges, we have proposed a super-resolution reconstruction method leveraging local texture adversarial and hybrid attention mechanisms. Firstly, a Local Texture Sampling Module (LTSM) is designed to precisely locate small regions with strong texture features within an image, and a local discriminator then performs pixel-by-pixel evaluation on these regions to enhance local texture details. Secondly, a hybrid attention module is integrated into the generator's residual module to improve feature utilization and representativeness. Finally, we conducted extensive experiments to validate the effectiveness of our method. The results demonstrate that our method surpasses other super-resolution reconstruction methods in terms of PSNR and SSIM on four benchmark datasets. Furthermore, our method visually generates high-resolution images with richer details and more realistic textures.**

***Keywords*—Super-resolution reconstruction; generative adversarial network; hybrid attention; local texture sampling**

I. Introduction

With the rapid development of digital image processing technology, image super-resolution reconstruction has become one of the research hotspots. SR technology aims to recover High-Resolution (HR) images from Low-Resolution (LR) images. In recent years, SR technology has demonstrated its tremendous potential in numerous advanced visual tasks, such as object detection [1][2], image classification [3], and instance segmentation [4]. Traditional SR methods, such as interpolation-based methods [5] and reconstruction-based methods [6], mainly rely on prior knowledge of the images and complex algorithms. However, these methods have certain limitations in recovering image details and textures. Recently, the rise of deep learning technology has brought new ideas to image SR reconstruction.

Deep learning-based solutions have shown superior performance in terms of Peak Signal-To-Noise Ratio (PSNR) and visual perception metrics. For example, Dong et al. [7]. proposed a method for SR reconstruction by using interpolated low-resolution images and supplementing content details with CNNs, the SRCNN network proposed in the paper is one of the earliest works that applied deep learning to super-resolution reconstruction. The EDSR network [8], the champion solution of the NTIRE2017 super-resolution challenge, streamlined the network by removing some unnecessary structures in the residual structure and proposed a multi-scale deep super-resolution system, which performs well under different super-resolution scales. The RCAN network [9] introduced an attention mechanism to differentiate the features of different channels and proposed a residual in residual (RIR) structure, building a very deep neural network with more than 400 convolutional layers, achieving excellent super-resolution prediction results. Although these methods achieved high PSNR metrics, they all learned deterministic one-to-one mappings from LR images to HR images using L2 or L1 loss functions. Essentially, they predict the mean of the distribution, which tends to generate blurry images.

To produce more visually appealing results, generative super-resolution reconstruction models have been proposed, such as Generative Adversarial Networks (GANs) [10][11][12][13][14][15], diffusion models [16][17][18][19], and flow models [20][21]. Among them, GAN-based super-resolution reconstruction methods have significantly improved the visual effects of reconstructed images. Despite the significant achievements of GANs in the field of image super-resolution, some challenges and areas for improvement remain. For instance, how to better utilize the feature information in images, improve the generalization ability and stability of the model, and more accurately restore local details of images are current research focuses. To address these issues, researchers have proposed various improvement strategies, such as introducing attention mechanisms to enhance the model's focus on important features, adjusting network structures to improve feature extraction efficiency, and adopting new regularization techniques to stabilize the training process.

In response to the issues of insufficient feature utilization and blurred local texture details in existing image super-resolution reconstruction methods, we propose a super-resolution reconstruction method based on local texture adversarial and hybrid attention generative adversarial networks. The hybrid attention module is added to the residual modules of the generator to enhance the model's utilization of features and the representativeness of each feature. To improve the quality of detail textures in generated images, we introduces LTSM, which can accurately locate patches with strong texture features based on the edge texture intensity of each local region in the input image, serving as a key reference for further processing. Along with the LTSM, a local discriminator is also employed, whose structure is identical to that of the global discriminator. Furthermore, the local discriminator

needs to make pixel-by-pixel judgments on the patches with the strongest texture information extracted by LTSM, making the local texture details of the reconstructed images more realistic and greatly enhancing the visual perception of the images.

The remainder of this paper is structured as follows: Section II provides a comprehensive review of related work, highlighting existing advancements and limitations in GAN-based and hybrid attention mechanisms for image super-resolution. Section III details the proposed method, including the generator and LTSM. Section IV presents extensive experimental results and analysis, comparing the proposed approach with state-of-the-art models on benchmark datasets. Finally, Section V concludes the paper, summarizing the contributions and discussing potential directions for future research.

II. Related Works

A. Single Image Super-Resolution Based on GANs

The goal of single SR is to enhance the resolution of a LR image to produce a corresponding HR image. Typically, LR images are obtained through a degradation process involving blurring and down-sampling. In classical image super-resolution reconstruction, bicubic down-sampling is widely used to simulate this degradation. By using it as a benchmark, different SR methods can be evaluated and directly compared, thereby verifying the effectiveness of new SR methods.

GANs [22] provide a principled approach to enhance the generator's ability to produce realistic images through adversarial training between the generator and discriminator. To improve perceptual quality, Johnson et al. [23] proposed a perceptual loss. Ledig et al. [10] introduced SRGAN, which performed adversarial training alongside the SRResNet generator, marking the first use of GANs for image super-resolution reconstruction. Subsequent improvements to generator architectures include Wang et al. [13], who proposed ESRGAN with a Residual-in-Residual Dense Block (RRDB) architecture, which has become a standard backbone for many state-of-the-art GAN-based super-resolution methods. Later, Rakotorinira et al. [24] enhanced ESRGAN with additional noise injection, presenting ESRGAN+ Zhang et al. [14] introduced a Ranker that learns perceptual metrics in RankSRGAN. For discriminator improvements, the relativistic discriminator concept proposed by RelativisticGAN [25] and the multi-discriminator strategy used by MPD-GAN [26] have provided greater training stability and better reconstruction image quality for GAN-based super-resolution methods.

Although the aforementioned GAN-based single image SR methods have made significant improvements in PSNR metrics and visual effects compared to interpolation- and regression-based methods, there is still considerable room for improvement in reconstructing local and highly textured regions of images.

B. Hybrid Attention Mechanism

In recent years, Transformer-based methods [27][28] have demonstrated remarkable performance in image restoration tasks, particularly in image SR and denoising. Despite these breakthroughs, attribution analysis reveals that existing networks have limited spatial utilization of input information. This indicates that the potential of transformers in current networks has not been fully exploited.

To better reconstruct images and activate more input pixels, Chen et al. proposed Hybrid Attention Transformer (HAT) [29]. HAT not only incorporates a channel attention mechanism to enhance the interaction efficiency between features but also introduces a window-based self-attention mechanism, further improving the model's ability to handle multi-scale features. This method effectively combines the global and local advantages of transformers, enhancing its performance in image restoration tasks. HAT can more meticulously focus on important features within the image, providing richer and more precise information for image restoration. However, Transformer-based SR reconstruction models often produce images with less realistic textures, whereas GANs can generate more visually appealing images. In terms of subjective visual effects, SR models based on GANs typically achieve better results. Additionally, GANs can combine various loss functions to adjust outputs, allowing them to perform well in different scenarios. Nevertheless existing models failed to effectively combined the advantages of transformer and GANs based approaches.

C. Existing Solutions and Limitations

Despite notable progress in image super-resolution (SR) research, existing methods still face critical limitations that hinder their effectiveness in addressing texture and detail reconstruction challenges. Table I summarizes the key limitations of prominent SR approaches and their unsuitability for the problem at hand.

The above limitations highlight the gaps in existing SR methods, particularly their inability to balance global structure preservation with detailed texture restoration. These shortcomings directly impact the visual realism and structural fidelity of reconstructed images. To address these challenges, the proposed approach introduces:

1) Hybrid Attention Residual Blocks (HARB): Combines window-based self-attention and channel attention to capture both global and local features, improving feature utilization and structural preservation.

2) Local Texture Sampling Module (LTSM): Targets high-frequency texture-rich regions for focused adversarial learning, enhancing detail realism and mitigating blurriness.

3) Dual adversarial branches: Integrates global and local discriminators to balance structural consistency and texture enhancement.

By addressing these gaps, the proposed method is particularly suited for generating high-resolution images with enhanced texture detail and structural fidelity, overcoming the limitations of existing approaches.

III. Proposed Method

The most distinctive feature of HR images is their intricate local texture patterns, which represent the distribution of local pixels. Specifically, high-frequency pixels concentrate around local edges, while low-frequency pixels smoothly spread adjacent to these edges. This separation pattern between high

TABLE I. LIMITATIONS IN EXISTING METHODS

Method	Advantages	Limitations	Suitability Issues for Current Problem
SRCNN[7]	Simple, pioneering CNN-based SR	Limited ability to capture high-frequency textures and complex details	Over-smooth outputs; insufficient texture restoration in high-resolution demands.
RCAN[8]	Channel attention for feature focus	High computational cost; limited enhancement of localized textures	Struggles with highly textured regions critical for detailed reconstructions.
SRGAN[9]	First GAN-based SR approach	Artifacts in outputs; struggles with preserving structural consistency	Insufficient detail fidelity in texture-rich and edge-dense areas.
ESRGAN[13]	Improved GAN design	Lacks mechanisms for enhancing localized texture details	Unable to accurately enhance localized, high-frequency textures.
SwinIR[27]	Transformer-based SR model	Effective global attention; high computational demand	Limited capability in generating realistic textures in local image regions.

and low-frequency elements starkly contrasts with LR images where high-frequency elements are either not distinctly separated or missing altogether. To address this, this study extends the framework of GANs by adding a patch-level learning branch. This branch adaptively applies adversarial learning to different local regions based on their edge characteristics, thereby enhancing the model's ability to capture texture patterns in HR images. Furthermore, to address the issue of insufficient feature utilization by existing models, we introduce a hybrid attention residual block in place of the original dense residual blocks within the generator. These hybrid attention blocks combine window-based multi-head self-attention mechanisms with channel attention mechanisms. This approach aims to activate more effective pixels for SR reconstruction tasks, thereby improving the utilization of features in input images. By integrating these advancements, the proposed method enhances the capability of GAN-based models to accurately reconstruct HR images while preserving and enhancing intricate local texture patterns.

A. Network Structure Overview

The network structure is depicted in Fig. 1, where I^{HR} represents the HR image;I^{LR} represents the LR image that obtained by bicubic interpolation and downsampling from;I^{SR} denotes the super-resolution image reconstructed by the generator. The high-resolution image are first input into the generator based on hybrid attention blocks to output super-resolution image, I^{HR} and I^{SR} are simultaneously input into the global discriminator, which outputs a grayscale image of the same height and width as the input image to determine whether the input image is a real high-resolution image or a super-resolution image generated by the generator, I^{HR} will also be sent into a pre-trained VGG-19 network, where the perceptual loss is calculated on the feature maps output from the middle convolutional layers of the network.

To better capture texture patterns that are more noticeable in local areas, a local adversarial learning branch is added. In this branch, LTSM is proposed, which constrains adversarial learning only in the local regions with the highest intensity. The LTSM takes mini-batches of I^{HR} and I^{SR} as input and outputs the top N patches I^{HR}_{patch} and I^{SR}_{patch} with the highest pixel intensities from these two mini-batches respectively. A local discriminator, which has the same structure as the global discriminator, simultaneously we established local discriminator to differentiate between the patches from I^{HR}_{patch} and I^{SR}_{patch} forming local adversarial learning, which has the same structure as the global discriminator. This promotes the generator to produce more realistic local texture details.

B. Generator

The existing model structure does not fully utilize the input features, leading to a loss of detail in the reconstructed images. we integrated Hybrid Attention Residual Blocks (HARB) into the Residual in Residual Dense Block(RRDB) structure. Specifically, an Hybrid Attention block(HAB) is embedded before the output of the RRDB module. The HAB combines channel attention and window-based multi-head self-attention in a parallel manner. Channel attention leverages global information, and self-attention has strong representation capabilities, ensuring that the network activates more effective pixels and extracts more input feature information. The structure of HARB is shown in Fig. 2. In the generator, only the last six RRDB blocks are replaced with HARB blocks.

The overall network structure of the generator is shown in Fig. 3. Since Batch Normalization (BN) layers can easily cause unwanted artifacts in SR reconstructed images, the entire generator structure does not use BN layers. All convolutional layers use LeakyReLU as the activation function, which addresses the zero-gradient issue for negative values, stabilizes model training, and accelerates model convergence. In the generator, a convolutional layer is first used to extract edge information from LR images, which is then fed into m RRDB blocks. The dense residual blocks and residual scaling techniques used in the RRDB blocks help train deeper network models, further improving the network's ability to capture semantic information. The intermediate feature maps produced by the RRDB blocks are then fed into n HARB blocks. These blocks use window-based multi-head self-attention to capture long-range dependencies in the sequence while focusing on important parts of the input feature information by paying attention to channel information. The upsampling part of the generator consists of two consecutive PixelShuffle [30], each of which doubles the resolution of the feature maps. Finally, two convolutional layers adjust the channels to output the SR reconstructed results.

C. Local Texture Sampling Module

In GANs, images reconstructed by the generator often exhibit blurriness and lack of detail. To improve the quality

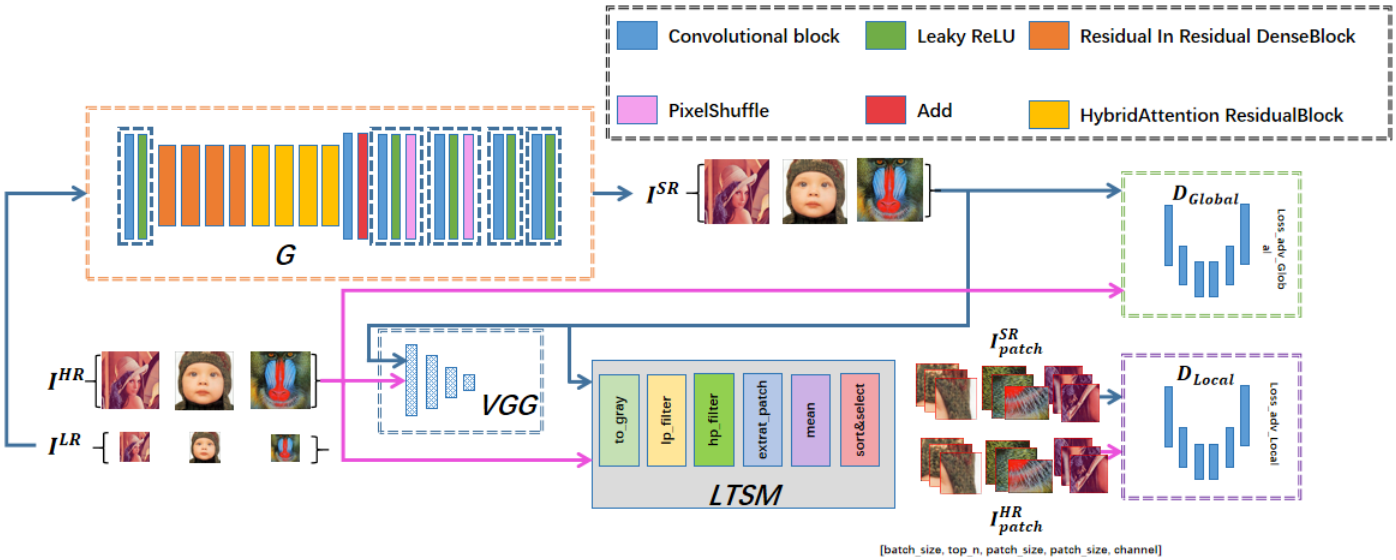


Fig. 1. The overall architecture of the proposed method, which consists of a global adversarial branch and a local adversarial branch. The LTSM is applied in the local branch to enhance the model's learning of texture details.

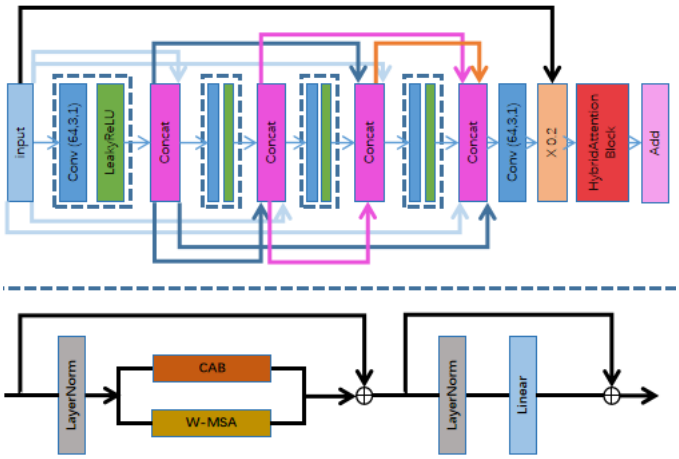


Fig. 2. The overall structure of the HARB is shown above the dashed line, consisting of Dense Residual Blocks and a Hybrid Attention Block (HAB). Below the dashed line is the structure of the HAB, which is composed of Channel Attention and Window-based Self-Attention mechanisms.

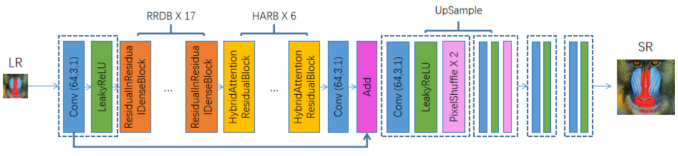


Fig. 3. The core of the generator consists of 17 RRDB and 6 HARB, after these blocks, an upsampling process using PixelShuffle is applied to increase the resolution of the image, followed by additional convolutional layers to produce the final HR image.

of local texture details in generated images, we proposes the LTSM. The LTSM is designed to extract local texture features from images. It uses an improved Sobel operator to calculate the edge strength of each local region in the input image and evaluates the texture features of these local regions based on their edge strength. The specific details of the LTSM are shown in Fig. 4. Specifically, in the preprocessing part of the LTSM, the input tensors I^{HR} and I^{SR} are first converted into ndarray format. Then, based on the hyperparameter $patchSize$, each group of images is divided into M patches I^{HR}_{patch} and I^{SR}_{patch}, here $M = Batch\_Size \times (\left|\frac{\mathrm{H}}{\mathrm{patchSize}}\right| + 1) \times (\left|\frac{\mathrm{W}}{\mathrm{patchSize}}\right| + 1)$ H and W represent the height and width of the image, respectively. At the same time, we also obtains a list of coordinates $patchCoordinates$ corresponding to the top-left corner of each patch in the original image. These segmented patches are processed through a guided-filter [31] $\mathcal{F}_{gf}$, which filters out noise from the image while retaining as much edge information as possible.

$$I_i^{patch} = \mathcal{F}_{gf}(I_i^{patch}, I_i^{patch}), i = 1, ..., Batch\_Size. \quad (1)$$

The denoised images are then fed into the improved Sobel operator, where the resulting four scores are squared and summed. Finally, the square root of the summed result is calculated, and the average value is taken to obtain the edge pixel intensity scores for all patches in an image. These scores serve as the keys for patch selection, and their values are calculated as follows:

$$\mathrm{Key_{j,k}} = \mathrm{Mean}(\sqrt[2]{\sum_{i=1}^{4}(I_{j,k}^{Patch} \otimes K_i)^2}), \quad (2)$$
$$\mathrm{j} = 1 \ldots Batch\_Size, \mathrm{k} = 1, \ldots, M$$

The symbol $\otimes$ represents the convolution operation. The Key values for all patches in a batch are calculated and sorted accordingly. Finally, the top N patches with the highest edge pixel intensity scores and their corresponding patch coordinates are obtained. Based on these coordinates, the correspond-

ing tensor patches are extracted from the original input tensors I^{SR} and I^{HR} preserving the original gradient information of the tensors. The architecture of LTSM is shown in Fig. 4:

D. Loss Function

1) Pixel-wise loss: traditional image super-resolution (SR) reconstruction methods are mostly based on the L2 pixel-level loss function mean-square error (MSE). Although this achieves a high PSNR value, using MSE tends to drive the solution towards a pixel-averaged result, which is overly smooth and perceptually poor. Therefore, in the pre-training phase, we only uses L1 loss to accelerate the convergence of the model. The pixel-wise loss is defined as shown in Eq. (3):

$$L_1 = \frac{1}{HW}\sum_{i=1}^{H}\sum_{j=1}^{W}\left|G(I^{LR})_{(i,j)} - I^{HR}_{(i,j)}\right| \tag{3}$$

where G represents the generator.

2) Perception loss: we uses a pre-trained VGG-19 network to extract features. The perceptual loss is calculated using the feature maps before the LeakyReLU activation, as these feature maps contain more detailed information compared to the more sparse features after activation, providing stronger supervision. Features are extracted from the conv1-2, conv2-2, conv3-4, conv4-4, and conv5-4 layers, and the perceptual loss from each layer is weighted and summed to obtain the final perceptual loss. The perceptual loss is defined as shown in Eq. (4):

$$L_{percep} = \left\|\varphi(G(\mathrm{I^{LR}})) - \varphi(\mathrm{I^{HR}})\right\|_1 \tag{4}$$

Where $\varphi(\cdot)$ represents the pre-trained VGG-19 network.

3) Global adversarial loss: The global adversarial loss aims to capture global content feature information. The super-resolution images generated by the generator are input into the global discriminator to obtain a score for each pixel. Compared to the traditional VGG-style discriminator, which outputs a scalar for loss calculation, the discriminator is based on the idea of a U-Net style discriminator. The discriminator's loss is defined as the average decision of all pixels. Pixel-level loss calculation can make the texture details of the reconstructed image more precise. The least squares loss function (LSGAN) [32] is used instead of the cross-entropy loss function to achieve better training stability. The global adversarial loss function is defined as shown in Eq. (7):

$$\begin{aligned} L^D_{Global} = {} & E_{I^{HR}}[(D_{Global}(I^{HR}) - 1)^2] \\ & + E_{I^{LR}}[(D_{Global}(G(I^{LR})))^2] \end{aligned} \tag{5}$$

$$L^G_{Global} = E_{I^{LR}}[(D_{Global}(G(I^{LR})) - 1)^2] \tag{6}$$

$$L_{advGlobal} = L^D_{Global} + L^G_{Global} \tag{7}$$

4) Local adversarial loss: The local adversarial loss constrains adversarial training in small local regions with the highest edge texture intensity in the image, better promoting the generator to capture local texture features of high-resolution images. The output of the local discriminator is the average decision of all pixels in these small regions. The local adversarial loss is defined as shown in Eq. (10):

$$\begin{aligned} L^D_{Local} = {} & E_{h^p_i \sim I^{HR}_{patch}}\left[\frac{1}{N}\sum_{i=1}^{n}(D_{Local}(h^p_i) - 1)^2\right] + \\ & E_{l^p_i \sim I^{LR}_{patch}}\left[\frac{1}{N}\sum_{i=1}^{n}(D_{Local}(l^p_i))^2\right] \end{aligned} \tag{8}$$

$$L^G_{Local} = E_{l^p_i \sim I^{LR}_{patch}}\left[\frac{1}{N}\sum_{i=1}^{n}(D_{Local}(l^p_i) - 1)^2\right] \tag{9}$$

$$L_{advLocal} = L^D_{Local} + L^G_{Local} \tag{10}$$

Here h^p_i and l^p_i are the i-th small regions extracted by the LTSM from the high-resolution image I^{HR} and the super-resolution image I^{SR}. Since LTSM extracts the top N small regions with the highest edge texture intensity from each input image, the local adversarial loss is calculated by summing the loss over these N regions and then taking the average.

5) Pre-training and training loss function: The pre-training loss and training loss are based on the aforementioned loss functions. In the pre-training phase, only the generator is trained. The generator's pre-training loss is defined as shown in Eq. (11):

$$L_{pre} = L_1 \tag{11}$$

The training phase includes both generator loss and discriminator loss. The total loss function of the generator is defined as shown in Eq. (12):

$$L_G = \gamma_1 L_1 + \gamma_2 L^G_{Global} + \gamma_3 L^G_{Local} + \gamma_4 L_{percep} \tag{12}$$

where the weights of the generator's loss functions are $\gamma_1 = 0.08$,$\gamma_2 = 0.04$,$\gamma_3 = 0.02$,$\gamma_4 = 1$.

IV. Experimental Results and Analysis

A. Experimental Setup

The experiments were conducted on two NVIDIA GeForce RTX 3090 GPUs. The experiment used 800 HR images from the DIV2K dataset [33] and the corresponding LR images, obtained by bicubic interpolation with a scaling factor of 4, as the training dataset. The test sets are four standard datasets commonly used in the field of image super-resolution reconstruction: Set5, Set14, BSD100 and Urban100. The experiment used PSNR and SSIM as evaluation metrics. The settings and hyperparameter selection for the model during the training process are as follows: During training, the DIV2K dataset was randomly cropped into 128x128 images and subjected to random rotation and random flipping. The batch size for each input was 64. The number of RRDB blocks m was 16, and the number of HARB blocks n was 6. In the pre-training phase, only the PSNR-oriented pixel-wise loss defined in Eq. (3) was used to update the generator. The pre-training phase consisted of a total 6.25×10^4 iterations, with an initial learning rate of 2×10^{-4} The learning rate was halved after every 1.25×10^4 iterations.After the pre-training phase, the official training phase used Exponential Moving Average(EMA) to stabilize the training, with a weighting factor $\beta = 0.999$, In the official training phase, the initial learning rate for the generator was 1×10^{-4}, and the initial learning rate for the discriminator

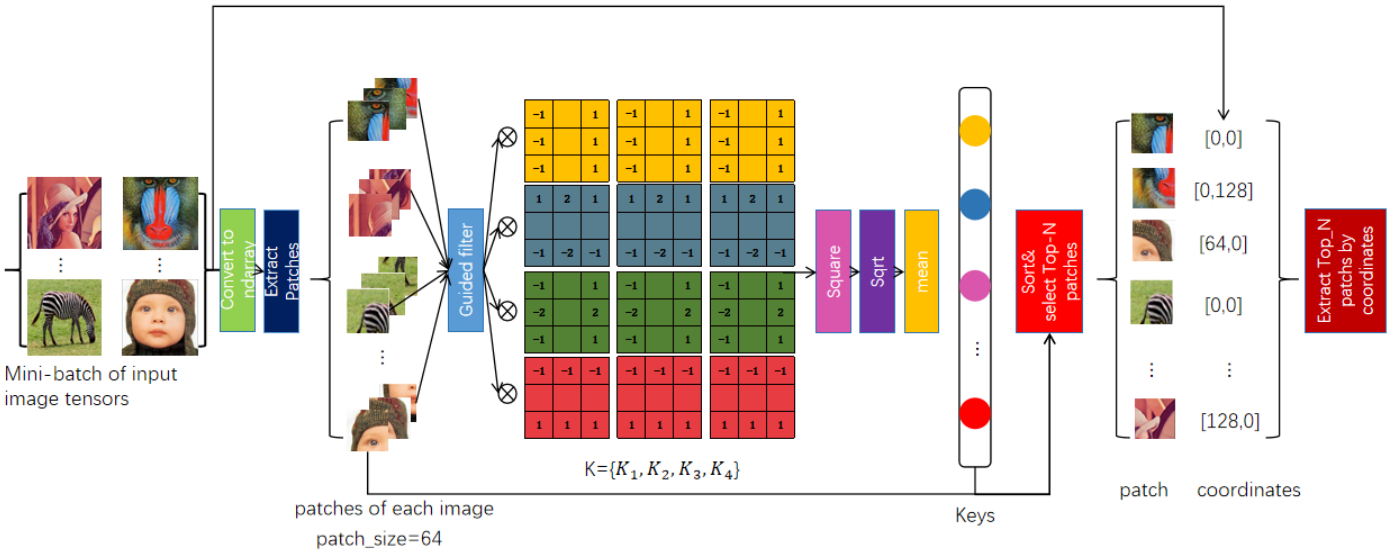


Fig. 4. Details of Local Texture Sampling Module (LTSM) which adaptively extracts local image patches with most salient texture features from each mini-batch of input images.

was 4×10^{-4}, The official training phase consisted of 7.5×10^{4} iterations. with the learning rates for both the generator and the discriminator halved after every 1.25×10^{4} iteration. Adam optimizer was used for all training phases, where $\beta_1 = 0.9$, $\beta_2 = 0.999$, $\varepsilon = 1\times10^{-8}$.

B. The Effects of Hybrid Attention Residual Blocks

The generator is implemented based on Hybrid Attention Residual Blocks. To validate the effectiveness of these blocks in extracting more feature information and activating more effective pixels, this section conducts experiments on the pre-trained generator and compares the changes in PSNR values. As shown in Table II, increasing the number of Hybrid Attention Residual Blocks from 8 to 16 resulted in PSNR improvements of 0.22 dB and 0.13 dB on the Set5 and Set14 test sets, respectively. Further increasing the blocks from 16 to 24 resulted in a PSNR improvement of 0.05 dB on the Set5 test set and 0.01 dB on the Set14 test set. However, with more than 16 Hybrid Attention Residual Blocks, the generator's network parameters became excessively large. Therefore, we ultimately used 16 Hybrid Attention Residual Blocks to construct the generator, ensuring a high PSNR value while keeping the network parameter size manageable.

TABLE II. THE EFFECTS OF HYBRID ATTENTION RESIDUAL BLOCKS

The Number of HARB	SET5 PSNR(dB)	SET14 PSNR(dB)
0	30.12	27.8
8	31.11	28.1
16	31.93	28.23
32	31.98	28.24

C. The Effects of Local Adversarial Branch and LTSM

To verify the effectiveness of the LTSM and its impact on the generator, this section conducts quantitative and qualitative comparisons based on PSNR metrics and the quality of super-resolution reconstructed images. Specifically, we compare models using only the global adversarial module, models without LTSM extracting patches but using all patches, and the complete model.

As shown in Table III, introducing the local adversarial branch results in improvements in PSNR and SSIM metrics on each dataset, indicating that the local adversarial branch effectively enhances the structural similarity of images. Furthermore, not using the LTSM and training with all patches led to decreases in both PSNR and SSIM metrics, further validating the importance of the LTSM in extracting critical texture information. Comparing the reconstruction results shown in Fig. 5, we can visually observe differences in detail preservation and edge handling among different models. The complete model using the local adversarial branch and LTSM excels in restoring edge textures, producing clearer images with richer details. In contrast, models using only the global adversarial module show blurrier edge handling, and those not using the LTSM exhibit deficiencies in detail representation. This visual improvement vividly reflects the contribution of the local adversarial branch and LTSM in enhancing the effectiveness of super-resolution reconstruction. By comparing the reconstruction results under different model configurations, this study concludes that the local adversarial branch and LTSM are crucial for enhancing the performance of super-resolution reconstruction. They not only improve quantitative evaluation metrics but also demonstrate significant visual improvements in qualitative analysis. These findings underscore the importance of considering local texture features in the design of super-resolution reconstruction models.

D. Comparison with Existing SR Models

1) Quantitative comparison: In this section, our model is compared with several existing super-resolution (SR) models. The models chosen for comparison include traditional bicubic interpolation, as well as several deep learning-based methods

TABLE III. EFFECTS OF LOCAL ADVERSARIAL BRANCH AND LTSM ON PSNR AND SSIM METRICS

Datasets	W/O Local Adversarial Branch		W/O LTSM(All patches)		ours(full model)	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Set5	32.30	0.9073	31.22	0.8987	**32.32**	**0.9110**
Set14	28.12	0.8025	27.92	0.7829	**28.15**	**0.8231**
BSD100	27.92	0.6882	27.12	0.6801	**28.31**	**0.7012**
Urban100	26.66	0.8029	26.85	0.8012	**27.18**	**0.8206**

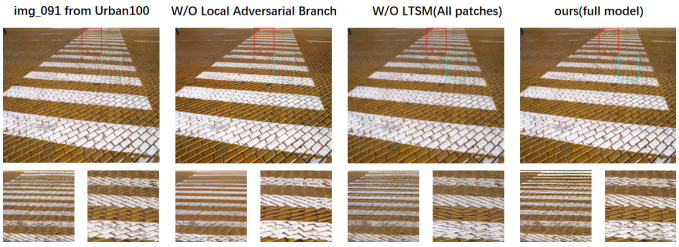


Fig. 5. Urban100 dataset img_091 Reconstruction Comparison, the results show that compared to model trained without the local adversarial branch and trained using all patches in the local branch, the model trained with the LTSM produces more realistic texture details.

such as SRCNN [7], RCAN [9], SRGAN [10], ESRGAN [13], and SwinIR [27]. Additionally, we incorporate the recently proposed Semantic-aware Discriminator (SeD) [34] into ESRGAN and SwinIR, a recent approach designed to enhance texture generation quality by leveraging semantic information. The improved versions of these models are denoted as ESRGAN+ and SwinIR+, respectively. Comparative experiments are conducted on four commonly used benchmark datasets: Set5 [35], Set14 [36], BSD100 [37], and Urban100 [38], with primary evaluation metrics being PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index).

In Table IV, our model demonstrates best performance across four commonly used datasets at all scales, especially achieves average improvement of 0.15 dB on PSNR compared to SwinIR+ [27][34] at $\times 4$ scale. From the SSIM results, it is evident that our model consistently achieves optimal performance across most datasets except for SSIM on BSD100($\times 4$). Compared to other models, our model shows an average SSIM improvement of 0.053 over SRCNN [7], 0.014 over RCAN [9], 0.047 over SRGAN [10], 0.056 over ESRGAN+ [13][34], and 0.003 over SwinIR+ [27][34]. These findings indicate that our model not only excels in image clarity (PSNR) but also performs exceptionally well in preserving image structure and details (SSIM).

In summary, through comparisons with various existing SR models, our proposed Generative Adversarial Network super-resolution reconstruction method based on local texture adversarial learning and hybrid attention demonstrates outstanding performance in both PSNR and SSIM metrics. This validates its effectiveness and superiority across different types of images.

2) Qualitative comparison: In terms of qualitative comparison, this study selected typical images from different datasets to visually assess the reconstruction results of various models. The specific results are shown in Fig. 6, 7 and 8.

Regarding image details and texture restoration, the proposed model demonstrates significant advantages Compared to other models, it preserves the details and textures of the original images better during reconstruction, the patches highlighted in red boxes represent critical regions for evaluating detail preservation and texture fidelity. For instance, in urban street scene images Img_014 and Img_087 from the Urban100 dataset, the proposed model not only reconstructs building edges and textures clearly but also presents more natural and realistic details. In contrast, other models like SRCNN [7], RCAN [9], and SRGAN [10] may exhibit blurriness or distortion in some details, which the proposed model effectively avoids.

Furthermore, on datasets like Set5 and Set14, the proposed model shows strong robustness and capability in restoring details in natural scenes and facial images. In Baboo from Set14, the proposed model performs a more natural reconstruction effect on facial details such as eyes and beard.

In comparison with existing SR models, the proposed model demonstrates superior performance in both quantitative metrics and qualitative effects. By integrating local texture adversarial learning and hybrid attention mechanisms, the proposed model not only enhances the accuracy of image reconstruction but also achieves a higher level of visual fidelity.

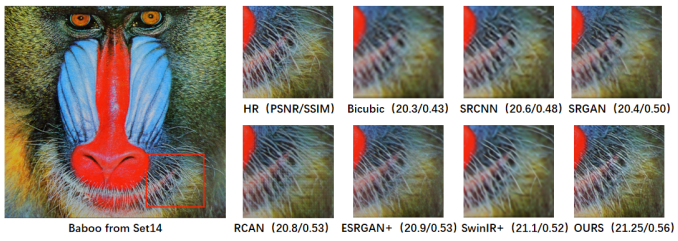


Fig. 6. Baboo from Set14 Reconstruction Comparison, the patches for comparison are marked with red boxes in the original images. PSNR/SSIM is calculated based on the patches to better reflect the performance difference.

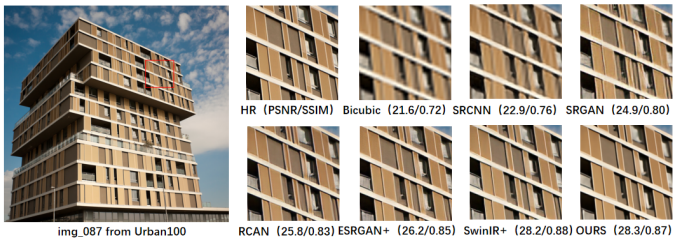


Fig. 7. Img_087 from Urban100 reconstruction comparison.

TABLE IV. QUANTITATIVE COMPARISONS (PSNR/SSIM) BEST PERFORMANCES ARE MARKED IN BOLD AND "+" INDICATES THAT METHODS INCORPORATE SED

Method	Scale	Set5		Set14		BSD100		Urban100	
		PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Bicubic	x2	33.66	0.9299	30.24	0.8688	29.56	0.8431	26.88	0.8403
SRCNN[7]	x2	36.66	0.9542	32.45	0.9067	31.36	0.8879	29.50	0.8946
RCAN[9]	x2	38.27	0.9614	34.12	0.9216	32.41	0.9027	33.34	0.9384
SRGAN[10]	x2	36.86	0.9560	33.56	0.9156	32.12	0.8996	32.36	0.9196
ESRGAN+[13][34]	x2	37.45	0.9592	33.76	0.9175	32.30	**0.9075**	32.56	0.9315
SwinIR+[27][34]	x2	38.39	0.9620	34.14	0.9227	32.44	0.9030	33.40	0.9393
Ours	x2	**38.41**	**0.9652**	**34.22**	**0.9231**	**32.55**	0.9038	**33.47**	**0.9425**
Bicubic	x3	30.39	0.8682	27.55	0.7742	27.21	0.7385	24.46	0.7349
SRCNN[7]	x3	32.75	0.9090	29.28	0.8209	28.41	0.7863	26.24	0.7989
RCAN[9]	x3	34.74	0.9299	30.65	0.8482	29.32	0.8111	29.09	0.8702
SRGAN[10]	x3	33.20	0.9101	29.89	0.8322	29.13	0.7850	28.91	0.8577
ESRGAN+[13][34]	x3	34.75	0.9223	30.44	0.8455	29.30	0.8128	28.99	0.8679
SwinIR+[27][34]	x3	34.89	0.9312	30.89	0.8503	29.35	0.8124	29.29	0.8744
Ours	x3	**34.93**	**0.9388**	**30.90**	**0.8521**	**29.40**	**0.8155**	**29.47**	**0.8782**
Bicubic	x4	28.40	0.7854	26.09	0.7486	24.98	0.6935	23.12	0.6577
SRCNN[7]	x4	29.07	0.8504	26.64	0.7602	26.90	0.7101	23.98	0.7213
RCAN[9]	x4	30.83	0.8878	26.75	0.7889	27.77	0.7236	25.92	0.7985
SRGAN[10]	x4	29.40	0.8213	26.21	0.7428	27.1	0.7223	24.37	0.7802
ESRGAN+[13][34]	x4	30.46	0.8525	26.86	0.7905	27.85	0.6528	26.15	0.7328
SwinIR+[27][34]	x4	32.25	0.9012	28.12	0.7914	28.29	**0.7311**	26.71	0.8164
Ours	x4	**32.32**	**0.9110**	**28.15**	**0.8231**	**28.31**	0.7012	**27.18**	**0.8206**

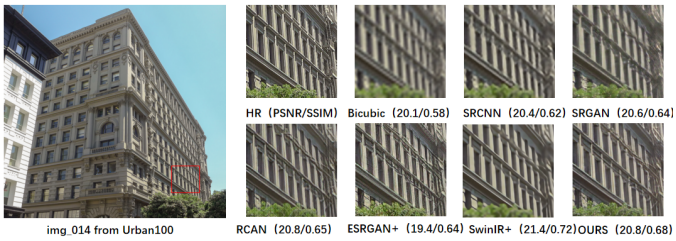


Fig. 8. Img_014 from Urban100 reconstruction comparison.

V. CONCLUSION

We had proposed a GAN based method for image SR reconstruction, leveraging local texture adversarial and hybrid attention residual block. LTSM is introduced to compute edge intensity in local image regions, this module effectively addresses issues of blurriness and detail loss commonly observed in traditional GAN-generated images. Additionally, a generator equipped with HARB is incorporated to enhance the utilization of input features during generation. This approach ensures better preservation of image structure and details, thereby improving overall image quality in reconstruction. Experimental validation on multiple standard datasets (Set5, Set14, BSD100, and Urban100) demonstrates superior performance in terms of PSNR and SSIM metrics, surpassing various existing super-resolution methods and exhibiting notable advantages in image detail and texture restoration. However it is not without limitations. One key limitation is the computational cost associated with the HARB and LTSM, which may limit its deployment in real-time applications or on devices with constrained resources. Additionally, while the LTSM effectively enhances local texture details, its reliance on patch selection based on edge intensity might overlook non-edge regions with critical texture information, leading to potential gaps in detail preservation in less textured areas.

For future work, we will explore optimizing the computational efficiency of the proposed framework by leveraging lightweight architectures or pruning techniques. Furthermore, incorporating adaptive mechanisms for selecting texture-rich regions, beyond edge intensity, could enhance the model's ability to generalize across diverse image types. Extending the current method to handle multi-frame super-resolution or domain-specific applications, such as medical imaging or satellite imagery, could also provide new directions for further exploration.

ACKNOWLEDGMENT

This work was supported by the Key Research and Development Program of Zhejiang Province (2020C03094), and the General Scientific Research Project of the Department of Education of Zhejiang Province (Y202250677, Y202250706, Y202250679).

REFERENCES

[1] Z. Cui, Y. Zhu, L. Gu, G. J. Qi, X. Li, R. Zhang, Z. Zhang, and T. Harada, "Exploring resolution and degradation clues as self-supervised signal for low quality object detection," 2022.

[2] D. Dai, Y. Wang, Y. Chen, and L. Van Gool, "Is image super-resolution helpful for other vision tasks?" 2015.

[3] L. Zhou, G. Chen, M. Feng, and A. Knoll, "Improving low-resolution image classification by super-resolution with enhancing high-frequency content," in *2020 25th International Conference on Pattern Recognition (ICPR)*, 2021.

[4] L. Wang, D. Li, Y. Zhu, L. Tian, and Y. Shan, "Dual super-resolution learning for semantic segmentation," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2020.

[5] A. Singh and J. Singh, "Content adaptive single image interpolation based super resolution of compressed images," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, p. 3014, 2020.

[6] X. Ma, J. Zhang, T. Li, L. Hao, and H. Duan, "Super-resolution geomagnetic reference map reconstruction based on dictionary learning and sparse representation," *IEEE Access*, vol. 8, pp. 84 316–84 325, 2020.

[7] C. Dong, C. C. Loy, K. He, and X. Tang, "Learning a deep convolutional network for image super-resolution," in *Computer Vision – ECCV 2014*, D. Fleet, T. Pajdla, B. Schiele, and T. Tuytelaars, Eds. Cham: Springer International Publishing, 2014, pp. 184–199.

[8] B. Lim, S. Son, H. Kim, S. Nah, and K. Mu Lee, "Enhanced deep residual networks for single image super-resolution," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, July 2017.

[9] Y. Zhang, K. Li, K. Li, L. Wang, B. Zhong, and Y. Fu, "Image super-resolution using very deep residual channel attention networks," in *Proceedings of the European Conference on Computer Vision (ECCV)*, September 2018.

[10] C. Ledig, L. Theis, F. Huszar, J. Caballero, A. Cunningham, A. Acosta, A. Aitken, A. Tejani, J. Totz, Z. Wang, and W. Shi, "Photo-realistic single image super-resolution using a generative adversarial network," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, July 2017.

[11] C. Ma, Y. Rao, Y. Cheng, C. Chen, J. Lu, and J. Zhou, "Structure-preserving super resolution with gradient guidance," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2020.

[12] T. R. Shaham, T. Dekel, and T. Michaeli, "Singan: Learning a generative model from a single natural image," in *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*, October 2019.

[13] X. Wang, K. Yu, S. Wu, J. Gu, Y. Liu, C. Dong, Y. Qiao, and C. Change Loy, "Esrgan: Enhanced super-resolution generative adversarial networks," in *Proceedings of the European Conference on Computer Vision (ECCV) Workshops*, September 2018.

[14] W. Zhang, Y. Liu, C. Dong, and Y. Qiao, "Ranksrgan: Super resolution generative adversarial networks with learning to rank," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 10, pp. 7149–7166, 2021.

[15] K. Ding, K. Ma, S. Wang, and E. P. Simoncelli, "Image quality assessment: Unifying structure and texture similarity," *IEEE transactions on pattern analysis and machine intelligence*, vol. 44, no. 5, pp. 2567–2581, 2020.

[16] S. Gao, X. Liu, B. Zeng, S. Xu, Y. Li, X. Luo, J. Liu, X. Zhen, and B. Zhang, "Implicit diffusion models for continuous super-resolution," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2023, pp. 10 021–10 030.

[17] H. Phung, Q. Dao, and A. Tran, "Wavelet diffusion models are fast and scalable image generators," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2023, pp. 10 199–10 208.

[18] R. Rombach, A. Blattmann, D. Lorenz, P. Esser, and B. Ommer, "High-resolution image synthesis with latent diffusion models," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2022, pp. 10 684–10 695.

[19] C. Saharia, J. Ho, W. Chan, T. Salimans, D. J. Fleet, and M. Norouzi, "Image super-resolution via iterative refinement," *IEEE transactions on pattern analysis and machine intelligence*, vol. 45, no. 4, pp. 4713–4726, 2022.

[20] Y. Kim and D. Son, "Noise conditional flow model for learning the super-resolution space," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 424–432.

[21] A. Lugmayr, M. Danelljan, L. Van Gool, and R. Timofte, "Learning the super-resolution space with normalizing flow," *ECCV, Srflow*, vol. 2, 2020.

[22] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," *Advances in neural information processing systems*, vol. 27, 2014.

[23] J. Johnson, A. Alahi, and L. Fei-Fei, "Perceptual losses for real-time style transfer and super-resolution," in *Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11-14, 2016, Proceedings, Part II 14*. Springer, 2016, pp. 694–711.

[24] N. C. Rakotonirina and A. Rasoanaivo, "Esrgan+: Further improving enhanced super-resolution generative adversarial network," in *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2020, pp. 3637–3641.

[25] A. Jolicoeur-Martineau, "The relativistic discriminator: a key element missing from standard gan," *arXiv preprint arXiv:1807.00734*, 2018.

[26] O.-Y. Lee, Y.-H. Shin, and J.-O. Kim, "Multi-perspective discriminators-based generative adversarial network for image super resolution," *IEEE Access*, vol. 7, pp. 136 496–136 510, 2019.

[27] J. Liang, J. Cao, G. Sun, K. Zhang, L. Van Gool, and R. Timofte, "Swinir: Image restoration using swin transformer," in *Proceedings of the IEEE/CVF international conference on computer vision*, 2021, pp. 1833–1844.

[28] Z. Chen, Y. Zhang, J. Gu, L. Kong, X. Yang, and F. Yu, "Dual aggregation transformer for image super-resolution," in *Proceedings of the IEEE/CVF international conference on computer vision*, 2023, pp. 12 312–12 321.

[29] X. Chen, X. Wang, W. Zhang, X. Kong, Y. Qiao, J. Zhou, and C. Dong, "Hat: Hybrid attention transformer for image restoration," *arXiv preprint arXiv:2309.05239*, 2023.

[30] W. Shi, J. Caballero, F. Huszár, J. Totz, A. P. Aitken, R. Bishop, D. Rueckert, and Z. Wang, "Real-time single image and video super-resolution using an efficient sub-pixel convolutional neural network," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 1874–1883.

[31] K. He, J. Sun, and X. Tang, "Guided image filtering," *IEEE transactions on pattern analysis and machine intelligence*, vol. 35, no. 6, pp. 1397–1409, 2012.

[32] X. Mao, Q. Li, H. Xie, R. Y. Lau, Z. Wang, and S. Paul Smolley, "Least squares generative adversarial networks," in *Proceedings of the IEEE international conference on computer vision*, 2017, pp. 2794–2802.

[33] E. Agustsson and R. Timofte, "Ntire 2017 challenge on single image super-resolution: Dataset and study," in *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*, 2017, pp. 126–135.

[34] B. Li, X. Li, H. Zhu, Y. Jin, R. Feng, Z. Zhang, and Z. Chen, "Sed: Semantic-aware discriminator for image super-resolution," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2024, pp. 25 784–25 795.

[35] M. Bevilacqua, A. Roumy, C. Guillemot, and M. L. Alberi-Morel, "Low-complexity single-image super-resolution based on nonnegative neighbor embedding," 2012.

[36] R. Zeyde, M. Elad, and M. Protter, "On single image scale-up using sparse-representations," in *Curves and Surfaces: 7th International Conference, Avignon, France, June 24-30, 2010, Revised Selected Papers 7*. Springer, 2012, pp. 711–730.

[37] D. Martin, C. Fowlkes, D. Tal, and J. Malik, "A database of human segmented natural images and its application to evaluating segmentation algorithms and measuring ecological statistics," in *Proceedings eighth IEEE international conference on computer vision. ICCV 2001*, vol. 2. IEEE, 2001, pp. 416–423.

[38] J.-B. Huang, A. Singh, and N. Ahuja, "Single image super-resolution from transformed self-exemplars," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 5197–5206.

Image Restoration of Landscape Design Based on DCGAN Optimization Algorithm

Wenjun Zhang*
School of Architecture and Urban Planning, Henan University of Urban Construction, Pingdingshan 467036, China

***Abstract*—To enhance the quality and effectiveness of image restoration in landscape design, this study optimizes the existing methods for low efficiency and incomplete feature extraction in processing high-resolution and detail rich landscape design images. Firstly, based on the traditional generative adversarial network (GAN), a novel deep convolutional generative adversarial network (DCGAN) model is proposed. Subsequently, the model's ability to extract detailed features was enhanced by integrating dense connected networks (DenseNet) and compressed excitation networks (SENet) into the network architecture. An improved DCGAN is designed for the restoration of landscape design images. According to the results, the optimized model had a restoration precision and repair recall rate of 0.97 in benchmark performance testing, which was significantly better than traditional deep convolutional generative adversarial network models. In practical applications, the model had an average accuracy of over 97% in repairing four different styles of landscape images, with an average repair time as low as 0.06s. From this, it can be seen that the designed model can provide a more efficient technical means for the restoration and digital preservation of landscape design images.**

***Keywords*—Deep convolutional generative adversarial network; image; restoration; landscape architecture; squeeze-and-excitation network; dense convolutional network**

I. Introduction

Influenced by social economy and urbanization, landscape design has gradually become important in urban planning. As a crucial component of urban green infrastructure, landscape architecture not only exerts a crucial function in beautifying the environment and improving ecology, but also has a significant impact on enhancing the quality of life of citizens and the cultural taste of the city [1-2]. However, landscape design images with a long history are often eroded by environmental factors, resulting in image damage and information loss, which affects the research and protection of landscape architecture and challenges its ability of digital preservation and inheritance.

The damaged landscape art images not only affect the research and protection of landscape architecture, but also pose challenges to the digital preservation and inheritance of landscape architecture [3-4]. Generative Adversarial Networks (GANs) have demonstrate strong potential and broad application prospects in image generation and restoration. Traditional image restoration methods mainly rely on manual or rule-based techniques, which often inadequate when dealing with complex scenes and details. In contrast, GAN can effectively capture complex texture and structural features in images through adversarial training mechanisms of generators and discriminators, achieving high-quality image generation and restoration.

However, traditional GAN still faces some specific challenges in landscape image restoration. First of all, in the training process, traditional GAN often has the problem of high training difficulty, and its training process is easily affected by mode collapse and instability, resulting in unstable image quality. Secondly, traditional image restoration techniques are often inadequate in processing complex textures and detailed features, and cannot fully retain the fine features and details in high-resolution landscape design images [5-6]. The main goal of this study is to improve the quality and effectiveness of landscape design image restoration by improving the traditional GAN optimization algorithm, especially in the aspects of feature extraction and restoration efficiency.

Therefore, a deep Convolutional generative adversarial network (DCGAN) model combining DenseNet and SENet is proposed. This new model aims to enhance the ability of the network to extract detailed features, so as to achieve more accurate image recovery in practical applications. The research innovatively introduces Dense Connected Convolutional Networks (DenseNet) and Squeeze-and-Excitation Networks (SENet) as generators, and uses Deep Convolutional Generative Adversarial Networks (DCGAN) as discriminators, ultimately enabling the constructed model to extract more detailed features, reduce computational complexity, and effectively restore the original image. The potential benefit of the research is that the successful implementation of this approach will have a profound impact in several fields. First of all, in urban planning and management, high-quality image restoration can provide more accurate visual basis for decision-making and support more effective land use and environmental design. Secondly, in the field of cultural heritage protection, it can help preserve and restore historical documents and artistic works to ensure the long-term preservation and transmission of cultural heritage. Finally, in the practice of digital preservation, the research results can provide strong technical support for the maintenance of various digital archives and promote the sustainable management and utilization of digital content.

The structure of this paper is divided into six sections. Section II, literature review, summarizes the achievements and shortcomings of domestic image restoration research. Section III introduces the proposed method, including the DCGAN architecture and the integration of DenseNet and SENet, to improve image restoration performance. Section IV presents the experimental results, verifies the performance of the model, and compares the performance of DS-DCGAN with other models. Section V discusses the advantages and potential

applications of DS-DCGAN. Finally, the research contributions were summarized and future research directions were proposed in Section VI.

II. Related Works

GAN is a deep learning approach, which includes a generator and a discriminator, which can generate realistic data through adversarial training between the two. Image restoration adopts computer technology to restore damaged or degraded images, to improve image quality or restore their original state. In image restoration, Liu G et al. designed an image restoration algorithm on the basis of GAN to address the low accuracy of traditional algorithms in restoring large-area damaged images. By extracting multi-scale edge details of the damaged area and constructing a GAN model, the model was trained to generate the best fake image. The results showed that the model could effectively combine contextual and perceptual information, significantly improve image restoration accuracy and image quality, and outperform existing algorithms [7]. In response to the significant impact of equipment and operators on the quality of retinal images, Deng Z et al. explored the retinal image restoration method in real clinical environments. Firstly, a clinical dataset Real Fundus was established, which included 120 pairs images. Secondly, a Transformer-based GAN was proposed to restore the clinical fundus images. The proposed model was helpful for in-depth analysis of clinical fundus images [8]. Yang J et al. proposed a new approach for restoring private facial images on the basis of semantic features and adversarial samples to address the serious threat posed by facial image feature leakage to user information security. Firstly, Segnet network was used for semantic segmentation of facial images, and then GAN was used to generate adversarial samples and perturb the semantic features of facial images. Compared with other advanced technologies, the generated private facial images had stronger median filtering defense capability [9].

In response to the limitations of Wasserstein-GAN in simulating complex distributions such as natural image distributions, Ma H et al. proposed a method to improve Wasserstein-GAN training by introducing pairwise constraints to optimize image restoration tasks. The research results showed that the Wasserstein-GAN model with paired constraints had better consistency and perceptual quality than existing technical methods [10]. Considering that artworks can be damaged over time due to changes in humidity, temperature, and improper storage, Kumar P et al. designed a new virtual restoration strategy for artworks based on GAN. This method adopted an improved U-Net as the generator part. A pre-trained residual network was used to construct the encoder to generate higher quality feature embeddings, improving the quality of image restoration. The research results indicated that this method performed well in performance indicators [11]. Liang M et al. designed a multi-scale self attention GAN to address the common local cross contamination or data loss in the acquisition and processing of pathological digital images. Then this network was applied to restore pathological images of tissue. The research results showed that this network structure could achieve pixel level realistic restoration of tissue pathological images, effectively restoring the detailed features of the images [12].

In summary, although the existing GAN optimization algorithm has made some progress in the field of image restoration, it still has shortcomings in processing high-resolution and detail-rich landscape design images. Therefore, a DCGAN model combining DenseNet and SENet optimization is proposed in this paper, which aims to further improve the quality and effect of image restoration by improving the structure of generator and discriminator. Compared with the current methods, the research method has improved the efficiency of feature extraction and processing. Traditional GAN models often face the problem of insufficient feature extraction when processing complex landscape design images, especially when recovering high-resolution images, fine texture and structural features are easy to ignore. By integrating DenseNet, DS-DCGAN can realize the close connection of features, so that the network can use the feature information from different levels more effectively, and enhance the ability to extract detailed features. At the same time, the introduction of SENet optimizes the channel incentive mechanism and makes the network focus more on important features by adaptively adjusting the weight of the feature map. This channel attention mechanism significantly improves the ability of the generator and discriminator to respond to key features, thereby reducing unnecessary computational overhead while maintaining image quality. Compared with traditional DCGAN, DS-DCGAN has been optimized by deep learning technology to reduce the computational complexity and improve the overall operating efficiency.

III. Landscape Image Restoration based on Improved DCGAN

To improve the restoration effect of landscape images, the DCGAN is first introduced to generate clear landscape images. Secondly, a new generative network is generated by combining DenseNet and SENet, and DCGAN is used as the discriminative network to compensate for the insufficient feature extraction of traditional DCGAN models in repairing landscape images.

A. Design of Landscape Image Restoration Algorithm Based on DCGAN

GAN is a deep learning model proposed in 2014, which introduces two networks, namely a generator and a discriminator, so that these two networks compete with each other during the training process to generate realistic data [13]. The generator is to produce fake data that is close to the true data distribution. It obtains a random noise vector as input and outputs a data point with the same dimension as the training data. The discriminator is to distinguish whether the input data is real or generated by a generator. It can receive data produced by the generator or real data as input and output a probability value to represent the probability that the input data is real. The GAN is displayed in Fig. 1.

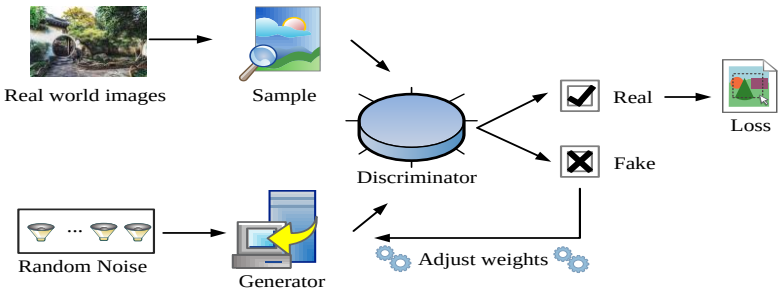


Fig. 1. GAN structure.

In Fig. 1, when training GAN, the generator first receives a random noise vector as input, and then uses this noise to generate a fake image, with the aim of making this image visually indistinguishable from the real image. Next, the discriminator may receive a fake image or a real image generated by the generator, and output a probability value to determine whether the image is real or produced by the generator. Through this adversarial learning, the generator gradually improves its ability to generate high-quality fake images to deceive the discriminator. The discriminator is constantly improving its accuracy in distinguishing between real and fake images. The dynamic confrontation between the two drives the continuous improvement of their performance until the generator can generate images that are almost unrecognizable as fake by the discriminator, while the discriminator accurately identifies the real and generated images as much as possible. The objective loss function of GAN is displayed in Eq. (1) [14-15].

$$\min_G \max_D V(D,G) = E_{x\sim p_{data}}[\log D(x)] + E_{z\sim p_z(z)}[\log(1-D(G(z)))] \quad (1)$$

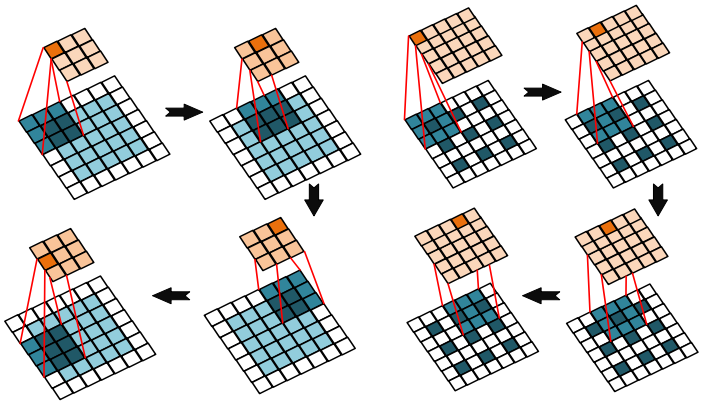
In Eq. (1), G signifies the generator. D signifies the discriminator. z represents noise. x and $G(z)$ signify real samples and produced samples. $D(x)$ and $G(x)$ signify the discriminant function and the generative function, respectively. E represents the expected value. p_{data} and $p_z(z)$ represent the real and the produced distributions. $D(G(z))$ signifies the probability that D will distinguish the data generated by G as real samples. According to Eq. (1), to train GAN, G and D are trained separately. The training process of D is shown in Eq. (2).

$$\max_D V(D,G) = E_{x\sim p_{data}}[\log D(x)] + E_{z\sim p_z(z)}[\log(1-D(G(z)))] \quad (2)$$

In Eq. (2), the meanings of x and z are the same as those in Eq. (1). At this point, if D can recognize x as a true sample, then the value of $\log D(x)$ will be larger. Similarly, if D can identify $G(z)$ as a false sample, then the value of $\log(1-D(G(z)))$ will also be as large as possible. When the values of $\log D(x)$ and $\log(1-D(G(z)))$ are both larger, D remains unchanged and G is trained to confuse D. Similarly, when training G, it is hoped that D in GAN cannot recognize false samples. The training process of G is displayed in Eq. (3).

$$\min_G V(D,G) = E_{z\sim p_z(z)}[\log(1-D(G(z)))] \quad (3)$$

In Eq. (3), the closer the $D(G(z))$ is to 1, the smaller the training value of the entire G. DCGAN is a special type of GAN that combines the advantages of GAN and convolutional neural networks. Convolutional layers are used to construct generators and discriminators, enabling the network to obtain local and global features and generate more refined and realistic images. Firstly, in DCGAN, stride convolution is used in the discriminator to reduce image size, while fractional stride convolution is used in the generator to increase image size. Two convolution methods are shown in Fig. 2.



(a) Stride convolution (b) Fractional stride convolution

Fig. 2. The convolution processes of stride convolution and fractional stride convolution.

Fig. 2(a) and 2(b) show the convolution processes of stride convolution and fractional stride convolution, respectively. In Fig. 2(a), stride convolution reduces the output feature map size by setting the convolutional kernel movement step size. In ordinary convolution operations, the convolution kernel typically slides over the input feature map at stride of 1, resulting in output feature maps of the same size. However, by setting a larger stride value, such as 2 or 3, the convolution kernel will skip multiple pixels each time it slides on the input feature map, effectively reducing its size. This operation not only reduces computational complexity, but also has a down-sampling effect to some extent, allowing subsequent layers to process smaller feature maps, and improving the efficiency of the network. In Fig. 2(b), fractional stride convolution, also known as transpose convolution or deconvolution. This type of convolution is applied to increase the size of the output feature map. Unlike stride convolution, fractional stride convolution inserts zero padding before the convolution operation, allowing the convolution kernel to produce larger output feature maps than the original size when sliding on the input feature map. This operation essentially involves inserting blank spaces between input feature maps, and then performing standard convolution on the expanded image to increase its size. The DCGAN structure combining these two convolution operations is shown in Fig. 3.

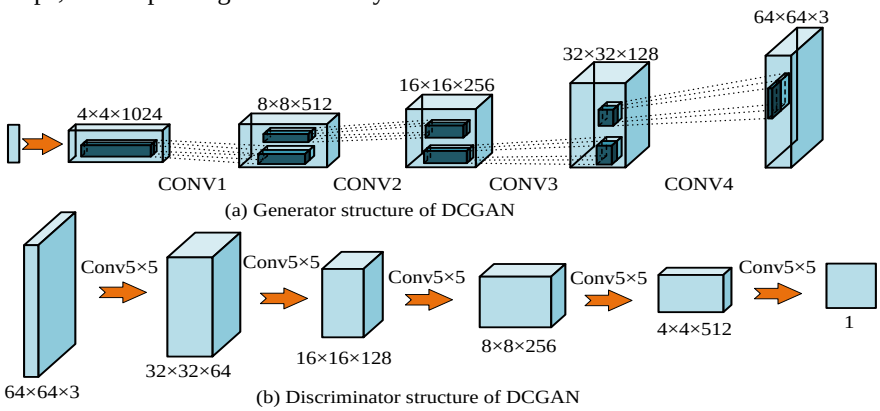


Fig. 3. DCGAN structure diagram.

The DCGAN in Fig. 3 consists of two main parts, namely the generator in Fig. 3(a) and the discriminator in Fig. 3(b). Among them, the former produces fake images. The later distinguishes between real images and generated fake images. The process of using DCGAN for image restoration includes the following key steps. Firstly, the generator takes a random noise vector as input and gradually enlarges the feature map through fractional stride convolutional layers, converting the noise into a fake image. Secondly, the discriminator will receive fake and real images generated by the generator, gradually reduce the size of the feature map through stride convolution layers, extract key features of the image, and output a probability value to represent the possibility that the input image is a real image. In this process, the generator and discriminator are continuously optimized through adversarial training. The generator attempts to generate increasingly realistic images to deceive the discriminator. The discriminator continuously distinguishes between real and fake images. After multiple rounds of iterative training, the generator is able to generate high-quality and realistic images, achieving the image restoration.

B. Construction of an Optimized DCGAN Model Combining DenseNet and SENet

Although DCGAN has better image feature extraction capabilities compared with GAN, there are still some shortcomings in using DCGAN for landscape design image restoration, such as unstable image quality, easy pattern collapse, high training difficulty, and poor feature extraction of some landscape images [16-17]. To address these issues, the DenseNet is combined with SENet to optimize the DCGAN. The structure of DenseNet is shown in Fig. 4.

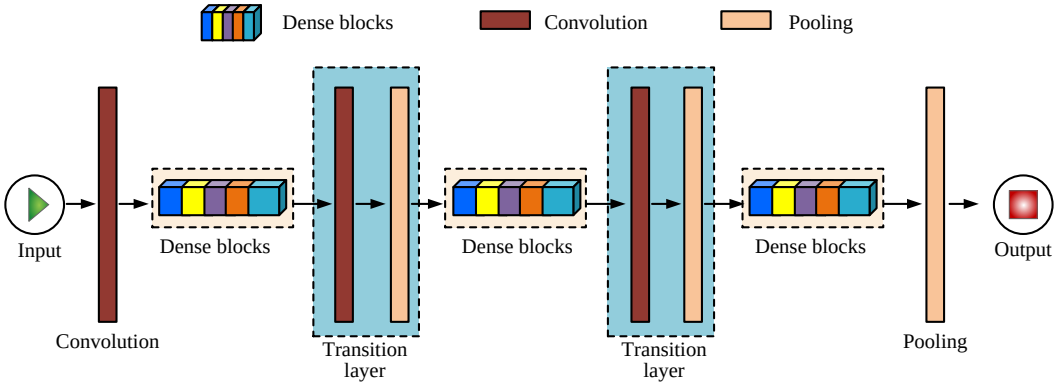


Fig. 4. DenseNet structure diagram.

The DenseNet in Fig. 4 is an innovative CNN structure characterized by the added densely connected modules. DenseNet consists of multiple dense convolutional blocks and transition layers. The layers in each dense convolutional block are directly connected to each other, meaning that the output of each preceding layer is the input of all subsequent layers. This design not only efficiently utilizes feature information, but also alleviates the gradient vanishing, thereby improving network performance. Another significant feature of DenseNet is to implement down-sampling through transition layers. The bottleneck layer in the transition layer can remove redundant information by reducing the number of feature maps, thereby reducing computational complexity and decreasing the parameters. x_0 represents the feature map obtained after convolution processing, which is the input of the dense convolution block to obtain the l-th layer output, as shown in Eq. (4) [18-19].

$$x_l = H_l\left(\left[x_0, x_1, \cdots, x_{l-1}\right]\right) \tag{4}$$

In Eq. (4), $H_l(\cdot)$ represents the transformation function of the l-th layer. $[x_0, x_1, \cdots, x_{l-1}]$ signifies the feature input composed of feature maps from layer 0 to $l-1$. x_l signifies the output of the l-th layer. In addition to using DenseNet to optimize the parameters of DCGAN and reduce the frequency of gradient vanishing, the study also adds SENet module to enhance channel sensitivity and lightweight the DCGAN structure. The SENet is displayed in Fig. 5.

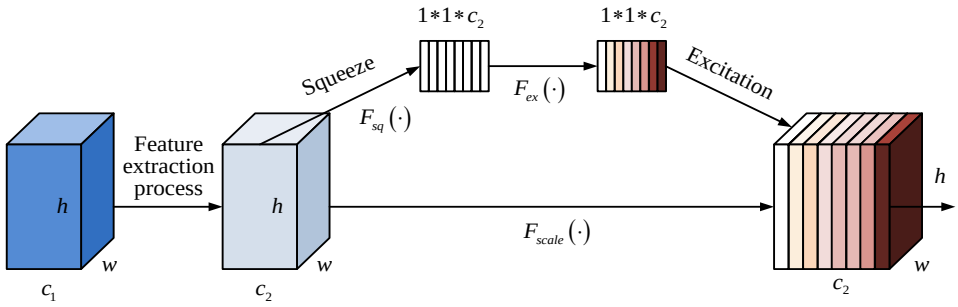


Fig. 5. SENet structure diagram.

In Fig. 5, the key component in the SENet structure is the excitation module, which can perform Squeeze and Excitation operations on the feature maps of the convolutional layer. Firstly, the feature map is compressed into a single value through global average pooling, which represents the global spatial information of the entire feature map. Then, this value is passed through a Fully Connected Layer (FCL) and ReLU function is used to learn the interrelationships between channels. Finally, this value through another FCL, and the Sigmoid is applied to output the weights of each channel. These weights will be used to re-weight the channels of the original feature map. The weights obtained through the incentive module will be multiplied with the corresponding channels to achieve feature re-calibration. After the above processing, the network can adaptively emphasize important features and suppress unimportant features. In the Squeeze operation, the original image feature size is $H*W*C$, where H, W, and C signify the height, width, and channels. Each channel is subjected to a global mean pooling operation to obtain a compressed feature map, which not only has a global receptive field but also has a size of $1*1*C$. The Squeeze operation is shown in Eq. (5).

$$z_c = F_{sq}\left(u_c\right) = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W} u_c\left(i, j\right) \tag{5}$$

In Eq. (5), z_c signifies the compressed feature map. u_c represents the feature map extracted by convolution operation. $F_{sq}(\cdot)$ represents the feature compression function. i and j represent the horizontal and vertical axes of the feature map, respectively. The expression for the Excitation operation is shown in Eq. (6).

$$s_c = F_{ex}\left(z, W'\right) = \sigma\left(g\left(z, W'\right)\right) = \sigma\left(W_2 \operatorname{Re} LU\left(W_1 z\right)\right) \tag{6}$$

In Eq. (6), s_c represents the weight coefficient with attention mechanism. $F_{ex}(\cdot)$ represents the characteristic excitation function. z represents the compressed feature map. g represents the gating function. σ represents the reshape function. W', W_1 and W_2 respectively represent the weight coefficients of the attention mechanism, the first FCL, and the second FCL. The weight coefficients obtained through Squeeze and Excitation operations are applied to each channel, as shown in Eq. (7).

$$x_c = F_{scale}\left(u_c, s_c\right) \tag{7}$$

In Eq. (7), $F_{scale}(\cdot)$ represents the feature re-scaling function. x_c represents the weight coefficients applied to each channel. The DCGAN optimized by combining DenseNet and SENet is referred to as DS-DCGAN, and its structure is shown in Fig. 6.

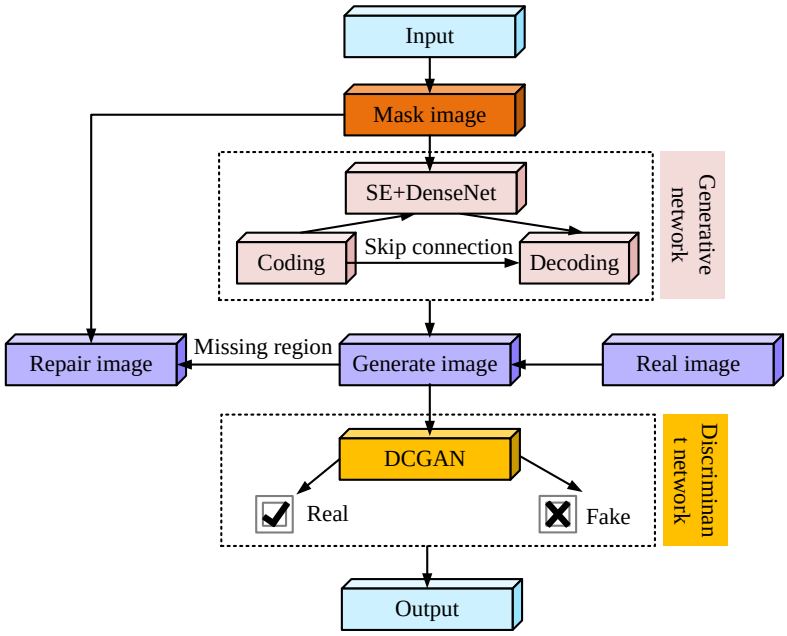


Fig. 6. DS-DCGAN structure.

In Fig. 6, the entire DS-DCGAN structure has the generator and the discriminator. DenseNet organizes the convolutional layers in a densely connected manner, meaning that each layer is directly connected to all the layers above it. In the generator, this dense connection can effectively transmit feature information, reduce information loss, and enable the network to better retain detailed features when generating images. The structure of DenseNet effectively alleviates the common phenomenon of gradient disappearance in deep networks. Since each layer is directly connected to the others, gradients can be passed more smoothly through the layers, ensuring that the generator can quickly learn effective feature representations during training. In the discriminator, by connecting the features of the front layer with the back layer, DenseNet can maximize the use of the features extracted from the front layer and form a stronger feature representation to judge the authenticity of the image. This enhanced feature utilization capability greatly improves the performance of the discriminator, which can more accurately distinguish the real image from the generated image. SENet enables the network to adaptively re-calibrate each channel by introducing a channel attention mechanism. Specifically, SENet acquires a global feature representation for each channel through global average pooling and generates channel weights through two fully connected layers. These weights are used to realign the importance of each channel in the input feature map. In the generator, the introduction of SENet enables the generated images to better highlight important feature channels, thus making the details of the generated images richer and more realistic. In the discriminator, SENet can effectively enhance the perception of key feature channels, making the discriminator pay more attention to the key features that may distinguish between real and generated images. SENet reduces the computational complexity and avoids the processing of meaningless features by cutting out unimportant feature channels. This not only improves computational efficiency, but also helps reduce overfitting and improves the network's ability to generalize on unseen data. In the DS-DCGAN structure, the loss function during training is shown in Eq. (8).

$$Loss_{train} = \lambda_{MSE} L_{MSE} + \lambda_{adv} L_{adv} + \lambda_{TV} L_{TV} \quad (8)$$

In Eq. (8), $Loss_{train}$, L_{MSE}, L_{adv}, and L_{TV} respectively represent the training set loss function, Mean Squared Error (MSE) function, adversarial loss function, and total variation loss function. λ_{MSE}, λ_{adv} and λ_{TV} represent the weights corresponding to the MSE function, adversarial loss function, and total variation loss function, respectively. The L_{MSE} is displayed in Eq. (9).

$$L_{MSE} = \left(x - G\left(M \otimes x\right)\right)^2 \quad (9)$$

In Eq. (9), M represents the binary mask. $\otimes$ represents multiplication between corresponding elements, while the meanings of other parameters remain consistent with those mentioned earlier. The L_{adv} is shown in Eq. (10).

$$L_{adv} = \log\left(D\left(x\right)\right) + \log\left(G\left(M \otimes x\right)\right) \quad (10)$$

In Eq. (10), the meanings of each parameter remain consistent with the previous text. The L_{TV} is shown in Eq. (11).

$$L_{TV} = \sum_{i,j} \left| G_{i+1,j}\left(M \otimes x\right) - G_{i,j}\left(M \otimes x\right) \right| + \left| G_{i,j+1}\left(M \otimes x\right) - G_{i,j}\left(M \otimes x\right) \right| \quad (11)$$

In Eq. (11), i and j still represent the horizontal-axis and longitudinal-axis of the feature map. The test set loss function is shown in Eq. (12).

$$L_{val} = \lambda_{context} L_{context} + \lambda_{prior} L_{prior} \quad (12)$$

In Eq. (12), L_{val}, $L_{context}$, and L_{prior} represent the training set loss function, text loss function, and prior loss function, respectively. $\lambda_{context}$ and λ_{prior} represent the weights of $L_{context}$ and L_{prior}, respectively.

IV. Restoration Effect Testing of Landscape Design Images based on DS-DCGAN

To exhibit the effectiveness of the DS-DCGAN model, the study selects DCGAN, Generative Adversarial Network-variant (GAN-variant), and Conditional GAN (CGAN) as comparison models. The benchmark performance and actual application effects of the four models are compared.

A. DS-DCGAN Model Benchmark Performance Testing

To validate the benchmark performance of the DS-DCGAN, two publicly available datasets for landscape architecture and landscape image restoration are selected for testing. Among them, the Places2 dataset contains over 10 million images of various natural scenes and buildings, widely used for image restoration and generation tasks. The Paris StreetView dataset contains high-resolution images of street view buildings, suitable for evaluating the performance of models in landscape architecture and landscape image restoration. The two datasets are separated into training and testing sets in an 8:2 to comprehensively assess the effectiveness and robustness in different types of image restoration tasks. The loss function value is used as a criterion to determine the stability of the model. The stability of the four models in two datasets is shown in Fig. 7.

Fig. 7(a) and 7(b) show the loss curves of CGAN, DCGAN, GAN-variant, and DS-DCGAN models. According to Fig. 7(a), CGAN, DCGAN, GAN-variant, and DS-DCGAN reached a stable state after 325, 278, 251, and 216 iterations, respectively. Similarly, in Fig. 7(b), CGAN, DCGAN, GAN-variant, and DS-DCGAN also reached a stable state after 296, 268, 223, and 172 iterations, respectively. Based on the two sub-graphs in Fig. 7, DS-DCGAN can iterate to a stable state faster compared with the other three comparison models, indicating its high training efficiency and strong adaptability of the model. The average time consumption of the four models in the decoding and encoding process is compared, as shown in Fig. 8.

Fig. 8(a) and 8(b) show the average encryption time and average decryption time of the four models during the training process, respectively. Based on Fig. 8, the CGAN model during training was 0.63 and 0.70, respectively. Its encryption and decryption process took the longest time, far higher than the DS-DCGAN model. In addition, the GAN-variant model was 0.35, the DCGAN model was 0.46 and 0.48, respectively, and the DS-DCGAN model was 0.21 and 0.19, respectively. Overall, the DS-DCGAN model has the shortest encryption and decryption time and the highest processing efficiency in image processing. The MSE and Mean Absolute Error (MAE) during the training process are displayed in Fig. 9.

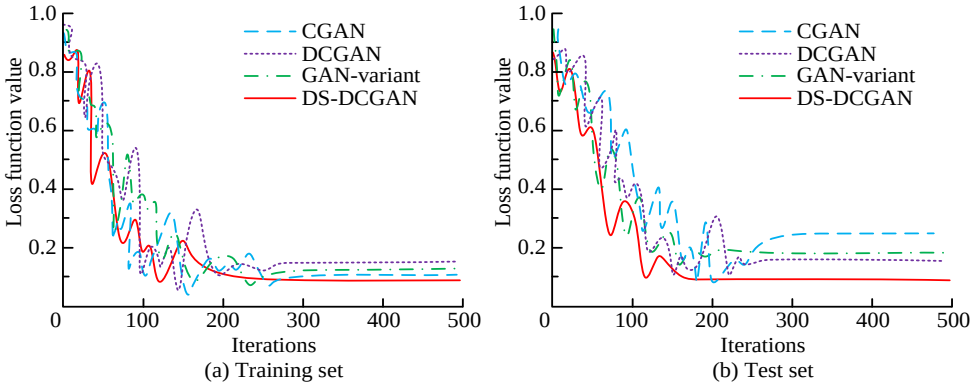


Fig. 7. Loss curve iteration of different models in two datasets.

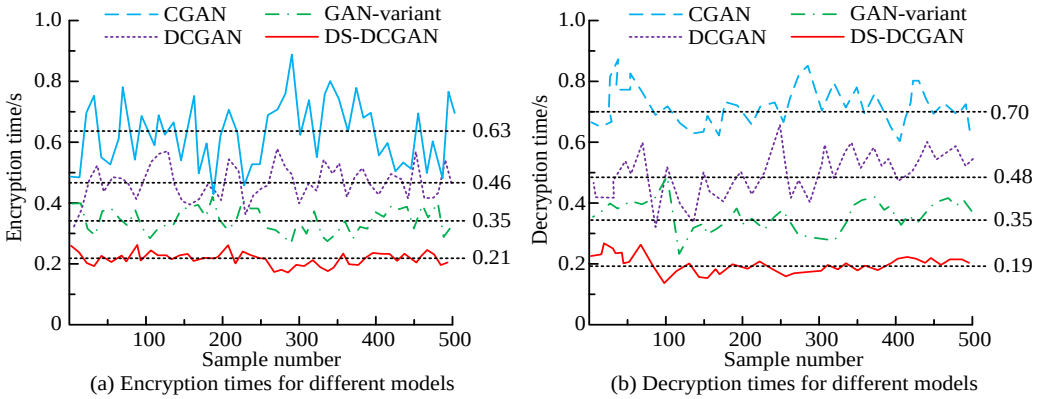
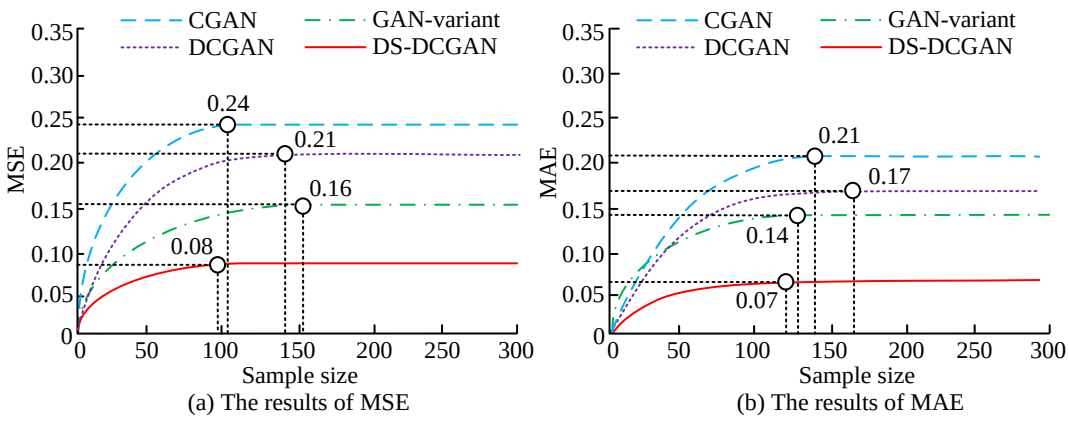


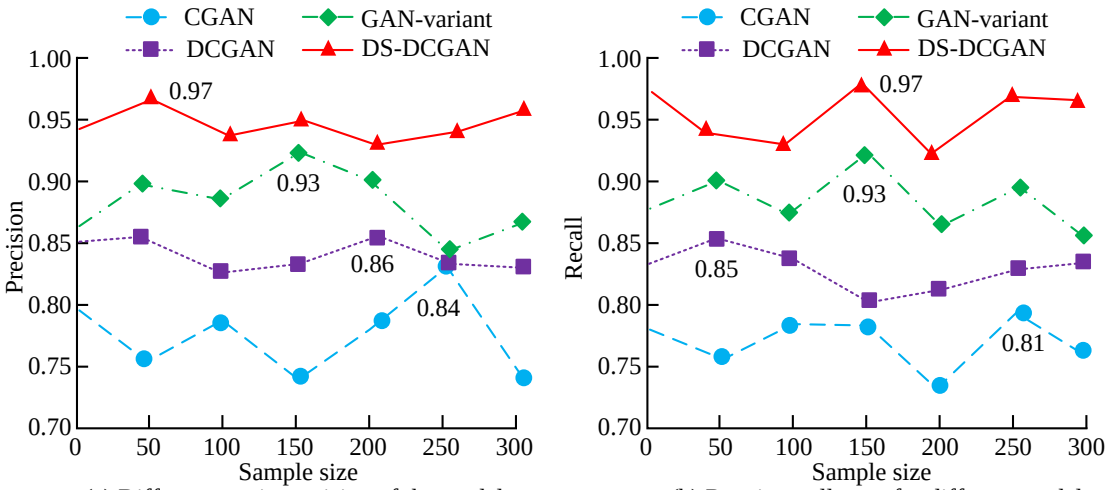
Fig. 8. Average encryption time and decryption time of various models.



(a) The results of MSE (b) The results of MAE

Fig. 9. Error representation of different models.

Fig. 9(a) and Fig. 9(b) respectively show the MSE and MAE values of the four models. MSE is a common index to measure the difference between the restored image and the real image, and is defined as the average of the square of the difference between the pixel values of the corresponding position of the restored image and the original image. MAE is another measure of the difference between the recovered image and the real image, and it is the average of the absolute values of the difference between the pixel values. According to Fig. 9(a), the MSE values of CGAN, DCGAN, GAN-variant, and DS-DCGAN models after reaching stability were 0.24, 0.21, 0.16, and 0.08, respectively. According to Fig. 9(b), the MAE values of CGAN, DCGAN, GAN-variant, and DS-DCGAN models after reaching stability were 0.21, 0.17, 0.14, and 0.07, respectively. Overall, the DS-DCGAN model performs better in terms of error during training, with lower MSE and MAE values. The repair precision and recall values during the training are compared, as displayed in Fig. 10.



(a) Different repair precision of the model (b) Repair recall rates for different models

Fig. 10. Repair precision and repair recall rate of different models.

Fig. 10(a) and Fig. 10(b) respectively show the repair accuracy and repair recall rate of CGAN, DCGAN, GAN-variant and DS-DCGAN. The repair accuracy is used to evaluate the accuracy of images recovered by the model, and it represents the ratio of the number of pixels successfully recovered to the total number of pixels. The repair recall rate reflects the ability of the model to identify and recover the actual damaged part, and it represents the ratio of the true positives of successful recovery to the actual damaged part. In Fig. 10(a), the maximum repair precision of CGAN, DCGAN, GAN-variant, and DS-DCGAN was 0.84, 0.86, 0.93, and 0.97, respectively. In Fig. 10(b), the maximum repair recall rate of CGAN, DCGAN, GAN-variant, and DS-DCGAN was 0.81, 0.85, 0.93, and 0.97, respectively. From this, the benchmark performance test results of DS-DCGAN are good, which has high repair precision and recall.

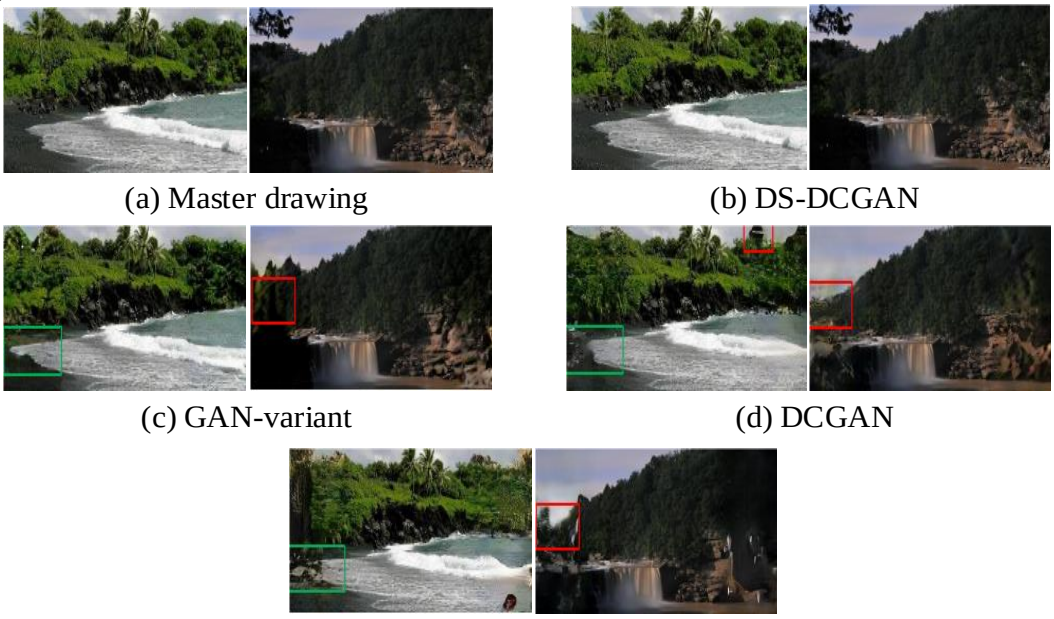
B. *Application Effect Analysis of DS-DCGAN in Landscape Design Image Restoration*

In addition to comparing the benchmark performance of several models, the study also applies four models to practical problems. The application effects in landscape design image restoration are compared. Four different styles of landscape images are selected as the research objects. The restoration time and accuracy of four models for restoring these four real landscape images are obtained, as shown in Table I.

TABLE I. ACTUAL REPAIR EFFECT OF THE MODEL

Image Type	Evaluation index	CGAN	DCGAN	GAN-variant	DS-DCGAN
Image 1	Repair time /s	0.36	0.21	0.14	0.08
	Repair accuracy rate /%	88.23	91.05	95.18	98.15
Image 2	Repair time /s	0.31	0.23	0.18	0.11
	Repair accuracy rate /%	89.94	92.10	96.65	98.57
Image 3	Repair time /s	0.25	0.16	0.09	0.06
	Repair accuracy rate /%	89.69	92.17	95.04	99.03
Image 4	Repair time /s	0.41	0.30	0.24	0.15
	Repair accuracy rate /%	85.74	89.43	93.38	97.96

According to Table I, the repair time for four images using the DS-DCGAN model was controlled within 0.20s, with a minimum of 0.06s required to complete the repair work. At the same time, the accuracy of repairing images 1, 2, 3, and 4 based on the DS-DCGAN model was higher than that of comparison models, reaching 98.15%, 98.57%, 99.03%, and 97.96%, respectively. Among the four models, the CGAN model has the worst performance in practical applications, with a repair time of up to 0.41s and a repair accuracy of only 85.74%. The restoration effects of four models on real landscape images are further compared, as shown in Fig. 11.



(a) Master drawing (b) DS-DCGAN

(c) GAN-variant (d) DCGAN

(e) CGAN

Fig. 11. Actual restoration effects of landscape design images under different models.

Fig. 11 shows the effectiveness of four models in restoring actual landscape design images. Based on Fig. 11, the CGAN, DCGAN, and GAN-variant models all generated features that did not match the original image when repairing images, while DS-DCGAN fully restored the true situation of the actual image without problems such as feature transfer or feature duplication. Overall, DS-DCGAN has the best restoration effect in practical applications. Based on the analysis of experimental results, the performance of the research method is shown in Table II.

TABLE II. PERFORMANCE RESULTS OF DS-DCGAN MODEL

Model	Repair accuracy (%)	Repair recall rate (%)	MSE	MAE	Average repair time (s)
CGAN	84	81	0.24	0.21	0.63
DCGAN	86	85	0.21	0.17	0.46
GAN-variant	93	93	0.16	0.14	0.35
DS-DCGAN	97	97	0.08	0.07	0.19

In Table II, DS-DCGAN's repair accuracy and recall rate are both as high as 97%, demonstrating excellent capabilities in detail recovery and extraction of important data. The high repair accuracy and recall rate indicate that DS-DCGAN is able to

capture critical information in images more comprehensively, thus providing more reliable image recovery results. DS-DCGAN has a MSE and MAE of 0.08 and 0.07, respectively, which are the lowest of all models and significantly reduce errors during image recovery. This shows that DS-DCGAN is able to reconstruct the original image more accurately, retaining more detailed information. The average repair time of DS-DCGAN is 0.19 seconds, which makes DS-DCGAN have good real-time performance in practical applications, especially suitable for scenarios that require fast recovery. The results show that DS-DCGAN provides higher recovery accuracy and speed, and provides effective support for practical applications that need to process high-definition images or large-scale data sets. Using DenseNet and SENet structure optimization, the model not only shows strong ability in processing complex image features, but also reduces the computational complexity after training, which lays a good foundation for the subsequent model iteration and application.

V. Discussion

In the above experimental results, the improved DCGAN model has a good performance and has obvious advantages in the field of image restoration. Therefore, this method also has certain application potential in other fields. In medical imaging, medical imaging technology is highly dependent on image quality. Images are often distorted by noise, motion artifacts, or equipment limitations. By applying the improved DCGAN model, damaged medical images can be effectively restored, enhancing the contrast and detail of the images, thereby helping doctors obtain more accurate diagnoses. DS-DCGAN can be used to process noise reduction and enhance image quality, improving the recognition and classification accuracy of pathology images, which is essential for early diagnosis. In medical image analysis, DS-DCGAN can be used to generate diverse training samples, help train other deep learning models, and promote the accuracy of cancer lesion detection or tissue classification. By generating high-quality composite images, the sample pool can be increased, helping to reduce overfitting and training time for the model. Medical imaging systems usually produce a large number of scanned images. As time goes on, storing and managing these images becomes increasingly important. DS-DCGAN can help digitally preserve expired and damaged medical images, making important historical medical records and records continuously accessible and usable.

In terms of digital heritage protection, many important historical documents, artworks and images of cultural assets face wear and degradation. DS-DCGAN can be used to effectively repair these damaged images, improve their visual effect, and help retain historical information and cultural memory. The improved DCGAN model can be applied in 3D reconstruction to generate 3D assets with a high degree of detail by restoring flat images. In addition, this restoration method can be combined with augmented reality technology to provide visitors with a more vivid experience of cultural heritage. In a virtual museum or exhibition, DS-DCGAN is capable of recreating historical scenes to provide a more immersive and informative presentation.

In other potential areas, such as in film and television post-production, it is often necessary to recover damaged footage or enhance the details of a scene. DS-DCGAN helps production teams quickly fix scenes and generate additional effects, saving processing time and money. In security monitoring, the images captured by cameras are often difficult to provide effective information because of insufficient illumination and blurred motion. DS-DCGAN applications improve the clarity of surveillance images and help analyze and identify potential security threats. In the intelligent traffic management system, DS-DCGAN can optimize traffic monitoring images and recover important road condition information. This can enhance the real-time processing of images and optimize the management and control of traffic flow.

VI. Conclusion

In order to effectively restore landscape design images, a landscape design image restoration model was constructed by combining DenseNet, SENet, and DCGAN. Compared with DCGAN, GAN-variant, and CGAN, the results showed that DS-DCGAN maintained stability after 216 iterations in the training set and 172 iterations in the testing set, with faster iteration speed. In addition, the MSE and MAE of DS-DCGAN were the smallest in stable state, which were 0.08 and 0.07, respectively, indicating that the algorithm had low error. The repair accuracy and recall rate of four algorithms were tested. It was found that the repair precision and recall rate of DS-DCGAN were both as high as 0.97, indicating that this method could better preserve the detailed information during the repair process. In practical applications, the average repair accuracy of this model was as high as 99.03%, and the average repair time was as low as 0.06s. From this, the proposed DS-DCGAN model has good repair performance and application effectiveness. By introducing an improved DCGAN model and combining DenseNet and SENet, a new approach is provided to process and restore landscape design images. This method not only improves the ability of feature extraction, but also significantly improves the accuracy and efficiency of image recovery. The implementation and results of the research will have a profound impact on related fields. Landscape design image restoration can provide more accurate data support for urban planning and management, and help decision makers to better carry out land planning, environmental management and public facilities layout. It provides a new methodology and direction for the field of image restoration, promotes academic accumulation in the field, and promotes the expansion of subsequent research into more complex and diverse image processing tasks. At the same time, due to the complexity of landscape design images and the diversity of their damage types, subsequent research can analyze more types of damaged image restoration. As a result, follow-up studies can add repair analysis for more types of damaged images. At the same time, multiple approaches can be explored to further generalize and adapt the DS-DCGAN model to different types of image restoration tasks. For example, exploring the application of DS-DCGAN to multimodal image restoration, such as combining different types of medical imaging to achieve more comprehensive image restoration; DS-DCGAN is extended to video processing and dynamic scene recovery to improve the image quality under the condition of motion blur and motion

artifact. DS-DCGAN is applied to super-resolution reconstruction tasks, especially scenarios where high-resolution images are recovered from low-resolution images. By exploring these directions in depth, the DS-DCGAN model can not only meet the needs of challenging image restoration, but also show greater value in diverse fields.

REFERENCES

[1] Yang G, Wei W, Pan Z. A Variational neural network for image restoration based on coupled regularizers. Multimedia Tools and Applications, 2024, 83(4): 12379-12401.

[2] Luo Q, Liao Y, Jing B, Gao X, Chen W, Tan K. Hir-net: a simple and effective heterogeneous image restoration network. Signal, Image and Video Processing, 2024, 18(1): 773-784.

[3] Saminu S, Xu G, Zhang S, Kader IAE, Aliyu HA, Jabire AH, Ahmed YK, Adamu MJ. Applications of Artificial Intelligence in Automatic Detection of Epileptic Seizures Using EEG Signals: A Review. Artificial Intelligence and Applications, 2023, 1(1): 11-25.

[4] Mao L, Wang M, Yang D, Zhang R. Mutual learning generative adversarial network. Multimedia Tools and Applications, 2024, 83(3): 7479-7503.

[5] Skandarani Y, Lalande A, Afilalo J, Jodoin P M. Generative adversarial networks in cardiology. Canadian Journal of Cardiology, 2022, 38(2): 196-203.

[6] Pan J, Dong J, Liu Y, Zhang J, Ren J, Tang J, Yang M H. Physics-based generative adversarial models for image restoration and beyond. IEEE transactions on pattern analysis and machine intelligence, 2020, 43(7): 2449-2462.

[7] Liu G, Li X, Wei J. Large-area damage image restoration algorithm based on generative adversarial network. Neural Computing and Applications, 2021, 33(10): 4651-4661.

[8] Deng Z, Cai Y, Chen L, Gong Z, Bao Q, Yao X, Ma L. Rformer: Transformer-based generative adversarial network for real fundus image restoration on a new clinical benchmark. IEEE Journal of Biomedical and Health Informatics, 2022, 26(9): 4645-4655.

[9] Yang J, Liu J, Han R, Wu J. Generating and restoring private face images for internet of vehicles based on semantic features and adversarial examples. IEEE Transactions on Intelligent Transportation Systems, 2021, 23(9): 16799-16809.

[10] Ma H, Liu D, Wu F. Rectified wasserstein generative adversarial networks for perceptual image restoration. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, 45(3): 3648-3663.

[11] Kumar P, Gupta V. Restoration of damaged artworks based on a generative adversarial network. Multimedia Tools and Applications, 2023, 82(26): 40967-40985.

[12] Liang M, Zhang Q, Wang G, Xu N, Wang L, Liu H, Zhang C. Multi-scale self-attention generative adversarial network for pathology image restoration. The Visual Computer, 2023, 39(9): 4305-4321.

[13] Pan X, Zhan X, Dai B, Lin D, Loy C C, Luo P. Exploiting deep generative prior for versatile image restoration and manipulation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021, 44(11): 7474-7489.

[14] Mitrofanov E, Grishkin V. Generative Adversarial Networks Quantization. Physics of Particles and Nuclei, 2024, 55(3): 563-565.

[15] Chen Y, Gao Q, Wang X. Inferential Wasserstein generative adversarial networks. Journal of the Royal Statistical Society Series B: Statistical Methodology, 2022, 84(1): 83-113.

[16] Alghazzawi D M, Hasan S H, Bhatia S. Optimized Generative Adversarial Networks for Adversarial Sample Generation. Computers, Materials & Continua, 2022, 72(2): 3877-3897.

[17] Zhang J, Dong Q, Song W. GGADN: Guided generative adversarial dehazing network. Soft Computing, 2023, 27(3): 1731-1741.

[18] Jafari A, Al-Mousa A, Jafar I. Speaker anonymization using generative adversarial networks. Journal of Intelligent & Fuzzy Systems, 2023, 45(2): 3345-3359.

[19] Kumar P, Gupta V. Restoration of damaged artworks based on a generative adversarial network. Multimedia Tools and Applications, 2023, 82(26): 40967-40985.

Tennis Action Evaluation Model Based on Weighted Counter Clockwise Rotation Angle Similarity Measurement Method

Danni Jiang[1], Ge Liu[2]*
Department of Physical Education, Jinling Institute of Technology, Nanjing, China[1]
Department of Physical Education, Zhongnan University of Economics and Law, Wuhan, China[2]

***Abstract*—In order to intelligently analyze tennis movements and improve evaluation efficiency, a counter clockwise rotation angle of limbs is proposed to solve the direction problem of tennis movements. A dynamic time regularization algorithm is optimized by combining global time weighting and adjacent frame weighting. The results indicated that the proposed counter clockwise rotation angle feature of limbs could effectively represent changes in limb direction and clearly distinguish action postures. The average accuracy of this method in action classification on the Tennis Stroke Dataset was 97.60%. In the action evaluation mode, the average frame rate of the client was between 17.35FPS and 17.49FPS, and the overall average frame rate was about 17.40FPS. The server exhibits higher efficiency in action processing and evaluation, which can process video frames faster. It is more efficient in processing data capabilities and utilizing data resources. This indicates that the performance of the system is relatively consistent in different modes and has stability. The optimized method has a higher generalization ability in recognizing non-tennis movements on different datasets. When dealing with fine movements, the optimized method performs excellently and can better capture subtle differences in the movements. Meanwhile, this enhances the real-time performance of the system, making it suitable for evaluating tennis movements in practical application scenarios. This provides a new technical path for analyzing tennis movements and also serves as a reference for evaluating movements in other sports.**

***Keywords*—Action evaluation; counter clockwise rotation angle; weighting; dynamic time warping; tennis**

I. INTRODUCTION

With the rapid development of artificial intelligence, the combination of computer technology and tennis has become one of the hot topics in the field of sports. As a popular competitive sport, the analysis and evaluation of tennis technique movements are of great significance for athlete training and competition [1]. The Tennis Movement Evaluation System (TME) helps to obtain more accurate match and training data, which can improve athletes' performance and training efficiency, and more scientifically analyze the movement posture during tennis sports [2]. The data representation in tennis videos is in the form of time series. For time series processing, a common task is to compare the similarity between two sequences. Comparing the similarity of time series is more conducive to identifying patterns and trends, which is of great significance for discovering patterns in action data and predicting future behavior. As one of the most important similarity measurement methods in time series analysis, Dynamic Time Warping (DTW) is the process of elongating or shortening unknown variables until they match the length of the reference template. The time axis of unknown data is distorted or bent, so that its feature quantities correspond to the standard pattern. However, traditional action evaluation methods often rely on manual observation and analysis, which have problems such as low efficiency and strong subjectivity [3].

Regarding the evaluation and classification of tennis movements, many researchers have adopted different algorithms and techniques for in-depth optimization, and have achieved certain results. To analyze the performance of the tennis evaluation platform, Wu et al. collected data through wearable devices and selected the Z-score normalized Support Vector Machine (SVM) to classify hitting actions. The accuracy reached 98.4% [4]. Giles et al. proposed a hierarchical clustering method and tennis directional change technique to distinguish tennis movement styles, identify movement features, and analyze temporal movement characteristics such as change speed and directionality. The results showed that this method was feasible [5]. Perri et al. considered the hitting situation in tennis training and used wearable devices and prototype learning to detect different movements to determine exercise load. The results showed that this technology had high accuracy [6]. Wood et al. used Krippendorffs alpha analysis to evaluate the reliability of tennis serve features in 2D videos. This method had high measurement accuracy [7]. Liu et al. extracted different features through the acceleration of the action and the deep mode data. The spatial and temporal convolutional neural network were combined to realize the specific action recognition. The results showed that the accuracy of this method was more than 99% [8]. In order to analyze the trajectory of tennis serve, Hu et al. combined SVM with frame difference technology and median filtering algorithm to locate targets and recognize trajectories. The results showed that the classification accuracy was 97.5% [9]. Perri et al. used wearable GPS devices to record the training serving load for tennis serving information recording. The results showed that this method had good detection performance [10]. Setyawan et al. evaluated the serving movements of athletes of different genders to improve the success rate of serving and evaluate the

differences in tennis serving performance. The results showed that this method was effective [11].

Some scholars have attempted to improve the DTW method in identifying abnormal charging, time series analysis, and image change detection, and have achieved good results. Shuai et al. developed a DTW model with the longest similar substring to identify abnormal charging situations and avoid excessive regularization of DTW for the safety of electric bicycle charging. The average recognition accuracy reached 94% [12]. Deriso et al. proposed a method that combined DTW and iterative refinement techniques to address the trade-off between time regularization characteristics in traditional DTW signal alignment errors. The results showed that this method was feasible [13]. Zhang et al. designed a fast DTW and sequence decomposition method to analyze different components in time series. The time series was decomposed and the similarity between different components was measured. The results showed that this method had high classification accuracy [14]. Xing et al. detected changes in satellite image time series using remote sensing image time series values and DTW to calculate the change amplitude map. The change results were detected in advance. The accuracy was improved by up to 5.10% [15]. Froese et al. proposed two run length encoding time series to improve DTW calculation speed, which shortened the running time and reduced the factors affecting time. The results shows that this method was effective [16]. Kumawat et al. developed a new framework for DTW and adversarial training to enhance the robustness of deep neural networks. Different adversarial examples were created and random alignment paths were implemented. The framework had high efficiency [17]. He et al. proposed Anticor to improve DTW similarity calculation to identify differences between different sequences. The results showed that the algorithm has good practicality [18]. Vorpe et al. introduced non-parametric DTW to capture the leading and trailing relationships between time series for obesity rate prediction. The results showed that this method had good predictive performance [19].

In summary, both the evaluation of tennis movements and the improvement of DTW have shown high accuracy and effectiveness. However, due to the directional information involved in tennis movements and the large computational complexity of DTW, an innovative TME system is developed for this purpose. The feature of Counter Clockwise Rotation Angle (CRA) of limbs is used to quantify and analyze action direction, and global time weighting and adjacent frame weighting are selected to optimize DTW. The research aims to improve computational efficiency and enhance the real-time performance of the system, thereby providing technical support for the field of tennis movement analysis. This study consists of four main parts. Section II is methods and materials. Among them, Part A introduces the physical CRA of tennis actions. The content of Part B is WCRA between adjacent frameworks and global time. Section III is the results of the study. Among them, Part A analyzes the TME system based on WCRA similarity measurement method. Part B introduces the performance analysis of the TME system. Section IV is discussion and conclusion.

II. Methods and Materials

A. Physical CRA of Tennis Actions

Tennis action videos are captured using cameras that can only capture images from one perspective, and these videos are processed and evaluated [20-21]. Considering that tennis courts include both indoor and outdoor environments, factors such as color and lighting affect video images. To cope with environmental impacts, video images need to be preprocessed. This includes adjusting the brightness of the image and performing noise reduction to improve image quality and ensure accuracy in subsequent processing. Monocular cameras can only capture channel information for the red, green, and blue colors of an image, but do not include distance information. Therefore, Two-Dimensional pose estimation is used to identify human skeletal joint points in images, that is, to determine the position information of each joint point. Each joint not only contains positional information, i.e. coordinates, but also semantic information, such as which joint is the shoulder and which is the knee. Simultaneously, the coordinates of joint points are extracted as the basis for subsequent action evaluation [22]. Because tennis movements are dynamic, there may be some joint points obscured in certain frames of the video, which can affect the accuracy of pose estimation. At this point, if the coordinates of the undetected joint point are set as the origin $O(0,0)$, the horizontal and vertical coordinate pair p_i for the i-th joint point is displayed in Eq. (1).

$$p_i(x,y)=\begin{cases} p_i(x,y), & \text{if } p_i \text{ detected} \\ O(0,0), & \text{if } p_i \text{ not detected} \end{cases} \quad (1)$$

Due to significant differences in body shape among individuals, even if two people perform the same action, the overlap rate of their contours may be low, resulting in inaccurate similarity calculation. However, in 2D skeleton nodes, only considering the angle between limbs has certain limitations. Because when the angle between two adjacent limbs formed by three adjacent joints is the same, i.e. $\theta_1=\theta_2$, the actual movement posture is not the same, which cannot accurately describe the movement characteristics [23-24]. The angle and CRA of the tennis movement limbs are shown in Fig. 1.

(a) Action 1 (b) Action 2

Fig. 1. The angle between tennis limbs and CRA.

In the TME system, to overcome the shortcomings of traditional contour overlap rate and simple angle analysis, this study aims to more accurately describe and evaluate human movements by combining directional information of limb angles. The CRA of the right wrist-right elbow-right shoulder in Fig. 1 (a) is denoted as α_1. The CRA of the right wrist-right

elbow-right shoulder in Fig. 1 (b) is denoted as α_2. The difference between angles α_1 and α_2 is obvious and will not be confused, so the CRA is used to more accurately describe the angle and human posture of the angle. The angle value range of CRA is between 0° and 360°. According to the cosine theorem, the angle between two vectors is calculated. Then, the vector product is used to determine their positional relationship [25]. The tennis movements exclude detailed changes in the head. The distribution of joint points and CRA in the limbs is shown in Fig. 2.

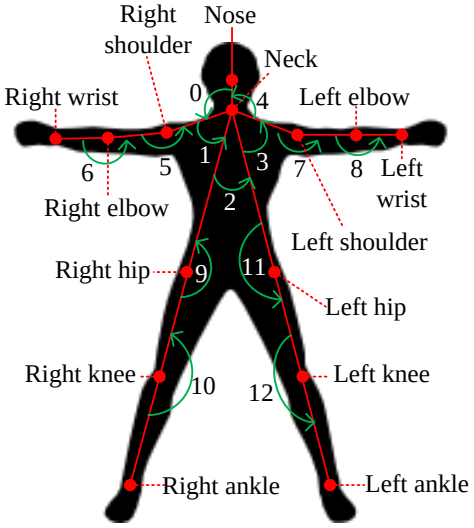


Fig. 2. Schematic diagram of limb joint points and CRA distribution.

In Fig. 2, there are 14 joint points in the limbs. In the template video, OpenPose is used to detect the human joint points of each frame image of two random tennis movements, obtaining 13 limb CRAs. The function of OpenPose is real-time multi person pose estimation and keypoint detection, which can detect the 2D poses of multiple people in images or videos in real time. It is suitable for single person and multi-person scenes and has excellent robustness. The input image or video uses a pre-trained model to identify key points in the human body, including the head, shoulders, elbows, wrists, hips, knees, and other key positions. By identifying and connecting these key points, OpenPose can generate a complete multi-person pose estimation result, thereby recognizing human actions [26-27]. The definition of partial limb CRA is displayed in Table I.

TABLE I. DEFINITION OF LIMB CRA

RA number	Joint number representation	CRA
0	0-1-2	Nose-neck-right shoulder
1	2-1-8	Left shoulder-neck-nose
2	8-1-11	Right Shoulder-neck-right Hip
3	11-1-5	Right Hip-neck-left Hip
4	5-1-0	Left Hip-neck-left Shoulder
5	3-2-1	Right elbow-right shoulder-neck

B. WCRA Between Adjacent Frames and Global Time

In tennis, athletes' movements and scenes change very quickly. Single frame real-time evaluation can quickly adapt to these changes, update evaluation results in a timely manner, and ensure accurate evaluation and feedback in dynamic scenes. Meanwhile, real-time processing of single frame data requires relatively less computation and can effectively utilize computing resources. Compared with processing the entire video stream, single frame evaluation can distribute the computational burden, avoid delays and lags, and ensure the real-time and smooth performance of the system [28]. The single frame evaluation is displayed in Fig. 3.

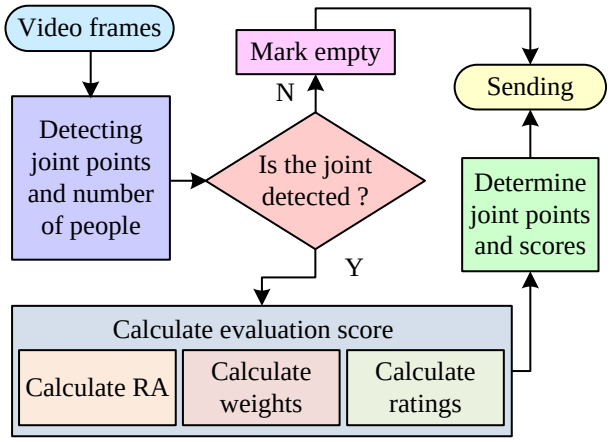


Fig. 3. Flowchart of single frame evaluation.

In Fig. 3, after inputting video frames with a resolution of 656×368, joint points and number of people are detected. If a joint is detected, the evaluation score is calculated from the Rotation Angle (RA), weight, and score to determine the joint points and score. If no joints are detected, it is marked as blank. To facilitate the evaluation of tennis movements in single frame videos, the frame rate of the template video and the input video are set to be the same [29]. The relationship between RA in various limbs of the human body is analyzed to obtain evaluation scores for each frame. The similarity score s_t of t-th frame has a value range of [0, 1], as shown in Eq. (2).

$$s_t = 1 - \frac{\sum_{i=1}^{n} W_i \left| \Delta \alpha_i^t \right|}{C} \tag{2}$$

In Eq. (2), n is the number of RAs. $\Delta \alpha_i^t$ is the difference between the t-th frame input video and the i-th RA of template video. C is the maximum value of RA. When s_t, it indicates that the actions of the template and the input video are completely consistent. When s_t is 0, it indicates that the actions of the template and the input video are completely different. The weight W_i for the i-th RA is expressed as Eq. (3).

$$W_i = aW_i^{\sigma} + bW_i^{\tau} \tag{3}$$

In Eq. (3), a and b are both parameters, with a value of 0.5. W_i^{σ} is the inter frame RA weight of i-th RA input video

actions. W_i^{τ} is the global time RA weight of the template video action for the i -th RA. To analyze TME more comprehensively, the study considers the action situation of the input video. Adjacent Frame Weighting (AFW) focuses on the change details between adjacent frames in the action sequence, which can capture small changes in the action and enhance the matching precision [30-31]. During the DTW process, weight allocation is performed on adjacent frame pairs. AFW considers the changes and interrelationships between adjacent frames, which is suitable for capturing local dynamic changes in sequences. In TME, subtle movement changes can also affect technical evaluation, and AFW can improve the sensitivity of DTW in details. AFW needs to first calculate the cumulative change in limb RA, with a required range between adjacent frames of the current frame, in order to obtain the RA weights between adjacent frames. W_i^{σ} is shown in Eq. (4).

$$W_i^{\sigma} = \begin{cases} \dfrac{\theta_i^{'} + \rho_i^{\sigma}}{\sum_{i=1}^{n} \theta_i^{'} + n\rho_i^{\sigma}} & 0 < \Delta T < t_c \\ 0 & \Delta T \geq t_c \end{cases} \tag{4}$$

In Eq. (4), t_c is the current frame. ΔT is between adjacent frames, and $\Delta T \in (0, t_c)$. $\theta_i^{'}$ signifies the ΔT cumulative change of the i -th RA in the input video from the previous t_c. ρ_i^{σ} is the smoothing term, as shown in Eq. (5).

$$\rho_i^{\sigma} = \sum_{t=t_c-\Delta T}^{t_c} \alpha_i^t \big/ \Delta T + 1 \tag{5}$$

$\theta_i^{'}$ is shown in Eq. (6).

$$\theta_i^{'} = \sum_{t=t_c-\Delta T-1}^{t_c-1} \left| \alpha_i^{t+1} - \alpha_i^t \right| \tag{6}$$

Global Time Weighting (GTW) is used to allocate reasonable weights to the entire action sequence in the time dimension, ensuring that each stage of the entire action process receives appropriate attention. It considers the temporal characteristics of the entire sequence and assigns higher weights to certain key moments or key action points. GTW can balance the importance of different time periods in action sequences, making the DTW algorithm more accurate in matching actions and avoiding certain important time periods from being ignored or underestimated. W_i^{τ} is shown in Eq. (7).

$$W_i^{\tau} = \frac{\theta_i + \rho_i^{\tau}}{\sum_{i=1}^{n} \theta_i + n\rho_i^{\tau}} \tag{7}$$

In Eq. (7), ρ_i^{τ} is the smoothing term, which serves to avoid a weight of 0. If the weight is 0, the corresponding RA information will be ignored, affecting the result. ρ_i^{τ} is shown in Eq. (8).

$$\rho_i^{\tau} = \sum_{t=1}^{T} \alpha_i^t \big/ T \tag{8}$$

In Eq. (8), T signifies the frame number of the template video. θ_i is the degree of change of a specific RA in the time series in the template video. By calculating θ_i, the dynamic variation characteristics of the angle during the action process can be captured. If a certain RA changes dramatically between different frames, θ_i will be larger, indicating that the action point has high dynamism in the entire action sequence and may need to be given higher weight. θ_i is shown in Eq. (9).

$$\theta_i = \sum_{t=1}^{T-1} \left| \alpha_i^{t+1} - \alpha_i^t \right| \tag{9}$$

To better reflect the true s_t, AFW and GTW are applied to the data. The overall evaluation score S for a certain tennis action is shown in Eq. (10).

$$S = \sum_{t=1}^{T} (w_t \cdot s_t), \sum_{t=1}^{T} w_t = 1 \tag{10}$$

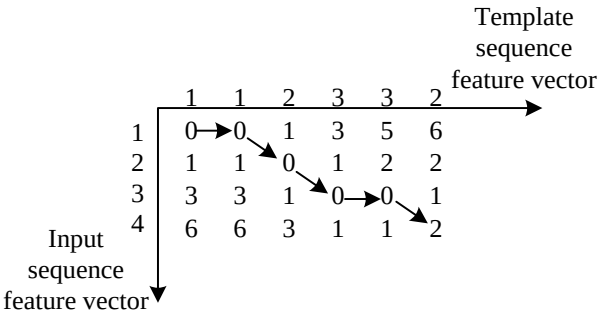
In Eq. (10), w_t is the weighted score, and $w_t \in (0,1)$. AFW focuses more on local changes, emphasizes the dynamic relationship between adjacent frames, and improves the precision and smoothness of matching. GTW focuses more on the temporal characteristics of the entire sequence, emphasizing the matching of critical moments to improve the accuracy and robustness of overall evaluation. Combining these two weighting methods can capture the importance of global key moments in action evaluation while not ignoring the details of local dynamic changes, achieving higher evaluation accuracy and robustness.

C. TME System Based on SDTW

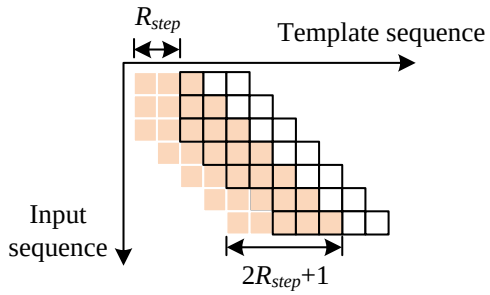
There are multiple similarity or distance functions in time series data in videos. DTW is used to calculate the similarity between two time series. DTW minimizes the cumulative distance between one time series and another by calculating the nonlinear mapping relationship between the two. DTW may not be able to output results in a timely manner, as it requires traversing a large amount of frame data to find the path with the minimum cumulative distance. To solve the real-time of the DTW algorithm, an improved algorithm called Segmented DTW (SDTW) is proposed. The core idea of SDTW is to segment the actions in the template video and perform path search within each segment. This method reduces time complexity and improves computational efficiency by limiting the search range. By segmenting and reducing computational complexity, SDTW can output calculation results in a timely manner at the end of frame processing in action videos, thus meeting real-time requirements. The schematic diagram of path search for DTW and the search area for SDTW with a step size of $R_{step} = 2$ are shown in Fig. 4.

In Fig. 4 (a), a 2D distance matrix D is constructed, with the total frame numbers of the input video and template video being n and m, respectively. The matrix element $d_{(i,j)}$ at the current position (i, j) is displayed in Eq. (11).

$$d_{(i,j)} = d_{\min} + \sqrt{\sum_{k=1}^{n} (\Delta \alpha_k)^2} \tag{11}$$



(a) DTW path search diagram



(b) SDTW's search area

Fig. 4. DTW path search and SDTW search area.

In Eq. (11), $d_{\min}$ signifies the minimum distance value obtained in the previous step. $\Delta\alpha_k$ is the difference between the k-th CRA of the input video and the template video. At the initial position (1,1), $d_{\min}$ is 0. At different positions, $d_{\min}$ is shown in Eq. (12).

$$d_{\min} = \min\left(d_{(i-1,j)}, d_{(i,j-1)}, d_{(i-1,j-1)}\right) \tag{12}$$

In Eq. (12), $(i-1,j)$ and $(i,j-1)$ are the adjacent positions on the upper and left sides of (i,j), respectively. $(i-1,j-1)$ is the upper left corner position of (i,j). DTW first starts from the initial position $(1,1)$ of the time series matrix, gradually accumulates and calculates the distance of each step by moving to the right, down, and right adjacent positions in the matrix, and finds the path in this process to minimize the total accumulated distance. Finally, the DTW algorithm uses this path to find the minimum cumulative distance at the endpoint position (n,m) of the matrix, which represents the minimum similarity distance between two time series. A small distance indicates that the two sequences are more similar in the time dimension, demonstrating that the shapes or patterns of the two sequences are closer. In Fig. 4 (b), when the template video time series is segmented, the step size is set to R_{step}. To better limit the range of path search, the width on both sides of the diagonal is specified to ensure that the search path is concentrated near the diagonal rather than spreading throughout the entire matrix R_{step}. In the case of segmented processing, the total width range of path search is determined by the step size R_{step}, with a maximum width of $2R_{step}+1$ and a minimum width of $R_{step}+1$. This means that the path search range will be limited to the diagonal and its left and right range R_{step}, thereby reducing computation and complexity. The endpoint position of the first segment of SDTW is (n, j_e), and the vertical axis satisfies $j_e \in \left(m+1-R_{step}, m+1+R_{step}\right)$. At this time, the search range of the path is on the diagonal, with a width of $2R_{step}+1$. The computational workload is reduced to avoid global search. Subsequently, by moving R_{step} steps each time, different path searches can be achieved. The average distance $\bar{d}$ for each step is shown in Eq. (13).

$$\bar{d} = \frac{c}{\kappa} \tag{13}$$

In Eq. (13), c and κ are the distance and length of the path. The conversion score s_d is shown in Eq. (14).

$$s_d = \frac{1}{1+h\bar{d}} \tag{14}$$

In Eq. (14), h is the coefficient that adjusts the magnitude of the score decrease, and $h = 0.25\kappa$. As $\bar{d}$ increases, the similarity between two time series decreases. At this time, the result of s_d is closer to 0. Two time series are completely identical, and $s_d = 1$. To evaluate human movements in a single frame video, it is necessary to ensure that the input video and the template video have equal frame rates. Analyzing the relationship between RA in various limbs of the human body can obtain a single frame calculation evaluation score. In practical operation, extracting human joint information is a time-consuming process and may cause delays during network transmission. To alleviate these issues, an offline processing module is added to the TME system. The function of this module is to process the template video in advance, extract and save the joint coordinates of each frame to the local file. Therefore, in the actual real-time evaluation process, the system only needs to read the stored joint information from the local file without recalculating and extracting, greatly reducing the time required for evaluation and improving efficiency. Therefore, the constructed architecture diagram of the TME system is shown in Fig. 5.

In Fig. 5, the client and server of the TME system use Socket to achieve data transmission. The client is connected to the monocular camera through USB, and can display a video interface and collect video data. Meanwhile, customers can preprocess video frame data and then transmit it to the server. The focus of the server is on extracting joint points and evaluating actions. The monocular camera is transmitted to the server via USB connection, and the server receives the data information and transmits the results to the client.

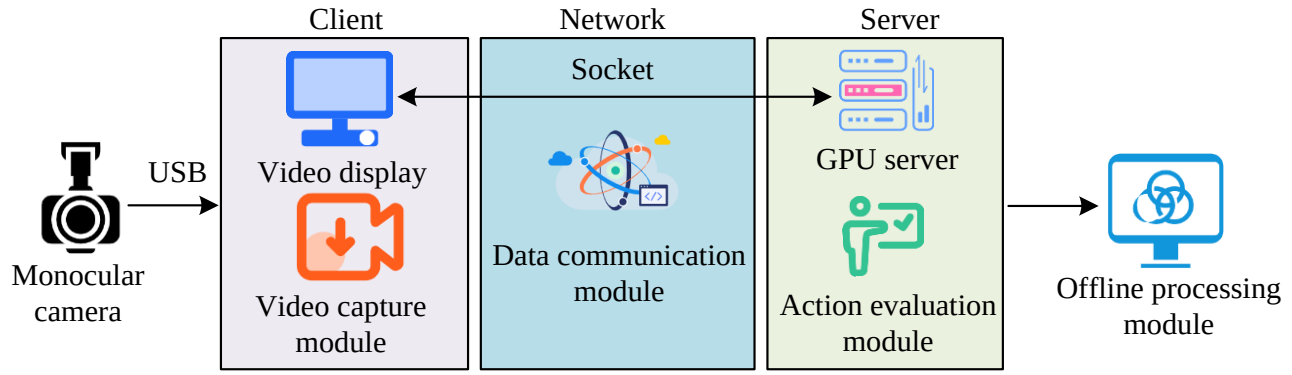


Fig. 5. TME system architecture diagram.

III. Results

A. Analysis of TME System Based on WCRA Similarity Measurement Method

The experimental datasets are the Tennis Videos Dataset and the Tennis Stroke Dataset, with the former containing a large number of tennis matches and training videos, typically used for video analysis, action recognition, and strategy analysis. The latter includes data on various tennis hitting movements, such as smashes, Forehand Strokes (FS), Backhand Strokes (BS), Forehand Cut (FC), and Backhand Cut (BC). The experimental setup is displayed in Table II.

TABLE II. Hardware Equipment and Software Environment for Experimental Setup

Hardware device	Device type	Software environment	Configuration information
GPU server	NVIDIA Tesla P40	Operating system	Ubuntu 14.04.5 LTS
GPU architecture	NVIDIA Pascal	Deep learning framework	Caffe
High definition digital camera	SONY HDR-CX405	GPU parallel computing architecture	CUDA 8.0
Monocular camera	RER-USBFHD01M	Computer vision library	OpenCV 2.4.13

The research indicators include similarity evaluation scores and accuracy. The similarity evaluation score is used to assess the similarity between actions of the same type (such as multiple backhands) and actions of different types (such as backhands and smashes). By calculating and comparing these scores, the similarity between different action types before and after improvement can be analyzed to evaluate the accuracy and effectiveness of the algorithm. Accuracy is used to measure the performance of algorithms in identifying and classifying action types, such as kill actions. By comparing the accuracy and average accuracy of different methods, the effectiveness and reliability of each method can be evaluated under different levels of action performance. To evaluate the impact of different algorithms on real-time performance when processing monocular camera videos using OpenPose. A monocular camera is conFig.d, with a video frame rate of 60FPS and a resolution of 1280×720. The required algorithm environment is set on the server, including OpenPose. Different algorithms are run sequentially and combined with OpenPose to process video streams, recording the actual frame rate per second during the processing. The experiment is conducted 20 times to ensure reliability and statistical significance, with each experiment lasting 10 minutes. In each experiment, the processed video frame rate and changes in frame rate are analyzed, as shown in Fig. 6.

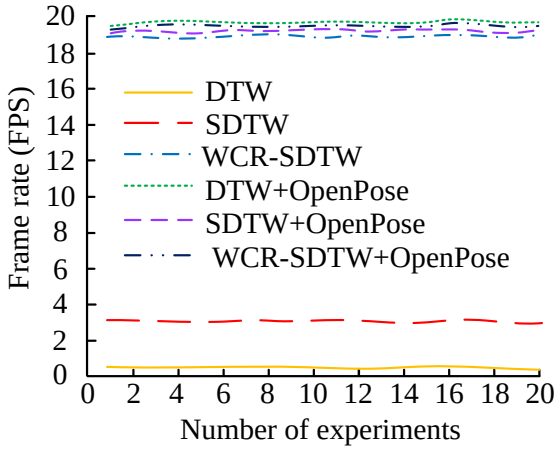


Fig. 6. The frame rate variation of different methods.

In Fig. 6, the average frame rate of DTW without OpenPose processing was the lowest, only 0.5FPS. The average frame rate under the action of WCR and SDTW was19.1FPS, while the average frame rate processed by OpenPose was 19.5FPS, which was time-consuming, but achieved high accuracy. The proposed algorithm, combined with OpenPose, can better maintain the real-time frame rate of the video.

To verify the effectiveness of the designed limb CRA, an analysis is conducted on the changes in CRA values of BS action and smash action, and a comparison between the two was obtained, as shown in Fig. 7.

In Fig. 7 (a), the angle value of CRA 8 fluctuated the most within 30 frames, indicating a more drastic change in the left arm. In Fig. 7 (b), there was a significant fluctuation in the angle value of the right arm CRA 6 during the smash action, ranging from 36° to 260°. Therefore, the proposed limb CRA can effectively represent changes in limb direction, clearly distinguishing between movement and posture situations.

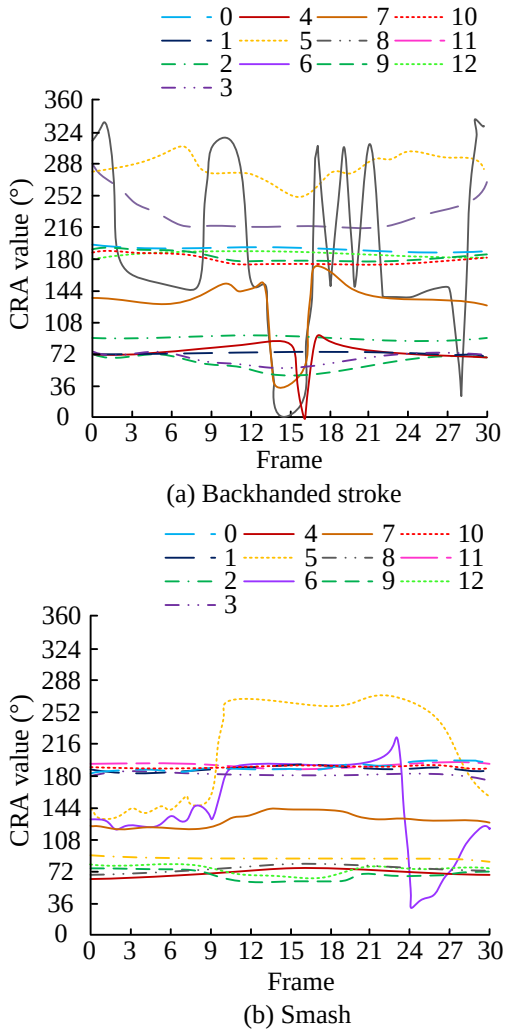


Fig. 7. Comparison of CRA value changes in backhand and smash movements.

To verify the proposed improvement method, the similarity scores between different action types are evaluated to analyze the performance of the improved method. The study randomly selects 250 tennis training videos from the dataset and selects five types of movements: FS, BS, FC, BC, and smash. The similarity scores are analyzed by action type. The similarity scores of same action types and different action types are calculated. The similarity of different action types before and after improvement is compared, as shown in Fig. 8.

In Fig. 8 (a), the similarity scores between actions of the same type and between actions of different types both exceeded 0.75 points. However, according to the similarity score results, the method before improvement was not able to distinguish action similarity scores well. The difference between the maximum and minimum scores for actions of the same type ranged from 0.02 to 0.16 points. In Fig. 8 (b), there was a clear distinction between the five types of actions, with a score difference ranging from 0.27 to 0.49 points. Therefore, the improved method has better discrimination than before.

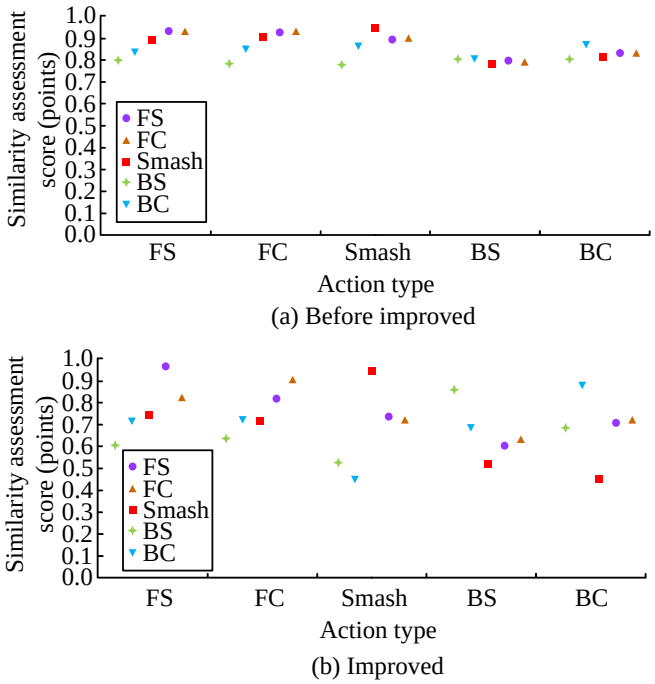


Fig. 8. The similarity score between different action types before and after improvement.

To analyze the accuracy of the improved method, different methods are selected for comparison, including 3D motion capture technology [32], Gaussian Distance-Improved DTW (GD-IDTW) [33], and Joint Angles and Movement Similarity (JA-MS) [34]. The action performance of the dataset is divided into three levels: good, average, and poor. The score for poor action performance ranges from 0.0 to 0.6, the score for average action performance ranges from 0.6 to 0.8, and the score for good action performance ranges from 0.8 to 1.0. The accuracy and average accuracy of different methods of smash actions among the three levels of performance are shown in Fig. 9.

In Fig. 9 (a), the accuracy of the improved method for the smash action was 98.12%, 100.00%, and 100.00% for good, average, and poor performance, respectively. The accuracy of GD-IDTW was relatively close to the improved method, with accuracy rate of 96.97%, 85.77%, and 100.00% for good, average, and poor action performance, respectively. The overall accuracy of the improved method was higher than other methods, because the improved method was significantly better than the GD-IDTW in handling fine actions, which could better capture subtle differences in these actions. In Fig. 9 (b), in the similarity evaluation with good action performance, the improved method had an average accuracy close to GD-IDTW, with 88.15% and 88.01% respectively, showing superior performance. In terms of average action performance, the improved method had an average accuracy of 90.12% in action performance, which was higher than other methods. In the similarity evaluation of poor action performance, the average accuracy of the improved method was 92.55%. The improved method not only enhances computational efficiency, but also improves the accuracy of similarity evaluation.

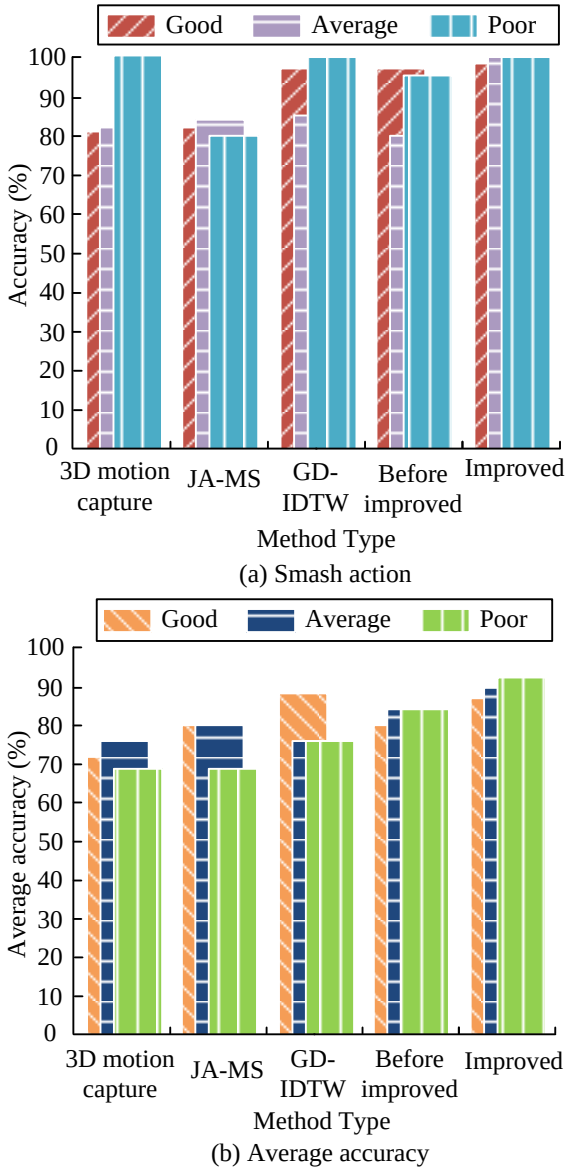


Fig. 9. Comparison of accuracy of different methods.

To verify the accuracy of the improved method for classifying tennis movements, the experiment selects five different types of movements from two datasets, the Tennis Videos Dataset and the Tennis Stroke Dataset, for analysis. The matrix element is the ratio of the number of recognized actions to the number of tested actions. The confusion matrix obtained for the five types of tennis movements is shown in Fig. 10.

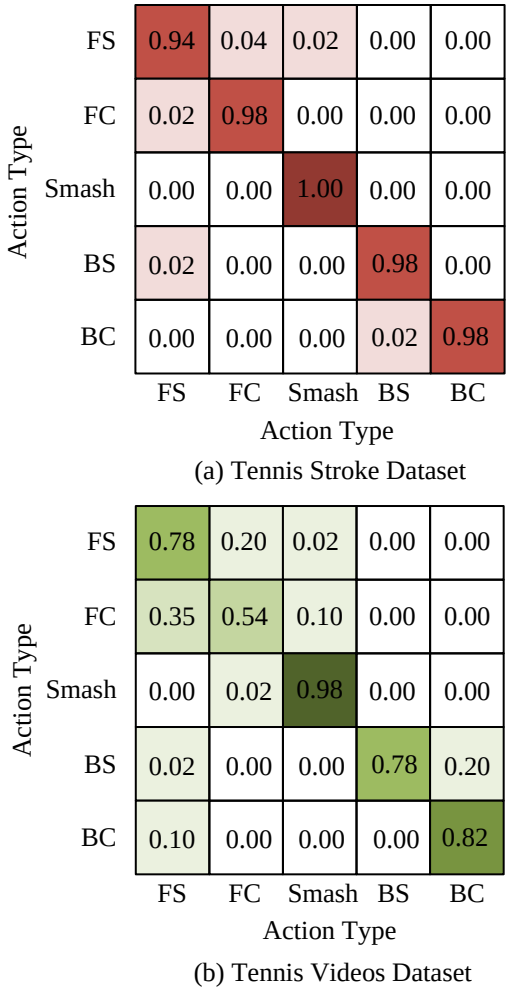


Fig. 10. Comparison of confusion matrices for different datasets.

In Fig. 10 (a), the five columns represent the five recognized action types, and the 5 rows represent the 5 tested action types. The average accuracy of action classification in the Tennis Stroke Dataset was 97.60%. In Fig. 10 (b), there were many classification errors between FS and FC actions in the Tennis Videos Dataset, with an average accuracy of 78.00% for action classification.

To analyze the generalization of the improved method, the study identifies non-tennis movements in two datasets. The number of tests for each type of action is 9, and duplicate videos are filtered out to obtain the recognition accuracy, as displayed in Table III.

TABLE III. RECOGNITION ACCURACY OF NON TENNIS MOVEMENTS

Dataset	Action Type	Bending	Capriole	Running	Walking	High five
Tennis Videos Dataset	Correct number	7	8	7	9	7
	Accuracy	0.78	0.89	0.78	1.00	0.78
Tennis Stroke Dataset	Correct number	6	7	6	8	9
	Accuracy	0.67	0.78	0.67	0.89	1.00

In Table III, for the five movements of bending, Capriole, running, walking, and high five, the average accuracy obtained using the improved method reached 82%. The recognition accuracy of the Tennis Videos Dataset was generally high, with walking movements achieving 100%, and the high five movements of the Tennis Stroke Dataset also achieving 100%. The proposed method has a certain degree of generalization ability in recognizing non-tennis movements on different datasets.

B. Performance Analysis of TME System

Client performance evaluates the real-time performance of video capture and transmission, ensuring that video frames captured by monocular cameras can be transmitted to the server in a timely manner. This includes the frame rate of the camera, data transmission delay, and stability of network transmission. Server performance refers to evaluating the real-time performance of the server in receiving, processing, and analyzing video frames. The server needs to quickly perform algorithm processing and return results after receiving video frames to ensure the overall system response speed. To comprehensively evaluate and optimize the performance of the system, and ensure that the entire TME system can run efficiently and stably in practical applications, real-time testing is conducted on the client and server of the TME system. Five tennis movements are selected for the experiment, and tested five times on both the client and server sides of the system. The average frame rate obtained is presented in Table IV.

In Table IV, the average frame rates of the server in action evaluation and action recognition were 18.52FPS and 18.51FPS, respectively, both higher than those of the client. In the action evaluation mode, the average frame rate of the client was between 17.35FPS and 17.49FPS, and the overall average frame rate was about 17.40FPS. The server exhibited higher efficiency in action processing and evaluation, which could process video frames faster. It is more efficient in processing data capabilities and utilizing data resources. In both modes, there is not much difference in frame rate between the client and server, but the overall trend is consistent. This indicates that the performance of the system is relatively consistent in different modes and has a certain degree of stability.

In the TME system, three individuals are selected for testing. Among the five types of tennis movements, three sets of imitative movements are tested for each movement. The performance levels are good, average, and poor. The similarity evaluation scores for different action types are shown in Fig. 11.

TABLE IV. COMPARISON OF AVERAGE FRAME RATES BETWEEN SERVER AND CLIENT

Mode type	Action Type	FS	FC	Smash	BS	BC	Average frame rate (FPS)
Average frame rate of action evaluation mode (FPS)	Client	17.38	17.35	17.37	17.39	17.49	17.40
	Server	18.50	18.57	18.56	18.43	18.54	18.52
Average frame rate of action recognition mode (FPS)	Client	17.24	17.28	17.38	17.28	17.27	17.29
	Server	18.53	18.51	18.48	18.51	18.49	18.51

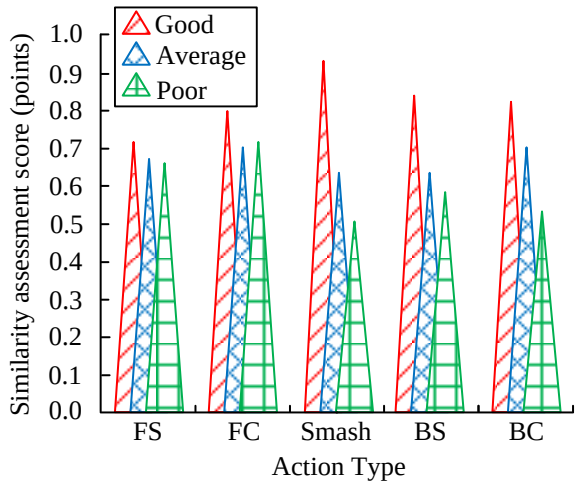


Fig. 11. Similarity evaluation scores for different action types.

In Fig. 11, the similarity evaluation score for the smash action with good performance was the highest, at 0.94, while the similarity evaluation score for this action with poor performance was the lowest, at 0.5. The evaluation scores for smash, BS, and BC actions were relatively high, while the similarity evaluation scores for FS and FC actions were relatively close, resulting in a lower degree of differentiation between the two.

IV. DISCUSSION AND CONCLUSION

There are significant challenges in efficiently and accurately evaluating tennis movements at present. In order to improve computational efficiency and real-time performance of the system, a TME system was developed. The limb CRA was used to quantify and analyze action direction. Then, AFW and GTW weighting were used to optimize DTW. The results showed that the angle value of CRA 8 fluctuated the most within 30 frames, indicating that the changes in the left arm were more severe. The angle value of CRA 6 in the right arm of the smash action fluctuated greatly, ranging from 36° to 260°. The similarity scores between actions of the same type and between actions of different types both exceeded 0.75 points. However, according to the similarity score results, the method before improvement was not able to distinguish action similarity scores well. To address this issue, Zhang et al. focused on evaluating the quality of actions in videos by using distributed autoencoders, likelihood loss sampling scores, and learning uncertainty parameters [35]. The difference between the maximum and minimum scores for actions of the same type ranged from 0.02 to 0.16 points. There was a clear distinction between the five types of actions, with a score difference of 0.27-0.49 points. Therefore, the improved method had better discrimination than before. For the smash action, the accuracy rates of the improved method for good, average, and poor performance were 98.12%, 100.00%, and 100.00%, respectively. The accuracy of GD-IDTW was relatively close

to the improved method, with accuracy rates of 96.97%, 85.77%, and 100.00% for good, average, and poor action performance, respectively. The overall accuracy of the improved method outperformed other methods, because the improved method was significantly better than the GD-IDTW in handling fine actions, which could better capture subtle differences in these actions. In the similarity evaluation of good action performance, the improved method had an average accuracy close to GD-IDTW, with 88.15% and 88.01%, respectively, showing superior performance. As for average action performance, the improved method had an average accuracy of 90.12%, which was higher than other methods. In the similarity evaluation of poor action performance, the average accuracy of the improved method was 92.55%. The improved method not only enhances computational efficiency, but also improves the accuracy of similarity evaluation. This method has a certain positive effect on the Estevam team in obtaining semantic information from videos for recognizing actions [36]. The improved method effectively achieves accurate and real-time action similarity evaluation, which is of great significance for various training and evaluation systems that require real-time feedback. Meanwhile, this innovative method will make significant contributions to the development of sports science research and intelligent sports evaluation systems. However, this study does not consider the impact of lighting environmental factors on the evaluation results. Excessive or insufficient lighting can lead to the loss of details in the image, which in turn affects the accuracy of action recognition and the reliability of similarity evaluation. In the future, experiments can be extended to different lighting environments, including natural light, artificial light sources, and changes in lighting intensity. By testing the performance of the algorithm under various lighting conditions, the robustness of the algorithm in different lighting environments can be identified and optimized.

ACKNOWLEDGMENT

The research is supported by: A Study on Teaching Reform and Learning Effectiveness Improvement of College Physical Education Curriculum Based on Mobile Application Embedding (No.2024GZJX072).

REFERENCES

[1] C. Schneider, J. Rothschild, and A. Uthoff, "Change-of-direction speed assessments and testing procedures in tennis: A systematic review," J. Strength Cond. Res., vol. 37, no. 9, pp. 1888-1895, September 2023.

[2] M. Aslanyan, "On mobile pose estimation and action recognition design and implementation," Pattern Recognit. Image Anal., vol. 34, no. 1, pp. 126-136, January 2024.

[3] J. Purohit and R. Dave, "Leveraging deep learning techniques to obtain efficacious segmentation results," Arch. Adv. Eng. Sci., vol. 1, no. 1, pp. 11-26, July 2023.

[4] M. Wu, R. Wang, Y. Hu, M. Fan, Y. Wang, Y. Li, and S. Wu, "Invisible experience to real-time assessment in elite tennis athlete training: Sport-specific movement classification based on wearable MEMS sensor data," Proc. Inst. Mech. Eng. P J. Sports Eng. Technol., vol. 237, no. 4, pp. 271-282, October 2021.

[5] B. Giles, P. Peeling, S. Kovalchik, and M. Reid, "Differentiating movement styles in professional tennis: A machine learning and hierarchical clustering approach," Eur. J. Sport Sci., vol. 23, no. 1, pp. 44-53, December 2021.

[6] T. Perri, M. Reid, A. Murphy, K. Howle, and R. Duffield, "Differentiating stroke and movement accelerometer profiles to improve prescription of tennis training drills," J. Strength Cond. Res., vol. 37, no. 3, pp. 646-651, March 2023.

[7] D. Wood, M. Reid, B. Elliot, J. Alderson, and A. Mian, "The expert eye? An inter-rater comparison of elite tennis serve kinematics and performance," J. Sports Sci., vol. 41, no. 19, pp. 1779-1786, December 2023.

[8] S. Liu, "Tennis players' hitting action recognition method based on multimodal data," Int. J. Biometrics, vol. 16, no. 3-4, pp. 317-336, April 2024.

[9] R. Hu, "IoT-based analysis of tennis player's serving behavior using image processing," Soft Comput., vol. 27, no. 19, pp. 14413-14429, July 2023.

[10] T. Perri, M. Reid, A. Murphy, and R. Duffield, "Tennis serve volume, distribution and accelerometer load during training and tournaments from wearable microtechnology," Int. J. Perform. Anal. Sport, vol. 24, no. 4, pp. 285-297, December 2024.

[11] H. Setyawan, S. Suharjana, S. Purwanto, J. V. García-Jiménez, and A. Adriansyah, "The differences result in serve skill of junior tennis players assessed based on gender and age," Retos: Nuevas Perspectivas de Educación Física, Deporte y Recreación, vol. 54, pp. 272-278, 2024.

[12] C. Shuai, Y. Sun, X. Zhang, F. Yang, X. Ouyang, and Z. Chen, "Intelligent diagnosis of abnormal charging for electric bicycles based on improved dynamic time warping," IEEE Trans. Ind. Electron., vol. 70, no. 7, pp. 7280-7289, July 2023.

[13] D. Deriso and S. Boyd, "A general optimization framework for dynamic time warping," Optim. Eng., vol. 24, no. 2, pp. 1411-1432, August 2022.

[14] Q. Zhang, C. Zhang, L. Cui, X. Han, Y. Jin, G. Xiang, and Y. Shi, "A method for measuring similarity of time series based on series decomposition and dynamic time warping," Appl. Intell., vol. 53, no. 6, pp. 6448-6463, July 2022.

[15] H. Xing, L. Zhu, B. Chen, L. Zhang, D. Hou, and W. Fang, "A novel change detection method using remotely sensed image time series value and shape based dynamic time warping," Geocarto Int., vol. 37, no. 25, pp. 9607-9624, December 2021.

[16] V. Froese, B. Jain, M. Rymar, and M. Weller, "Fast exact dynamic time warping on run-length encoded time series," Algorithmica, vol. 85, no. 2, pp. 492-508, September 2022.

[17] T. Belkhouja, Y. Yan, and J. R. Doppa, "Dynamic time warping based adversarial framework for time-series domain," IEEE Trans. Pattern Anal. Mach. Intell., vol. 45, no. 6, pp. 7353-7366, June 2022.

[18] H. He and H. Li, "A new boosting algorithm for online portfolio selection based on dynamic time warping and anti-correlation," Comput. Econ., vol. 63, no. 5, pp. 1777-1803, May 2024.

[19] K. Vorpe, S. Hessinger, R. Poth, and T. Miljkovic, "Clustering regions with dynamic time warping to model obesity prevalence disparities in the United States," J. Appl. Stat., vol. 51, no. 4, pp. 793-807, March 2023.

[20] M. Hasanvand, M. Nooshyar, E. Moharamkhani, and A. Selyari, "Machine learning methodology for identifying vehicles using image processing," Artif. Intell. Adv., vol. 1, no. 3, pp. 170-178, April 2023.

[21] M. Poignard, G. Guilhem, M. Jubeau, E. Martin, T. Giol, B. Montalvan, and F. Bieuzen, "Cold-water immersion and whole-body cryotherapy attenuate muscle soreness during 3 days of match-like tennis protocol," Eur. J. Appl. Physiol., vol. 123, no. 9, pp. 1895-1909, September 2023.

[22] L. Wang, L. Lin, Y. Sun, S. Hou, and J. Ren, "The effect of movement speed on audiovisual temporal integration in streaming-bouncing illusion," Exp. Brain Res., vol. 240, no. 4, pp. 1139-1149, April 2022.

[23] A. Visser, D. Büchel, T. Lehmann, and J. Baumeister, "Continuous table tennis is associated with processing in frontal brain areas: an EEG approach," Exp. Brain Res., vol. 240, no. 6, pp. 1899-1909, June 2022.

[24] B. M. Pluim, M. G. T. Jansen, S. Williamson, C. Berry, S. Camporesi, K. Fagher, and C. L. Ardern, "Physical demands of tennis across the different court surfaces, performance levels and sexes: a systematic review with meta-analysis," Sports Med., vol. 53, no. 4, pp. 807-836, April 2023.

[25] H. He, H. Sun, and Y. Chen, "Analysis and assessment of ground motion characteristics and similarity using dynamic time warping distance," J. Seismol., vol. 27, no. 6, pp. 1013-1033, December 2023.

[26] M. Kumawat and A. Khaparde, "Development of adaptive time-weighted dynamic time warping for time series vegetation classification using satellite images in Solapur district," Comput. J., vol. 66, no. 8, pp. 1982-1999, August 2023.

[27] J. Xia and Y. Yamashita, "Online batch process monitoring with a combination of normal operating history data and physical knowledge," J. Chem. Eng. Jpn., vol. 55, no. 1, pp. 38-50, January 2022.

[28] A. Sabarinath, A. N. Rajesh, and S. S. G. V. L. Kumar, "Application of deep learning algorithms to correct bias in CMIP6 simulations of surface air temperature over the Indian monsoon core region," Int. J. Climatol., vol. 43, no. 16, pp. 7496-7515, December 2023.

[29] M. V. L. Pazini, H. de Abreu Corrêa, H. Haan, G. Zanon, and T. G. R. Clarke, "A dynamic time warping approach to access fatigue damage in composite pipes," Exp. Mech., vol. 64, no. 6, pp. 839-849, June 2024.

[30] Z. Yu, Z. Wang, and J. Wang, "Continuous wavelet transform and dynamic time warping-based fine division and correlation of glutenite sedimentary cycles," Math. Geosci., vol. 55, no. 4, pp. 521-539, April 2022.

[31] J. P. Choe, I. W. Hwang, J. H. Park, C. Amo, and J. M. Lee, "How valid is the commercially available tennis match analysis mobile application? Is it good enough?," Int. J. Perform. Anal. Sport, vol. 24, no. 1, pp. 58-73, October 2023.

[32] J. S. Israel, S. R. Loushin, S. U. Tetzloff, T. Ellenbecker, K. R. Kaufman, and S. Kakar, "Wrist motion assessment in tennis players using three-dimensional motion capture and dynamic electromyography," J. Wrist Surg., vol. 13, no. 3, pp. 264-271, July 2024.

[33] A. X. Chen, B. W. Yang, B. Lu, D. G. Nie, E. M. Jin, and F. X. Wang, "Gesture scoring based on Gaussian distance-improved DTW," Elektron. Elektrotech., vol. 30, no. 2, pp. 18-27, April 2024.

[34] W. Yan, X. Cao, and P. Ye, "Application of human posture recognition algorithms based on joint angles and movement similarity in sports assessment for physical education," Scalable Comput. Pract. Exp., vol. 25, no. 4, pp. 2385-2397, June 2024.

[35] B. Zhang, J. Chen, Y. Xu, H. Zhang, X. Yang, and X. Geng, "Auto-encoding score distribution regression for action quality assessment," Neural Comput. Appl., vol. 36, no. 2, pp. 929-942, October 2023.

[36] V. Estevam, R. Laroca, H. Pedrini, and D. Menotti, "Tell me what you see: A zero-shot action recognition method based on natural language descriptions," Multimed. Tools Appl., vol. 83, no. 9, pp. 28147-28173, September 2023.

Internet of Things User Behavior Analysis Model Based on Improved RNN

Keling Bi*
School of Information Engineering, Liaodong University, Dandong 118003, China

***Abstract*—Currently, there are issues with low efficiency and outdated Internet of Things resource allocation. To study real Internet of Things user behavior data, a Bayesian optimization algorithm is used to automatically select hyperparameter combinations and construct an Internet of Things user behavior analysis model based on long short-term memory. The results showed that the prediction accuracy of the model reached 96.8% and 97.53% on the training and validation sets, while in the set 50 maximum iterations, the model achieved 80.78% on the test set. In comparing the performance between the research model and the traditional recurrent network model, it was found that the optimal prediction accuracy of the research model was 80.78%, which was better than the comparison model. The application results of the research model in short-term power load forecasting also indicated that the prediction accuracy of the Internet of Things user behavior analysis model based on the improved recurrent network has reached a good level, far superior to the comparative model. The results have important application value for allocating energy and resources in Internet of Things systems.**

Keywords*—Internet of Things; user behaviors; recurrent neural network; Bayesian optimization; long short-term memory; hyperparameter

I. Introduction

The continuous progress of science and technology has led to an exponential growth trend in the amount of information, and the Internet of Things (IoT) technology has also been further developed. In recent years, the further popularization of 5G technology, the further reduction of hardware costs, and the development of big data technology have led to a significant advancement in the IoT. At this stage, the IoT is no longer merely a network of objects and systems; it has evolved into a comprehensive system that connects all the people, processes, and resources involved, forming a seamless and automated interaction process [1-2]. At the current stage of development, the IoT integrates the interactive factors related to people. The data types and quantities involved in the whole IoT system have greatly increased, and the traditional processing system technology has been unable to meet the actual needs of [3-4]. At this time, artificial intelligence (AI) technologies have emerged as the optimal avenue for industrial advancement within the IoT domain. Furthermore, the integration of AI has become pervasive across various production and operational processes. However, the practical application of AI technology in the IoT often has the problem of poor timing [5-6]. Given this, many scholars have researched the analysis of IoT user behavior, and methods such as mathematics, data mining, and machine learning (ML) have emerged [7-8]. Mathematical methods are characterized by high complexity, limited interpretability, and greater difficulty in achieving results. In contrast, data mining and simple calculation technology are relatively straightforward, yet they often prove ineffective in predicting user behavior. Based on this, the long and short-term memory (LSTM) recurrent neural network (RNN) method in the ML method is used to construct the prediction model. At the same time, to solve the problems of high complexity and optimization difficulty of ML methods, the Bayesian optimization algorithm (BOA) is studied based on the prediction model of LSTM-RNN, which can realize the automatic optimization of the prediction model. This study first hopes to find out the correlation and the implied behavior mode of the user behavior data of the IoT, aiming to provide more temporal data for more accurate, fast, and convenient IoT services. Secondly, the study is expected to construct a user behavior prediction model for the IoT that can adapt to different environmental characteristics. This will provide a basis for user behavior information that can be used to improve the quality of system services in the IoT and further improve the efficiency of resource allocation in the system. Finally, the study validates the model through training in terms of losses, effects, and load forecasting. Through these verification methods, the performance and practical application of the proposed method can be effectively analyzed.

II. Literature Review

In the context of IoT research pertaining to user behavior analysis (UBA), to promote the application of big data in various fields, Hou et al. proposed an IoT unstructured big data analysis online client algorithm built on ML algorithm. The algorithm was used in other big data analysis scenarios and verified to be more efficient than other comparative algorithms [9]. Abdelmoumin et al. conducted research on the performance of IoT-based anomaly-based intelligent intrusion detection system (IDS) ML model. Compared with deep learning-based IDS, anomaly-based ML-based IDS exhibited lower performance and prediction accuracy (PA) in detecting intrusions in IoT [10]. Xu et al. proposed a data-driven intrusion and anomaly detection method using IoT automatic ML to address the current issues of IoT network attacks and intrusions. This algorithm technology not only saved the computational cost of runtime test data, but also solved a multi-class classification problem with an accuracy of 99.7%, with significant advantages over existing algorithms [11]. To solve the optimal pricing and bundling problem of ML-based IoT services, Alsheikh et al. defined data value and service quality from the perspective of ML and proposed an IoT market model. Compared to independent sales, bundling IoT services could maximize the profits of service providers [12]. Woźniak et al.

analyzed the network traffic of various IoT solutions based on deep learning models to address network security issues in network physical systems. The results confirmed that even when the number of evaluated network features decreased, the model was very effective in identifying potential threats, with an accuracy rate of over 99% [13]. Zhao et al. proposed an IoT intrusion detection method based on lightweight deep neural networks. On two real NID datasets, this method had good classification performance, lower model complexity, and smaller model size, making it suitable for IoT traffic classification in both normal and attack scenarios [14].

In studies employing LSTM networks for behavioral prediction, the LSTM network will also be utilized to conduct such studies based on the most abundant user purchase and social behavior data available on the Internet. For example, Sakar et al. used a multi-layer perceptron for feature classification and trained a LSTM-RNN to predict the probability of the user leaving the current site. The purpose was to take corresponding measures to improve the purchase conversion rate of the website [15]. LSTM networks are also used in some prediction studies of action and behavioral trajectories. To estimate the movement intention of people in intelligent manufacturing service of human-robot cooperation, Liu et al. used LSTM network to extract the time pattern of human movement and automatically output the prediction results before the movement. This approach was taken to ensure the efficiency and safety of the system [16]. Huang et al. proposed three properties of asymmetric driving behavior and constructed a vehicle following model based on a LSTM-RNN [17]. Yimin et al proposed a human-centered trajectory tracking control strategy, using a LSTM network to design a model predictive control method considering insertion vehicle driver behavior to track the reference trajectory [18].

In conclusion, many scholars have achieved notable advancements in the enhancement of IoT-UBA performance, economic value, and network security. However, existing IoT-UBA research focuses on predicting whether a certain behavioral action will occur, without considering the usage characteristics of items in IoT and the relationships between users and items. In addition, existing research only considers the sequence relationship between user behavior occurrence, that is, using pre-order behavior to analyze the possible behaviors that may occur in the post-order. This merely indicates the potential for future behavior without specifying the timing of subsequent actions. Consequently, it is unable to enhance the precision, speed, and accessibility of IoT services or provide more detailed temporal data. Based on this, this study innovatively proposes the use of BOA for model hyperparameter selection, improves RNN, and constructs an IoT-UBA model that can adapt to different environmental characteristics. The model can provide more time-series data for more accurate, fast, and convenient IoT services. Furthermore, it can enhance the efficiency of resource allocation within the system.

III. Methods and Materials

This study first conducts relevant data mining and preprocessing based on real IoT user behavior data. Subsequently, the user behavior dataset is employed to train an IoT-UBA model founded upon LSTM-RNN, and BOA is utilized to automatically select model hyper-parameter combinations.

A. Research Data Mining and Preprocessing

The dataset used contains sensor activation data from 00:00:00 to 23:59:59 every second within 30 days in an IoT environment for TWO family members. 86,400s of data are generated every day, with a total of 2,592,000 pieces of data included in the 30 day period. The activation of each sensor represents the use of a certain item, so the activation data of sensors can to some extent represent the behavior of residents in the IoT environment. Table I shows the location, type, and ID of the sensors.

In Table I, the dataset folder "ARAS" contains two folders: "HouseA" and "HouseB", representing two different households. Each household folder contains 30 text files in the format "DAY_x" and one "Readme" text file to explain the basic information of data, sensor information, and activity instructions. Before mining and further processing data, the first is to compress and merge the data. Considering that the IoT-UBA model constructed using RNN is used, this study uses a total of 30 days of monthly data for merging and compression. After conducting a series of pre-experiments, the dataset compressed in units of 20s performs the best in three candidate scenarios: 10s, 20s, and 30s. Therefore, this study will compress the data in units of 20 seconds, meaning that every 20 rows of data will be merged into one row. The merged data in this row will take the maximum activation data of all sensors within 20 seconds, that is, all activated sensors within 20 seconds will be marked as "1". Subsequently, this study formats the data based on the time step determined during the data mining auto-correlation analysis process. The time window processed sequence dataset is shown in Fig. 1.

Dataset $\{x_1, x_2, ..., x_n\}$ is processed into the format shown in Fig. 1 using a time window of length t. The n sequence data are processed into n-t+1 sequence data with a time step of 1. Among them, in the data used, size is to be determined as the hyper-parameter of the model, and the input data dimension is 20 dimensions. The time step is determined by auto-correlation analysis to be 60, which means that the behavior of IoT users in the first 60 time units will have an impact on the current IoT user behavior. The original data consist of 129,600 20 dimensional sensor activation data, with a data format of (129,600*20). After processing through a time window of 60 in length, it has been transformed into a 3D dataset in the shape of (129,541*60*20). Among them, 129,541 is calculated by (129,600-60+1).

TABLE I. ID, TYPE, AND LOCATION OF SENSORS

Sensor ID	Sensor Type	Place
Ph1	Photocell	Wardrobe
Ph2	Photocell	Convertible Couch (Used as bed for Resident 2)
lr1	IR	TV receive
Fol	Force Sensor	Couch
Fo2	Force Sensor	Couch
Di3	Distance	Chan
Di4	Distance	Chair
Ph3	Photocell	Fridge
Ph4	Photocell	Kitchen Drawer
Ph5	Photocell	Wardrobe
Ph6	Photocell	Bathroom Cabinet
Co1	Contact Sensor	House Door
Co2	Contact Sensor	Bathroom Door
Co3	Contact Sensor	Shower Cabinet Door
So1	Sonar Distance	Hall
So2	Sonar Distance	Kitchen
Di1	Distance	Tap
Di2	Distance	Water Closet
Te1	Temperature	Kitchen
Fa3	Force Sensor	Bed

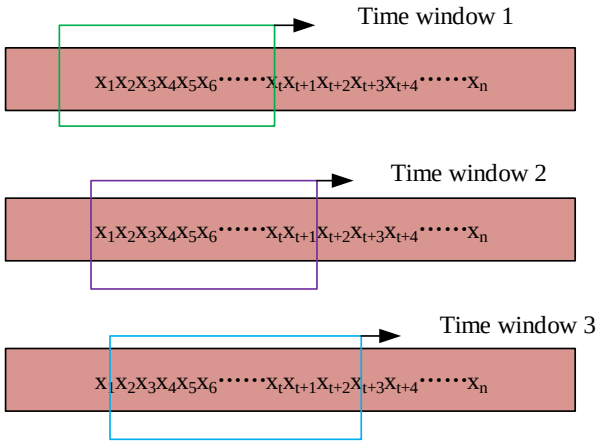


Fig. 1. Time window processed sequential dataset.

The data used in this study is relatively large (greater than 10,000 but less than 100,000), so the data are segmented into a 60% training set, a 20% validation set, and a 20% testing set. After format transformation, 129,541 pieces of data will be divided into the first 77,727, middle 25,907, and last 25,907 pieces according to the time series for model construction. Among them, 77,727 pieces of data are used for the preliminary construction and optimization of the model, and 25,907 pieces of data are used to verify the model's generalization ability during the optimization process. After the model construction is completed, the generalization ability of the final model is tested using the last 25907 pieces of data.

B. Building an IoT-UBA Model Based on Improved RNN

In solving problems related to time series data, complete and continuous strings, images, etc., there is a certain degree of correlation between the front and back data of the dataset involved. That is to say, in model training, the data cannot only enter the neural network unilaterally and independently for parameter training . To build a better IoT-UBA model, it is necessary to fully consider the information carried by the pre-order data in the process of drawing conclusions. Among them, RNN is used to solve sequence related problems. In RNN, the parameter W used for information transmission in hidden states is the same. In the backpropagation gradient descent method used to solve parameters, the chain rule of differentiation will result in the solved gradient containing the multiplication of weights. When the weight value is greater than or less than 1, multiplication will cause the gradient to expand infinitely or approach zero infinitely. The former is called gradient explosion, while the latter is called gradient disappearance. The gradient explosion problem can be solved using gradient truncation, which limits the maximum value of gradients [19-21]. Similarly, if the gradient vanishing problem is to be solved by restricting the minimum value of the gradient, it will result in the obtained weights not reflecting the actual impact of the node well. This study proposes to use LSTM network to solve this problem, and its network structure is shown in Fig. 2.

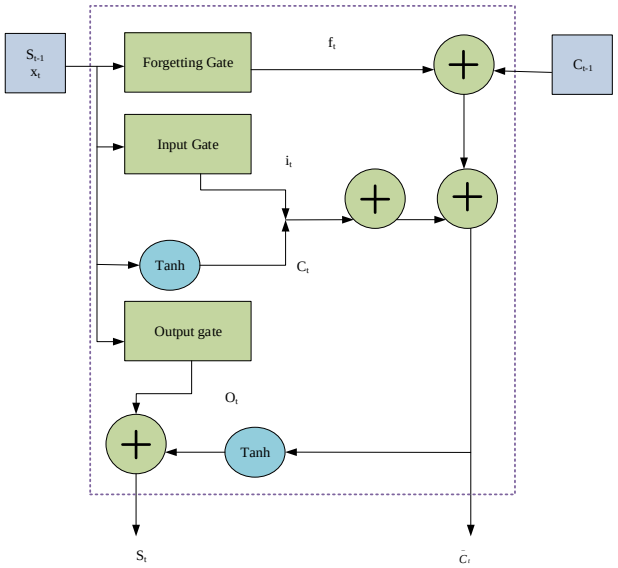


Fig. 2. Internal structure of LSTM unit.

The LSTM unit has three parts: input gate, output gate, and forget gate. The activation function corresponding to the three control gates is the sigmoid function. The output of sigmoid is between 0 and 1. The activation function can be understood as a control valve in the layman's sense, where "0" represents the control valve being closed and the information being completely filtered. "1" represents the control valve closing, and the information is completely retained. By controlling the opening and closing of the valve, important information can be filtered. If the x_t, the previous unit state S_{t-1}, and the long-term state (LTS) C_{t-1} that was memorized in the previous time are input, the unit is entered first and the forget gate is entered next. At this point, a vector f_t composed of numbers is obtained, as shown in Eq. (1).

$$f_t = \sigma\left(W_f \times S_{t-1} + U_f + x_t + b_f\right) \tag{1}$$

In Eq. (1), $f_t \in [0,1]$. W_f, U_f, and b_f represent the weights of the forget gate. The multiplication of f_t and the LTS C_{t-1} from the previous moment determines how much information in C_{t-1} enters C_t, as shown in Eq. (2).

$$K_t = f_t \otimes C_{t-1} \tag{2}$$

In Eq. (2), K_t represents the need to retain the information of the LTS C_t at this moment, and this result will be used as one of the inputs to the input gate. In the input gate, x_t and S_{t-1} are processed by a tanh function to obtain the information $\bar{C}_t$ of the LTS to be added, as shown in Eq. (3).

$$\bar{C}_t = \tanh\left(W_C \times S_t - 1 + U_C + x_t + b_C\right) \tag{3}$$

In Eq. (3), W_C, U_C, and b_C represent the weights of long-term unit states, similar to forgetting gates. x_t and S_{t-1} will also pass through a signoid function to obtain a vector i_t composed of numbers. This vector is multiplied by $\bar{C}_t$ to determine how much information needs to be added to the LTS C_t at this moment, as shown in Eq. (4).

$$i_t = \sigma\left(W_i \times S_{t-1} + U_i + x_t + b_i\right) \tag{4}$$

In Eq. (1), $i_t \in [0,1]$. W_i, U_i, and b_i are the weights of the input gate. By combining the calculation results of the forget and input gates, the LTS C_t is obtained, as shown in Eq. (5).

$$C_t = K_t + i_t \otimes \bar{C}_t \tag{5}$$

In Eq. (5), C_t is only transmitted within the network and will be passed to the next unit as one of the inputs to the next unit. Similarly, passing through the signoid function will generate a numerical vector o_t, as shown in Eq. (6).

$$o_t = \sigma\left(W_o \times S_{t-1} + U_o + x_t + b_o\right) \tag{6}$$

The LTS C_t at this moment is processed by the tanh function and multiplied by o_t to determine how much information in the LTS C_t is output as the unit state S_t at that moment, as shown in Eq. (7).

$$S_t = o_t \otimes \tanh\left(C_t\right) \tag{7}$$

Among them, the unit state S_t on the last time step is the final output of the model. After each batch of data is transmitted into the network, parameters are updated through gradient descent to reduce the loss between actual and predicted values. This study uses binary cross entropy as the loss function M, as shown in Eq. (8).

$$M = -\frac{1}{20}\sum_{I=1}^{20}\left[y_i \log\left(\bar{y}_i\right) + \left(1 - y_i\right)\log\left(1 - \bar{y}_i\right)\right] \tag{8}$$

In Eq. (8), y represents the numerical vector of the true value. $\bar{y}$ represents the numerical vector of the predicted value. In relatively fixed and bounded usage scenarios like IoT, user behavior interacts with relatively fixed objects within a certain range, with limited influencing factors and following certain patterns. To this end, an IoT-UBA model is constructed based on LSTM, as shown in Fig. 3.

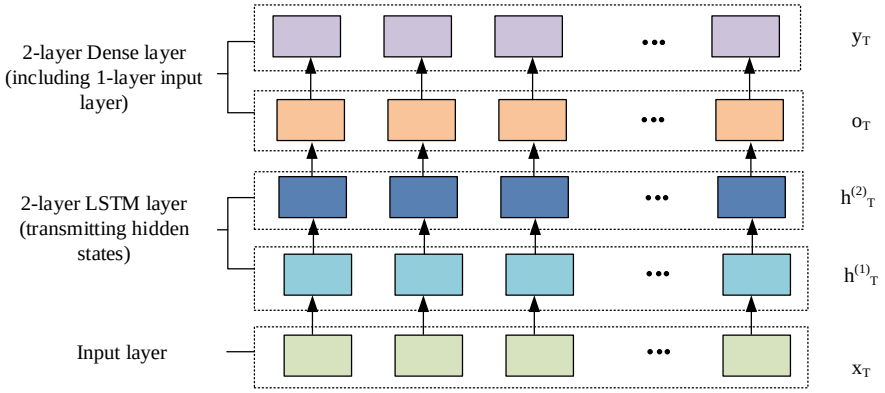


Fig. 3. Schematic diagram of the research model.

This model is a neural network model consisting of two LSTM layers, one Dense layer, and one output layer. On the data of each time step t (t∈[1,T])) with a total of T time steps, the hidden state $h_t^{(1)}$ (t∈[1, T]) of the first layer LSTM layer and the hidden state $h_t^{(2)}$ (t∈[1,T])) of the second layer LSTM layer will be passed to the next LSTM layer at the next time step. Moreover, the hidden state includes LTS C_t^i (i∈[1,2],t∈[1,T]) and short-term state S_t^i (i∈[1,2],t∈[1,T]), thereby achieving the effect of memorizing the hidden information in the preceding data. In addition, this study relies on experience to select hyperparameters that may have a better analytical effect on the model (Table II).

TABLE II. SELECTION OF MODEL HYPERPARAMETERS

Hyper-parameter	Value	Type
Lstm_layer	2	int
Activation_lstm	Tanh	string
Lstm_output_dim	110	int
Dense_layer	2	int
Activation_dense	Softsign	string
Activation last	Sigmoid	string
Drop_out	0.2	float
Batch_size	64	int
Nb_epoch	4	int
Optimizer	Rmsprop	string
Loss	Binary cross entropy	string

C. Optimization of Hyperparameters Based on BOA

After constructing an IoT-UBA model based on LSTM, it is found that having too many hyperparameters can lead to an increase in model complexity and easily lead to overfitting. To solve overfitting problems and improve model generalization ability, ML engineers generally adjust hyper-parameter combinations based on experience to achieve a better level of generalization [22]. However, manual parameter tuning is difficult to fully consider all relevant influencing factors and historical performance. Even though time and manpower are spent manually adjusting parameters and achieved good results, the constructed prediction model only performs well in the IoT-UBA corresponding to specific datasets. The predictive ability of this hyperparameter combination among more IoT users is still unknown [23]. This study proposes using BOA to construct an adaptive hyperparameter selection algorithm, selecting personalized hyperparameter combinations that perform best for different users. The purpose of hyperparameter optimization (HPO) in ML is to find the hyper-parameters of a given ML, which returns the best performance measured on the validation set. Unlike model parameters, hyperparameters need to be set before training. The HPO equation is shown in Eq. (9).

$$\lambda = \arg\min_{\lambda \subseteq x} f(\lambda) \tag{9}$$

In Eq. (9), λ represents the hyperparameter and $f(\lambda)$ represents the minimum objective score evaluated on the validation set, which is also the loss that needs to be optimized for the model. BOA combines the advantages of manual parameter tuning with manual experience and grid search, as well as automatic selection through random search, to track past evaluation results. It forms a probability model by using these results, seeking a combination of hyperparameters in the

probability model that can minimize losses. Before using automatic optimization algorithms to search for the optimal combination of hyperparameters, it is necessary to define the domain space for hyperparameter search. This study constructs a large-scale hyperparameter domain space based on the research model. HPO requires defining the objective of BOA optimization, which is the loss of the objective function. The ultimate goal of selecting hyperparameter combinations in this study is to improve the model's generalization ability. The greater the generalization ability of the model, the better, but the loss of the BOA function can only be the minimum value, so the loss value Q of BIA is shown in Eq. (9).

$$Q = 1 - Pa \quad (9)$$

In Eq. (9), Pa represents the PA of the test set. To learn the "black box" between hyperparameter combinations and optimization objectives, this study uses tree-structured Parzen estimator (TPE) to construct optimization algorithms. The TPE algorithm can construct a probability model for optimization objectives by combining existing hyperparameters and their corresponding loss values. Through this probability model, it is possible to find the hyperparameter combination that minimizes the optimization objective and maximizes the probability. Then, based on the selected hyperparameter combination, the trained model updates the input-output pairs and continues to construct a new probability model. Cycling the above process until the loss value reaches its lowest point, and thus completing the construction of the IoT-UBA model based on improved RNN. The construction process of the model is shown in Fig. 4.

The research model construction in Fig. 4 first involves data mining and preprocessing based on real IoT user behavior data. Then, a prediction model needs to be constructed based on LSTM network, and hyperparameters need to be selected based on experience. Finally, BOA is used to automatically select model hyperparameter combinations.

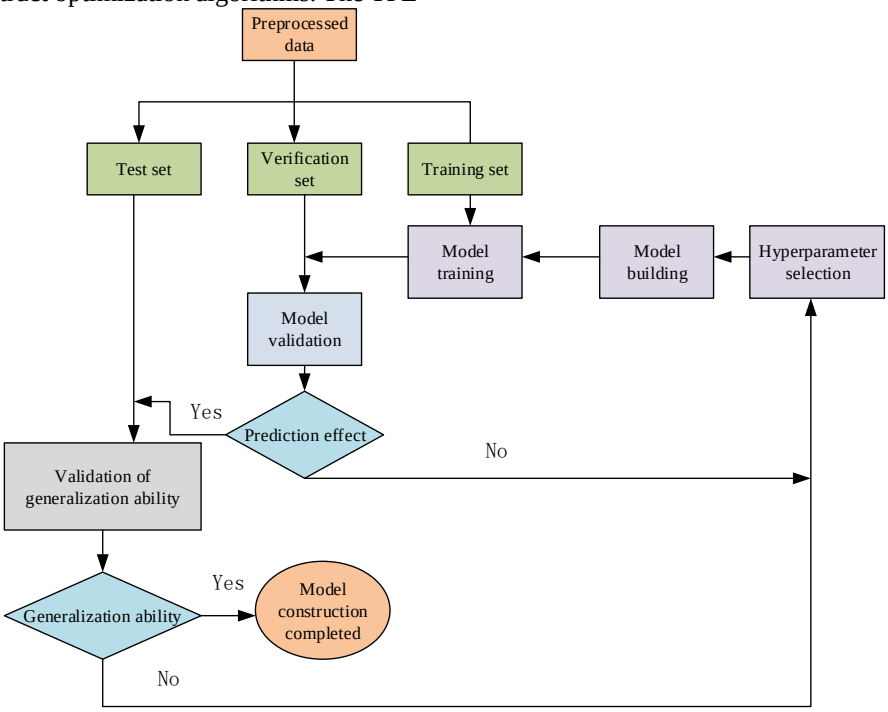


Fig. 4. Model construction process.

IV. RESULTS

A. Training and Validation of Research Models

To test the model effectiveness, this experiment uses the processed training and validation sets for model training and validation and uses the test set to test the model's generalization ability. Table III shows the relevant experimental environments.

This experiment is conducted using XiaoXinPro 14ITL 2021, with a processor environment of 11th GenIntel(R)Core (TM)i5-1135G7@2.40GHz-2.42GHz, a memory capacity of 16.0GB, and the operating system of Windows10. The software used in data mining is SPSS Modeler18.0. The programming environment involved is Python 3.8.3 and the programming IDE used is Anaconda3. Python is used for data preprocessing, model construction, and optimization algorithms. The divided training set and validation set are put into the constructed model. Based on research data and model characteristics, binary classification accuracy is used as a measure of model PA and binary classification cross entropy is adopted as a loss function. The training results of the research model are displayed in Fig. 5.

In Fig. 5, as the training iteration progresses, the loss of the research model on the training and validation sets decreases continuously. At the completion of the last epoch of training, the loss on the training set decreases from the initial 0.1800 to 0.1084, and on the validation set from the initial 0.1362 to 0.0915. The learning ability of the model continues to improve. The PA of the model on both the training and validation sets

surpasses 90%, and as the iteration process continues to rise, the final accuracy reaches 96.8% and 97.53%. The dataset, hyperparameter domain space, and objective function are input into BOA, and the hyperparameter combinations selected for each iteration of BOA, their corresponding training time, and loss values are recorded for tracking optimization history. The optimal combination of hyperparameters for localization prediction is shown in Fig. 6.

TABLE III. EXPERIMENTAL OPERATING ENVIRONMENT

Parameter	Experimental Environment
Tool	XiaoXinPro 14ITL 2021
Processor	11th GenIntel(R)Core (TM)i5-1135G7@2.40GHz-2.42GHz
Memory capacity	16.0GB
Operating system	Windows10
Data mining software	SPSS Modeler18.0
Programming environment	Python3.8.3
Programming IDE	Anaconda3
model building	Python3.8.3

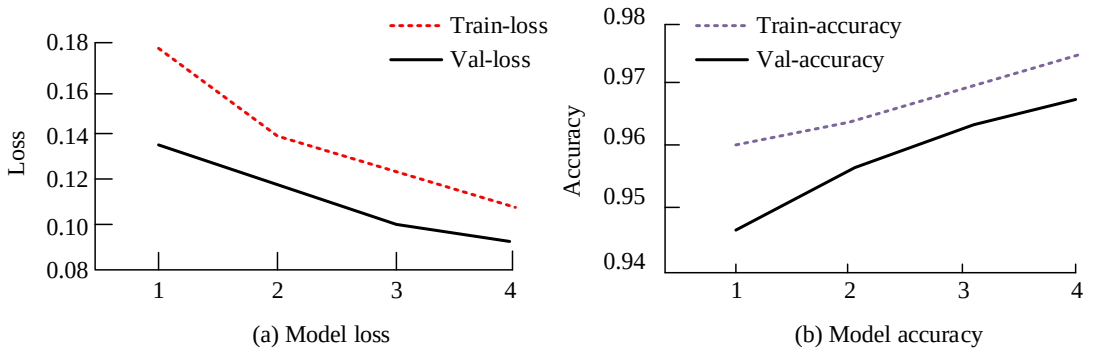


Fig. 5. Model training results.

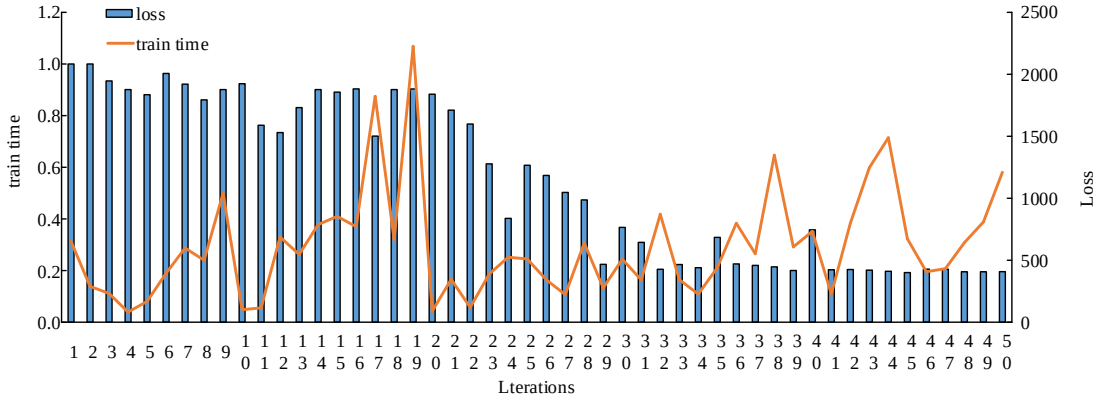


Fig. 6. Iteration loss and training time.

In Fig. 6, the loss shows a significant downward trend with the number of iterations, indicating that when selecting hyperparameter combinations, BOA will choose hyperparameters that are more likely to perform better based on the probability model of the loss with respect to hyperparameters. In the set maximum of 50 iterations, the loss of the objective function reaches its minimum value in the 45th iteration, and the optimal model loss trains under the corresponding hyperparameter combination conditions in this iteration is 0.19. The model's PA on the test set reaches 80.78%, showing that BOA enhances its generalization ability, and searches for a model hyperparameter combination with better prediction ability based on the user behavior characteristics in the IoT environment. To further validate the improved RNN in IoT-UBA, a similar neural network model is constructed using traditional RNN, and BOA is also used to select the optimal hyper-parameter combination. The experimental results are shown in Fig. 7.

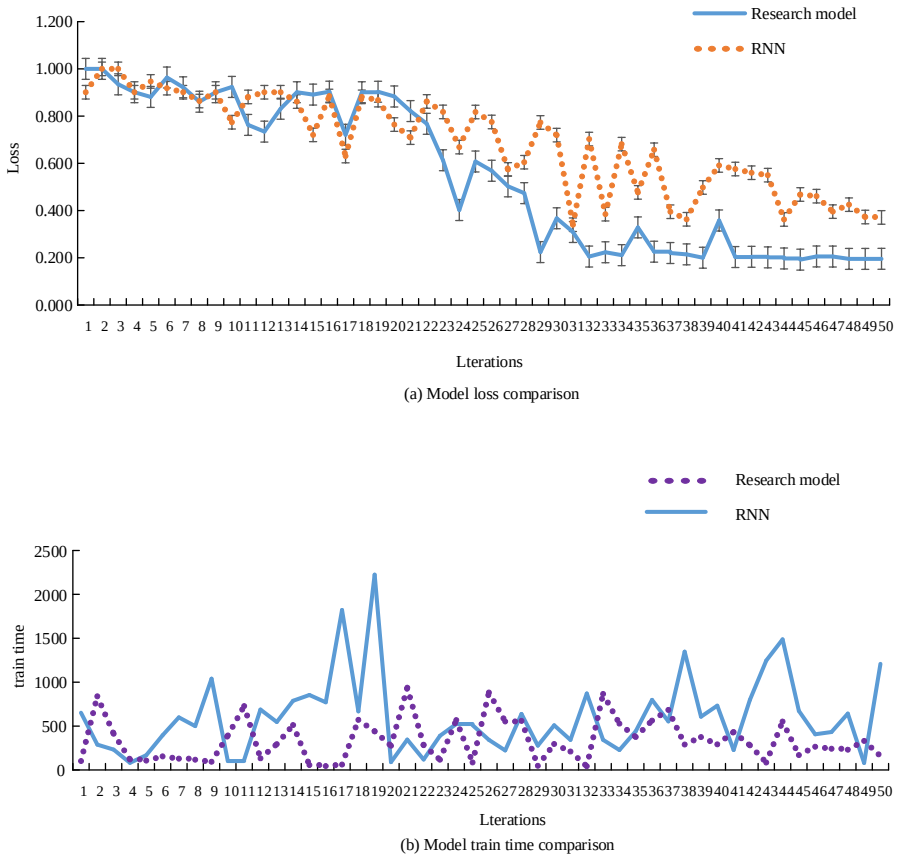


Fig. 7. Comparison of research model and RNN model effects.

Fig. 7 (a) shows the comparison of the loss value changes between the traditional RNN model iteration process and the research model. Both models show a spiral downward trend as the iterations increase. Among them, the minimum loss value of the traditional RNN is 0.34, which means its best PA is only 66.01%, lower than the 80.78% of the research model. Fig. 7 (b) shows the comparison of training time between LSTM and RNN models. The research model reaches the minimum loss value in the 31st iteration, while RNN only selects the optimal hyper-parameter combination in the 45th iteration. The average training time for the research model is 338 seconds, and this value for the RNN model reaches 614 seconds. In terms of iteration times and training time, the research model is significantly better than the RNN model.

B. *Application of Research Models in Short-term Power Load Forecasting*

To test the practicality of the IoT-UBA built on improved RNN, this study selects two benchmark models, auto-regression model (AR) and back propagation neural network (BPNN), to validate the proposed improved RNN model. This study selects three different datasets, namely three load datasets provided by official websites in three foreign regions. The first one is the electricity load data of region A from February 1, 2023 to August 31, 2023, with a sampling rate of 1 hour and a sample size of 5112. The second one is the electricity load data of region B for the whole year of 2023, with a sampling rate of 1 hour and a sample size of 8760. The third one is the electricity load data of region C for the whole year of 2023, with a sampling rate of 1 hour and a sample size of 8760. The power load data of these three regions are processed through data preprocessing and the processed data are divided into datasets. The daily load forecasting results of each model on three different datasets are displayed in Fig. 8.

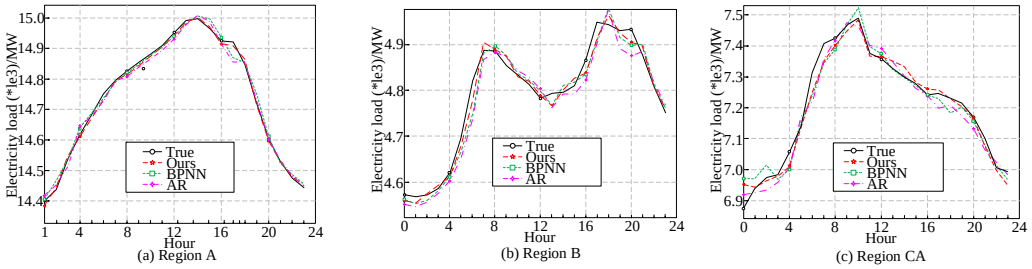


Fig. 8. Daily load forecasting results of each model on three different datasets.

From Fig. 8 (a), in region A, the prediction effect of each model is overall and the load prediction curve in the figure almost coincides with the actual situation. However, Fig. 8 (a) shows that the prediction effect of the research model is better than that of other comparison models. In particular, in the two periods of 13:00 and 17:00, the error rate of the research model is only 0.13% and 0.09%, which is small and has more accurate PA than the comparison model. In the data set of Fig. 8 (b) in region B, in general, at the very beginning, each model has a good prediction effect. However, with the increase of mean absolute percentage error (MAPE), the deviation between the prediction of various models and the reality are increasing, which leads to the decrease of the accuracy of the prediction. Especially in the period of 20:00, each model prediction deviation reaches the largest. The AR model, BPNN model, and acting model of daily load prediction error rates reach 12.13%, 5.72%, and 1.39%, respectively. Among them, the research model error rate is lower than other contrast model. The prediction results and the actual load change trend are the most consistent and the performance effect is better. In region C of Fig. 8 (c), in general, the prediction effect of each model is not good. With the increase of MAPE, the deviation between the prediction of various models and the reality are increasing, leading to a decrease in the accuracy of the prediction. Among them, the period of 2:00 appears the largest prediction error. In the 17:00 period, the AR model reaches the largest error in the prediction. In both 2:00 and 17:00, the prediction effect of the research model is relatively excellent. This indicates that although traditional power system modeling methods can describe the overall trend of the power system, as the complexity of the system increases, the operational efficiency of the power system also decreases, resulting in huge economic losses to the power system. The root mean square error (RMSE) and MAPE of load forecasting for each model within seven days are exhibited in Fig. 9.

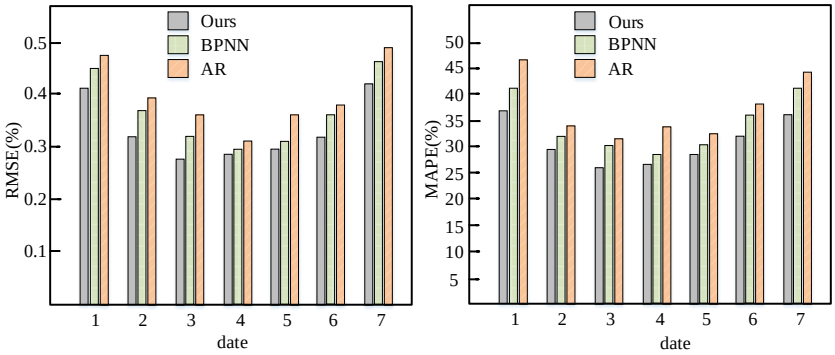


Fig. 9. Comparison of weekly load prediction errors among different models.

In Fig. 9, the weekly load PA of the IoT-UBA is much better than that of BPNN and AR, and BPNN is higher than AR. The comparison between its predicted load value and the actual load value shows that through more accurate prediction of user behavior, the prediction of load value has completed a good level.

V. Discussion

As the IoT technology becomes increasingly pervasive in all aspects of people's daily lives, the collection of user data within IoT systems will become more comprehensive. The data accurately reflect the behavioral patterns and living habits of users. Providing better services and timely responses to users, effectively utilizing this information to predict user behavior and needs, and systematically improving management and service quality are key to enhancing the competitiveness and service level of various industries in the future. The proposed method sets a maximum of 50 iterations. At 45 iterations, the objective function has the smallest loss, and the optimal model has a loss of only 0.19 (test set), with an accuracy of 80.78%. The results of this study are consistent with the predictions of the lightweight dense random neural network proposed by Latif et al. [24] for IoT intrusion detection, and the model performs well. This is because when selecting appropriate inputs for the research model, BOA selects a more promising hyperparameter based on loss estimation. This can search for super parameter combinations with higher predictive performance based on user behavior characteristics in IoT scenarios, thereby enhancing the performance of the model. In this study, the model lost the smallest loss in 31 cycles, the best PA was 80.78%, and the learning time was 338s, which showed better performance. However, the accuracy of the industrial IoT detection method based on graph neural network proposed by Wu et al. [25] can only reached 79.71%. This is because the hyperparameters have been optimized, shortening the iteration and learning time of the model, thereby improving its generalization ability. In summary, the analysis shows that using BOA to select model hyperparameter combinations further improves the generalization ability of the prediction model, enabling the model to construct adaptive prediction models based on the characteristics of different users in different IoT environments.

VI. Conclusion

In response to the current problems in the application of IoT technology, this study utilized BOA to construct an IoT-UBA model based on an improved RNN that can adapt to different environmental characteristics. The results demonstrated that the PA of the research model on both the training and validation sets was greater than 90%, and as the iteration process continued to increase, the final accuracy reached 96.8% and 97.53%. In 50 maximum iterations, the model achieved a PA of 80.78% on the test set. In the comparison of the performance between the research model and RNN, the minimum loss value of traditional RNN was 0.34, which meat its best PA was only 66.01%, lower than the 80.78% of the research model. The research model reached the minimum loss value in the 31st

iteration, while RNN only selected the optimal hyper-parameter combination in the 45th iteration. The average training time for the research model was 338 seconds, and this value for the RNN model reached 614 seconds. In terms of iteration times and training time, the research model was significantly better than the RNN model. The application results of the research model in short-term power load forecasting also indicated that the PA of the IoT-UBA model based on improved RNN has reached a good level, far superior to other comparative models. However, this study is based on a sufficient amount of historical user behavior data. In practical use, the IoT-UBA model will inevitably face the situation of insufficient historical user behavior data at the initial startup of the system. In the future, in-depth research will be conducted in this area.

REFERENCES

[1] Sarker I H, Khan A I, Abushark Y Bl. Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 2023, 28(1): 296-312.

[2] Liu Y, Wang J, Li J. Machine learning for the detection and identification of Internet of Things devices: A survey. IEEE Internet of Things Journal, 2021, 9(1): 298-320.

[3] Saheed Y K, Abiodun A I, Misra S. A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 2022, 61(12): 9395-9409.

[4] Ullah A, Anwar S M, Li J. Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment. Complex & Intelligent Systems, 2024, 10(1): 1607-1637.

[5] Zhou H, She C, Deng Y. Machine learning for massive industrial internet of things. IEEE Wireless Communications, 2021, 28(4): 81-87.

[6] Saharkhizan M, Azmoodeh A, Dehghantanha A. An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic. IEEE Internet of Things Journal, 2020, 7(9): 8852-8859.

[7] Khalil R A, Saeed N, Masood M. Deep learning in the industrial internet of things: Potentials, challenges, and emerging applications. IEEE Internet of Things Journal, 2021, 8(14): 11016-11040.

[8] K. Bhosle and V. Musande.Evaluation of Deep Learning CNN Model for Recognition of Devanagari Digit. Artif. Intell. Appl.2023,1(2):114-11.

[9] Hou R, Kong Y Q, Cai B. Unstructured big data analysis algorithm and simulation of Internet of Things based on machine learning. Neural Computing and Applications, 2020, 32(10): 5399-5407.

[10] Abdelmoumin G, Rawat D B, Rahman A. On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the internet of things. IEEE Internet of Things Journal, 2021, 9(6): 4280-4290.

[11] Xu H, Sun Z, Cao Y. A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things. Soft Computing, 2023, 27(19): 14469-14481.

[12] Alsheikh M A, Hoang D T, Niyato D. Optimal pricing of Internet of Things: A machine learning approach. IEEE Journal on Selected Areas in Communications, 2020, 38(4): 669-684.

[13] Woźniak M, Siłka J, Wieczorek M. Recurrent neural network model for IoT and networking malware threat detection. IEEE Transactions on Industrial Informatics, 2020, 17(8): 5583-5594.

[14] Zhao R, Gui G, Xue Z. A novel intrusion detection method based on lightweight neural network for internet of things. IEEE Internet of Things Journal, 2021, 9(12): 9960-9972.

[15] Sakar C O, Polat S O, Katircioglu M. Real-time prediction of online shoppers' purchasing intention using multilayer perceptron and LSTM recurrent neural networks. Neural Computing and Applications, 2019, 31(10): 6893-6908.

[16] Liu Z, Liu Q, Xu W. Deep learning-based human motion prediction considering context awareness for human-robot collaboration in manufacturing. procedia cirp, 2019, 1(83): 272-278.

[17] Huang X, Sun J, Sun J. A car-following model considering asymmetric driving behavior based on long short-term memory neural networks. Transportation research part C: emerging technologies, 2018, 1(95): 346-362.

[18] Chen Y, Hu C, Wang J. Human-centered trajectory tracking control for autonomous vehicles with driver cut-in behavior prediction. IEEE Transactions on Vehicular Technology, 2019, 68(9): 8461-8471.

[19] Wijnands J S, Thompson J, Aschwanden G D P A. Identifying behavioural change among drivers using Long Short-Term Memory recurrent neural networks. Transportation research part F: traffic psychology and behaviour, 2018, 1(53): 34-49.

[20] Pei Z, Qi X, Zhang Y. Human trajectory prediction in crowded scene using social-affinity long short-term memory. Pattern Recognition, 2019, 1(93): 273-282.

[21] Chander N, Upendra Kumar M. Metaheuristic feature selection with deep learning enabled cascaded recurrent neural network for anomaly detection in Industrial Internet of Things environment. Cluster Computing, 2023, 26(3): 1801-1819.

[22] Belhadi A, Djenouri Y, Djenouri D. Group intrusion detection in the Internet of Things using a hybrid recurrent neural network. Cluster Computing, 2023, 26(2): 1147-1158.

[23] Thota S, Menaka D. Botnet detection in the internet-of-things networks using convolutional neural network with pelican optimization algorithm. Automatika, 2024, 65(1): 250-260.

[24] Latif S, e Huma Z, Jamal S S. Intrusion detection framework for the internet of things using a dense random neural network. IEEE Transactions on Industrial Informatics, 2021, 18(9): 6435-6444.

[25] Wu Y, Dai H N, Tang H. Graph neural networks for anomaly detection in industrial internet of things. IEEE Internet of Things Journal, 2021, 9(12): 9214-9231.

Network Security Based on Improved Genetic Algorithm and Weighted Error Back-Propagation Algorithm

Junjuan Liang
Henan Polytechnic Institute, Nanyang, 473000, China

***Abstract*—In order to solve the problem of feature selection and local optimal solution in the field of network security, a network security protection model based on improved genetic algorithm and weighted error back-propagation algorithm is proposed. The model combines the dynamic error weight and adaptive learning rate of the weighted error back-propagation algorithm to improve the learning ability of the model in dealing with classification imbalance and dynamic attack mode. In addition, the global search capability of genetic algorithm is utilized to optimize the feature selection process and automatically adjust the hyperparameter settings. The experimental results show that the proposed model has an average accuracy of 96.7%, a recall rate of 93.3% and an F1 value of 0.91 on the CIC-IDS-2017 dataset, which has significant advantages over traditional detection methods. In many experiments, the accuracy of normal data is up to 99.97%, the accuracy of known abnormal behavior data is 99.31%, and the accuracy of unknown abnormal behavior data is 98.13%. These results show that this method has high efficiency and reliability when dealing with complex network traffic, and provides a new idea and method for network security protection research.**

***Keywords*—Genetic algorithm; weighted error back-propagation; multiple strategies; network security**

I. INTRODUCTION

With the speedy prosperity of information technology, network security matters have become more and more notable, and the ways of network attacks have become more complex and diverse. These attacks not only affect the operations of businesses and government agencies, but also pose a significant threat to the privacy and data security of individual users [1]. At the same time, with the rapid growth of network traffic, how to effectively detect and identify potential security threats has become a non-negligible problem that requires urgent handling in the current field of network security. Traditional network security detection methods often rely on matching rules or feature libraries, making it difficult to cope with rapidly evolving attack patterns [2-3].

Thus, a lot of domestic and foreign researchers have promoted in-depth study on network security detection. Wei K et al. focused on optimizing network intrusion detection technology, using a combination of algorithm technology and artificial intelligence to achieve intrusion detection and defense of network security systems. Focusing on the issues of low efficiency and poor detection precision of classical K-means clustering algorithm, an improved K-means clustering algorithm network security detection model was proposed, and experiments were conducted using a dataset. The results indicated that this improvement measure could significantly improve detection efficiency and accuracy [4]. Chen Z optimized traditional network security detection algorithms in response to constantly changing and upgrading network attack techniques. A new network security detection model was constructed using radial basis function neural networks as the main body, optimized through simulated annealing algorithm and hybrid hierarchical genetic algorithm (GA), and relevant experiments were conducted. The results showed that the optimized detection model's predicted values in 15 samples highly approached the true values, which could provide assistance for maintaining network security [5]. Khan M and Ghafoor L explored the special challenges brought by adversarial attacks in the field of network security, and strengthened machine learning-based network security detection systems to address challenges such as the dynamic nature of network environments and the need for real-time decision-making. The experimental results indicated that the research method could provide more powerful and resilient solutions when facing network attacks [6]. Yin L and Zhang D raised a network security detection algorithm grounded on vague reasoning. Firstly, they combined fuzzy reasoning and probability density features to evaluate security data. Then the features of network intrusion data were extracted to achieve safety possibility computation and virus attack detection. The data showed that the raised algorithm had higher calculation precision for network safety possibility, achieved network safety possibility computation and data checking, and enhanced the network's security defense capability [7].

Memon I proposed an authentication key establishment protocol based on IPv6 to protect sensitive information in road network environment. The protocol eliminated duplicate address detection by allowing a moving vehicle to pick up a unique address from a neighboring vehicle or roadside unit, while automatically recycling the address space leaving the vehicle for reallocation. The proposed protocol had the characteristics of anonymous authentication, confidentiality and high efficiency, and the evaluation results showed that the protocol effectively improved the performance of address configuration, and was also very secure in preventing passive and active attacks [8]. Aiming at the growing network demand and massive data traffic management, Farhan N et al. proposed a method based on hybrid clustering to improve the wireless resource management effect of heterogeneous networks [9]. By

analyzing different clustering classifications and existing technologies, they aim to achieve high throughput, low interference and low latency in ultra-dense networks. The results showed that the hybrid clustering technology could effectively improve the wireless resource management in HetNets, increase throughput, and reduce the inter-layer and intra-layer interference, thus enhancing the network performance. Junejo M H et al. addressed the growing security threat in Vehicle ad-hoc networks (VANETs) by proposing cybersecurity solutions that combined machine learning and artificial intelligence techniques to enhance the safety and efficiency of public transportation. In this study, the trust mechanism was compared with cryptography, and its different performance in VANET application and security requirements was analyzed [10]. Although the above methods have high recognition accuracy in the known attack behavior, they may have limitations in the face of new and unknown attack modes. In the actual network environment, the characteristics of network traffic may change with time, and the strategies and techniques of attackers also develop dynamically. Although the feature selection of the current model is optimized based on GA, how to dynamically update and re-select the features to adapt to such changes is still an urgent problem to be solved.

Therefore, a network security protection model based on Weighted Error Back-Propagation (WEBP) and Improved GA (IGA) is proposed in this study. Compared with the existing researches, the main objective of this study is to solve the problem that the efficiency of feature selection is insufficient, resulting in insufficient model learning, and thus affecting the detection accuracy and efficiency. The study is also devoted to solving the problem that the fixed learning rate is difficult to adjust dynamically and cannot adapt to the change of data flow in real time, which is easy to cause the model to fall into the local optimal. Moreover, the study hopes to address the problem that current methods are unable to respond to rapidly evolving attack patterns in a timely and effective manner. The innovation of this model lies in the introduction of a weighted error mechanism, which allows the model to adjust the learning process based on the importance of different samples, thereby improving its adaptability to complex network environments and combining the population search characteristics of GA. Feature selection and hyperparameter optimization are implemented to enhance the global search capacity and robustness of the model. The contribution of the research is to solve the problem of low feature selection efficiency on high-dimensional data, so as to effectively improve model performance and learning efficiency. It provides an effective solution for the field of network security detection, can better deal with the complex network attack mode, and provides a new idea for the practical application of data protection and network firewall.

The research structure mainly includes four parts. The first part constructs the network security detection model based on the WEBP algorithm, analyzes the limitations of the model, and further optimizes it. The second part verifies the performance of the proposed model, and designs experiments to analyze the network security protection capability of the proposed model. The third part is the summary and analysis of the experimental results, and the comparison with the same type of research, emphasizing the advantages of the research method. The last part summarizes the content of the article, and points out the current limitations and future development direction.

II. Methods and Materials

A. Network Security Detection Model Grounded on WEBP Algorithm

WEBP is an improved Back-Propagation Neural Network (BPNN). In traditional back-propagation algorithms, all training samples are assigned the same importance, while the WEBP algorithm allows for adjusting errors during the training process based on the importance or confidence of different samples [11-12]. WEBP essentially introduces error weights in the back-propagation of BPNN to adjust errors. BPNN is a widely studied algorithm in ANN, with the core idea of bidirectional signal transmission [13-14]. Forward transmission refers to the sequential transmission from the input end to the output end. Reverse propagation is when there is a deviation in the results during forward propagation, and the error results are reversed and distributed to each layer structure to correct the weights in the structure [15]. BPNN is usually constructed from three parts: Input Layer (IL), Hidden Layer (HL), and Output Layer (OL). The specific composition model is shown in Fig. 1.

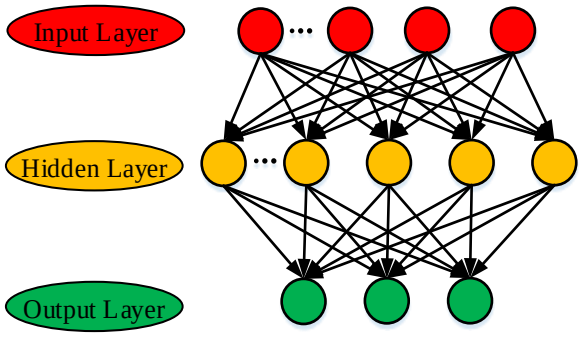


Fig. 1. Example diagram of BPNN structure.

In Fig. 1, after receiving the information data from IL, HL in the BPNN structure will pass the data information to the next layer through a weight function and organize it in the last layer to obtain the final output data. At the same time, BPNN continuously adjusts the weights and thresholds of the structure grounded on the deviation values between the output results and the actual results. The amount of neurons in the IL and OL is defined by the dimensions of the input samples and output results, respectively. However, the selection of neurons in the HL is more sophisticated, and the current intelligence determines it through empirical formulas, as shown in Formula (1).

$$O = \sqrt{n+m} + a \tag{1}$$

1. In Formula (1), 0 represents the HL neuron. n and m represent the number of neurons in the IL and OL separately. a represents a constant, with values ranging from [1,10]. Formula (1) in network security, the strong generalization ability enables the model to handle unseen attack patterns and normal data, effectively identifying potential

threats. In conventional BPNN, using a fixed learning rate makes it difficult to ensure the network has the best learning efficiency in realistic tasks. To solve this issue, research is being conducted on using adaptive learning rates in network structures. Assuming the initial learning rate is $\mu(0)$ and the network fault obtained by the model during the iteration process is denoted as $E(n)$, the change in learning rate is shown in Formula (2).

$$\mu(n)=\begin{cases}\beta\mu(n-1) & E(n)<E(n-1),(1<\beta<1.5)\\ \gamma\mu(n-1) & E(n)>E(n-1),(0.5<\gamma<1)\\ \mu(n-1) & other\end{cases} \quad (2)$$

In Formula (2), β and γ represent constant coefficients, with values of 1.05 and 0.7, respectively. Formula (2) In the dynamic environment of network security, attack patterns and normal traffic are constantly changing, and adaptive learning rates can make the model more flexible in adapting to these changes. In the process of error back-propagation, adaptive adjustment of learning rate can effectively improve convergence speed. Nevertheless, the model continues to disregard the direction of gradient descent throughout the entire process, which renders the model unstable and susceptible to becoming trapped in local optima. The problem of gradient descent direction is solved by introducing error weights, and its description is represented in Formula (3).

$$\Delta w(n)=\alpha\Delta w(n-1)-\mu\frac{\partial E(n)}{\partial w(n)} \quad (3)$$

In Formula (3), α is the momentum term and w represents the weight. Formula (3) can be regarded as a first-order difference formula of $\Delta w(n)$, and its formula is represented in Formula (4).

$$\Delta w(n)=-\mu\sum_{t=0}^{n}\alpha^{n-t}\frac{\partial E(n)}{\partial w(n)} \quad (4)$$

In Formula (4), t represents the time series. The above is the correction of weights, and the specific way to adjust the weights of BPNN is shown in Formula (5).

$$w(n+1)=w(n)-\mu(n)\sum_{t=0}^{N}\alpha^{n-t}\frac{\partial E(n)}{\partial w(n)} \quad (5)$$

Formulas (4) and (5) provide specific methods for weight updating, enabling the model to more accurately correct weights and adapt to new data inputs. In network security protection, it can help detection models quickly adjust to adapt to new threats.

B. Construction of Network Security Protection Model Based on GA-WEBP

Although WEBP improves the performance of BPNN by introducing mechanisms such as weights and adaptive learning rates, the capacity of the model largely relies on the selection and representation of input features. Incorrect or insufficient feature selection may result in the model learning insufficient information, while traditional feature selection methods may be inefficient in processing high-dimensional data. In the field of network security, the feature space is usually large, and anomaly detection is highly sensitive to features. Therefore, the study optimized the model by introducing GA. The logic of GA is represented in Fig. 2.

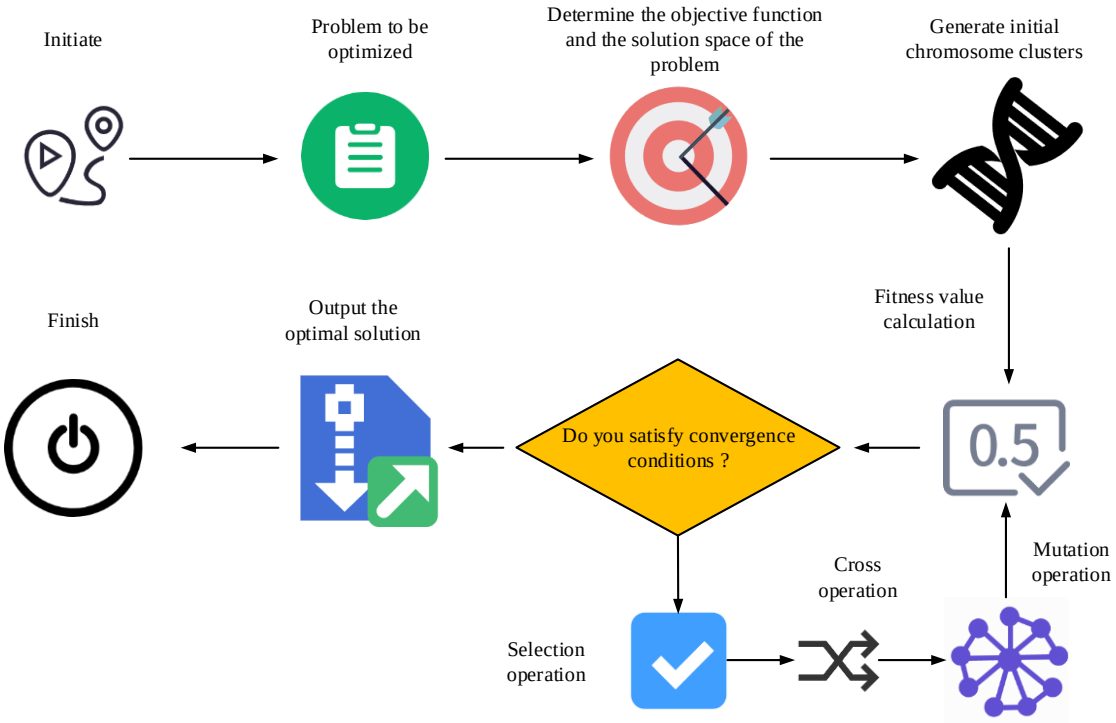


Fig. 2. Schematic diagram of GA process.

In Fig. 2, during the initial stage of GA, the algorithm randomly generates a series of individuals and evaluates each individual based on a predetermined goal, assigning them a fitness value. By comparing these fitness values, individuals who perform well as the new generation are selected. On this basis, screening is conducted to eliminate individuals with poor performance [13-14]. Then, the selected individuals are recombined through crossover and mutation operations to produce the next generation of individuals with excellent traits, gradually approaching the best remedy. Finally, the optimal one is extracted from the last generation population to obtain an approximate optimal solution to the problem. Overall, the process of traditional Gas involves encoding, selection, crossover, and mutation [15-16]. Finally, when the termination conditions are met, that is, when the specified number of iterations or iteration accuracy is reached, as well as the target conditions, the iteration can be stopped. In network security protection, binary encoding is studied as the encoding method for Gas. The second step is the selection operation, which selects high-quality individuals based on their fitness in the environment, in order to use them for generating the next generation. This step is grounded on the law of natural selection, where individuals with greater fitness have a greater possibility of being chosen, while individuals with less fitness have a smaller possibility of being chosen. The study used random sampling as the model selection operation, in which the selection probability of each individual is grounded on their fitness, but the selection process is random. This means that even individuals with lower fitness have the opportunity to be chosen. The possibility of an individual being chosen is shown in Formula (6) [20].

$$F(x_i)=\frac{f(x_i)}{\sum_{i=1}^{Nind} f(x_i)} \tag{6}$$

In Formula (14), $F(x_i)$ points to the fitness of an individual. In network security, fitness usually reflects the effectiveness of an individual under specific security policies or protective measures, such as the ability to detect attacks and reduce false positive rates. $f(x_i)$ points to the possibility of an individual being chosen. In network security applications, this probability determines which individuals (i.e. protection policies or system configurations) can continue to be optimized and evolved, playing a crucial part in improving the comprehensive security of the system. The GA increases the fitness value of individuals by performing crossover operations on different parents in the third step, where the single point crossover structure is shown in Fig. 3.

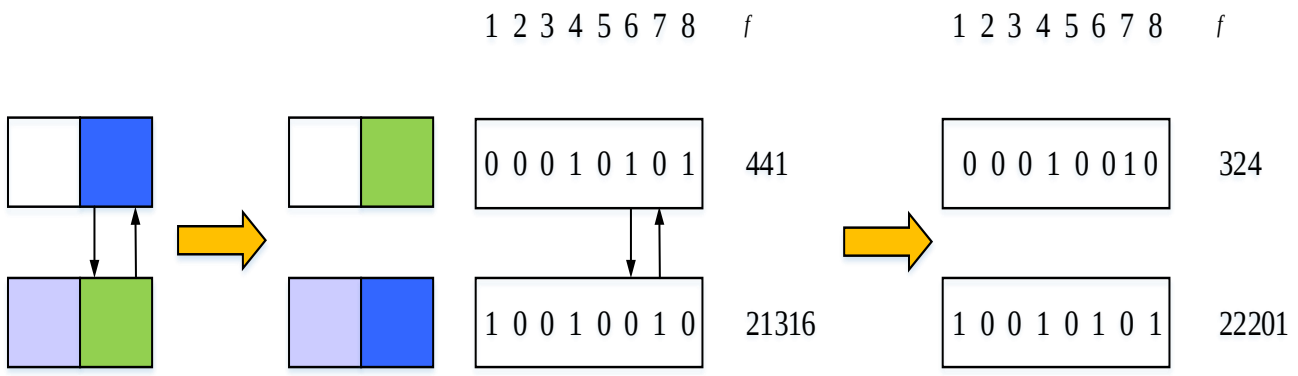


Fig. 3. Single point cross structure.

In Fig. 3, a random crossover point is selected on the chromosome, and the chromosome is divided into front and back parts. Gene exchange is performed in the front or back part of the crossover point to generate new offspring individuals. The mathematical expression for crossover operation is shown in Formula (7) [21].

$$\begin{cases} X_A^{t+1}=\varepsilon X_B^t+(1-\varepsilon)X_A^t \\ X_B^{t+1}=\varepsilon X_A^t+(1-\varepsilon)X_B^t \end{cases} \tag{7}$$

In Formula (7), X_A^t and X_B^t represent the parent individuals performing the crossover operation, and the two parent individuals represent two different protection strategies or configurations. X_A^{t+1} and X_B^{t+1} represent the offspring individuals formed after cross operation, and the newly generated individuals can display different combinations of security policies, helping the network security team find better protection solutions. ε represents the intersection rate. If the intersection rate is high, the algorithm will explore more combinations and may find more effective security protection methods; If it is too low, it may lead to insufficient exploration and inability to adapt to rapidly changing threats. After crossover operation, the GA finally performs mutation operation, as shown in Formula (8).

$$X^{t+1}=X^t-0.5L\Delta \tag{8}$$

In Formula (8), L represents the range of variable values, defining the range within which individuals can vary, ensuring that the mutated individuals remain within the valid parameter space, thereby enhancing the practical applicability of the model. The GA-WEBP network security protection model constructed above, although capable of supporting hyperparameter optimization, may not be able to adapt in a timely manner when facing rapidly changing attack patterns and network traffic. Therefore, research will focus on targeted optimization of Gas from multiple perspectives.

C. Improved Optimization Grounded on GA-WEBP Model

In the optimization of network security protection models based on GA-WEBP, research is conducted from the perspectives of convergence speed, crossover probability, mutation probability, etc. In terms of algorithm convergence speed, the selection of the initial population has a direct correlation. Therefore, the study adopts a real number chromosome as the initial population, and its calculation is represented in Formula (9).

$$X_i = \lceil X_{i\max} - X_{i\min} \times random[0,1] + X_{i\min} \rceil \quad (9)$$

In Formula (9), $\lceil \cdot \rceil$ represents the upward rounding function, X_i represents the value of genes on chromosomes, $X_{i\max}$ and $X_{i\min}$ represent the maximum and minimum values of the values, and $random$ represents any real number within a certain interval range. In network security protection, a good initial population can accelerate the initial exploration of the model, enabling GA to find feasible solutions faster, thereby cutting the amount of subsequent iterations and enhancing algorithm validity. Its expression is shown in Formula (10).

$$\begin{cases} o_c = \begin{cases} \dfrac{s_1(f_{\max} - f_c)}{f_{\max} - f_{avg}} & f_c \geq f_{avg} \\ s_2 & f_c < f_{avg} \end{cases} \\ o_m = \begin{cases} \dfrac{s_3(f_{\max} - f_m)}{f_{\max} - f_{avg}} & f_m \geq f_{avg} \\ s_4 & f_m < f_{avg} \end{cases} \end{cases} \quad (10)$$

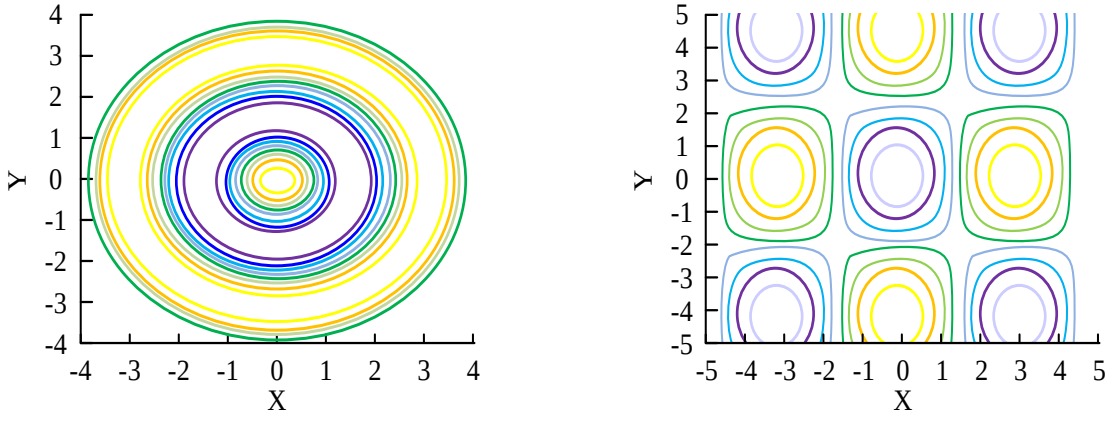
In Formula (10), o_c represents the crossover probability. In network security protection, a higher crossover probability can help discover new attack defense strategies and more effective protection measures. o_m represents the probability of mutation. Enhanced mutation operations can encourage the model to consider non-traditional attack methods and response strategies, thereby improving the adaptability of protection capabilities. s represents the adaptive parameter, and the value of the adaptive parameter is a constant not greater than 1. As the attack and defense strategies continue to evolve, the model can adjust the strategy based on real-time fitness feedback. f represents the fitness value. In Formula (10), the value of the adaptive parameter is greater than the value that should satisfy Formula (11).

$$\begin{cases} s_1 > s_2 \\ s_3 > s_4 \end{cases} \quad (11)$$

In the initial stage of the algorithm, individuals with higher fitness in the population will be retained, but the retained individuals are not the best ones. Therefore, to improve the performance of the algorithm's best remedy, further improvements should be made to crossover and mutation operations. The main purpose of improvement is to ensure that the algorithm can continue to perform crossover and mutation operations even when it has the best individual, as shown in Formula (12).

$$\begin{cases} o_c = \begin{cases} o_{c1} \dfrac{1}{(o_{c1} - o_{c2}) + e^{\frac{f_c - f_{avg}}{f_{\max} - f_{avg}}}} & f_c \geq f_{avg} \\ s_2 o_{c1} & f_c < f_{avg} \end{cases} \\ o_m = \begin{cases} o_{m1} \dfrac{1}{(o_{m1} - o_{m2}) + e^{\frac{f_c - f_{avg}}{f_{\max} - f_{avg}}}} & f_m \geq f_{avg} \\ s_2 o_{m1} & f_m < f_{avg} \end{cases} \end{cases} \quad (12)$$

In Formula (12), the value of $o_{c1} = 0.9$ is adjusted to 0.9, the value range of o_{c2} is [0.5,1], the value of $o_{m1} = 0.1$ is adjusted to 0.1, and the value range of o_{m2} is [0.05,0.1]. For network security protection, continuous crossover and mutation operations can help models adapt to new attack methods and traffic patterns, enhancing their dynamic defense capabilities. The study will use two sets of benchmark functions to testify the solving ability of the improved algorithm, namely the Schaffer function and the Griebank function. The contour plots of the two sets of functions are shown in Fig. 4.



(a) The Schaffer function (b) The Griewank function

Fig. 4. Contour map of two benchmark functions.

Fig. 4 shows the contour plots of the Schaffer function and the Griewank function. Contour plots plot the variation of a function in a given input space by connecting points with the same function values into lines. Through this visualization method, the function value distribution and its fluctuation characteristics in different regions can be intuitively understood. The Schaffer function is often used to test the performance of optimization algorithms because it has multiple local minima and one global minimum, usually near the origin. The contours shown in the figure present a highly concentrated and complex region centered on a smaller function value surrounded by a ring region of larger function values. This distribution shows that the solution of the optimization problem is usually near the origin and the optimization process is complicated. The Griewank function is another classical multi-variable function used to test global optimization algorithms. It is characterized by the existence of a large number of local minima, and the zero point is in a large region. The regular wavy structure in the contour map indicates its various local minima. These local minima are evenly distributed, which indicates the high complexity of the function.

III. Results

A. Performance Testing Based on Improved GA-WEBP Algorithm

The study conducted simulation experiments using MATLAB and analyzed the performance of the IGA through two selected benchmark functions. Firstly, the study analyzed the Schaffer function, which reached its maximum at the origin. Therefore, the study set the parameter values of the GA as follows: the initial population size was 100, the parameter settings satisfied $s_1 = 2s_2 = s_3 = 2s_4 = 1$, and the maximum iteration number of the GA was 100. By improving the GA to solve the Schaffer function, the results are shown in Fig. 5.

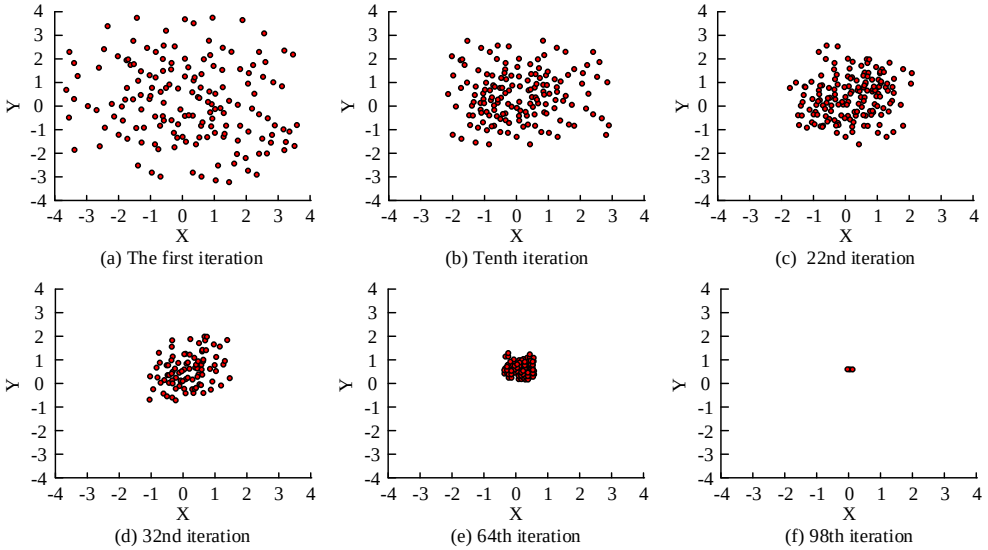
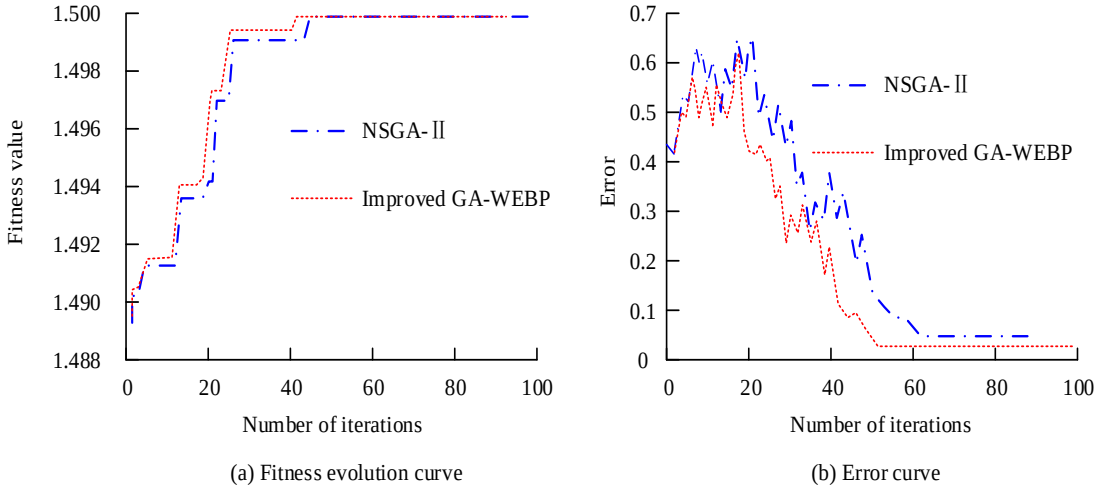


Fig. 5. Partial solution process of Schaffer function.

Fig. 5(a)-5(f) show the results of the algorithm's first, tenth, 22nd, 32nd, 64th, and 98th iterations, respectively. The results showed that the IGA gradually converged at the 32nd iteration, and the algorithm basically completed convergence at the 64th iteration. The results showed the ability of the model to explore the search space efficiently. Compared with the traditional algorithm, the improved GA had a faster convergence rate, which was due to the introduction of adaptive mechanism. As a result, the algorithm can effectively filter out the best solution in the early stage. The research used the fitness curve and iteration error curve of Schaffer function as the evaluation index of algorithm performance, and compared with the Non-dominated Sorting GA II (NSGA-II) to verify the effectiveness and progressiveness of the IGA. The results are shown in Fig. 6.

Fig. 6(a) shows the fitness curve results of the Schaffer function, where the NSGA-II algorithm began to converge at the 48th iteration, the proposed algorithm began to converge at the 42nd iteration, and the algorithm had a solution value of 1.5 for the multivariate unimodal function. Fig. 6(b) shows the iterative error curve of the Schaffer function, where the NSGA-II algorithm reached its minimum error at the 60th iteration, with a minimum error of 4.8%; The IGA proposed in the study achieved the minimum error at the 53rd iteration, and the minimum error result was 2.7%. In the Griebank function, there were two extrema in the domain, and the local minima had a regular arrangement. The study set the population size to 100, the adaptive parameters satisfied $s_1 = 2s_2 = s_3 = 2s_4 = 1$, and the maximum number of iterations was 250. The results showed that the research algorithm could achieve efficient feature selection and optimization in high-dimensional and complex optimization environments [19], especially in the field of network security, where it was crucial to quickly adapt to the dynamic changing environment in the face of complex network traffic data. By improving the GA to solve the Griebank function, the results are shown in Fig. 7.

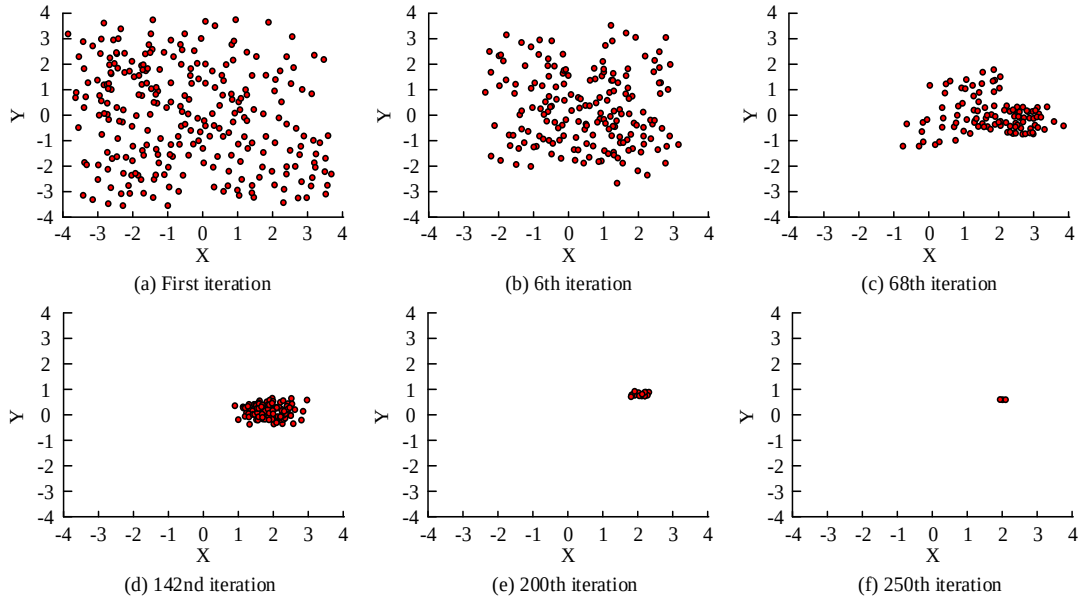


(a) Fitness evolution curve (b) Error curve

Fig. 6. The fitness curve and iteration error curve of Schaffer function.

Fig. 7(a)-7(f) show the results of the first, sixth, 68th, 142nd, 200th, and 250th iterations of the algorithm, respectively. The results showed that the IGA gradually converged at the 68th iteration, and the algorithm basically completed convergence at the 130th iteration. Due to the complexity of Griewank function, the research method showed a good search strategy ability to find the global optimal solution in a large number of local minima, indicating its effectiveness for testing complex optimization problems. The fitness curve and iteration error curve of the Griewank function were studied as evaluation indicators for algorithm performance, and the results are shown in Fig. 8.

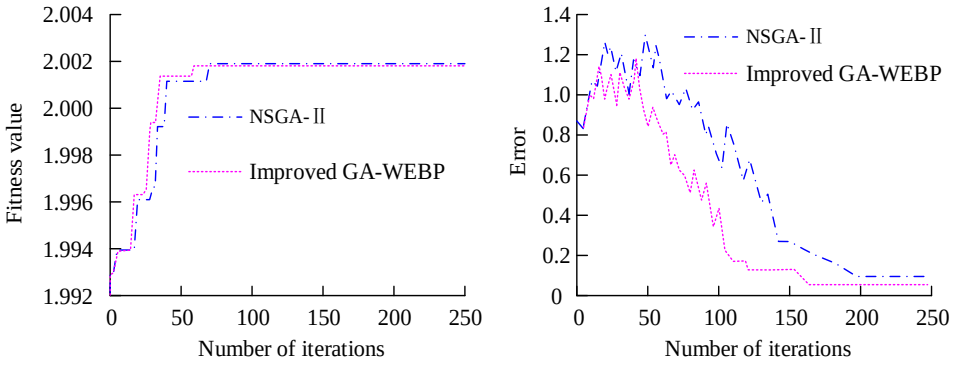
Fig. 8 (a) gives the fitness curve results of the Griewank function, where the NSGA-II algorithm began to converge at the 72nd iteration, the proposed algorithm began to converge at the 65th iteration, and the algorithm had a solution value of 2.0 for the multivariate unimodal function. Fig. 8 (b) gives the iterative error curve of the Griebank function, where the NSGA-II algorithm reached its minimum error at the 200th iteration, with a minimum error of 7.7%. The IGA proposed in the study achieved the minimum error at the 164th iteration, and the minimum error result was 5.2%. In the network attack detection, the attack mode was often varied, and the local minimum represented the misjudgment or omission of certain characteristics. The strong anti-interference ability ensured the robustness of the network security detection system, enabled it to effectively identify various attacks in the real environment, and reduced the false positive rate and false negative rate. Based on the analysis of the results in Fig. 7 and Fig. 8, the proposed IGA had good global optimization ability and fast convergence, and its effectiveness had been verified.



(a) First iteration (b) 6th iteration (c) 68th iteration

(d) 142nd iteration (e) 200th iteration (f) 250th iteration

Fig. 7. Partial solution process of Griebank function.



(a) Fitness evolution curve (b) Error curve

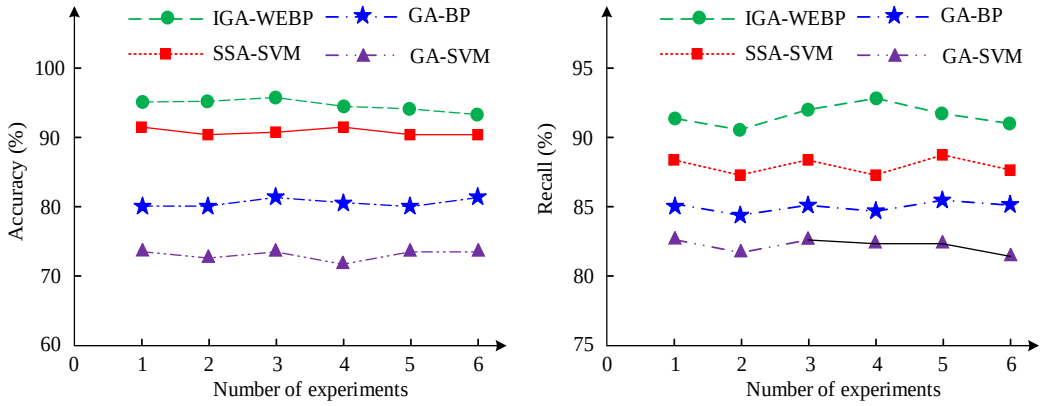
Fig. 8. The fitness curve and iteration error curve of the Griebank function.

B. *Network Security Protection Analysis Based on Improved GA-WEBP Algorithm*

To testify the effectiveness of the proposed algorithm, it was compared and analyzed with the Genetic Back-Propagation Algorithm (GA-BP), Genetic Support Vector Machine (GA-SVM), and Sparrow Search Support Vector Machine (SSA-SVM) algorithms [17]. The algorithm performance was validated using the CIC-IDS-2017 dataset, and precision, recall, F1 value, PR curve, ROC curve, and mean absolute error were used as comparison indicators for performance comparison. The accuracy and recall results of the four algorithms are represented in Fig. 9.

Fig. 9 (a) shows the accuracy comparison results of four algorithms. According to Fig. 9 (a), the accuracy curves of IGA-WEBP were higher than the other three compared algorithms in all four algorithms, with an average accuracy of 96.7%, which was higher than the 91.4% of SSA-SVM algorithm, 81.0% of GA-BP algorithm, and 74.6% of GA-SVM algorithm. Fig. 9 (b) shows the comparison results of recall rates for four algorithms. According to Fig. 9 (b), the recall curves of IGA-WEBP in all four algorithms were higher than the other three compared algorithms, and its average recall rate was 93.3%, which was higher than the 88.6% of SSA-SVM algorithm, 85.4% of GA-BP algorithm, and 83.0% of GA-SVM algorithm. The above results indicated that, in terms of accuracy and recall, the SSA-SVM algorithm outperformed the three compared algorithms in terms of performance. The good balance of accuracy and recall meant that the model could effectively reduce false alarms in cybersecurity, reduce the burden on security operations teams, and improve response efficiency. This helped to enhance the accuracy of decision-making in practical applications, making network protection measures more targeted. The PR curves and F1 values of the four algorithms are shown in Fig. 10.

Fig. 10 (a) shows the comparison results of PR curves for four algorithms. According to Fig. 10 (a), the space under the PR curve of IGA-WEBP in the four algorithms was 0.89, which was higher than the 0.83 of SSA-SVM algorithm, 0.76 of GA-BP algorithm, and 0.53 of GA-SVM algorithm [18]. Fig. 6(b) shows the comparison results of F1 values for four algorithms. According to Fig. 6(b), the F1 value curves of IGA-WEBP in all four algorithms were higher than the other three compared algorithms, and its average recall rate was 0.91, which was higher than the 0.86 of SSA-SVM algorithm, 0.79 of GA-BP algorithm, and 0.70 of GA-SVM algorithm. The above results indicated that, in terms of accuracy and recall, the ISSA-SVM algorithm outperformed the three compared algorithms in terms of performance. The PR curves and F1 values of the four algorithms are shown in Fig. 11.



(a) Accuracy rate comparison results (b) Recall rate comparison results

Fig. 9. Comparison results of accuracy and recall.

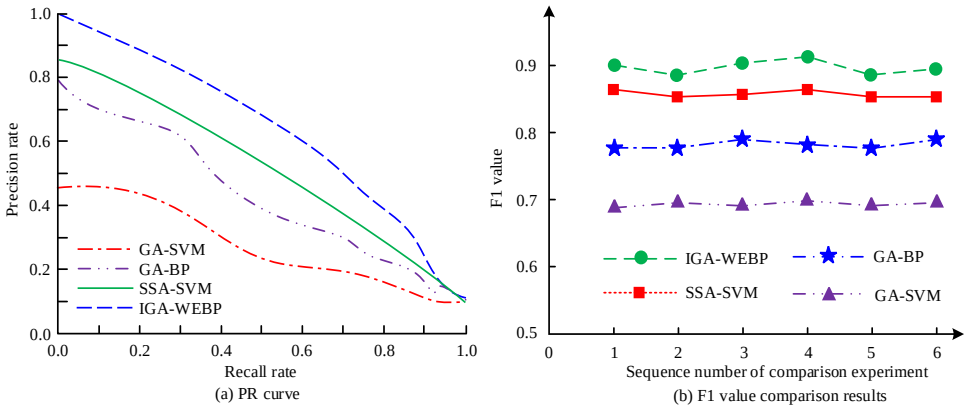


Fig. 10. Comparison results of PR curve and F1 value.

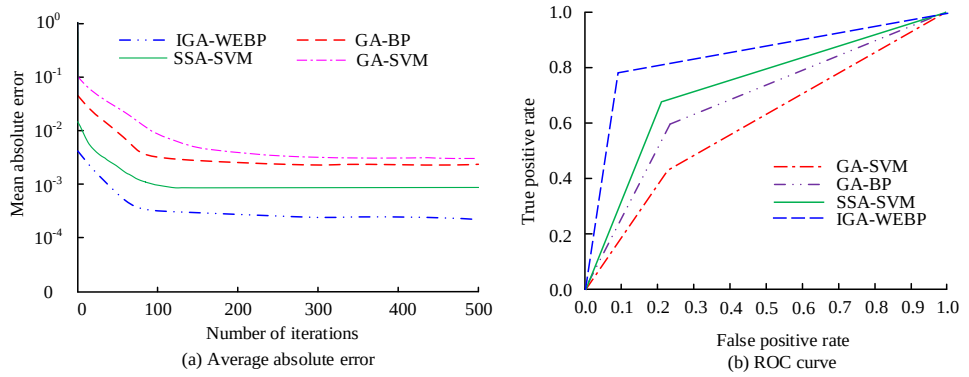


Fig. 11. Mean absolute error and ROC curve.

Fig. 11 (a) shows the comparison results of the average absolute error curves of four algorithms. According to Fig. 11 (a), IGA-WEBP had the lowest average absolute error curve among the four algorithms, and its stable average absolute error was 0.0034. Below 0.0023 for SSA-SVM algorithm, 0.0084 for GA-BP algorithm, and 0.0083 for GA-SVM algorithm. Fig. 11 (b) shows the comparison results of ROC curves for four algorithms. According to Fig. 11 (b), the space under the ROC curve of IGA-WEBP in the four algorithms was 0.88, which was higher than the 0.77 of SSA-SVM algorithm, 0.72 of GA-BP algorithm, and 0.64 of GA-SVM algorithm. The above results indicated that, in terms of average absolute error and ROC curve dimensions, the capacity of the IGA-WEBP algorithm was superior to the three compared algorithms. The results showed that the model had high efficiency in abnormal traffic detection, which indicated that the algorithm could not only handle normal traffic well, but also accurately capture abnormal traffic. The low error rate meant that the system could monitor and analyze the network in a more precise manner, and discover potential threats in time to enhance the security of the network environment. In addition, the actual performance of the network security protection system designed for research was analyzed, and the results are represented in Table I.

TABLE I. VERIFICATION RESULTS OF NETWORK SECURITY PROTECTION PERFORMANCE

Number of experiments	Data type	Input quantity	Correct corresponding quantity	Accuracy of measurement (%)
The first time	Normal data	9000	8974	99.71
	Known abnormal behavior data	3300	3276	99.27
	Unknown abnormal behavior data	560	543	96.96
The Second time	Normal data	11000	10997	99.97
	Known abnormal behavior data	3500	3476	99.31
	Unknown abnormal behavior data	500	486	97.20
The third time	Normal data	10000	9862	98.62
	Known abnormal behavior data	3000	2976	99.20
	Unknown abnormal behavior data	480	471	98.13

Table I shows that the proposed algorithm achieved recognition accuracy of over 95% for normal data, known abnormal behavior data, and unknown abnormal behavior data in each test. In the recognition of normal data, the highest accuracy reached 99.97%; the highest accuracy in identifying known abnormal behavior data was 99.31%; the recognition accuracy of unknown abnormal behavior data reached a maximum of 98.13%. The results indicated that the research method could effectively detect and distinguish normal traffic and potential abnormal behavior when facing different types of data streams, which helped to improve the effectiveness of network security protection in practical applications. These high recognition accuracy data reflected the high sensitivity and adaptability of the algorithm to network traffic changes, and could provide strong support for real-time protection. In network security applications, fast and accurate response capabilities are key to preventing data breaches and system breaches.

IV. Discussion

In the above experiment, when testing the performance of the improved method on two benchmark functions, the minimum error of the improved algorithm in the Schaffer function fitness curve was 2.7%, while NSGA-II was 4.8%; In the fitness curve of the Griebank function, the improved algorithm achieved a minimum error of 5.2% at the 164th iteration, while NSGA-II achieved a minimum error of 7.7% at the 200th iteration. For the analysis of network security protection based on the IGA-WEBP algorithm, the average accuracy of the IGA-WEBP model is 96.7%, the average recall is 93.3%, and the F1 value is 0.91, which is significantly better than the comparison algorithm. The reason why the model proposed by the research has excellent performance is mainly due to its structural advantages. The WEBP used in the IGA-WEBP model dynamically adjusts the weights of each sample. Unlike BPNN which relies solely on error feedback, WEBP allows the model to update based on the importance of the samples during the learning process. This enables samples that are more representative in specific situations to commit a greater effect on the practicing of the model, thereby improving the model's ability to recognize complex attack patterns. The importance of GA lies in its ability to optimize algorithm feature selection and hyperparameter settings through natural selection and genetic operations. Traditional feature selection methods have low efficiency in high-dimensional data processing, while GA can efficiently traverse the search space and find the optimal feature combination. In the same type of research, Unnisa N et al. proposed an intrusion detection system mainly used for detecting threats, and conducted research using various algorithms implemented by machine learning, achieving certain results in network intrusion detection [22]. Kim S et al. conducted a comprehensive review of the security threats faced by cyber physical systems. At the same time, the impact and implementation limitations of typical cyber physical attacks were analyzed, and for each established cyber physical attack, the time response of the physical system using conventional physics-based anomaly detectors was clearly explained [23]. Compared with the model proposed by the research, the methods summarized above exhibit low computational efficiency when the feature space is too large, making them less ideal for time sensitive real-time detection.

V. Conclusion

With the increasing complexity of network attack patterns, the limitations of traditional methods in network security protection have become increasingly apparent. A network security protection model grounded on improved GA-WEBP was proposed to address this issue. This model introduced the dynamic error weight and adaptive learning rate of WEBP, combined with the feature selection and hyperparameter optimization capabilities of GA, to demonstrate the effectiveness of the model in improving network security. Through experiments, the study not only verified the adaptability of the improved GA-WEBP model to dynamic changes in data during feature selection and weight updating, but also demonstrated its ability to effectively reduce false alarm rates and improve detection accuracy in practical applications. Although this research had derived important achievements in improving model performance, there were still some shortcomings. For example, the adaptability of the model to new and unknown attack patterns was still limited, which might affect its security in truly dynamic environments. Therefore, future research can focus on analyzing new feature selection and dimensionality reduction techniques to optimize the performance of the model in real-time environments, in order to further enhance the effectiveness and efficiency of network security protection.

References

[1] Fei R, Guo Y, Li J, Hu B, Yang L. An improved BPNN method based on probability density for indoor location. IEICE TRANSACTIONS on Information and Systems, 2023, 106(5): 773-785.

[2] Saminu S, Xu G, Zhang S, Kader IAE, Aliyu HA, Jabire AH, Ahmed YK, Adamu MJ. Applications of Artificial Intelligence in Automatic Detection of Epileptic Seizures Using EEG Signals: A Review. Artificial Intelligence and Applications, 2023,1(1): 11-25.

[3] Mokayed H, Quan T Z, Alkhaled L, Sivakumar V. Real-time human detection and counting system using deep learning computer vision techniques. Artificial Intelligence and Applications. 2023, 1(4): 221-229.

[4] Wei K, Zang H, Pan Y, Wang G, Shen Z. Strategic application of ai intelligent algorithm in network threat detection and defense. Journal of Theory and Practice of Engineering Science, 2024, 4(01): 49-57.

[5] Chen Z. Research on internet security situation awareness prediction technology based on improved RBF neural network algorithm. Journal of Computational and Cognitive Engineering, 2022, 1(3): 103-108.

[6] Khan M, Ghafoor L. Adversarial Machine Learning in the Context of Network Security: Challenges and Solutions. Journal of Computational Intelligence and Robotics, 2024, 4(1): 51-63.

[7] Yin L, Zhang D. The Calculation Method of the Network Security Probability of the Multi-rail Division Based on Fuzzy Inference. Mobile Networks and Applications, 2022, 27(4): 1368-1377.

[8] Memon I. A Secure and Efficient Communication Scheme with Authenticated Key Establishment Protocol for Road Networks. Wireless Personal Communications, 2015, 85(3):1167-1191.

[9] Farhan N, Rizvi S, Shabbir A, Memon I. Clustering Approaches for Efficient Radio Resource Management in Heterogeneous Networks. VFast Transactions on Software Engineering, 2021, 9(3): 68-77.

[10] Junejo M H, Ab Rahman A A H, Shaikh R A, Yusof K M, Kumar D, Memon I. Lightweight trust model with machine learning scheme for secure privacy in VANET. Procedia Computer Science, 2021, 194: 45-59.

[11] Xie Y, Wang K, Huan H. BPNN based indoor fingerprinting localization algorithm against environmental fluctuations. IEEE Sensors Journal, 2022, 22(12): 12002-12016.

[12] Zhang C, Tian Y X, Fan Z P. Forecasting sales using online review and search engine data: A method based on PCA–DSFOA–BPNN. International Journal of Forecasting, 2022, 38(3): 1005-1024.

[13] Lin J, Yang X, Zhou J, Wang G, Liu J, Yuan Y. Algorithm of BPNN-UKF based on a fusion model for SOC estimation in lithium-ion batteries. IET Power Electronics, 2023, 16(5): 856-867.

[14] Zhang P, Cui Z, Wang Y, Ding S. Application of BPNN optimized by chaotic adaptive gravity search and particle swarm optimization algorithms for fault diagnosis of electrical machine drive system. Electrical Engineering, 2022, 104(2): 819-831.

[15] Gunawan A, Thamrin S, Kuntjoro Y D, Idris A M. Backpropagation neural network (BPNN) algorithm for predicting wind speed patterns in East Nusa Tenggara. Trends in Renewable Energy, 2022, 8(2): 107-118.

[16] An K, Zhang J. Application of Genetic Algorithm in the Innovative Design of Animation Image. Journal of Electrical Systems, 2024, 20(9): 469-475.

[17] Ye F, Doerr C, Wang H, Back T. Automated configuration of genetic algorithms by tuning for anytime performance. IEEE Transactions on Evolutionary Computation, 2022, 26(6): 1526-1538.

[18] Ghezelbash R, Maghsoudi A, Shamekhi M, Pradhan B, Daviran M. Genetic algorithm to optimize the SVM and K-means algorithms for mapping of mineral prospectivity. Neural Computing and Applications, 2023, 35(1): 719-733.

[19] Feng Y, Lan C, Briseghella B, Fenu L, Zordan T. Cable optimization of a cable-stayed bridge based on genetic algorithms and the influence matrix method. Engineering Optimization, 2022, 54(1): 20-39.

[20] Maskooki A, Deb K, Kallio M. A customized genetic algorithm for bi-objective routing in a dynamic network. European Journal of Operational Research, 2022, 297(2): 615-629.

[21] Alhijawi B, Awajan A. Genetic algorithms: Theory, genetic operators, solutions, and applications. Evolutionary Intelligence, 2024, 17(3): 1245-1256.

[22] Unnisa N, Yerva M, Kurian M Z. Review on intrusion detection system (ids) for network security using machine learning algorithms. International Research Journal on Advanced Science Hub, 2022, 4(3): 67-74.

[23] Kim S, Park K J, Lu C. A survey on network security for cyber–physical systems: From threats to resilient design. IEEE Communications Surveys & Tutorials, 2022, 24(3): 1534-1573.

Q-FuzzyNet: A Quantum Inspired QIF-RNN and SA-FPA Optimizer for Intrusion Detection and Mitigation in Intelligent Connected Vehicles

Abdullah Alenizi
Department of Information Technology-College of Computer and Information Sciences,
Majmaah University, Al-Majmaah 11952, Saudi Arabia

***Abstract*—In the evolving landscape of Intelligent Connected Vehicles (ICVs), ensuring cybersecurity is crucial due to the increasing number of cyber threats. Besides, challenges like data breaches, unauthorized access, and hacking attempts are prevalent due to the interconnected nature of ICVs. Several methods have been proposed to secure ICVs; however, accurate intrusion detection remains a challenging task yet to be fully achieved. For this reason, this paper proposes a comprehensive intrusion detection scheme denoted a Q-FuzzyNet, which is specifically tailored to safeguard ICV networks using Deep Learning (DL) approaches. This Q-FuzzyNet approach consists of five phases: (i) Data Collection (ii) Data Pre-processing (iii) Feature extraction (iv) Dimensionality Reduction and (v) Intrusion Detection and Mitigation. Initially, the raw data are gathered from the CICIoV2024 dataset. The collected data are pre-processed via Mean Imputation (MI) for data cleaning. Then, significant features are extracted through higher-order statistical features, Proposed Improved Mutual Information (IMI), Correlation, and Entropy approaches. Subsequently, the dimensionality is reduced via new Improved Linear Discriminant Analysis (ILDA). Ultimately, the data are classified (attacker/Normal) via the Meta-Heuristic Quantum-Inspired Fuzzy-Recursive Neural Network (QIF-RNN) model by combining the Quantum Neural Network (QNN), Recurrent Neural Network (RNN), and Fuzzy logic. The membership function of fuzzy logic is optimized via the new Self Adaptive-Flower Pollination Algorithm (SA-FPA). The identified attackers are mitigated from the network using the Policy Gradient Method. The acquired outcomes from Q-FuzzyNet are validated in terms of Accuracy, Precision, Sensitivity, and F1-score, as well. The highest accuracy of 98.6% has been recorded by the proposed model.**

Keywords*—Cybersecurity; intelligent connected vehicles; artificial intelligence; quantum neural network; recurrent neural network; flower pollination algorithm

I. INTRODUCTION

The automotive industry has greatly changed since the gasoline-fueled automobile was first created in the late 19th century [1]. At first, the trade was more interested in straightforward advancements in machines and mass production strategies illustrated by Henry Ford's assembly line [2]. Over time, improvements in safety, fuel economy and design transformed it into better, dependable vehicles. The incorporation of electrification, automation and connectivity into the industry has provided the era of ICVs over the past few years [3]. This change is not just altering how people drive but is also giving rise to new concepts in transportation and mobility [4].

ICVs are developing fast with the help of automation and connectivity, but these are cybersecurity threats as well [5]. ICVs are susceptible to different types of cyber-attacks such as in-vehicle attacks where hackers intrude into the vehicle's systems like the CAN bus to gain control of sensitive operations like brakes and doors [6]. V2X communication systems which are very vital for vehicle safety and efficiency are vulnerable to attacks such as replay, Sybil, and DoS which can compromise the exchange of important information between vehicles and other structures [7]. Besides, viruses and scams are capable of corrupting vehicle software, thus eradicating core functions and granting unauthorized access to information. Another issue is data privacy, which is an issue since people in ICVs are constantly sharing information with each other and personal information such as location data could easily be leaked in the process [8] [9]. Moreover, other parts of a vehicle, like TPMS and smart keys, which are sensor-based, are also vulnerable to the attack, which can result in vehicle tracking or unauthorized access. However, due to the constant development of ICVs, new risks arise and therefore, the need for strong and dynamic security measures [10].

Intelligent connected vehicles (ICVs) rely on advanced technologies that could be at risk of cyber threats, making cybersecurity critical [11]. Critical vehicle systems could be hacked to produce unsafe conditions in the car which would cause accidents if there were no strong cybersecurity measures to protect them. Moreover, strong cybersecurity measures also protect individual privacy by safeguarding their data against breaches and help to build public confidence in ICVs [12] [13]. This is of utmost importance if we are to have large-scale adoption of these driving machines. In addition, cyber security prevents big money loss and protects national interests by securing important transport facilities. Thus, for ICVs to be deployed safely and successfully, cyber safety has to be considered important [13].

Intrusion detection in intelligent connected vehicles involves signature-based, anomaly-based, behaviour-based, hybrid, Machine Learning (ML)-based, network-based, and hardware-based systems. All of these have several merits but also some remarkable demerits. Signature-based IDS works quite effectively against known threats, which mostly suffer

from novel ones and require a frequent signature update [14]. The problems in anomaly-based IDS are high false positives and adaptation. Behavioural-based IDSs are complex, and are not scale; hybrid systems are balanced yet resource-intensive, and hard to integrate. In ML-based IDSs, volumes of data are needed, and it is susceptible to model drift. In general, network-based IDS suffers from difficulties related to encrypted traffic and impacts on performance. Hardware-based IDSs are expensive and challenging to integrate [15]. Traditional Intrusion Detection Systems (IDS) suffer from to evolving attack patterns, limitations in terms of real-time detection, scalability, and ease of adaptation. Most proposed models suffer from excessive false positives, computational intensiveness, and poor feature selection that further degrades performance in dynamic ICV environments. There is a need for efficient intrusion mitigation mechanisms, which are often lacking in such approaches. Most of the existing traditional systems primarily concentrate on detection alone without having many opportunities to respond or mitigate attacks in real-time. Moreover, most of the mitigation techniques are dependent upon the static rule-based approach, which proves to be ineffectual enough for adaptive and evolving threats in the connected vehicle networks. To cope with these challenges, this paper has introduced Q-FuzzyNet, a comprehensive deep learning-based framework specifically designed for intrusion detection and mitigation in ICV networks. The novelty proposal within Q-FuzzyNet comes from the novel integration of Quantum-Inspired Neural Networks (QNN), Fuzzy Logic, and the Self Adaptive-Flower Pollination Algorithm (SA-FPA) in order to optimize membership functions with improved boosting of detection accuracy.

This paper introduced a novel IDS to tackle the previous challenge by attaining enhanced accuracy. The key contributions are:

- To propose a specialized IDS referred to as Q-FuzzyNet tailored for ICVs to enhance network cybersecurity.
- To introduce higher-order statistical features, IMI, correlation, and entropy for significant feature extraction from the CICIoV2024 dataset.
- To use ILDA to reduce data dimensionality while retaining essential information.
- To combine QNN, RNN, and fuzzy logic into a novel QIF-RNN, for efficient.
- To optimize the fuzzy logic membership functions using the SA-FPA to enhance classification performance.
- To utilize the Policy Gradient Method to mitigate the attacker from the ICV network.

This article is structured as a recent literature on IDS in Section II. Section III explains the proposed architecture. Experimentation and results are given in Section IV. Discussion is given in Section V and finally, Section VI concludes the paper.

II. Literature Study

A. Recent Research

In 2022, Cheng et al. [16] presented a new model for detecting automotive intrusion based on the STC features of the in-vehicle communication traffic. This model was based on encoding-detection architecture, in which spatial and temporal relations were encoded at the same time. The model employed the spatial and channel features through an attention-based convolutional network and the temporal features through an attention short-term memory network.

In 2021, Alladi et al. [17] have put forward an AI-driven intrusion detection model for IoV. This architecture also entailed DL Engines (DLEs) that were aimed at detecting and categorizing vehicular traffic into possible cyber threats. To support the dynamism of vehicles and the time-sensitive nature of IoV networks, these DLEs were hosted on MEC servers rather than cloud computing.

In 2022, Yu et al. [18] proposed a federated LSTM neural network-based intrusion detection approach to IVNs in ICVs. This method involved the development of an LSTM neural network model to determine the periodicity of the ID sequence of IVN messages for the prediction of the incoming message IDs. A Network IDS (NIDS) based on ID prediction was then proposed.

In 2021, Pascale et al. [19] developed an IDS that was integrated into the automotive industry, which employed a two-step algorithm to identify potential cyber threats. In the first step, the system first screened the messages in the Controller Area Network (CAN-Bus) using spatial and temporal analysis. When messages were detected as potentially malicious, a Bayesian network was then used to calculate the likelihood that an event was an attack.

In 2022, Ge et al. [20] presented an approach to a distributed longitudinal platooning control of Connected Automated Vehicles (CAVs) that improved robustness and safety under DoS attacks on V2V communications. They came up with a model that was capable of handling such factors as variable mass of the vehicle, delays in the engine and non-linear forces of resistance.

In 2022, Park and Park [21] proposed the PIER method that was used to evaluate cybersecurity threats in CAVs. This method improved on conventional risk analysis by including new factors such as exposure and recovery factors in addition to probability and impact factors. The PIER method was tested with regards to software updates over the air and collision avoidance capabilities and it was shown that it was indeed capable of reducing risk indices.

In 2021, Ahmed et al. [22] developed a solution for DL-based IDS to improve security for CAN in vehicles. Based on the VGG structure, the system is capable of learning multiple network intrusion patterns and recognizing different types of attacks including DoS and fuzzy attacks. The proposed system was tested with the CAN-intrusion dataset to obtain an accuracy of 96% and a low FPR of 0. 6 % accuracy in comparison with more conventional ML approaches.

In 2021, Li et al. [23] presented two model update schemes for ML-based intrusion detection in the IoV. The first scheme, the cloud-assisted update, used a small set of labelled data for new attacks from the IoV cloud. The second scheme which was the local update comes into play when the cloud cannot afford to provide labeled data in time by using pseudo-labels of the pre-classified unlabeled data.

In 2021, Yang et al. [24] proposed a three-layered hierarchical IDS for protecting both the intravehicle and external vehicular networks. This IDS used both the signature-based approach and the anomaly-based approach as a way of detecting both known and unknown attacks. The experimental results show that the proposed system attains a recognition rate of 99. 9% accuracy for known attacks on the CAN-intrusion dataset and 99. The proposed model achieved a CICIDS2017 dataset accuracy of 88%.

In 2023, Alladi et al. [25] presented three DL-based misbehavior classification schemes for intrusion detection in IoV networks. DCLEs were developed for single or multi-step classification on vehicular edge servers using LSTM and Convolutional Neural Networks (CNNs). The schemes include preprocessing vehicular data collected by Road Side Units (RSUs) and forwarding the data to edge servers for classification.

B. Problem Statement

Table I defines the advantages and challenges of recent IDS using various methods. As ICVs become increasingly integrated into modern transportation systems, they are vulnerable to a myriad of cyber threats that can compromise their functionality and safety. The complexity of ICV networks, characterized by dynamic data flows and diverse communication protocols, necessitates robust IDS to identify and mitigate potential attacks in real-time. Traditional IDS methods often struggle to adapt to the evolving nature of threats, making it imperative to develop advanced solutions using ML and DL techniques to enhance detection accuracy and responsiveness. Utilizing ML and DL for IDS provides several advantages, including improved accuracy in detecting anomalies and previously unseen attacks due to their ability to learn from vast amounts of data and recognize complex patterns. These approaches can also adapt to changing environments, making them suitable for the dynamic nature of ICV networks. However, challenges remain, such as the need for high-quality labeled data for training, which is often scarce in cybersecurity contexts. Additionally, the computational requirements of ML/DL models can be significant, potentially leading to delays in real-time detection. Balancing model complexity with efficiency while ensuring robustness against adversarial attacks poses further hurdles that must be addressed in the development of effective IDS for ICVs.

TABLE I. ADVANTAGES AND CHALLENGES OF RECENT IDS USING VARIOUS METHODS

Authors/Year	Methods	Database	Advantages	Challenge	Achievements
Cheng *et al*, 2022	STC features, attention-based convolutional network, attention-short-term memory network	real-world vehicle attack dataset	Encodes spatial and temporal features simultaneously, and achieves strong anomaly classification with spatial-temporal attention features.	Model complexity due to dual-frame approaches, dependent on hyperparameter tuning.	Accuracy = 97% Precision = 93%
Alladi *et al*, 2021	DLEs	IoV Network Traffic Dataset	Uses MEC servers for real-time data processing, suitable for dynamic and time-sensitive IoV networks.	Limited details on specific datasets used, and potential scalability issues with MEC servers.	Accuracy = 95% Precision = 92% Recall = 90%
Yu *et al*, 2022	Federated LSTM neural network	IVN Attack Dataset	Federated learning framework for privacy-preserving model training, LSTM for ID sequence prediction.	Reliance on timely data from the IoV cloud is less effective if cloud data is not available.	Precision = 92% Recall = 91%
Pascale *et al*, 2021	Two-step algorithm: spatial-temporal analysis and Bayesian network	CAN-Bus Cyber-Attack Dataset	Integrates spatial and temporal analysis with Bayesian network for attack probability calculation, good accuracy on common attacks.	Reduced performance on Free State Attacks; limited to specific types of attacks.	Accuracy = 95%
Ge *et al*, 2022	Distributed longitudinal platooning control, resilient control law, design algorithm for DoS resilience	CAV-Platoon-Resilience Dataset	Handles diverse vehicle dynamics and DoS attacks, designed for stability, resilience, and scalability.	Focused on platooning control, may not address other types of attacks beyond DoS.	Accuracy = 93%
Park and Park, 2022	PIER method: exposure, recovery, probability, and impact factors for risk assessment	CAV-Cybersecurity-Risk Assessment Dataset	Enhances traditional risk assessment by including new factors, and improves risk determination efficiency and coverage.	Limited application scope, and effectiveness dependent on the implementation of security measures.	Accuracy = 92% Precision = 88%
Ahmed *et al*, 2021	DL-based IDS with VGG architecture	CAN-intrusion dataset	High accuracy in detecting various attacks, significantly lower false positive rate compared to conventional methods.	Focused primarily on the CAN network, may need further validation on other network types.	Accuracy = 96% FPR = 0.6%
Li *et al*, 2021	Two model update schemes: cloud-assisted and local update with pseudo-labels	AWID Dataset	Increases detection accuracy by 23%, local update scheme enables updates without cloud-provided labelled data.	Potential dependence on the availability of labelled data, local schemes may be complex.	Accuracy = 92% FNR = 13%

Yang *et al*, 2021	Three-layered hierarchical IDS combining signature-based and anomaly-based approaches	CAN-intrusion dataset, CICIDS2017	High accuracy in detecting known attacks, effective zero-day attack detection with fast processing times.	May need to optimize for specific types of zero-day attacks and large data processing requirements.	Accuracy = 99% F1 score = 80%
Alladi *et al*, 2023	DL-based misbehavior classification using LSTM and CNNs	VeReMi Extension datas et	Identifies 18 types of vehicular behavior; high F1-scores and fast processing times.	May require extensive computational resources for deep learning models.	F1 score = 95.58%

III. A Novel IDS Model

A. Proposed Architecture

This paper presents an advanced IDS designed to secure ICV networks through DL techniques. The framework is divided into five key phases: (i) Data Collection, (ii) Data Pre-processing, (iii) Feature Extraction, (iv) Dimensionality Reduction, and (v) Intrusion detection and mitigation. Initially, raw data from the CIC IoV dataset 2024 are pre-processed using MI for data cleaning. Significant features are then extracted using higher-order statistical features, Proposed IMI, Correlation, and Entropy methods. Dimensionality reduction is performed via ILDA. Finally, the intrusion classification is achieved using the Meta-Heuristic QIF-RNN, which integrates QNN, RNN, and Fuzzy Logic. Membership function optimization of fuzzy logic (decision maker) is carried out using the SA-FPA, and the outcome is obtained by fusing QNN, RNN, and optimized fuzzy logic. The identified attackers are mitigated via the Policy Gradient Method. Fig. 1 shows the overview of the proposed model.

B. Data Collection

Raw data are first obtained from the CIC IoV 2024 dataset (https://www.unb.ca/cic/datasets/iov-dataset-2024.html). The topmost CICIoV2024 dataset directory contains four subdirectories pertaining to three different files named as follows:

- Hexadecimal: Data captured in hexadecimal mode (benign, DoS, spoofing-GAS, spoofing-RPM, spoofing-SPEED, and spoofing-STEERING_WHEEL).
- Decimal: Data captured in decimal mode (benign, DoS, spoofing-GAS, spoofing-RPM, spoofing-SPEED, and spoofing-STEERING_WHEEL).
- Binary: Data captured in binary mode (benign, DoS, spoofing-GAS, spoofing-RPM, spoofing-SPEED, and spoofing-STEERING_WHEEL).

C. Data Pre-Processing

It plays a crucial role in enhancing data quality by cleaning and normalizing the raw input, which helps eliminate noise and irrelevant information.

1) MI: It is a simple technique used to handle missing data by replacing missing values with the mean of the available data for a particular feature. This method is commonly used to maintain the dataset's size and ensure continuity in the analysis without distorting the data [26]. Eq. (1) shows the MI procedure. For a feature X, with N observed values, $\hat{X}$ points to the observed value's mean, and X_i signifies non-missing values.

$$\hat{X} = \frac{1}{N}\sum_{i=1}^{N} X_i \quad (1)$$

D. Feature Extraction

Feature extraction includes selecting or transforming relevant features from the CICIoV2024 dataset. It helps in improving the efficiency of the subsequent classification process. From the pre-processed data, features like proposed higher orders statistical features, IMI, Correlation, and Entropy are extracted.

1) Higher-order statistical features: It is used to capture non-linear dependencies and subtle statistical properties in data that are not evident through basic statistical measures like mean or variance. These features are often derived from moments and cumulants, which describe the shape and characteristics of data distributions beyond first and second-order statistics. Table II shows the Higher-order Statistical features and their mathematical expressions [27].

TABLE II. Higher-Order Statistical Features and their Equations

Features	Formula	Description
Skewness V_z	$V_z = \frac{1}{Q}\sum_{l=1}^{q}\left(\frac{a_l-\mu}{\sigma}\right)^3$	Q is total number of values, q is number of values ranging from 1 to Q, a_l be the individual values in the set, μ means the mean value, σ be the standard deviation, $\sum_{l=1}^{q}\left(\frac{a_l-\mu}{\sigma}\right)^3$ be the values deviate from the mean in terms of the cube.
Kurtosis N	$N = \frac{1}{Q}\sum_{l=1}^{q}\left(\frac{a_l-\mu}{\sigma}\right)^4$	$\sum_{l=1}^{q}\left(\frac{a_l-\mu}{\sigma}\right)^4$ be the Sum of the fourth power differences.
Higher-Order Moments M_h	$M_h = \frac{1}{Q}\sum_{l=1}^{q}(a_l-\mu)^h$	h indicates the order of the moment, with $h \geq 3$ representing higher-order moments beyond variance (second-order)

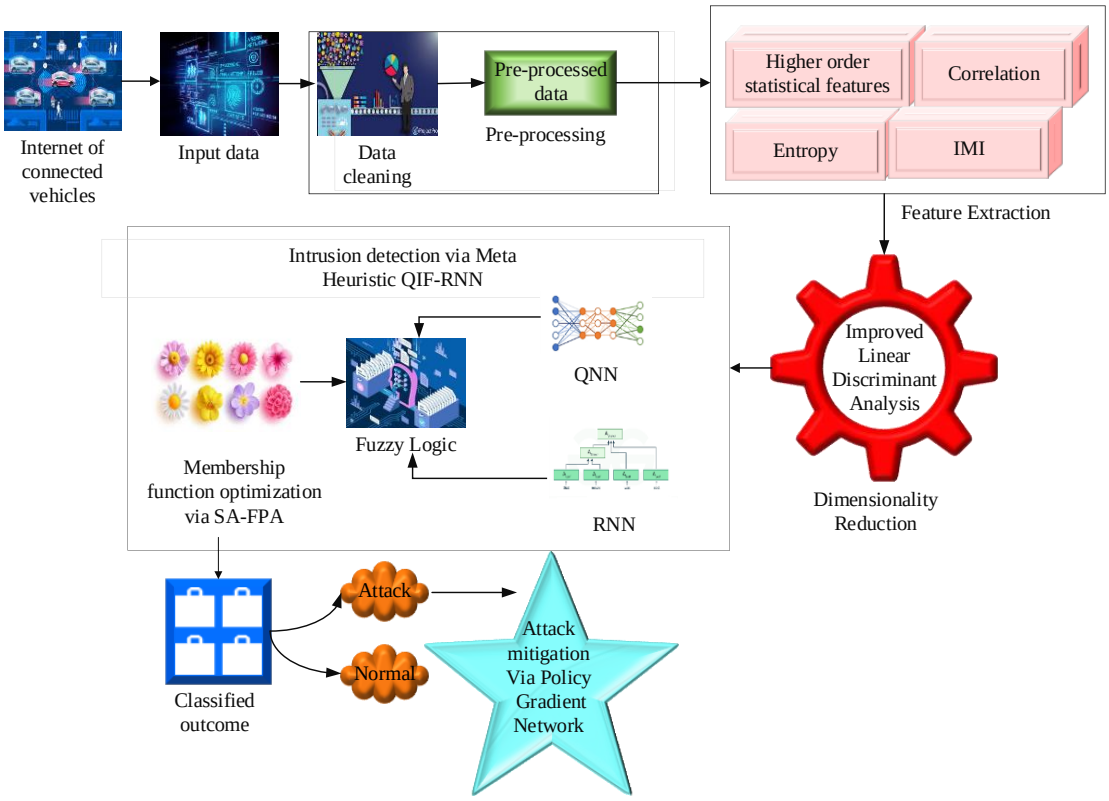


Fig. 1. Overview of the proposed model.

2) Entropy: In the context of an IDS, entropy is used to measure the distribution of different types of network packets, protocols, or system events. A significant deviation in entropy indicates unusual behavior, like a Distributed Denial of Service (DDoS) attack, where packet distributions change unexpectedly. Eq. (2) describes the entropy feature $E(X)$ extraction for IDS, in which $\rho(x_i)$ specifies the probability of occurrence of i^{th} event or value in the dataset, and n refers to total number of unique events or values.

$$E(X) = -\sum_{l=1}^{N} \rho(x_i)\rho(x_i) \quad (2)$$

3) IMI: An intuitive method for measuring the uncertainty of random variables and the information they share is provided by information theory, where two key ideas are mutual information and entropy [28]. A measure of the uncertainty of random variables is the entropy K. Assuming A to be a discrete random variable with alphabet χ and a probability mass function of $s(a) = Su\{A = a\}\, a\epsilon A$, the entropy of A is expressed as shown in Eq. (3).

$$K(A) = -\sum_{a\epsilon A} s(a)log(s(a)) \quad (3)$$

Although two random variables communicate information through a metric known as mutual information, which is shown in Eq. (4).

$$K(B;A) = \sum_{a\epsilon A} \sum_{b\epsilon B} s(b,a)log\frac{s(a,b)}{s(a)s(b)} = K(B) - K(\frac{B}{A}) \quad (4)$$

Where $K(\frac{B}{A})$ is the conditional entropy of B in the case of A is known, and can be represented as in Eq. (5).

$$K(\frac{B}{A}) = -\sum_{a\epsilon A} \sum_{b\epsilon B} s(b,a)log\left(s\left(\frac{b}{a}\right)\right) \quad (5)$$

The IMI and entropy for continuous random variables are defined in Eq. (6) – Eq. (8), respectively.

$$K(B) = -\int_a s(a)\ log\ log\left(s(a)\right) da \quad (6)$$

$$K(\frac{B}{A}) = -\int_{a,b} s(b,a)\ log\ log\left(s\left(\frac{b}{a}\right)\right) da\ db \quad (7)$$

$$K(B;A) = \int_{a,b} s(b,a)\ log\ log\ \frac{s(a,b)}{s(a)s(b)}\ da\ db \quad (8)$$

TABLE III. COMPARATIVE ANALYSIS: PROPOSED AND EXISTING FEATURE EXTRACTION APPROACHES

Metric	IMI	Entropy	Mutual Information
Accuracy	92%	85%	90%
Computational Time	12 seconds	20 seconds	15 seconds
F1-Score	0.88	0.8	0.86
Precision	0.89	0.81	0.87
Recall	0.88	0.79	0.85
Variance Explained	97%	93%	95%

Table III denotes comparative analysis of proposed and existing feature extraction approaches. The accuracy values reflect the fact that IMI substantially enhances the classifier's performance compared to traditional entropy and mutual information measures. The improvement from 85% to 92% shows the capture power of IMI for complex relations between variables. Furthermore, the relative computational time for the IMI measure is relatively low, which is only 12 seconds, while for entropy it took 20 seconds and for mutual information 15 seconds. This efficiency becomes highly valuable in those areas where large datasets are involved, or applications that require prompt outputs.

4) Correlation: A linear relationship among two variables is measured for both its strength and direction using correlation. Correlation is a technique used to determine the relationship between features in the context of feature extraction. A low correlation suggests independence, while a high correlation might point to redundancy.

E. Dimensionality Reduction

From the feature-extracted data, the dimensionality of the extracted features is reduced by utilizing ILDA.

1) ILDA: Statistical methods such as LDA [29] are now commonly employed as ML models for pattern recognition. The method involves projecting data into lower dimensional spaces in order to maximize class separability. Using Fisher's criteria, the optimal strategy for class separation is to maximize the ratio of the average difference to the total number of variables in the projection space for the two groups. The eigenvalue and eigenvector of the ideal projection transformation matrix $T_X^{-1}T_C$, where T_X and T_C are respectively the within-class and between-class scatter matrices, are the outcomes of the maximum ratio. More precisely, ILDA resolves the subsequent optimal problem utilizing Eq. (9).

$$K(x) = \frac{|\tilde{\mu}_1 - \tilde{\mu}_2|^2}{\tilde{T}_1^2 \tilde{T}_2^2} = \frac{x^{U}T_C x}{x^{U}T_C x} \quad (9)$$

where $\tilde{T}_1$ and $\tilde{T}_2$ are respective distribution matrices for classes 1 and 2. Consequently, $K(x)$ represents a measure of the within-class scatter matrix adjusted by a measure of the class mean difference. To determine $K(x)$'s maximum, differentiate and equal to zero and their mathematical expression is shown in Eq. (10) and Eq. (11).

$$\frac{d}{dx}K(u) = \frac{d}{dx}\left(\frac{x^{U}T_C x}{x^{U}T_C x}\right) = 0 \quad (10)$$

$$T_X^{-1}T_C - K(x)x = 0 \quad (11)$$

Resolving the problem of generalized eigenvalues is presented in Eq. (12).

$$T_X^{-1}T_C x = \lambda x \; where \; \lambda = K(x) = Scalar \quad (12)$$

Yield, the mathematical expression of x^* is shown in Eq. (13) and Eq. (14), respectively.

$$x^* = arg\ arg\ Max\ x\ K(x) = arg\ arg\ Max\ x\ \frac{x^{U}T_C x}{x^{U}T_C x} \quad (13)$$

$$x^* = T_X^{-1}(\mu_1 - \mu_2) \quad (14)$$

The mathematical expression of z is presented in Eq. (15).

$$z = x^{U}y, \quad (15)$$

where, y is a variable input, x vector projection, and z is a new feature in projection space used to find the projection space.

TABLE IV. COMPARATIVE ANALYSIS: LDA VS. ILDA

Metric	LDA	ILDA
Accuracy	85% (170/200)	90% (180/200)
Recall	0.8	0.85
F1-Score	0.81	0.86
Precision	0.82	0.88
Variance Explained (%)	95%	96%
Dimensionality Reduced (D)	10 to 2	10 to 2
Computational Time (s)	25	15

A comparison of the ILDA (Incremental Linear Discriminant Analysis) with the classic LDA (Linear Discriminant Analysis) highlights very important advantages of ILDA over a dynamic and evolving dataset, as depicted in Table IV, that the accuracy of ILDA is superior compared to LDA, where there is a great improvement from 85% to 90%. This indicates that ILDA could classify instances more effectively as the dataset grows or changes. It can be noticed from precision and recall values that it has resulted in increased accuracy. ILDA reflected a much greater precision at 0.88 compared with that of LDA, which was only 0.82. The same thing happened with recall: ILDA at 0.85 versus 0.80 with LDA. These improvements, therefore, say ILDA to be more effective in true positive identification, minimizing false positives as well as false negatives.

F. Classification

Using the dimensionality-reduced features, the data is classified via a Meta-Heuristic QIF-RNN. The suggested model is a combination of the QNN, RNN, and Fuzzy logic. The membership function optimization is acquired via the SA-FPA. Then the QNN, RNN, and membership function optimization are fused in the fuzzy logic to acquire an outcome.

1) QNN: A Neural Network (NN) inspired by quantum computing principles that helps in capturing complex relationships within the data, providing more powerful learning capabilities than traditional neural networks [30]. The QNN functions as a quantum circuit by acting on quantum input data through a series of parameter-dependent quantum gates, also known as unitary operators. Typically, a QNN is displayed in Eq. (16).

$$V(\theta) = \prod_{m=1}^{O} W_m V_m(\theta_m) \quad (16)$$

Eq. (16) results from O quantum layers. The product of parametric quantum gates $V_m(\theta_m)$ and non-parametric quantum gates V_m, where θ_m are variational parameters, that make up the l^{th} quantum layer. The parametric quantum gates $V_m(\theta_m)$ in the m^{th} layer is expressed as the generation of T parametric quantum gates and its mathematical expression is shown in Eq.

(17), in which Euler's formula is used to translate each parametric quantum gate $V_{m,k}(\theta_{m,k})$ as shown in Eq. (18).

$$V_m(\theta_m) \equiv T \otimes k = 1\, V_{m,k}(\theta_{m,k}) \quad (17)$$

$$exp\left(-j\theta_{m,k}Q\right) = J\, cos(\theta_{m,k}) - j\, sin(\theta_{m,k})Q \quad (18)$$

where Q is a Pauli operator functioning on qubits from the set $\{Y, Z, A\}$, $J\ is\ a\ 2 \times 2$ identity matrix, and j is the imaginary integer. The measurement result based on the readout qubits' computational basis is the QNN's output. Given that a qubit's measurement result is probabilistic, the measurement findings' expectation value, or E, is the QNN output. The expression of F is shown in Eq. (19).

$$F = \langle \Psi_y | V^{\dagger}(\theta) N V(\theta) | \Psi_y \rangle \quad (19)$$

where $|\Psi_y\rangle$ is represented as the QNN's input quantum state, and N is a linear amalgamation of Pauli operators that act as readout qubit observables. In a hybrid quantum-classical model, the loss M of a training example is computed conventionally on a classical device. An objective function $m(.)$ of the task is used to determine the loss L for the given training sample based on the actual output F and the expected output z. expression of the M is presented in Eq. (20).

$$M = m(F, z) \quad (20)$$

In the model optimization stage, the QNN update its variational parameters via back-propagation and gradient descent, just like a standard NN. It computes the gradient of a variational parameter θ_l in the $l-th$ quantum layer with respect to loss M using the following Eq. (21).

$$\frac{\partial M}{\partial \theta_l} = \frac{\partial M}{\partial F}\frac{\partial F}{\partial \theta_l} \quad (21)$$

$\partial M/\partial F$ is easily obtained using the objective function $m(.)$. $\partial F/\partial \theta_l$ is computed using Eq. (22).

$$\frac{\partial F}{\partial \theta_l} = j\langle \Psi_y | V_{-}^{\dagger}\left[Q_l,\, V_{+}^{\dagger} I V_{+}\right] V_{-} | \Psi_y \rangle \quad (22)$$

where, the Eq. (23) is represented as,

$$V_{+} = \prod_{m=l+1}^{o} W_m V(\theta_l)\ \ and\ V_{-} = \prod_{m=1}^{m=l} W_m V(\theta_l) \quad (23)$$

2) RNN [31]: It serves as a pivotal component, contributing to the model's efficacy in processing sequential data and capturing hierarchical dependencies within the input features. The proposed QIF-RNN excels in identifying complex patterns and relationships within the input features, ultimately enhancing its performance in data classification tasks by utilizing the inherent ability of RNNs to capture dependencies in sequential data. Fig. 2 shows the Structure of the QIF-RNN.

3) Fuzzy logic: It is a mathematical framework that deals with uncertainty and imprecision, where traditional binary logic fails. It helps to capture the vagueness in data, making the system more flexible and robust [32].

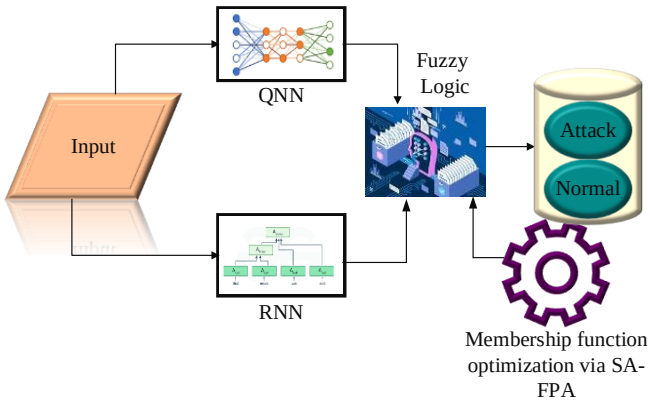


Fig. 2. Architecture of QIF-RNN.

a) Fuzzy sets: Crisp sets that have had their characteristic function changed to the membership function A: X →[0,1] are known as fuzzy sets.

b) Properties of fuzzy sets: Various properties of Fuzzy sets is presented in Table V. Algorithm 1 shows the pseudocode of Fuzzy decision-making.

TABLE V. PROPERTIES OF FUZZY SETS

Operation	Crisp	Fuzzy
Addition	$J + V$	$\tilde{J} + \tilde{V} = [J_1^{(\propto)} + V_1^{(\propto)}, J_3^{(\propto)} + V_3^{(\propto)}]$
Subtraction	$J - V$	$\tilde{J} - \tilde{V} = [J_1^{(\propto)} - V_3^{(\propto)}, J_3^{(\propto)} - V_1^{(\propto)}]$
Multiplication	$J \cdot V$	$\tilde{J} \cdot \tilde{V} = [J_1^{(\propto)} \cdot V_1^{(\propto)}, J_3^{(\propto)} \cdot V_3^{(\propto)}]$
Division	$J \div V$	$\tilde{J} + \tilde{V} = [J_1^{(\propto)} \div V_3^{(\propto)}, J_3^{(\propto)} \div V_1^{(\propto)}], if\ 0 \notin [V_1^{(\propto)}, V_3^{(\propto)}]$

4) Membership function optimization: It is acquired via the SA-FPA.

Algorithm 1: Pseudocode for Fuzzy Decision Making
Using fuzzy decision-making entails the subsequent actions:
Step 1: The identification of variables and the completion of the alternatives is the first phase.
Step 2: The linguistic parameters are transformed from real variables throughout the fuzzification process.
Step 3: The user chooses the variables that must be entered into the knowledge base.
Step 4: A membership function is the expression of a membership function in a mathematical function.
Step 5: Giving the if-then condition rule is the next step. One rule is represented by each variable.
Step 6: Converting the fuzzy value to an output variable is the next step.
Step 7: Practical implementation of the alternative is the final stage of the fuzzy process. If the implementation is successful, the system's performance will improve concerning the process's goal.

a) Proposed SA-FPA: Flowering plants reproduce, and FPA mimics this process [33]. The proposed SA-FPA is used for optimizing the fuzzy membership functions. Membership functions define how each data point belongs to a fuzzy set (e.g., low, medium, high). SA-FPA adapts these membership functions for optimal performance, ensuring that the fuzzy logic system can accurately represent the underlying uncertainties in the data. Algorithm 2 defines the FPA procedure.

Algorithm 2: SA-FPA Procedure
Step 1: The process of biotic pollination is regarded as worldwide, with pollinators carrying out Levy flights.
Step 2: The process of abiotic pollination is seen as a local one.
Step 3: Flower constancy is examined using the hypothesis that the degree of similarities between the flowers in question and the likelihood of reproduction are inversely connected.
Step 4: Whether a pollination technique is local or global is determined by a switching probability p in the interval [0, 1].

A flower m represents a solution vector b_m in FPA. Two distinct search techniques are used by the algorithm: local and global pollination. Utilizing the following Eq. (24), the first and third FPA criteria could be used to numerically express the global pollination procedure.

$$b_m^{x+1} = b_m^x + \gamma \cdot P(\lambda) \cdot (k^* - b_m^x) \quad (24)$$

where $k^*$is the finest flower in the populace of flowers at iteration x, b_m^x represents flower m at iteration x, λ is a constant, γ is a constant scaling aspect to control the step size and $P(\lambda) > 0$ is the Le´vy flight step size, which is drawn from a Le´vy distribution and characterizes the strength of the pollination; $\Gamma(\lambda)$ is the usual gamma function and $w > 0$. The mathematical expression of p is presented in Eq. (25).

$$P \sim \frac{\lambda \Gamma(\lambda) sin sin\left(\frac{\pi\lambda}{2}\right)}{\pi} \cdot \frac{1}{w^{1+\lambda}}, (w > 0), \quad (25)$$

Conversely, the following Eq. (26) represents the local pollination rule (second rule) and floral dependability (third rule), where e is taken from a uniform distribution in [0, 1] and b_n^x and b_o^x are distinct flowers of the same population.

$$b_m^{x+1} = b_m^x + \varepsilon \cdot (b_n^x - b_o^x) \quad (26)$$

As per the fourth rule, a switch probability t in [0, 1] determines the kind of flower pollination (local or global). Reiterating the earlier data. Eq. (27) expresses the fitness estimation of proposed SA-FPA, in which ρ_i refers to prediction error for each fuzzy set, c_i indicates complexity of the membership function, $s(M)$ signifies constraint function ensuring feasible membership function structures, and γ addresses regularization parameter balancing error minimization and function complexity.

$$f_{opt} = \left(\sum_{i=1}^{N} \left(\frac{\rho_i}{c_i}\right) + \gamma s(M) \right) \quad (27)$$

Fig. 3 displays the FPA flowchart, where r is the population size of flowers and h is the number of problem dimensions. Once the QNN and RNN have processed the data, the outputs are fused with the optimized fuzzy logic system. The fusion helps in incorporating both the sequential information (handled by RNN) and the non-binary decision-making capacity (handled by fuzzy logic).

The final classification output O is derived by combining the outputs from QNN, RNN, and the fuzzy system. Let O_{qnn} and O_{rnn} be the outputs from the QNN and RNN, and O_{fuzzy} be the fuzzy logic decision, Eq. (28) states the overall classification output, in which α, β, and γ means for weighting factors to balance the contributions from each component.

$$O = \alpha \cdot O_{qnn} + \beta \cdot O_{rnn} + \gamma \cdot O_{fuzzy} \quad (28)$$

This combined approach allows the QIF-RNN model to utilize the strengths of quantum-inspired learning, sequence prediction, and handling of uncertainty to achieve a highly accurate classification.

G. Attack Mitigation via Policy Gradient Method

The Policy Gradient method is one such technique in reinforcement learning, which achieves those situations where the number of possible actions is high dimensional or continuous is practical for Q-learning. Unlike Q-learning, which emphasizes verdict optimal actions, policy gradient seeks optimal parameters θ for a policy π_θ which would maximize the total reward. The chief aim of the policy gradient is to maximize the expectation of return or collected reward starting from a given initial state. That is, it is apprehended by Eq. (29).

$$J(\pi_\theta) = E_{\tau \sim \pi_\theta}[r(\tau)] = \int \pi_\theta(\tau) r(\tau) d\tau \quad (29)$$

Here, $\pi_\theta(\tau)$ indicates the probability of observant trajectory τ. The method learns the optimal parameter θ by calculating the gradient $\nabla_\theta J(\pi_\theta)$ as per the Eq. (30).

$$\nabla_\theta J(\pi_\theta) = E_{\tau \sim d_{\pi_\theta}}[\sum_{t=1}^{T} r(s_t, a_t) \sum_{t=1}^{T} \nabla_\theta log\ log\ \pi_\theta(s_t, a_t)] \quad (30)$$

In the above equation, d_{π_θ} is the distribution of trajectories produced by policy π_θ . The derivation encompasses the substitution in the Eq. (31).

$$\pi_\theta(\tau) = p(s_1) \prod_{t=1}^{T} \pi_\theta(s_t, a_t) p(s_{t+1} | s_t, a_t) \quad (31)$$

Here, $p(\cdot)$ is independent of the policy parameter θ, and for simplicity, it's not explicitly encompassed in the derivation.

TABLE VI. ATTACK MITIGATION APPROACH: A COMPARATIVE ANALYSIS OF POLICY GRADIENT APPROACH AND Q-LEARNING

Method	Convergence Speed	Average Total Reward	Sample Efficiency	Robustness
Policy Gradient	Fast	High (85)	Moderate	High (10% drop)
Q-Learning	Moderate	Moderate (70)	Low	Low (30% drop)

As indicated in Table VI, we compare the two leading reinforcement learning methods, Policy Gradient and Q-Learning, with a focus solely on attack mitigation. In these dimensions—convergence speed, average total reward, and robustness—the Policy Gradient approach performs better than the Q-Learning method. Hence, this makes policy gradient more viable for dynamic and complex environments.

IV. SIMULATION RESULTS

A. Simulation Setup

The proposed IDS model via suggested QIF-RNN was developed via Python on an Intel core® i5 processor @2.6GHz, 16 GB RAM, 64-bit OS. Here, CICIoV2024 dataset was utilized for detection which is accessible via (https://www.kaggle.com/datasets/hassan06/nslkdd) [Accessed

Date: 24-09-2024]. 70% of the collected data has been used for training and 30% for testing. This assessment considered various metrics like sensitivity, specificity, accuracy, precision, False Positive Rate (FPR), False Negative Rate (FNR), NPV, F1-score, Matthews Correlation Coefficient (MCC), and Recall.

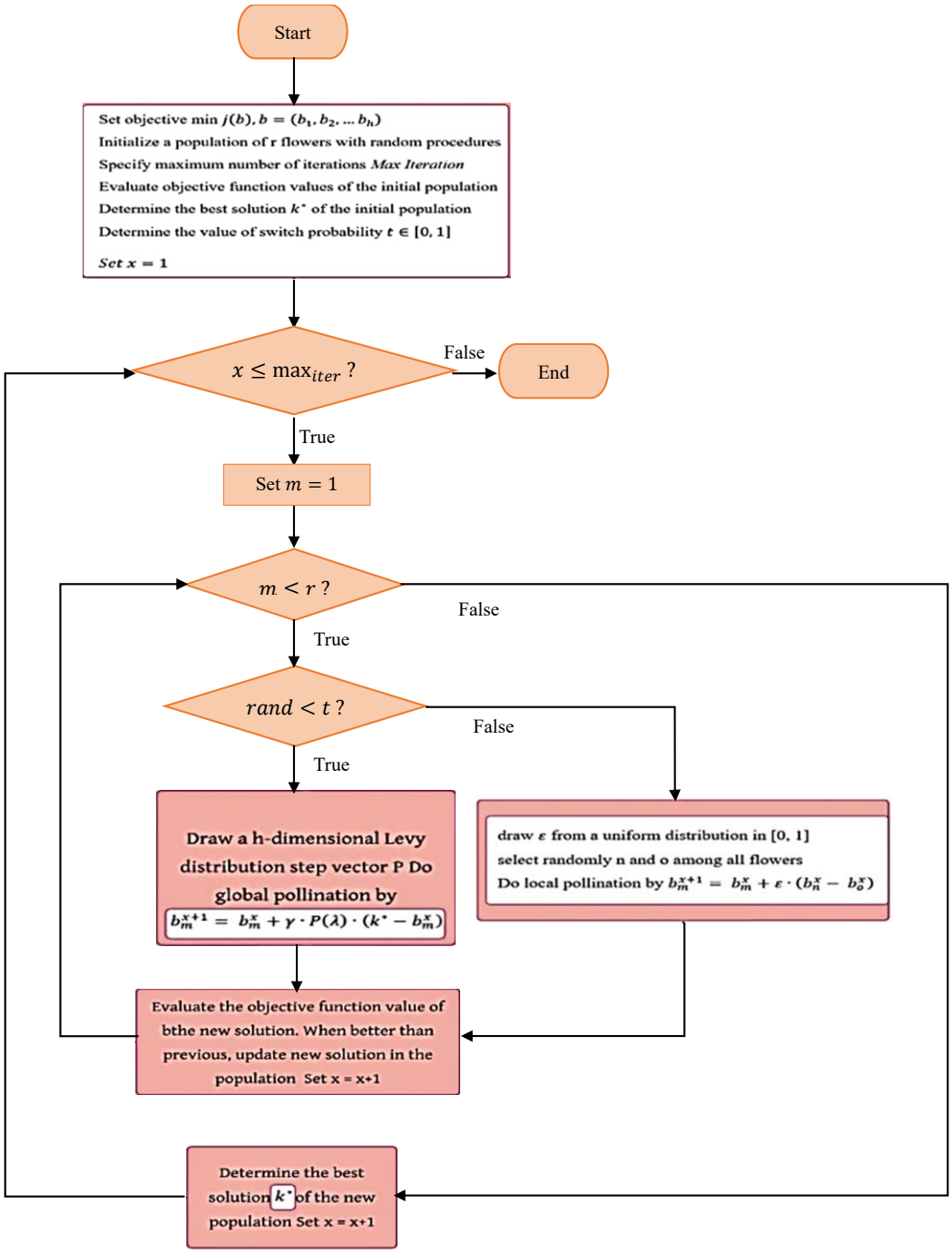


Fig. 3. Flow chart of proposed SA-FPA.

B. *Intrusion Detection Network: Performance Analysis for 70/30 Data Split*

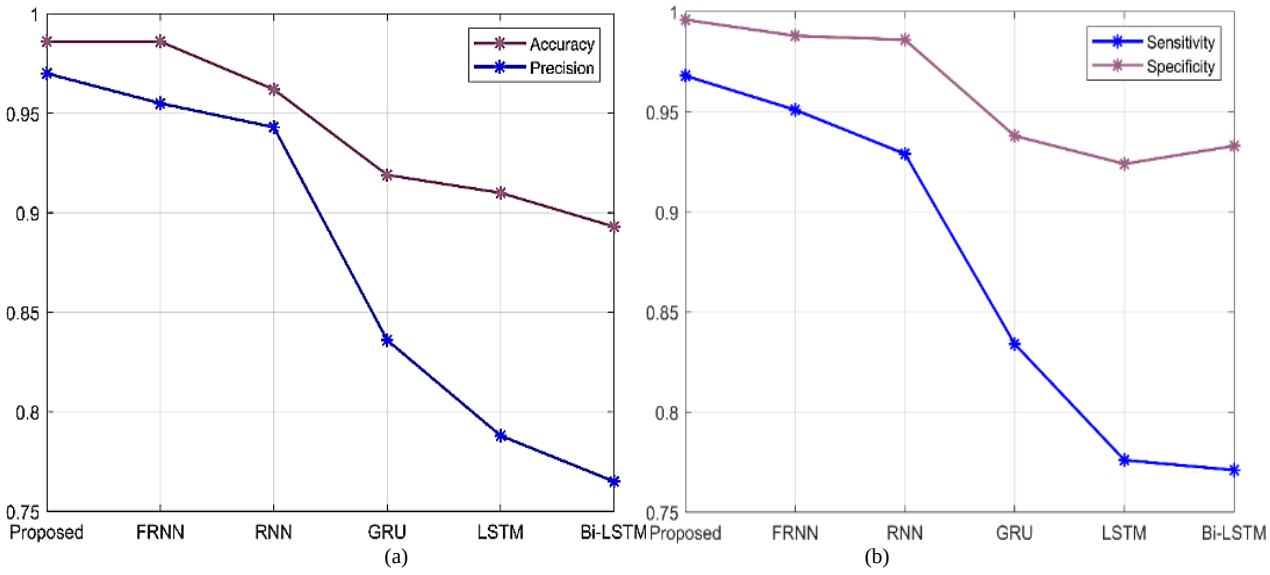
The comprehensive performance analysis demonstrates the superiority of the suggested ensemble framework with quantum learning over the other models already in use, such as Fuzzy RNN (FRNN) [34], RNN, GRU [35], LSTM [35], and Bi-LSTM [36], on a range of critical metrics in Fig. 4. With a sensitivity of 96.8%, the suggested model outperforms FRNN (95.1%), RNN (92.9%), GRU (83.4%), LSTM (77.6%), and Bi-LSTM (77.1%). This indicates the enhanced ability of the suggested model to precisely identify affirmative cases, which is essential for successful intrusion detection. The suggested model outperforms FRNN (98.8%), RNN (98.6%), GRU (93.8%), LSTM (92.4%), and Bi-LSTM (93.3%) in terms of

specificity, achieving a phenomenal 99.6%. The high specificity highlights how well the suggested model can identify negative instances and reduce false positives, which is an important consideration in real-world intrusion detection scenarios. The suggested model's total accuracy is 98.6%, which is higher than that of FRNN (98.6%), RNN (96.2%), GRU (91.9%), LSTM (91.0%), and Bi-LSTM (89.3%). This high accuracy illustrates how the suggested ensemble architecture is resilient in producing accurate and trustworthy classifications for both positive and negative examples. The suggested model's precision, a crucial parameter for assessing the model's capacity to reduce false positives, is reported to be 97%, surpassing that of FRNN (95.5%), RNN (94.3%), GRU (83.6%), LSTM (78.8%), and Bi-LSTM (76.5%). The accuracy with which the suggested model identifies intrusions is demonstrated by its precision.

The suggested model's F1-score, which weighs recall and precision, is stated as 96.4%, indicating that it can successfully strike an equilibrium between accuracy and completeness. This is superior to LSTM (79.7%), Bi-LSTM (77.3%), GRU (83.0%), RNN (94.5%), and FRNN (96.1%). The suggested model consistently outperforms other models in addition to maintaining a high Negative Predictive Value (NPV) of 99.2%. The remarkably low FPR and FNR, which stand at 2.9% and 7%, correspondingly, highlight the potential of the suggested approach to reduce misclassifications. The suggested model's overall Matthews Correlation Coefficient (MCC), which measures how well the model captures genuine correlations in the data, is stated as 94.6%. When compared to FRNN, RNN, GRU, LSTM, and Bi-LSTM, the suggested ensemble architecture consistently performs better across sensitivity, specificity, accuracy, precision, recall, F-measure, NPV, and Matthews Correlation Coefficient. The suggested model is shown by this thorough analysis as a cutting-edge and promising data categorization method, especially for data classification. Table VII shows the Comparative analysis of the suggested framework and existing model performance metrics.

TABLE VII. COMPARATIVE ANALYSIS OF PERFORMANCE METRICS WITH EXISTING MODELS

Metrics	Sensitivity	Specificity	Accuracy	Precision	F1-Score	NPV	FPR	FNR	MCC
Proposed	0.968	0.996	0.986	0.97	0.964	0.992	0.029	0.07	0.946
FRNN	0.951	0.988	0.986	0.955	0.961	0.992	0.036	0.072	0.921
NN	0.929	0.986	0.962	0.943	0.945	0.983	0.038	0.089	0.897
GRU	0.834	0.938	0.919	0.836	0.83	0.962	0.078	0.206	0.771
LSTM	0.776	0.924	0.91	0.788	0.797	0.947	0.099	0.259	0.707
Bi-LSTM	0.771	0.933	0.893	0.765	0.773	0.931	0.108	0.271	0.689



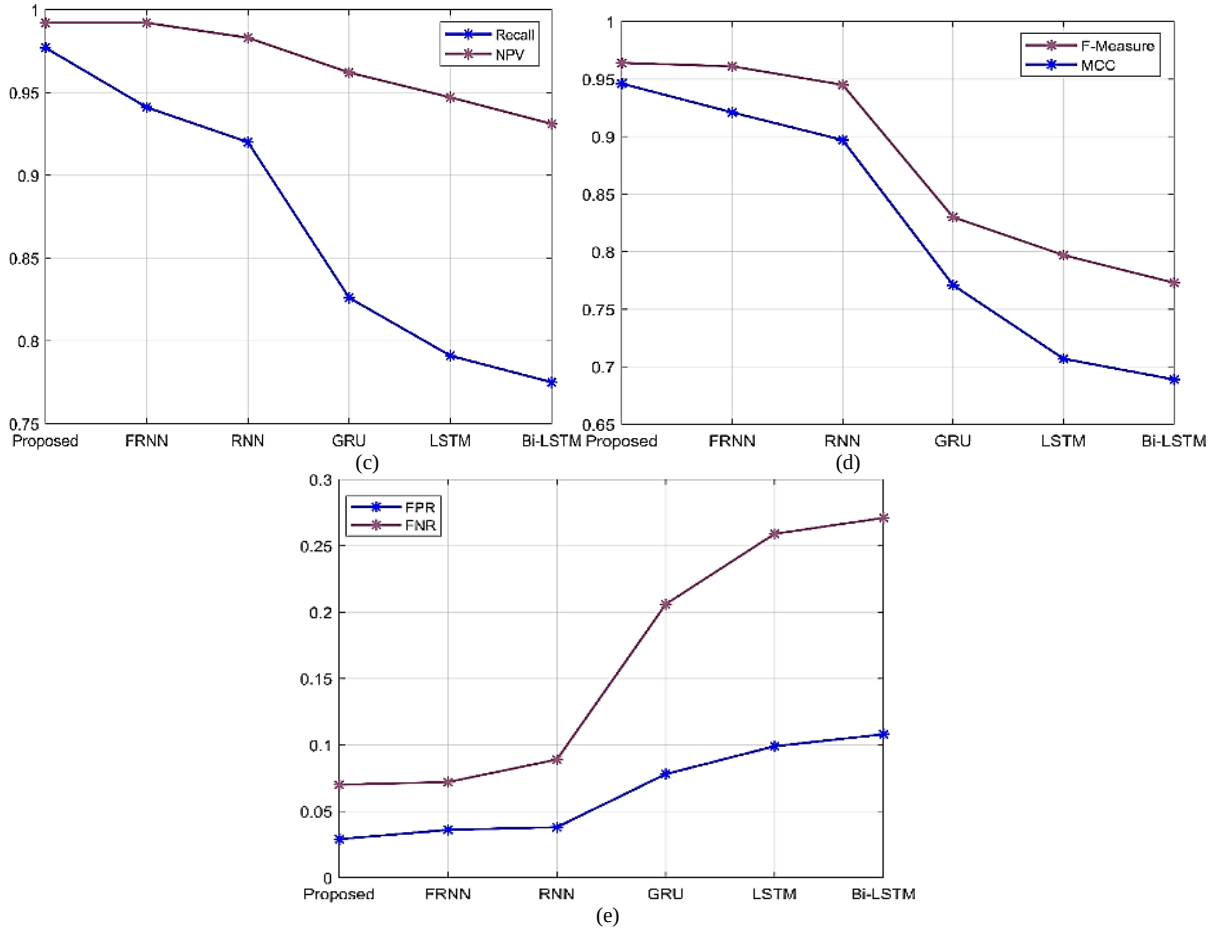


Fig. 4. Performance of proposed QIF-RNN over other algorithms for (a) Accuracy and precision, (b) Sensitivity and specificity, (c) Recall and NPV, (d) F1-Score and MCC, and (e) FPR and FNR.

C. Comparative Analysis of Proposed Intrusion Detector Model over SOTA Approaches for Varying Learning Rate

The research proposed a novel Meta-Heuristic QIF-RNN for IDS, structured into five phases: (i) Data Collection, (ii) Pre-processing, (iii) Feature Extraction, (iv) Dimensionality Reduction, and (v) Meta-Heuristic QIF-RNN-based Data Classification.

Table VIII shows the performance of the proposed model in comparison to the prevailing models in terms of Accuracy, Precision, Sensitivity, F-score, Specificity, MCC, FPR, and FNR. The proposed Model gives highest accuracy value of 98.261%, the precision of 98.095%, and F1-score of 97.549%, hence overall better performance due to higher values of correct classification. The Quantum network along with fuzzy and meta-heuristic optimization assisted in enhancing the classification accuracy of the model.

Table IX discusses the contrast of the performance of the proposed model with the existing models on metrics such as Accuracy, Precision, Sensitivity, F-score, Specificity, MCC, FPR, and FNR. The proposed Model reflects better performance on all these metrics with the highest value in accuracy of 99.755% and precision of 99.901%. Its high sensitivity of 98.655% and specificity of 99.075% show its higher classification accuracy in identifying the attacks. The fuzzy logic-based classification has enhanced the detection accuracy of the model. Thus, making it accurate in detecting the attacks.

TABLE VIII. COMPARATIVE ANALYSIS OF PERFORMANCE METRICS WITH EXISTING MODELS

Model	Accuracy	Precision	F-Score	Specificity	Sensitivity	MCC	FPR	FNR
Proposed	0.98261	0.98095	0.97549	0.98961	0.98108	0.98398	0.0263	0.0107
LSTM [18]	0.95429	0.95683	0.95927	0.95939	0.95892	0.95478	0.0571	0.0639
CNN [25]	0.96828	0.96545	0.96118	0.96321	0.96478	0.96828	0.0441	0.0512
MTH-IDS[24]	0.95105	0.95323	0.95124	0.95806	0.95308	0.95939	0.0501	0.0436
QNN [30]	0.94048	0.94685	0.95118	0.95621	0.94478	0.95828	0.0431	0.0312

TABLE IX. COMPARATIVE ANALYSIS OF PERFORMANCE METRICS WITH EXISTING MODELS

Model	Accuracy	Precision	F-Score	Specificity	Sensitivity	MCC	FPR	FNR
Proposed	0.99755	0.99901	0.98404	0.99075	0.98655	0.99765	0.0141	0.0092
LSTM [18]	0.96765	0.96909	0.96683	0.96333	0.96909	0.96675	0.0461	0.0553
CNN [25]	0.97081	0.97683	0.97771	0.97684	0.97308	0.97617	0.0361	0.0223
MTH-IDS[24]	0.96538	0.96323	0.96118	0.96286	0.96694	0.96828	0.0421	0.0323
QNN [30]	0.95833	0.95683	0.96393	0.96231	0.95254	0.96161	0.0391	0.0236

V. DISCUSSION

The proposed Meta-Heuristic QIF-RNN model for IDS brings several advantages. First, the structured approach involves multiple phases such as data preprocessing steps that ensure only relevant and clean data are used for classification. The use of higher-order statistical features, IMI, correlation, and entropy ensures that the model captures critical attributes of the data. These data helped in detecting intrusions more effectively. Furthermore, the integration of QNN, RNN, and Fuzzy Logic in the classification phase allows the model to handle both sequential and fuzzy data, leading to high classification accuracy of 98.6%. The SA-FPA optimization of the membership function enhances the precision of the decision-making process. Also, the Policy Gradient Method contributes to effective attack mitigation. These features make the model robust in detecting and mitigating cyber threats in ICVs.

Despite these advantages, the model also has limitations. While the use of dimensionality reduction (ILDA) helps minimize the computational load, the complexity introduced by combining multiple components (QNN, RNN, Fuzzy Logic, and SA-FPA) leads to increased computational overhead. This might limit its scalability in real-time environments, particularly when dealing with large-scale and high-speed networks like those in ICVs. Another potential limitation is the static nature of the dataset used (CICIoV2024). It may not represent real-time or evolving attack scenarios. As the research suggests, future improvements could focus on incorporating real-time data streams and advanced optimization techniques to address these limitations.

VI. CONCLUSION

The research proposed a novel Meta-Heuristic QIF-RNN for IDS, structured into five phases: (i) Data Collection, (ii) Pre-processing, (iii) Feature Extraction, (iv) Dimensionality Reduction, and (v) Meta-Heuristic QIF-RNN-based Data Classification. Initially, raw data were collected from the CICIoV2024 dataset, which then underwent preprocessing through a data-cleaning technique. From the pre-processed data, significant features including Higher-Order Statistical Features, IMI, Correlation, and Entropy were extracted. The dimensionality of these extracted features was subsequently reduced using ILDA. Finally, the data were classified using the dimensionality-reduced features in conjunction with the Meta-Heuristic QIF-RNN model, which integrated QNN, RNN, and Fuzzy Logic. The optimization of the membership function was achieved through SA-FPA. The attack mitigation is achieved via the Policy Gradient Method. The proposed model attained 98.6% accuracy and outran existing models. Integrating complex DL algorithms (QNN, and RNN) requires considerable computational time. Future work could focus on enhancing the Meta-Heuristic QIF-RNN model by incorporating real-time data streams for dynamic intrusion detection in ICVs. Additionally, exploring advanced optimization algorithms and integrating ensemble learning techniques improve classification accuracy and robustness. Investigating the model's adaptability to emerging cyber threats and conducting extensive performance evaluations in diverse network environments could further strengthen its applicability. Finally, expanding the feature extraction methods to include DL-based approaches yields richer insights and enhances the model's predictive capabilities.

DATASET ACCESSIBILITY

The dataset used in your study, CICIoV2024, is referenced as accessible through the link to the Kaggle dataset (https://www.kaggle.com/datasets/pushpakattarde/ciciov2024decimalcsv), which is publicly available for download. This ensures reproducibility for anyone looking to replicate the results.

ACKNOWLEDGEMENT

The author extends the appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through the project number (R-2024-1153).

REFERENCES

[1] Hadjilambrinos, C. (2021). Reexamining the automobile's past: What were the critical factors that determined the emergence of the internal combustion engine as the dominant automotive technology?. Bulletin of Science, Technology & Society, 41(2-3), 58-71.

[2] Boysen, N., Schulze, P., & Scholl, A. (2022). Assembly line balancing: What happened in the last fifteen years?. European Journal of Operational Research, 301(3), 797-814.

[3] Cao, J., Lin, L., Zhang, J., Zhang, L., Wang, Y., & Wang, J. (2021). The development and validation of the perceived safety of intelligent connected vehicles scale. Accident Analysis & Prevention, 154, 106092.

[4] Campisi, T., Severino, A., Al-Rashid, M. A., & Pau, G. (2021). The development of the smart cities in the connected and autonomous vehicles (CAVs) era: From mobility patterns to scaling in cities. Infrastructures, 6(7), 100.

[5] Xie, Y., Zhou, Y., Xu, J., Zhou, J., Chen, X., & Xiao, F. (2021). Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: state-of-the-art and future challenges. Software: Practice and Experience, 51(11), 2108-2127.

[6] Feng, Y., Huang, S. E., Wong, W., Chen, Q. A., Mao, Z. M., & Liu, H. X. (2022). On the cybersecurity of traffic signal control system with connected vehicles. IEEE Transactions on Intelligent Transportation Systems, 23(9), 16267-16279.

[7] Garcia, M. H. C., Molina-Galan, A., Boban, M., Gozalvez, J., Coll-Perales, B., Şahin, T., & Kousaridas, A. (2021). A tutorial on 5G NR V2X

communications. IEEE Communications Surveys & Tutorials, 23(3), 1972-2026.

[8] Rahman, M. A., Rahim, M. A., Rahman, M. M., Moustafa, N., Razzak, I., Ahmad, T., & Patwary, M. N. (2022). A secure and intelligent framework for vehicle health monitoring exploiting big-data analytics. IEEE Transactions on Intelligent Transportation Systems, 23(10), 19727-19742.

[9] Dakić, P. (2024). IMPORTANCE OF KNOWLEDGE MANAGEMENT FOR CI/CD AND SECURITY IN AUTONOMOUS VEHICLES SYSTEMS. Journal of Information Technology & Applications, 14(1).

[10] Zhi, P., Zhao, R., Zhou, H., Zhou, Y., Ling, N., & Zhou, Q. (2021). Analysis on the development status of intelligent and connected vehicle test site. Intelligent and Converged Networks, 2(4), 320-333.

[11] Guan, T., Han, Y., Kang, N., Tang, N., Chen, X., & Wang, S. (2022). An overview of vehicular cybersecurity for intelligent connected vehicles. Sustainability, 14(9), 5211.

[12] Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Warren, M. (2023). Modelling cybersecurity regulations for automated vehicles. Accident Analysis & Prevention, 186, 107054.

[13] Cao, J., Lin, L., Zhang, J., Zhang, L., Wang, Y., & Wang, J. (2021). The development and validation of the perceived safety of intelligent connected vehicles scale. Accident Analysis & Prevention, 154, 106092.

[14] Anbalagan, S., Raja, G., Gurumoorthy, S., Suresh, R. D., & Dev, K. (2023). IIDS: Intelligent intrusion detection system for sustainable development in autonomous vehicles. IEEE Transactions on Intelligent Transportation Systems, 24(12), 15866-15875.

[15] Sousa, B., Magaia, N., & Silva, S. (2023). An intelligent intrusion detection system for 5g-enabled internet of vehicles. Electronics, 12(8), 1757.

[16] Cheng, P., Han, M., Li, A., & Zhang, F. (2022). STC-IDS: Spatial–temporal correlation feature analyzing based intrusion detection system for intelligent connected vehicles. International Journal of Intelligent Systems, 37(11), 9532-9561.

[17] Alladi, T., Kohli, V., Chamola, V., Yu, F. R., & Guizani, M. (2021). Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles. IEEE Wireless Communications, 28(3), 144-149.

[18] Yu, T., Hua, G., Wang, H., Yang, J., & Hu, J. (2022, May). Federated-lstm based network intrusion detection method for intelligent connected vehicles. In ICC 2022-IEEE International Conference on Communications (pp. 4324-4329). IEEE.

[19] Pascale, F., Adinolfi, E. A., Coppola, S., & Santonicola, E. (2021). Cybersecurity in automotive: An intrusion detection system in connected vehicles. Electronics, 10(15), 1765.

[20] Ge, X., Han, Q. L., Wu, Q., & Zhang, X. M. (2022). Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks. IEEE/CAA Journal of Automatica Sinica, 10(5), 1234-1251.

[21] Park, S., & Park, H. (2024). PIER: cyber-resilient risk assessment model for connected and autonomous vehicles. Wireless Networks, 30(5), 4591-4605.

[22] Ahmed, I., Jeon, G., & Ahmad, A. (2021). Deep learning-based intrusion detection system for internet of vehicles. IEEE Consumer Electronics Magazine, 12(1), 117-123.

[23] Li, X., Hu, Z., Xu, M., Wang, Y., & Ma, J. (2021). Transfer learning based intrusion detection scheme for Internet of vehicles. Information Sciences, 547, 119-135.

[24] Yang, L., Moubayed, A., & Shami, A. (2021). MTH-IDS: A multitiered hybrid intrusion detection system for internet of vehicles. IEEE Internet of Things Journal, 9(1), 616-632.

[25] Alladi, T., Kohli, V., Chamola, V., & Yu, F. R. (2023). A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems. Digital Communications and Networks, 9(5), 1113-1122.

[26] Madhu, G., Lalith Bharadwaj, B., Sai Vardhan, K., & Naga Chandrika, G. (2020). A normalized mean algorithm for imputation of missing data values in medical databases. In Innovations in Electronics and Communication Engineering: Proceedings of the 8th ICIECE 2019 (pp. 773-781). Springer Singapore.

[27] Dahiya, D. (2023). DDoS attacks detection in 5G networks: hybrid model with statistical and higher-order statistical features. Cybernetics and Systems, 54(6), 888-913.

[28] Piras, D., Peiris, H. V., Pontzen, A., Lucie-Smith, L., Guo, N., & Nord, B. (2023). A robust estimator of mutual information for deep learning interpretability. Machine Learning: Science and Technology, 4(2), 025006.

[29] Graf, R., Zeldovich, M., & Friedrich, S. (2024). Comparing linear discriminant analysis and supervised learning algorithms for binary classification—A method comparison study. Biometrical Journal, 66(1), 2200098.

[30] Park, S., Baek, H., Yoon, J. W., Lee, Y. K., & Kim, J. (2024). AQUA: Analytics-driven quantum neural network (QNN) user assistance for software validation. Future Generation Computer Systems.

[31] Donkol, A. A. E. B., Hafez, A. G., Hussein, A. I., & Mabrook, M. M. (2023). Optimization of intrusion detection using likely point PSO and enhanced LSTM-RNN hybrid technique in communication networks. IEEE Access, 11, 9469-9482.

[32] Alohali, M. A., Elsadig, M., Al-Wesabi, F. N., Al Duhayyim, M., Mustafa Hilal, A., & Motwakel, A. (2023). Enhanced chimp optimization-based feature selection with fuzzy logic-based intrusion detection system in cloud environment. Applied Sciences, 13(4), 2580.

[33] Yang, X. S., Karamanoglu, M., & He, X. (2014). Flower pollination algorithm: a novel approach for multiobjective optimization. Engineering optimization, 46(9), 1222-1237.

[34] Zhang, Z., He, H., & Deng, X. (2023). An FPGA-implemented antinoise fuzzy recurrent neural network for motion planning of redundant robot manipulators. IEEE transactions on neural networks and learning systems.

[35] Al-kahtani, M. S., Mehmood, Z., Sadad, T., Zada, I., Ali, G., & ElAffendi, M. (2023). Intrusion detection in the Internet of Things using fusion of GRU-LSTM deep learning model. Intelligent Automation & Soft Computing, 37(2).

[36] Zhang, J., Zhang, X., Liu, Z., Fu, F., Jiao, Y., & Xu, F. (2023). A Network Intrusion Detection Model Based on BiLSTM with Multi-Head Attention Mechanism. Electronics, 12(19), 4170.

Predicting Learners' Academic Progression Using Subspace Clique Model in Multidimensional Data

Mr. Oyugi Odhiambo James, Prof. Waweru Mwangi, Dr. Kennedy Ogada
Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

***Abstract*—Subspace clustering examines the traditional clustering techniques that have previously been considered the best approaches to clustering data. This study uses a subspace clustering approach to predict learners' academic progress over time. Using the subspace clustering method, a model was developed that improves the classic Clique by optimizing clustering performance and addresses the clustering challenges posed by inaccuracies due to additional data size and increased dimensionality. The study used an experimental design that included data validation and training to predict students' academic progress. Clustering evaluation metrics including accuracy, precision, and recall measures were identified. The optimized model recorded a better performance index with 98.90% accuracy, 98.50% precision, and 98.50% recall which directly shows the efficiency of the optimized model in predicting learning academic progress through clustering. In this regard, conclusions are drawn for an alternative approach to predictive modeling through cluster analysis, so that educational institutions have a better opportunity to manage learners by ensuring adequate preparation in terms of resources, policies and knowledge. It highlights career guidance for learners based on their academic progress. The result validates the suitability of the model for clustering multidimensional data.**

Keywords*—Subspace clustering; clique model; academic progression; multidimensional data; feature engineering; cross validation and principal component analysis

I. Introduction

A. Introduction

This component describes the background of the study, the objectives and the problems of the study. The literature of the study within the local, regional and international perspectives on the use and application of clique models, the importance and the gaps addressed in this study.

B. Background of Study

Academic progress is important in a learning environment where each learner must be assessed to determine their progress to the next level of learning. Various considerations are taken into account and typically indicators of progress in a learning environment are well established and clearly stated, although this may vary from institution to institution. There are standard learning levels such as certificate, diploma, bachelor's, master's and doctoral. It is also notable that educational institutions need to understand learners' progress to ensure efficient and effective management of learners.

The main objective of this study was to develop a model that predict leaners' academic progression. The improved Subspace Clique model was expected to address the challenges of classical Clique in clustering of data. For instance, the process of finding clusters in multidimensional data space is a complex procedure due to the large number of attributes and tuples involved. In the case of multidimensional data, the density points are at their lowest level. The approach taken by traditional Clique cannot stand due to the inaccuracies and inconsistencies, thus misleading in finding the objective clusters. Because of various scores of attributes involved, clusters are not always found in their actual multidimensional data space [1]. This means that it could be possible to find these clusters in specific subspace of the entire dataset space. The problem of dimensionality is common in data mining, for instance the dimension increases with the increase in the number of attributes in a particular dataset leading to the curse of dimensionality which an optimized Clique can address. In [2], improved Clique algorithm from a hybrid of Clique and K-means, the experiment was conducted on artificially simulated dataset, which revealed that the hybrid was not sensitive to the input parameters used in classical Clique but was silent on the dimensionality challenge and different dataset effect. Ultimately a significant number of attributes are normally dropped before the actual experiments are conducted which may affect the results if not well accounted for [3]. On the other hand, traditional clustering algorithms break when employed in multidimensional data spaces, and that they present many irrelevant attributes that could limit the possibility of clustering. The current subspace clustering methods are mainly used in either numerical or categorical data but not all [4]. The method recommended in this study takes into account the different data types that are subject to proper data preprocessing. In this study, an improved Clique algorithm was proposed, which takes into account students' academic performance in predicting learning progress. This is an area that many researchers have overlooked when conducting behavioral analysis using Clique algorithm.

C. Literature Review

This study is based on the subspace clique clustering technique. The focus of this study was on predicting learners' academic progress using multidimensional data. To achieve this, future forecasts were made based on the available data. Whereas a Cluster is an ordered list of data which have the familiar characteristics [5], Clustering refers to an ill-posed problem which aims to reveal interesting structures in the data or to derive a useful grouping of the observations. However, specifying what is interesting or useful in a formal way is challenging. This complicates the specification of suitable criteria for selecting a clustering method, or a final clustering solution [6] also emphasized this point. He argued that the definition of the true clusters depends on the context and on the

aim of clustering. Therefore, given the data, there is no clear clustering solution, but different aims of clustering imply different solutions, and analysts should in general be aware of the ambiguity inherent in cluster analysis and thus be transparent about their clustering aims when presenting the solutions obtained [7].

CLIQUE is a subspace clustering algorithm that operates on a grid and density basis. By combining the advantages of density-based clustering with the advantages of grid-based clustering, it can find clusters of any shape while still managing large amounts of data [8]. The clustering process starts with a single dimension scaling upwards to higher dimensions. Clique divides the N-dimensional data space into non-overlapping rectangular units from which dense units are identified. A unit is considered highly dense if the sum of the total data points in the unit runs over an input parameter, Clusters are then created from the original data space using the Apriori principle [9]. CLIQUE finds high-quality clusters only in subspaces with the highest dimensionality, making it an efficient method. The threshold density and grid size must be properly adjusted in order to produce meaningful clustering results.

Research on Clique-based Model in Predictive Analysis has been conducted by several scholars, such as [10], One such study focused on forecasting future weights based on a partial order set using the Clique Algorithm for pattern analysis to cluster high-dimensional data [11]. In text mining [12], Customer Segmentation and trend analysis [13], Further, intrusion detection in IoT networks [14]. The study in [15] proposed dimensionality reduction via feature reduction. as well as imaging processing [16]. Student behavioral data [17] among other fields. This study proposed Clique model in predicting leaners academic progression in multidimensional dataset.

Numerous studies have been carried out to forecast the development, effectiveness, and behavior of leaners. For instance, [12] used the vector space model and the clique subspace model to study critical text mining of learners' behavioral patterns in Kenya. The findings demonstrated that even for large data sets, the processing time in Clique is significantly less; however, the researcher noted that grid cell consideration, density threshold, and parameter input requirements are limitations.

Similarly, [18] studied in the USA to find course clusters and course cliques based on the degree of grade correlation between student grades in pairs of courses in one of the universities using subspace clique and network diagrams, where courses are represented as nodes and are connected to courses if they have a high degree of grade correlation. The ability of Clique to cluster academic data is demonstrated by an analysis of the results for course pairs and courses grouped by academic department.

For example, [17] research on student behavior patterns was done in China. In an effort to address the issue, the study suggested an unsupervised clustering framework that combined behavioral data from students with grade point averages to find behavioral patterns, a similar study reflected in study [19]. The suggested framework incorporated the views of statistics and entropy to extract behavior features, which are combined with k-means and density-based spatial clustering of applications with noise (DBSCAN) algorithms to find behavioral patterns. An analysis was conducted to compare the enhanced model with the conventional Clique subspace clustering model. In comparison to the improved model, the results showed that Clique performed a little bit worse. The findings demonstrate that the framework is able to identify both mainstream and anomalous behavioral patterns. Although this was the case, future selection only considered variance and correlation rather than cross validation and principal component analysis, meaning that the data management of clustering was not given much thought.

A similar study by [20] was conducted in Korea on various clustering algorithms with a focus on pattern identification. Clique became one of the algorithms used and tried to study the convergence speed and accuracy of clustering. The study used small data sets that achieved high accuracy with sensitivity to density and hyperparameter tuning. It was not clear how the optimization that resulted in high accuracy was achieved, as the study did not specify the limitations of small datasets and dimensionality management, which has been addressed in this study.

In the United Kingdom, [21] conducted research to design a system for assessing and guiding the mental health of college students. The study examined the applications of clustering data mining algorithms relevant to the researcher's area of interest. The research involved college students and used performance testing to determine the system's accuracy and effectiveness in assessing and managing students' mental health. However, the study acknowledged the pattern recognition ability of the Clique algorithm, although it focused on developing an artificial intelligence-based system for analyzing the mental health of college students. Further suggestions from [22] affirm that the CLIQUE algorithm can perform effective cluster analysis and automatically adapt to different subspaces.

A study by [23] to find nonlinear feature relationship pattern recognition in India. Even in cases where feature relationships are nonlinear, the method enables the discovery of bi-clusters based on feature relationships. The suggested approach used datasets from various domains and did not require the user to provide any parameters. Clustering with the Clique algorithm was used to assess performance. The fact that the new approach outperformed the original Clique, suggests that it needs to be improved. The research in [24] are among the other benchmarked studies with similar findings.

In summary, the studies conducted in Kenya, the United States, the United Kingdom, China, India and Korea using the Clique algorithm clustering technique have not only shown the scope bias but also found serious gaps, which accompany the implementation and use of the Clique algorithm, which require attention. For example, most studies have been conducted to analyze student behavior patterns, but not to direct academic progress and/or performance, which is critical to excelling in an academic learning environment and in managing learners. Other notable challenges would be data preparation before use, data size, methods used for dimensionality reduction, future selection, and consideration of hyperparameters, which in turn affect the accuracy of the clustering method. Other studies that

conducted a comparative analysis between ordinary Clique and other existing models, trying to recommend a model that provides a better performance index for some specific data, which is not necessarily academic in nature did not pay attention to improving the models.

In countering the gaps with studies conducted in Kenya and reflected elsewhere, this study recommends predicting students' academic progress using an improved subspace clique in multidimensional data, which considers model optimization through feature engineering, data standardization, dimensionality reduction and cross-validation.

In other sections, the paper further extends to provide information on study-related work, data acquisition and preprocessing, the design, methods, tools used, and the implementation of the predictive subspace Clique model. The paper concludes by presenting and discussing the results, conducting a comparative analysis, and exploring the significance of the research. Additionally, it draws conclusions and offers recommendations for future work.

II. Related Work

A. Introduction

This section includes a detailed review of the relevant literature and recent studies on implementing the subspace clique model for predicting learners' academic progress in multidimensional data, as well as a summary of results from such applications.

B. Subspace Clique Model

Research on the topic of using Subspace Clique to predict student academic progress and related learning areas, or such behavioral environments is extensive. For example, in a study by [25], blended aerobics learning is analyzed and guided using data mining. Action learning is combined with blended aerobics instruction to promote learning progress. The study proposed a Clique clustering algorithm that meets the following criteria: (1) identify embedded clusters in high-dimensional data subspaces; (2) scale; (3) understand end-user results; and (4) predict cluster descriptions into minimized density expressions to promote understanding [25]. In the modern educational environment, blended learning has enormous growth potential. The study examined the practical value of meta-learning theory in its application to aerobics instruction. The results showed that students have potential meta-learning, can deliberately improve students' meta-learning ability, and it is important to increase students' interest in aerobic skills through appropriate learning strategies [26]. Subjects were tested on basic questions, aerobic technical skills and physical fitness in the experimental data set. A comparative analysis of the semester's academic performance was reviewed following a teaching exam that lasted 15 weeks, equivalent to a full semester at the university. After applying the classic clique model to the dataset and analyzing the results using accuracy, precision, and recall metrics, it was found that the model had an accuracy of 86.5%, a precision of 85.99%, and a recall of 85.9%. Although the accuracy was higher on average, the study's margin of error of 14.5 percent on accuracy was noted and could be associated with certain observations such as the unclear explanation of data management, feature selection, and dimensionality reduction with respect to cross-validation.

In a separate study conducted by [24], investigating clustering algorithms based on grids, the focus was on the appropriate selection of grid cells that contributed to the field, and a novel grid-based algorithm that employs an automated method for calculating the number of grid cells was proposed. The study covered the idea of grid cells in the Clique algorithm and used the Clique model to contrast the outcomes of the upgraded model. A simulated educational dataset was run through a Python script in order to identify learning patterns, which produced results with accuracy of 95.23%, precision 95.0% and a recall of 95.20%. The well-known Clique algorithm was used in the experiment as a benchmark, allowing a quick pinpoint on a few observations; even though the Clique model was efficient at establishing clusters when clustering data. Notably, it required two input parameters, i.e., the threshold for density and the number of intervals. The parameters in this case were difficult to calculate. Based on this study, we can conclude that the model did not function as well as the researcher had hoped.

In a related study, [17] used the clustering approach to analyze student behavior patterns. The study's goal was to assist the institution in setting targeted rules, particularly for unexpected patterns, and in determining more effective ways to provide specialized services and management. To address the issue, the study took into account a clustering technique. The study analyzed the relationships between various behavior patterns and students' grade point averages by conducting experiments on six different types of behavioral data generated by university students (eating behavior, shopping behavior, library entry behavior, and gateway login behavior, respectively). The six attributes were gathered from 9024 university students. Grade point averages served as the foundation for the computation of extrinsic metrics, which quantify the relationship between various behaviors and academic achievement. The characteristics corresponding to each type of behavior were derived from a central tendency perspective. With a comparative performance evaluation against the Clique algorithm, the study proposed a hybrid clustering algorithm that combines the best features of DBSCAN and K-means. Using the Clique algorithm, the results showed an accuracy of 92.0%, precision of 91.83% and recall of 90.12%. This explained the model's ability to group educational data. The researcher added that the improved model performed better than Clique by achieving an accuracy performance of 92.0%, which was only a small improvement. The experimental results show that the proposed method can not only detect abnormal behavior patterns but also identify different behavior patterns more accurately. Based on the clustering results, student departments can take more targeted interventions and specialized services. The study recommended that future work focus on creating meaningful features, creating new distance measures, reducing the dimensionality of feature spaces, and, lastly, investigating behavioral patterns and student labels in order to improve clustering analysis.

In a related study by [18], the researcher in this study computes the correlation of student grades between pairs of courses in a university, based on academic performance, in an

attempt to replicate the course groupings. Courses are represented as nodes in the course network graphs created for the study, and courses are connected if their grade correlation is high. Graph mining and network analysis tools were used in conjunction with the clique algorithm to visualize course networks and detect cliques and clusters within them, where the Pearson correlation was used to determine how similar two courses are to one another. Recall that the Clique concept was used in this study to visualize the results and obtain graphical Cliques. A k-clique is a collection of k nodes that are all connected to one another directly by an edge. In this study, the 0.5 correlation threshold was exceeded by 25% of course pairs and the 0.7 correlation threshold by 5% of pairs when at least 20 common students were examined, these results were evaluated against the metrics of accuracy, precision and recall. Which indicated a uniform performance of 75% for the three metrics. The study found a high correlation between student performance and a number of course pairs. Within the course correlation networks, cliques and modularity classes were recognized as course clusters. Course pairings and course groupings based on academic department were examined. According to the study, there is a significant grouping of courses with strong similarities across scientific disciplines, pre-health courses, and computer science subfields. Notably, the researcher stated that no study that used the concept of course similarity had ever been carried out using the clustering technique in a predictive way.

According to a study by [23] on a free relative density-based clustering method in nonlinear feature relationship patterns. The method proposed in this study allowed finding clusters based on feature relationships, even if the relationships are nonlinear. Since the proposed method did not require any input from the user, it could be applied to datasets from different domains. Fifteen simulated datasets were used for the experiments and eleven different clustering algorithms were used to compare their performance. Among them was the Clique clustering algorithm. For most simulated datasets used to identify behavioral patterns in learning environments, the proposed method appeared to provide better results. After several clustering operations on different simulated datasets, the Clique model showed an average performance of 93.9% accuracy, 94.3% precision and 93.5% recall; this was the best Clique performance in all of the researcher's experiments. The need for research in various dimensions is explained by the fact that the study did not achieve 100% accuracy even after using different data sets.

We can quickly identify a few issues based on the observations made in the various literature in the study for the use of Clique subspace clustering in predicting learners' progress. According to [25] study, Clique was able to perform clustering when used to predict learning progress in Aerobics. However, the algorithm was viewed with disdain due to its ambiguous explanation of data management, feature selection, and dimensionality reduction in relation to cross-validation. In a separate study by [24] Encompassing grid-based clustering algorithms and the use of well-known Clique algorithms in the experiment, it was reiterated that although the Clique model was efficient in forming clusters when clustering data, it required input parameters, a density threshold and the number of intervals required what was difficult to calculate. [17] used the Clique clustering approach to examine patterns of student behavior in a related study. Based on the findings, the study suggested that future research concentrate on developing new distance measures, dimensionality reduction, and behavioral pattern analysis to enhance clustering analysis. Similar to the course groupings created by [18], the researcher in this study used the Clique algorithm to calculate the correlation of student grades between pairs of courses in a university based on academic performance. The researcher noted that no study that used the notion of course similarity had ever employed the clustering technique in a predictive manner. Consequently [23] conducted a study on nonlinear feature relationship patterns. They proposed a free relative density-based clustering method and compared it directly to the Clique algorithm. The research used fifteen different data sets, but it did not establish a clear connection between the research and students' academic progress. However, the literature reveals significant deficiencies in each of the reviewed studies, including shortcomings in input parameters, dimensionality reduction, density threshold, data management, performance metrics and specific areas of application, resulting in inaccuracies in cluster analysis. This study adopts a unique strategy to address these issues and enhance the performance of the Clique algorithm in predicting learners' progress in a multidimensional dataset.

C. Existing Prediction Models

A popular clustering technique for predicting leaner behavior is the K-Means algorithm. This was the main choice made by researchers in a study by [29] titled “Identifying student behavior patterns in higher education using K-Means clustering.” This method is mainly used because it is very simple and gives better, easy-to-understand results. The data set used in the study was obtained from a university database. The dataset includes data derived from student files according to their academic, behavioral and demographic characteristics. Various tuning parameters were used to optimize the model. After several analyses, the results revealed an accuracy rate of 93%, a recall rate of 94%, and a precision rate of 93%. According to the study, universities must recognize student behavior patterns and identify students at risk early on. For example, students may have a positive attitude at the beginning of the semester but perform poorly towards the end, or the opposite. However, by optimizing data preprocessing activities and experimenting in various data sets with different characteristics, the researcher found that K-means clustering should be enhanced to improve the results.

In a study on the BIRCH algorithm (Balanced Iterative Reducing and Clustering Using Hierarchies) to analyze the integration of core competencies in sports and health courses at universities based on data mining techniques by [28]. This study conducted research to examine the state of courses in universities using data mining techniques. The study focused on identifying patterns of information on the essential competencies of university health and physical education courses. Various experiments were conducted to determine the ability of the BIRCH algorithm in predictive analysis. The aftermath experiment outlined the result as follows using the metrics of accuracy (91.1%), recall (91.1%) and precision (91%). The algorithm made credible predictions, but with

limitations in the accuracy and reliability of the results, for instance BIRCH can only process metric attributes. A metric attribute is any attribute whose values can be represented in Euclidean space, i.e. there should be no categorical attributes, which the researcher believed could be addressed by improving the algorithm.

In research conducted by [31], Density-based spatial clustering of applications with noise (DBSCAN) was used in academic performance analysis at higher education institutions with educational data mining in a normally detection manner. Academic data in the form of study findings over a specific time period makes up the data set that was used. It was discovered that the DBSCAN algorithm can identify academic data anomalies with accuracy of up to 91.0%, precision of 90%, and recall of 90% after a series of experiments were carried out to identify data anomalies from academic data. In other words, the variation leaves a gap that can be filled by additional study. Consequently, in order to enhance the effectiveness and dependability of the clustering algorithm, DBSCAN is highly sensitive to the epsilon parameter setting; a low value will result in the clusters being classified as noise. The clusters will merge and become denser simultaneously with the shift to a higher value [30]. One potential issue with DBSCAN could be the global constant parameter needed to determine the neighborhood's radius, since it could have an impact on the accuracy of the findings.

D. Research Gaps

In summary, we can quickly identify the gaps in the literature that led to this study. A number of studies conducted to predict learner behavior or analyze using the Clique model or in comparison with other models have drawbacks, including the initialization of probabilities or the creation of ratios for starting experiments, which become apparent and later affects the accuracy of the results. The choice of data set, whether linear or nonlinear, categorical or numerical, is challenging for some algorithms in such a context. The problem with parameter tuning, which sometimes leads to biased results, has been highlighted in a number of studies. Challenges in reducing dimensionality due to multidimensional data that some of the methods examined in this study could not address. The density threshold limitation for density-based clustering methods, the scope and specific focus of application sometimes does not ensure reliable results, lack of appropriate evaluation metrics caused by inconsistency in metric evaluation for the same algorithm in a similar study area is itself a major gap and finally ambiguity in clustering objectives that affect cluster analysis.

However, in order to predict learners' academic progress using multidimensional data, this study adopted a different strategy and thought about how best to solve these problems. For example, feature engineering is used to process data and is considered effective in feature selection and data labeling. Principal component analysis was used to address data dimensionality, reducing the dimensions to a more manageable set of attributes. The rationale for appropriate parameter tuning and metrics for evaluating results have been addressed in detail in this study to ensure consistency. To confirm the validity of the results, data validation was performed and our work was compared with that of other researchers to ensure new contribution. This study used academic performance data from a university, which represents the main factor in learners' progress and makes the results legitimate and relevant, as opposed to other studies that widely examine general behavioral analysis and not progression. For example, to exploit how unique the application area is from other studies, when a learner completes a course of study and, on the other hand, that learner is good at co-curriculum activities such as sports, the institution, on the assumption that sports is not a subject of study, takes into account academic performance when it comes to the transition to the next academic level, even though sport can have an influence on students' academic performance.

III. Methodology

A. Introduction

The data collection, preprocessing, methodology design, methods and tools for the research are outlined in this section.

B. Data Acquisition and Preprocessing

The study examined the subspace clique algorithm in predicting students' academic progress through interesting pattern analysis. This study retrieved data from a university database consisting of students' average grades over the past five years. In total, the data from 3153 students were examined. The dataset contained the following fields: student number marked D for privacy policy, diploma year 1, diploma year 2, average and grade as indicated in Table I below. A diploma course will probably only take two years. After this, the student is either expected to advance to BSc or not.

TABLE I. Sample Working Data

S/No	diplomaY1	diplomaY2	Average	Grade
D1	69.88	53.42	61.65	Credit
D2	53.33	63.40	58.36	Pass
D3	61.36	67.13	64.24	Credit
D4	60.89	59.90	60.39	Credit
D5	52.09	61.88	56.98	Pass
D6	55.93	53.61	54.77	Pass
D7	72.94	69.72	71.33	Distinction
D8	54.87	52.37	53.62	Pass
D9	61.97	68.13	65.05	Credit
D10	62.82	61.97	62.39	Credit

In the dataset, the grading is divided into the categories “Pass”, “Credit”, “Distention” and “Fail”. Students who achieve “Credit” or above are allowed to progress to BSc, while those who achieve “Pass” and “Fail” are not allowed to progress to BSc. Cleaning the data was done by trying to fill in the missing values, identifying and removing the outliers, which in the end solved the problems of inconsistencies that existed in the data before, this was achieved by Python's Jupyter Notebook. This study employed future engineering in grade assignment, ration creation, and binary label creation to predict student behavior patterns.

C. Design Methodology, Methods and Tools

The study used an experimental research design methodology to validate the use of the Clique subspace clustering model to predict learner's academic progress. Subspace clustering uses a new approach to the traditional clustering technique that aims to find clusters in different subspaces within a dataset (a subspace is a space that is

completely contained in another space or whose points or elements are all in one location in another room). It can also be defined as a vector space that is completely contained in another space. In this context, cluster analysis is about discovering groups or clusters of similar objects. The objects are usually represented as a measurement vector or point in a multidimensional space. The similarities between objects are usually determined by an observable distance measure from different dimensions in a data set. Subspace clustering uses all dimensions selected before clustering performance [27]. The study relied on the following expressed Subspace clique mathematical assumptions;

D. General Subspace Notations

1) Considering data matrix X: $X = \left(x_1, x_2, ..., x_n\right) \in R^{dxn}$ where $x_i \in R^d$ represents a data point in d-dimensional space, and n is the number of data points.

2) A subspace $S_i \subseteq R^d$ is spanned by a subset of the dimensions. For example, if S_i is spanned by dimensions $\left[j_1, j_2, ...j_k\right]$, then: $S_i = Span\left[\ell_{j1}, \ell_{j2}, ..., \ell_{jk}\right]$ where ℓ_j is the unit vector along dimension *j*.

3) The projection of a data ¬oint *x* onto a subspace S_i is given by: $Proj_{S_i}\left(x\right) = p_i\left(x\right)$ where p_i is the projection matrix corresponding to S_i.

4) The goal of subspace clustering is to find a partition of the data points and corresponding subspaces that minimize some form of error. A common objective function is:

$$C_1, C_2, ..., C_k^{min}, s_1, s_2, ...s_k \sum_{i=1}^{k} \sum_{x \in C_i} \left\| x - \Pr oj_{S_i}\left(x\right) \right\|^2$$

where:

- C_i represents the set of data points assigned to the *i*-th cluster.
- S_i represents the subspace corresponding to the *i*-th cluster.

E. CLIQUE (Clustering In QUEst) Algorithm

CLIQUE is a density and grid-based approach of subspace clustering model. It reflects a grid-based approach thus represents the data space through grid and examines the density by counting the number of points in a grid cell. By density-based approach a cluster refers to a maximal set of co-joined dense units in a subspace, a unit therefore is dense if the fraction of total data points contained in the unit exceeds the input model parameter.

Subspace cluster describes a set of neighboring dense cells in an arbitrary subspace, it does unveil some minimal descriptions of the clusters. It systematically recognizes subspaces of high dimensional data space that allow better clustering than original space by concept of a priori algorithm. Mathematically the steps in the Clique algorithm are as follows:

Step 1: Data preparation

1) Let X be a dataset with m rows (also called data size/observation) and n columns (also called number of features)

Step 2: Finding 1-dimensional Dense Units

We define D_1 as the set of 1-dimensional dense units thus a 1-dimensional dense unit is a subset of data points within a feature that satisfies a certain density threshold denoted by τ

2) Let F_i denote the $i-th$ column/feature in the dataset X, for $i = 1, 2, ..., n.$

3) Let u_{ij} denote the $j-th$ in the feature F_i

4) Then, the set D_1 is defined as: $D_1 = \left\{u_{ij} \in F_i : \left\|u_{ij}\right\| > m\tau, \forall i, j\right\}$

Step 3: Candidate Generation for Higer Dimensions

5) Let k be the number of higher dimensions (i.e., $k = 2, 3, ..., n$), C_K be the set of k-dimensional dense units. For $k > 1$, we generate candidate dense units C_k by performing a self-join operation on D_{k-1} where the conditions ensure that the units share ($k-2$) dimensions.

Step 4: Finding Higher dimensional Dense Units

From the candidate dense units C_K,we filter out the units D_k such that ($k-1$) projections of a unit are in D_{k-1}.

Step 5: finding clusters

6) For each feature set $f = \left\{F_1, F_2, ..., F_k\right\}$ containing dense units C_K,we build a graph G where dense units are nodes and connection between dense units (having a common face) are edges. We then find connected components in G to identify clusters.

7) Let ρ_c be the density of combination $c \in C_k$, calculated as:

$$\rho_c = \frac{\text{Number of data points containing all features in c}}{\text{Total number of data points in X}}$$

.

8) The i-th dense unit in the feature set *f* is obtained by the formula:

$$U_i = \arg\max_{c \in C_k}(\rho_c)$$

This formula finds the combination *c* from C_k that maximizes the density.

9) To check whether dense units V and W are connected based on sharing at least one feature can be expressed as follows:

$$\begin{cases} 1, \text{ if } V \cap W \neq \phi \\ 0, \text{ otherwise} \end{cases}$$

10) Let V be the set of vertices in the graph G. The number of connected components in G is obtained by the formula:

$$p = \left| \{ \mathrm{DFS}(v) : v \in V \} \right|$$

where DFS(v) denotes the Depth-First Search traversal algorithm starting from vertex v in V.

F. The Choice for Subspace Clique Algorithm

Because of its distinct benefits in addressing the problems identified in previous research concerning the prediction of learner behavior and academic progress, the Clique Subspace method was selected for this study. Clique is particularly good at handling multidimensional, high-dimensional, and heterogeneous data, which is frequently present in educational datasets that contain a variety of learner information types, including academic performance and extracurricular activities, in contrast to traditional clustering techniques. The following explains why Clique is a good fit in this situation:

- Subspace Clustering for Multidimensionality: Clique is an algorithm for subspace clustering that is specifically tailored to detect clusters within high-dimensional spaces by identifying dense areas in subspaces instead of the entire dimensional space. This capability is particularly important in educational data analysis, where datasets frequently encompass various dimensions such as test scores, participation levels, background information, and extracurricular activities. By concentrating on relevant subspaces, Clique facilitates a natural reduction in dimensionality, effectively tackling the challenges associated with dimensionality reduction in a way that surpasses traditional clustering techniques.
- Density-Based Clustering Advantages: Clique employs a density-based technique that allows for the identification of clusters within subspaces by establishing adjustable density thresholds. This capability facilitates the exclusion of noise and irrelevant information. Such an approach effectively mitigates challenges encountered by other density-based clustering techniques, which often face limitations related to thresholds, resulting in inconsistent clusters when used with multidimensional educational data.
- Robustness to Mixed Data Types: Educational datasets generally comprise both categorical and numerical data. Clique effectively handles mixed data types by partitioning the data into grid cells, which facilitates efficient clustering while minimizing reliance on assumptions regarding the data distribution, whether linear or nonlinear. This characteristic renders Clique especially robust and dependable for analyzing various attributes of learner data.
- Minimization of Bias from Parameter Tuning: Clique stands out from certain clustering techniques that necessitate extensive parameter adjustments, which may lead to bias and inconsistency. Its parameters, specifically density thresholds and grid size, are relatively simple and can be determined either empirically or through domain expertise. This approach mitigates the tuning bias often highlighted in earlier research, thereby promoting stability and replicability in the results.
- Efficient for Large Datasets: The study makes use of extensive academic data, and Clique's grid-based clustering approach which provides a highly computational efficiency, making it well-suited for the large datasets commonly found in educational settings. This effectively resolves the scalability challenges faced by certain other clustering techniques, especially when managing substantial, multidimensional educational datasets.

The purpose of the study was to analyze complex and multidimensional educational data in order to make predictions about learner behavior and academic progression. The traditional clustering techniques have several challenges when applied in this scenario. For example, the K-Means approach requires a predetermined number of clusters, assumes spherical cluster forms, and is sensitive to outliers. On the other hand, BIRCH is only capable of supporting numerical data, it is however, not ideal for the mixed categorical and numerical data that is typically present in educational datasets. In spite of the fact that DBSCAN can recognize clusters of any shape, it is extremely sensitive to the epsilon parameter, which has an effect on the consistency of the clusters.

Importantly, the study considered the following procedures to ensure that the full capability of the experimental design methodology was maximized and the desired outcome was achieved:

a) Data partitioning: The dataset was divided into two separate folds, fold1 and fold2, where fold1 was used for the training dataset and fold2 was used for validation. The training dataset was used to build the Clique model, while the validation dataset was used to perform hyperparameter tuning to optimize the model. The two partitions can be seen in Table II below;

TABLE II. DATA PARTITIONS

Partition	Number of records
Fold 1	1884
Fold 2	1269

b) Benchmark model: The study conducted two different attempts to train the model. The first experiment was used as the main model training, in which the output results of the second experiment were compared.

c) Performance comparison: Precision, accuracy, and recall were used as performance metrics to compare how effective the enhanced Clique model predicted learners' academic progress with the main model.

d) Sensitivity analysis: The study examined the performance of the developed model across a range of datasets and conditions by exploiting variations for the initial state probabilities.

IV. Clique Model for Predicting Learners Academic Progress

A. Introduction

This section explains the basic steps to develop the model, as well as the required parameters and model architecture.

B. Background

Learning is a broad concept that varies depending on the area of application. The common learning environment familiar to many is school, from primary school to secondary school to colleges and universities. In the case of university, students participate in their studies in different categories, from the lowest level (certificate, diploma, bachelor's degree, master) to the highest level (doctoral degree). All of these categories require learners to progress gradually to the highest level after completing the requirements of a particular category. Several factors can determine learners' progress from one category to another, including academic skills, co-curricular activities, government scholarships and many others. The common determinant of a student moving from one category to another is the student's academic performance, usually determined through examination and grading in accordance with the academic policy of the university system. In this study, student performance based on academic grade was considered the primary determinant of progress.

The study examined various grades from students, which are divided into the following categories: A pass is considered to be a performance that is greater than or equal to 50 percent but less than 60 percent; a credit is considered to be an achievement that is greater than or equal to 60 percent but less than 70 percent. A performance of less than 50 percent is considered a failure; an award is given for achievements of 70 percent or more. Each category was assigned an observation that indicates the desired learning progression behavior. Table III below illustrates the state symbols for grade observation.

TABLE III. Grade Observation States

Grade	Observation state	Progress State to BSc
Distinction	Yes	Progress
Credit	Yes	Progress
Pass	No	No Progress
Fail	No	No Progress

For any student who scores a distinction grade automatically qualifies to progress to the BSc Degree, again when a student scores a credit grade the student meets the threshold to proceed to BSc Degrees, on the other hand when a student scores a Pass that student does not qualify to proceed to BSc Degree, consequently when a student gets a Fail that student does not Progress to the Category of learning that is BSc Degree. The mapping can be represented in Fig. 1 below.

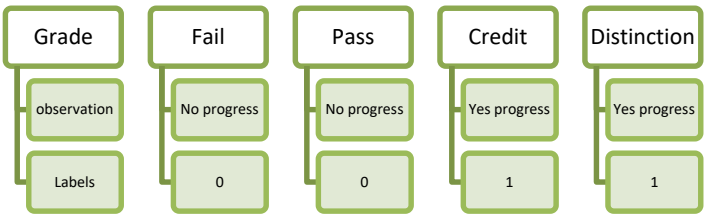


Fig. 1. Observation state mappings.

In this study, the correct assignment of different data categories was carried out, as shown in Fig. 1 above. Grades are assigned to the observed states and indicated by the labels, where “no” means (0) and “yes” means (1). For example, “Fail” means a learner has not made progress and “Credit” means progress. The states “No” and “Yes” are the hidden patterns that need to be discovered through prediction.

C. Predicting Learners Academic Progress

We used a Python script to implement the learner's academic progress in the study. This script is a comprehensive data processing and machine learning pipeline that includes data preparation, feature engineering, dimensionality reduction, clustering, evaluation, and visualization. Below is a detailed step-by-step explanation of how this script works:

- Data preparation is the first step in this process. The very first activity in this phase is to create a dictionary called Data that contains four categories of grades: Credit, Distinction, Fail, and Pass. and the corresponding number of students who answered “no” and “yes” to a particular condition. This data is then converted into a Pandas Data Frame “df” for easier editing and analysis.
- The second step included the task of Feature engineering, feature engineering involves selecting, modifying, and transforming raw data into features suitable for application in machine learning algorithms. Feature engineering was performed in three main stages;

a) Categorical to numerical conversion: The script maps the categorical grades (`Fail`, `Pass`, `Credit`, `Distinction`) to numerical values using a dictionary (`grade mapping`). This is crucial because machine learning models typically work with numerical data.

b) Creating a new feature (`Ratio`): The ratio of "Yes" responses to the total number of students (sum of "No" and "Yes") is calculated. This feature might represent the likelihood or propensity of students to answer "Yes."

c) Label creation: A new binary label, `Label`, is created where 1 indicates that more students answered "Yes" than "No," and 0 indicates the opposite. This served as the ground truth for model evaluation.

- In the third step, the script performed feature selection, where the script selects relevant features (“Grade”, “No”, “Yes”, “Ratio”) from the Data Frame to form the feature matrix “X”. The labels (0 or 1) are stored in the variable “y”.

- In step four we performed data standardization, which involved standardizing the features in "X" using the "Standard Scaler." This ensures that each feature contributes equally to the model and avoids bias due to scale differences.
- In the fifth step, the experiment involved dimensionality reduction using principal component analysis (PCA). This technique reduces the dimensionality of Scaled from 4 to 2 dimensions, which makes the data easier to visualize and also reduces noise. The transformed data is stored in "X_pca".
- In the sixth step, the experiment performed clustering using the clique subspace for cluster analysis and cluster prediction. The script applied clique subspace clustering with 2 clusters ("n_clusters=2") to the PCA-transformed data ("X_pca"). The algorithm attempts to divide the data into two groups based on the input features. To predict clusters, the Clique subspace algorithm assigns each data point to one of the two clusters, and these assignments are stored in y_pred.
- In step seven, cluster label assignment and model evaluation were implemented as follows; since clustering of clique subspaces is unsupervised, the clusters may not correspond directly to the original labels ("y"). The script checks the accuracy of the initial clustering. If it is less than 50%, the cluster labels ("y_pred = 1 – y_pred") are inverted to match the actual labels. During model evaluation, the script calculated key performance metrics including: accuracy (the percentage of correct predictions), precision (the proportion of actual correct positive identifications), and recall (the proportion of actual positive identifications that were correctly identified).
- In the last step the experiment performed results display and visualization. The script adds the predicted cluster labels (`y_pred`) to the Data Frame `df` under the column `Predicted Progression'. It then prints the Data Frame to show the original data along with the predicted progression. Through Visualization a scatter plot of the PCA-reduced data (`X_pca`) is generated, where data points are colored according to their cluster assignments. Horizontal and vertical gridlines are added to the plot to enhance readability. The plot includes labeled axes, a title, and a color bar that indicates cluster labels. This process can be seen in Fig. 2 of the architectural diagram presentation.

Finally, the research examined key points to strengthen its contribution to the existing scientific knowledge base. Key aspects included hyperparameter optimization using density thresholds and input parameters, as well as experimental validation of results through training. Feature engineering was used to create accurate grade assignments, ratios and labels. By standardizing performance metrics, bias reduction and data scalability were achieved. Principal component analysis was used to eliminate noise and prevent overlapping clusters in multidimensional data, allowing clear presentation of study results. However, research highlights a notable strength of the Clique model in predicting learners' academic progress, making it an attractive choice for scholarly contributions. These are presented below:

- This behavioral analysis investigation provided excellent prediction and significantly improved the model analysis by applying the subspace clustering technique and fine-tuning hyperparameters until optimal results were achieved.
- Unlike numerous previous studies, this research adopted a unique strategy by predicting learners' academic progress based on their academic performance, which generally reflects their progress at different stages of academic learning. The scope is more focused and relevant.
- There are various characteristics associated with a situation, such as a student achieving one credit often triggers the transition to a BSc, driven by an invisible urge for advancement. In contrast, a student who receives a passing grade under the policy cannot advance, but there is a compelling reason in this policy that educational institutions should recognize. This unspoken pattern becomes clear through precise mapping in this study.
- A number of multidimensional data sets were used as part of managing multidimensional data for this study. These datasets were manipulated and analyzed using feature engineering techniques and principal component analysis, demonstrating their effectiveness and applicability in cluster analysis. This contributes positively to the existing scientific knowledge.

D. Feature Engineering

This study used feature engineering to ensure appropriate data management, which contributes to the accuracy and reliability of the results. The dataset initially contained multiple columns, which were transformed and used to create new features. Here's a step-by-step breakdown of the feature engineering process:

Step 1. Categorical Conversion (Mapping Grades to Numerical Values):

- Objective: To convert categorical grade information into numerical form, which is necessary for further numerical analysis.
- Implementation: A mapping dictionary (grade_mapping) was created where each grade (e.g., 'Fail', 'Pass', 'Credit', 'Distinction') was assigned a corresponding numerical value (0, 1, 2, 3). The 'Grade' column in the DataFrame was then mapped to these numerical values. Grade_mapping = {'Fail': 0, 'Pass': 1, 'Credit': 2, 'Distinction': 3}.

Step 2. Creation of a New Feature: Ratio of 'Yes' to Total Students:

- Objective: To introduce a new feature that captures the ratio of 'Yes' responses (e.g., passing students) to the total number of students for each grade category.

- Implementation: The ratio was computed by dividing the 'Yes' count by the total number of students ('No' + 'Yes'). This new ratio feature was added as a column ('Ratio') in the DataFrame. df['Ratio'] = df['Yes'] / (df['No'] + df['Yes']).

Step 3. Creation of a Label Column:

- Objective: To generate a binary label indicating whether the number of 'Yes' responses exceeds the number of 'No' responses for each grade category.
- Implementation: A binary label was created using np. where, assigning a value of 1 if 'Yes' responses were greater than 'No' responses, and 0 otherwise. This label was stored in the 'Label' column of the DataFrame. df['Label'] = np. where(df['Yes'] > df['No'], 1, 0).

Step 4. Feature Selection:

- Objective: To select specific columns as features for further analysis.
- Implementation: The script selected the columns 'Grade', 'No', 'Yes', and 'Ratio' as features (X), and the 'Label' column as the target (y). X = df [['Grade', 'No', 'Yes', 'Ratio']] y = df['Label'].

Step 5. Standardization of Features:

- Objective: To standardize the features, ensuring they have a mean of 0 and a standard deviation of 1. This step is crucial for algorithms that are sensitive to the scale of input data, such as PCA and Clique subspace algorithm.
- Implementation: The features in X were standardized using StandardScaler from sklearn. The standardized data was stored in X_scaled. scaler = StandardScaler () X_scaled = scaler.fit_transform(X).

Step 6. Dimensionality Reduction Using PCA (Principal Component Analysis):

- Objective: To reduce the dimensionality of the data, potentially improving the performance of clustering algorithms and enabling visualization in a 2D space.
- Implementation: PCA was applied to the standardized data, reducing it to 2 principal components. The transformed data was stored in X_pca. pca = PCA(n_components=2) X_pca = pca.fit_transform(X_scaled).

Step 7. Clustering Using Clique subspace algorithm:

- Objective: To group the data into clusters based on the transformed features, aiming to identify patterns in the data.
- Implementation: The Clique subspace algorithm was applied to the PCA-transformed data with 2 clusters. The predicted cluster labels were stored in y_pred. Clique subspace algorithm = Clique subspace algorithm (n_clusters=2, random state=42) Clique subspace algorithm. Fit(X_pca) y_pred = Clique subspace algorithm.

Step 8. Manual Label Adjustment:

- Objective: To ensure that the cluster labels align with the actual labels, particularly when the initial clustering might have assigned the labels inversely.
- Implementation: The accuracy of the initial clustering was checked. If the accuracy was below 0.5, the labels were swapped (1 for 0, and 0 for 1). if accuracy score (y, y_pred) < 0.5: y_pred = 1 - y_pred.

Step 9. Evaluation of Clustering Performance:

- Objective: To assess the accuracy of the clustering model.
- Implementation: The accuracy of the clustering compared to the true labels was calculated and printed. accuracy = accuracy score(y, y_pred) print(f"optimized Accuracy: {accuracy * 100:.2f}%").

In summary this systematic feature engineering process effectively transformed the original dataset, enabling the use of advanced clustering techniques to analyze and predict patterns in the data.

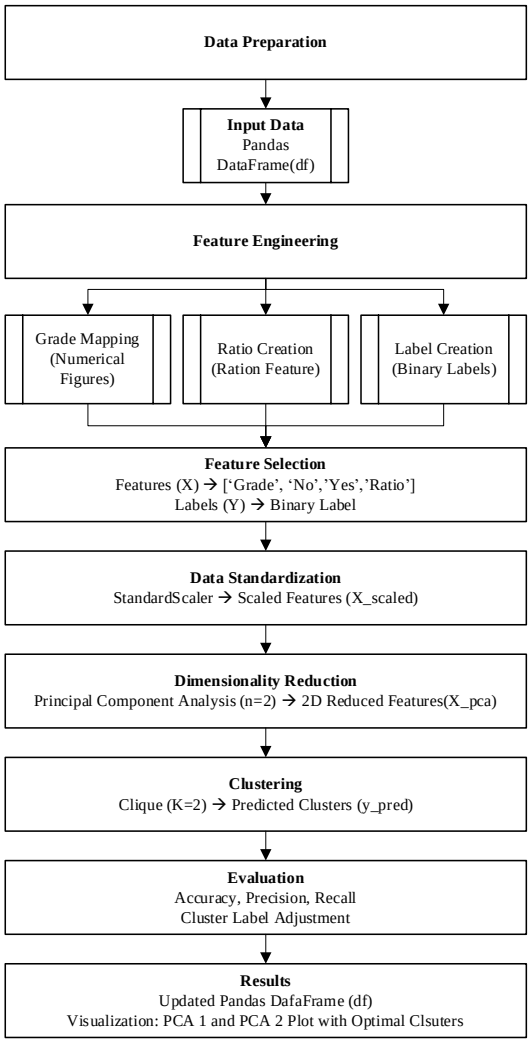


Fig. 2. Clique model for predicting learners' academic progress architectural diagram.

E. Dimensionality Reduction using PCA (Principal Component Analysis)

The experiment involving the use of principal component analysis in this study was conducted in three main phases, namely: feature reduction, clustering using clique, and cluster prediction adjustment.

In the first phase before plotting, the script uses PCA to reduce the dimensionality of the data from four features ("Grade", "No", "Yes" and "Ratio") to two main components. PCA is a linear technique that transforms the data into a new coordinate system in which the axes (principal components) correspond to the directions of maximum variance in the data. By reducing the data to two dimensions, we can visualize it in a 2D graph while retaining as much of the original variability as possible. The PCA(n_components=2) call creates a PCA object that is configured to reduce the data to two dimensions. The "fit transform(X_scaled)" method then applies this transformation to the standardized features ("X_scaled"), resulting in a two-dimensional array ("X_pca"). This array represents the data points in the new coordinate system defined by the first two principal components.

In the second phase, the Clique script applies subspace clustering to the two-dimensional PCA-transformed data. Clique Subspace is an unsupervised machine learning algorithm that divides the data into a certain number of clusters (in this case 2 clusters). The Clique Subspace (n_clusters=2, random state=42)" call initializes the Clique Subspace algorithm to form 2 clusters. The "fit(X_pca)" method is used to fit the model to the PCA transformed data ("X_pca"). The clustering process involves randomly initializing cluster centers (centroids) and iteratively adjusting them by minimizing variance within the cluster until convergence is achieved. After fitting, the model assigns each data point to one of the two clusters and the resulting cluster labels ("y_pred") are saved.

In the third phase of cluster prediction adjustment: Since Clique Subspace randomly assigns cluster labels, the script includes a step to align these predicted labels ("y_pred") with the actual labels ("y"). If the initial precision is below 50%, the script reverses the predicted labels ("y_pred = 1 – y_pred") to optimize the performance metrics (accuracy, precision, and recall). The accuracy of the initial clustering is calculated using the "Accuracy Score (y, y_pred)". If the accuracy is less than 50%, it indicates that the clusters are mislabeled. The script then reassigns the labels by flipping them to ensure that Cluster 1 is more likely to represent the positive class ("Yes" progression). The final step is to visualize the clustering results in a 2D scatterplot. This plot helps understand the distribution and separation of clusters in the transformed feature space. Fig. 3 and Fig. 4 below provide a visual representation of the diagrams.

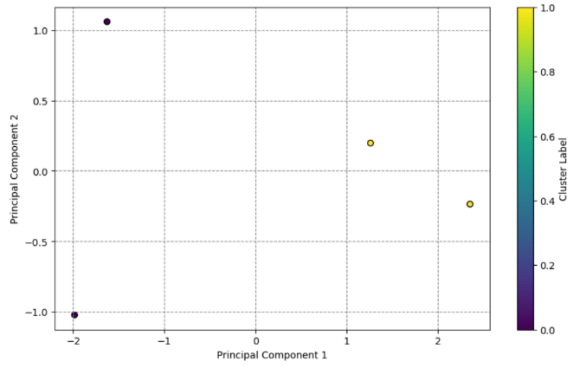


Fig. 3. Training data PCA.

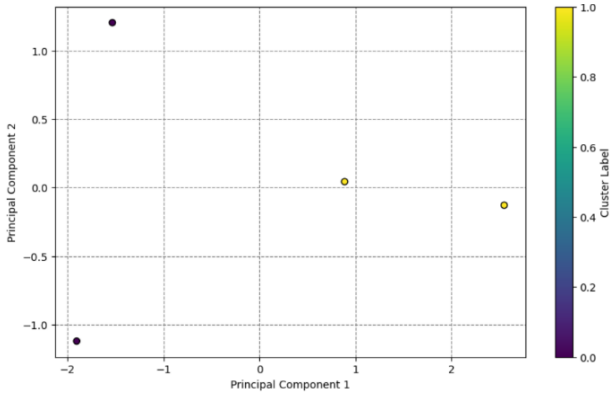


Fig. 4. Validation data PCA.

In summary, the graphs illustrate how well the Clique Subspace algorithm combined with Principal component analysis divides the data into two clusters. The spacing and distribution of points in the graph can provide insights into the natural grouping of data and the effectiveness of the clustering algorithm. Well-separated clusters with minimal overlap indicate that the algorithm has successfully identified different groups within the data. Aligning the principal component analysis axes with the inherent variability of the data ensures that clustering is based on the most informative aspects of the data even after dimensionality is reduced. This detailed process shows how machine learning techniques such as PCA and Clique Subspace are used together to group high-dimensional data and how the results can be scientifically visualized and interpreted.

V. Results

A. Introduction

This part describes the training and validation of the results using the ordinary clique model and the optimized clique model. It provides a comparative analysis of the results at different levels and subsequent discussions and conclusions.

B. Model Training and Validation

The model was trained and validated using the first and second folds of the dataset, respectively. You can see the results in Tables IV and V below.

TABLE IV. MODEL TRAINING RESULTS

Results without Modification						
S/No	Grade	No	YES	Ratio	Labels	Predicted Progression
0	2	156	127	0.449	0	1
1	3	16	269	0.943	1	1
2	0	261	0	0	0	0
3	1	1055	0	0	0	0
Performance Evaluation Metrics						
Precision	75%					
Accuracy	75%					
Recall	75%					
Results with Modification						
S/No	Grade	NO	YES	Ratio	Labels	Predicted progression
0	2	80	203	0.717	1	1
1	3	16	269	0.944	1	1
2	0	261	0	0	0	0
3	1	1055	0	0	0	0
Performance Evaluation Metrics						
Precision	98.50%					
Accuracy	98.90%					
Recall	98.50%					

TABLE V. MODEL VALIDATION RESULTS

S/No	Grade	NO	YES	Ratio	Labels	Predicted Progression
0	2	118	165	0.583	1	1
1	3	9	276	0.968	1	1
2	0	97	0	0	0	0
3	1	604	0	0	0	0
Performance Evaluation Metrics						
Precision	98.50%					
Accuracy	98.90%					
Recall	98.50%					

Training was performed using data fold 1 in Table II of the data partition, which considered the student's academic performance with random initial state probabilities. Training was performed by subjecting the data to two training trials with different hyperparameter tunings and then recording the results. In the first training attempt there was no modification, i.e. no parameter optimization because the implementation used the common and existing Clique algorithm and presented the results. Using the ordinary clique, the model showed an average performance of 75% for precision, 75% for accuracy, and 75% recall.

To confirm the consistency of our working model, we adjusted the dataset and performed some hyperparameter tuning as we observed new prediction patterns. The results showed better patterns with some common predictions from the previous model. We evaluated the performance of the model using the same clustering metrics such as precision, accuracy, and recall. The results with the model modifications showed exemplary performance with a precision value of 98.50%, an accuracy value of 98.90% and a recall value of 98.50%. This performance was consistent with the performance of the validation model. The model built in this study demonstrated efficiency and effectiveness when run on different datasets under different circumstances. During both training and validation, the model showed an accuracy rate of 98.90%. The applicability of the model developed on the entire dataset is consistent with the performance, which is well summarized.

C. Comparison with Related Work

In this study we examined various studies recently undertaken that used the same model and compared the results against our developed Model. The results are presented in Table VI as shown below:

TABLE VI. COMPARISON WITH OTHER STUDIES

Author	Algorithm	Accuracy	Precision	Recall
Oyugi et al. (2024)	Clique Model	98.90%	98.50%	98.50%
[25]	Clique Model	86.5%	85.99%	85.9%
[23]	Clique Model	93.9%	93.5%	94.3%
[15]	Clique Model	93%	93%	93%
[16]	Clique Model	98.6%	98.2%	97.5%
[18]	Clique Model	75%	75%	75%
[17]	Clique Model	92.0%	91.83%	90.12%

From Table VI above, our study is related to other studies, which can be seen from the result of this study. For example, the Clique algorithm was observed to display an overall cluster analysis with above-average performance of at least 75% for all metrics used in the evaluation, namely precision, recall and accuracy. It has also been observed that the accuracy, precision and recall displayed when using clique models are above 90% in most cases with the exception of a few instances reported by [18] in which the findings for all assessed metrics revealed 75%, and similar to [25]. which reported accuracy as 86.5%, precision as 85.99%, and 85.9% recall, this was slightly lower than the performance of clique models generated in other studies. According to our study, our model achieved 98.90% accuracy, 98.50% precision, and 98.50% recall. This was far higher than the value of all other related studies we examined in this study. However, after a careful comparison between our model and the other studies, it is entirely reasonable to conclude

that our model showed excellent performance in predictive cluster analysis. However, this can be attributed to the proper scope, use of future engineering that ensured sufficient and accurate future selection, proper management of the data, proper dimensionality reduction, and scientific cross-validation of the dataset that ultimately resulted in accurate prediction of learner progression.

TABLE VII. COMPARISON WITH OTHER MODELS

Author	Algorithm	Accuracy	Precision	Recall
Oyugi et al.	Clique Model	98.90%	98.50%	98.50%
[29]	K-Means	93%	94%	93%
[28]	BIRCH	91.1%	91.1%	91%
[31]	DBSCAN	91%	90%	90%

As shown in Table VII above, the accuracy rate for K-Means was 93%, for BIRCH was 91.1%, for DBSCAN was 91%, and for the Clique model was 98.90%. According to the other metrics, Clique scored the highest with a precision recall of 98.50 percent, while DBSACN scored the lowest with 90 percent. Clique recorded a maximum recall rate of 98.50 percent, while DBSCAN recorded a minimum recall rate of 90 percent. The above results show that our model performs better than the other models. Based on this study, it is advisable to consider using Clique.

In this study, the subspace Clique model has been analyzed and contrasted with other behavior analysis frameworks and similar methodologies employed in learner prediction research. Furthermore, to assess the challenges identified and the objectives achieved in this investigation, we engage in a thorough analysis and discussion of the pertinent literature. This research aims to enhance decision-making and learner management in educational contexts by predicting learner' academic progress based on their assessment scores. When evaluated against alternative models such as BIRCH, K-Means, and DBSCAN, the Clique subspace model demonstrated commendable performance. However, it is essential to address several issues that emerged from the studies conducted.

In the study of [28] Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH) algorithm for behavior analysis prediction, the researcher observed that BIRCH was particularly effective for clustering large datasets. Nonetheless, it exhibited several limitations, especially in its ability to manage complex data distributions, overlapping clusters and sensitivity to the input parameters. In contrast, the CLIQUE algorithm demonstrated a superior capacity for handling large datasets and accommodating various data distributions, whether categorical or non-categorical, linear or non-linear which formed the features of our academic data. This adaptability positioned the CLIQUE model as a more efficient option for clustering in scenarios involving complex, multidimensional datasets within the scope of this study.

DBSCAN (Density-Based Spatial Clustering of Applications with Noise) is a widely utilized clustering algorithm recognized for its effectiveness in identifying clusters of arbitrary shapes and managing noisy datasets. However, it presents certain limitations, especially when applied to multidimensional data and scenarios involving varying densities [31]. Subspace Clique addresses these shortcomings by concentrating on dense subspaces, effectively managing different density levels, automatically determining critical dimensions, and offering enhanced scalability for predictive clustering.

K-means is an effective and straightforward algorithm designed for low-dimensional, approximately spherical clusters; however, it encounters difficulties when dealing with complex cluster shapes, Multidimensional datasets, and the presence of outliers [29]. The Subspace Clique model offers a solution to these challenges by considering dense subspace clustering techniques. This approach allows for the identification of arbitrary cluster shapes, the management of high-dimensional data, the adaptive determination of cluster structures, and resilience against outliers. Consequently, the subspace CLIQUE model emerges as a more appropriate option for predictive clustering in the context of academic progression as demonstrated in this study results.

Other researchers [16], [15], and [23] who employed the subspace clique method for behavior analysis reported performance levels of 98.6%, 93%, and 93.9% accuracy, respectively. These figures are marginally lower than the accuracy achieved by our model, which stands at 98.90%. Additionally, studies conducted by [25], [18], and [17] yielded accuracies of 86.5%, 75%, and 92%, all of which are again inferior to the performance of the clique model at 98.90%. The discrepancies in accuracy may be attributed to various challenges, including adaptive grid sizing, parameter optimization, and insufficient principal component analysis, all of which could enhance the accuracy of subspace CLIQUE algorithms. In contrast, our model effectively addressed these challenges through the computational efficiency of feature engineering, dimensionality reduction, and cross-validation.

D. Significance of the Research

This study used the subspace clique model to predict learners' academic progress patterns in multidimensional data. The results showed that the model was successfully able to predict learners' progress through clustering and establish hidden patterns that can help in decision making about learners. Student progress is crucial, particularly if they have started at a low level, such as a certificate or diploma in mainstream higher education, and was therefore crucial to this study. Although various studies have looked at the areas of learning in clustering, our study took a different approach and was limited to students' academic progress, which plays a key role in learners' progress as it can reflect the reality of progress in an academic environment Advice on teaching tasks as well as career guidance for the future can be used. It is right that we keep learners under control so that they do not lose track of their progress, as many students drop out of university due to poor performance, which results in them being unable to progress to the next level of learning. The behavioral patterns uncovered in

this study confirm the model's ability to perform predictive and accurate cluster analysis on an educational dataset.

VI. Conclusions and Future Work

The study aimed to predict learners' academic progress using subspace clustering in multidimensional data. However, the study was limited to a grid-based subspace clustering method using the clique model. To achieve this goal, we improve the Clique algorithm through optimization and parameter tuning. These improvements were achieved through future engineering, principal component analysis, data standardization, and cross-validation. The introduction of subspace served to reduce, if not eliminate, noise while performing clustering, which is called the "curse of dimensionality," where the number of dimensions increases as data size increases, resulting in overlapping clusters. Principal component analysis and future engineering helped find a solution to the overlapping clusters. By integrating density-based, grid-based, and subspace clustering, CLIQUE detects clusters embedded in subspaces of high-dimensional data without requiring users to select the subspaces of interest. The algorithm provided an effective and efficient method for pruning the space of dense units to counteract the inherent exponential nature of the problem. However, there was a trade-off for pruning dense units in the sparse coverage subspaces. Although the algorithm was faster, there is an increased chance of missing clusters. Furthermore, while CLIQUE does not require users to select subspaces of interest, its susceptibility to noise and ability to identify relevant attributes depend heavily on the user's choice of unit intervals and sensitivity threshold. The intent of the research was to search the data to reveal learners' progress from one stage to the next, the results clearly demonstrated that it is possible to determine learners' progress in clustering using the subspace clique technique. In summary, subspace clustering is complex but efficient and effective in performing clustering assessment of multidimensional data regardless of its size, and can be used to perform analysis for critical decisions, especially determining learner progression. Subspace clustering can also be used in dimensionality reduction to simplify the complex nature of grid-based bottom-up clustering evaluation methods. Future research can explore different methods and potentially consider a spectral clustering learning approach that leverages clique prediction capabilities to learn more about behavior analysis. Future engineering is recognized as a significant contribution to this study, yet it is sometimes perceived as biased due to its absence of a standardized execution method, consequently, further research is imperative. Given that this study focused on human behavior analysis in educational learning environments, I suggest that future studies be conducted in various settings.

References

[1] Albaity, M., Mahmood, T., & Ali, Z. (2023). Analysis and applications of artificial intelligence in digital education based on complex fuzzy clustering algorithms. *Mathematics*, *11*(14), 3184.

[2] [2] He, H., Sun, B., Yang, Y., & Chen, J. (2022). A K-means optimization algorithm suitable for fast clustering of WebGIS massive data. In *Journal of Physics: Conference Series* (Vol. 2171, No. 1, p. 012069). IOP Publishing.

[3] Mazarbhuiya, F. A. A., & Shenify, M. (2023). Finding IoT Anomaly using Rough Fuzzy Periodic Subspace Clustering Approach.

[4] Jia, H., & Cheung, Y. M. (2017). Subspace clustering of categorical and numerical data with an unknown number of clusters. *IEEE transactions on neural networks and learning systems*, *29*(8), 3308-3325.

[5] Wenz, V., Kesper, A., & Taentzer, G. (2023). Clustering heterogeneous data values for data quality analysis. *ACM Journal of Data and Information Quality*, *15*(3), 1-33.

[6] Hennig, C. (2015). What are the true clusters? *Pattern Recognition Letters*, *64*, 53-62.

[7] Grün, B. (2019). Model-based clustering. In *Handbook of mixture analysis* (pp. 157-192). Chapman and Hall/CRC.

[8] Ma, F., Wang, C., Huang, J., Zhong, Q., & Zhang, T. (2024). Key grids-based batch-incremental CLIQUE clustering algorithm considering cluster structure changes. *Information Sciences*, *660*, 120109.

[9] Shetty, N., & Shirwaikar, R. (2013). A comparative study: BIRCH and clique. *Int. J. Eng. Res. Technol*, *2*, 2019-2023.

[10] Cao, M., Hu, Y., & Yue, L. (2023). Research on variable weight CLIQUE clustering algorithm based on partial order set 1. *Journal of Intelligent & Fuzzy Systems*, *44*(6), 9461-9473.

[11] Fatehi, K., Rezvani, M., & Fateh, M. (2020). ASCRClu: an adaptive subspace combination and reduction algorithm for clustering of high-dimensional data. *Pattern Analysis and Applications*, *23*, 1651-1663.

[12] Kwale, F. M. (2014). An Overview of VSM-Based Text Clustering Approaches. *International Journal of Advanced Research in Computer Science*, *5*(1), 69-73.

[13] Nayagam, S. C. (2015). Comparative study of subspace clustering algorithms. *Int. J. Comput. Sci. Inform. Technol*, *6*(5), 4459-4464.

[14] Zhu, J., & Liu, X. (2024). An integrated intrusion detection framework based on subspace clustering and ensemble learning. *Computers and Electrical Engineering*, *115*, 109113.

[15] Madran, U., & Soyoglu, D. (2023). Compatibility of Clique Clustering Algorithm with Dimensionality Reduction. *Appl. Math*, *17*(5), 839-849.

[16] He, H., He, Y., Wang, F., & Zhu, W. (2022). Improved Clique algorithm for clustering non-spherical data. *Expert Systems*, *39*(9), e13062.

[17] Li, X., Zhang, Y., Cheng, H., Zhou, F., & Yin, B. (2021). An unsupervised ensemble clustering approach for the analysis of student behavioral patterns. *Ieee Access*, *9*, 7076-7091.

[18] Leeds, D. D., Zhang, T., & Weiss, G. M. (2021). Mining course groupings using academic performance. In *International Conference on Educational Data Mining*.

[19] Chi, D. (2021, January). Research on the application of k-means clustering algorithm in student achievement. In *2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE)* (pp. 435-438). IEEE.

[20] Chaudhry, M., Shafi, I., Mahnoor, M., Vargas, D. L. R., Thompson, E. B., & Ashraf, I. (2023). A systematic literature review on identifying patterns using unsupervised clustering algorithms: A data mining perspective. *Symmetry*, *15*(9), 1679.

[21] Hu, X., & Ye, N. (2023). The Design of College Students' Mental Health Analysis System Based on Human-Computer Interaction. *Innovation in Science and Technology*, *2*(6), 34-42.

[22] Budler, L. C., Gosak, L., & Stiglic, G. (2023). Review of artificial intelligence-based question-answering systems in healthcare. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *13*(2), e1487.

[23] Jain, N., Ghosh, S., & Ghosh, A. (2024). A parameter free relative density based biclustering method for identifying non-linear feature relations. *Heliyon*.

[24] Starczewski, A., Scherer, M. M., Książek, W., Dębski, M., & Wang, L. (2021). A novel grid-based clustering algorithm. *Journal of Artificial Intelligence and Soft Computing Research*, *11*(4), 319-330.

[25] Ge, Z., & Xia, Q. (2024). Research on action analysis and guidance in aerobics blended learning based on data mining. *Applied Mathematics and Nonlinear Sciences*, *9*(1).

[26] Guo, Y., Dietrich, F., Bertalan, T., Doncevic, D. T., Dahmen, M., Kevrekidis, I. G., & Li, Q. (2021). Personalized Algorithm Generation: A Case Study in Meta-Learning ODE Integrators. *arXiv preprint arXiv:2105.01303*.

[27] Peng, X., Feng, J., Zhou, J. T., Lei, Y., & Yan, S. (2020). Deep subspace clustering. *IEEE transactions on neural networks and learning systems*, *31*(12), 5509-5521.

[28] Liu, H. (2024). Pedagogical Integration of Core Literacy in College Physical Education and Health Courses Based on Data Mining Techniques. *Applied Mathematics and Nonlinear Sciences*, *9*(1).

[29] Mohd Talib, N. I., Abd Majid, N. A., & Sahran, S. (2023). Identification of student behavioral patterns in higher education using k-means clustering and support vector machine. *Applied Sciences*, *13*(5), 3267.

[30] Mohamed Nafuri, A. F., Sani, N. S., Zainudin, N. F. A., Rahman, A. H. A., & Aliff, M. (2022). Clustering analysis for classifying student academic performance in higher education. *Applied Sciences*, *12*(19), 9467.

[31] Chrisnanto, Y. H., & Abdullah, G. (2021). The uses of educational data mining in academic performance analysis at higher education institutions (case study at UNJANI). *Matrix: Jurnal Manajemen Teknologi dan Informatika*, *11*(1), 26-35.

Enhanced TODIM-TOPSIS Framework for Interior Design Quality Evaluation in Public Spaces Under Hesitant Fuzzy Sets

Lu Peng*
Hunan Urban Construction College, Xiangtan, 411100, Hunan, China

***Abstract*—The evaluation of interior landscape design in public spaces involves several aspects, including aesthetics, functionality, sustainability, and user experience. Aesthetic evaluation focuses on the visual appeal and stylistic consistency of the design. Functionality considers the practicality and convenience of the space layout. Sustainability evaluates the environmental friendliness of materials and energy efficiency of the design. Additionally, user experience assessment gathers feedback to gauge comfort and satisfaction. These evaluation criteria help designers optimize spaces to be both attractive and practical while meeting user needs. The interior design quality evaluation in public spaces is multiple-attribute decision-making (MADM) problem. Recently, the TODIM and TOPSIS methods have been applied to address MADM challenges. Hesitant fuzzy sets (HFSs) are used to represent uncertain information in the evaluation of interior landscape design in public spaces. In this study, we developed a hesitant fuzzy TODIM-TOPSIS (HF-TODIM-TOPSIS) approach to tackle Multiple Attribute Decision Making (MADM) issues within the context of HFSs. A numerical case study focused on the interior design quality evaluation in public spaces demonstrates the validity of this approach. The primary contributions of this paper include: (1) Extending the TODIM and TOPSIS approaches to incorporate HFSs; (2) Utilizing information entropy to determine weight values under HFSs; (3) Establishing the HF-TODIM-TOPSIS method for managing MADM in the presence of HFSs; (4) Conducting algorithmic analysis and comparative studies based on a numerical example to assess the practicality and effectiveness of the HF-TODIM-TOPSIS approach.**

Keywords*—Multiple-attribute decision-making (MADM); hesitant fuzzy sets (HFSs); TODIM; TOPSIS; design quality evaluation

I. Introduction

The evaluation of interior landscape design in public spaces involves several key aspects, including aesthetics, functionality, sustainability, and user experience. Aesthetic evaluation focuses on the visual appeal and consistency of style, ensuring overall harmony and beauty. Functionality examines the practicality of layout and convenience of facilities to meet diverse user needs. Sustainability emphasizes the environmental friendliness and energy efficiency of materials, highlighting long-term ecological and economic benefits. Additionally, user experience evaluation gathers feedback to assess comfort and satisfaction. These comprehensive evaluations not only help optimize design but also provide valuable references for future projects, enhancing the overall quality and utility of public spaces. The evaluation of interior landscape design in public spaces has become increasingly important over the past decade as urbanization continues to shape our environments. This literature review synthesizes findings from some significant studies, including some Chinese and some English publications. Li, et al. [1] conducted a pivotal study highlighting the relationship between environmental design and human behavior in public spaces. They advocated for a user-centered approach, emphasizing that aesthetic considerations must align with functional needs to enhance user satisfaction. This work laid the groundwork for understanding how design influences user interactions with public spaces. Kaplan [2] examined the psychological impacts of landscape design, asserting that incorporating natural elements is crucial for fostering emotional well-being in urban environments. This study reinforced the idea that landscapes should do more than just please the eye; they should also promote mental health. Zhao and Chen [3] focused on the aesthetic evaluation of public parks in China. Their research identified key design elements that contribute to user satisfaction, such as visual coherence and cultural relevance. This study was significant in emphasizing the cultural context in landscape design and its effect on user perceptions. Gomez, et al. [4] explored the role of social interaction in public spaces. They proposed that landscape design should facilitate community engagement, suggesting a framework for evaluating designs based on social connectivity and highlighted the social dimension of public spaces, suggesting that design can foster community ties. In the same year, Sun, et al. [5] investigated the effectiveness of biophilic design, concluding that integrating natural elements significantly enhances user satisfaction and well-being in public interiors. Their findings supported the notion that environments rich in nature positively impact users' experiences. Miller [6] further contributed to the discourse by examining sustainable design practices in public spaces. He advocated for eco-friendly materials and practices, providing an evaluation framework for assessing the environmental impact of landscape designs. His work was instrumental in integrating sustainability into the conversation around public space design. In 2017, Zhang and Li [7] discussed the influence of cultural elements on public space design in China. They emphasized the importance of incorporating local heritage into landscape design to enhance community identity, showcasing how cultural context can inform design practices. Haq and Lynch [8] conducted a comparative study on evaluation methods for public space design across different cultures. Their findings underscored the variability in user preferences and highlighted

* Corresponding Author

the need for culturally sensitive evaluation frameworks in landscape design. In 2020, Chen, et al. [9] focused on the integration of technology in evaluating public spaces. Their study introduced a digital evaluation tool aimed at enhancing user feedback, marking a shift toward more interactive and user-driven design evaluations. Fang and Zhao [10] explored the psychological effects of urban green spaces on public health. They proposed a robust evaluation framework that prioritized mental and physical well-being, further emphasizing the health-related aspects of landscape design. The following year, Martin, et al. [11] investigated community participation in the design and evaluation of public spaces. Their findings indicated that involving users in the design process leads to better outcomes and ensures that designs meet community needs. Wang and Liu [12] analyzed climate-responsive design strategies in public spaces, advocating for adaptive landscapes that respond to environmental changes. Their work highlighted the importance of resilience in landscape design, particularly in the face of climate change. In 2023, Zhou, et al. [13] proposed a comprehensive framework that combines qualitative and quantitative methods to assess user experiences in public spaces. Their emphasis on inclusivity and accessibility reflects a growing recognition of diverse user needs in landscape design. Smith and Johnson [14] examined the role of sensory experiences in public space design. They proposed that effective evaluations should consider auditory, visual, and tactile elements, thereby broadening the scope of design evaluations. Lastly, Lu, et al. [15] focused on the integration of smart technologies in public space design evaluation. Their research suggested that smart solutions can enhance user engagement and feedback processes, indicating a future direction for landscape design. The past decade has witnessed significant advancements in the evaluation of interior landscape design in public spaces. Emerging trends emphasize user experience, sustainability, cultural relevance, and the integration of technology. The studies reviewed highlight the necessity of adopting a multidimensional approach to effectively evaluate and enhance public spaces, ultimately contributing to better urban environments.

Multi-attribute decision-making (MADM) is.2000000000000000000000000000000000000111111111111110 a method used to evaluate and select options when multiple conflicting criteria are involved [16-20]. It's widely applied in fields like engineering, economics, and management [21-25]. The decision-making process typically includes defining objectives and evaluation criteria, assigning weights to each criterion, assessing the performance of each option against these criteria, and ultimately selecting the optimal solution based on a comprehensive score [26-29]. Due to the cognitive limitations of decision-makers and the complexities of the decision-making environment [30-34], the process of MADM is often characterized by significant uncertainties, which preclude the accurate representation of evaluation objects using precise numerical values [35-39]. In response, Zadeh [40] proposed the use of fuzzy numbers to address decision-making challenges. However, in specific contexts, a single numerical value fails to adequately capture the nuances of the evaluation object. Consequently, Torra [41] introduced hesitant fuzzy numbers as a means to enhance the understanding of uncertainty within the decision-making process, thereby yielding more precise outcomes [42-48]. This advancement represents a significant breakthrough in MADM research. Interior design quality evaluation in public spaces exemplifies classical MADM. Recently, the TODIM approach [49-52] and the TOPSIS method [53-57] have been applied to address MADM issues. Hesitant fuzzy sets (HFSs) [41] serve as a tool for characterizing uncertain information in this context. To date, few approaches have integrated information entropy [58] with the TODIM-TOPSIS framework under HFSs [41]. Therefore, an integrated hesitant fuzzy TODIM-TOPSIS (HF-TODIM-TOPSIS) approach has been developed to manage Multi-Attribute Group Decision Making (MAGDM). This study presents a numerical example of interior design quality evaluation in public spaces and conducts a comparative analysis to validate the HF-TODIM-TOPSIS approach. The primary research objectives and motivations outlined in this paper are: (1) the extension of the TODIM and TOPSIS methods to HFSs; (2) the application of information entropy to manage weight values within HFSs; (3) the establishment of HF-TODIM-TOPSIS framework for managing MADM under HFSs; and (4) an algorithmic analysis of interior design quality evaluation in public spaces, supported by numerical example to demonstrate the feasibility and effectiveness of HF-TODIM-TOPSIS approach.

The structure of this paper is outlined as follows. Section II discusses the management of HFSs. Section III presents the HF-TODIM-TOPSIS approach applied to HFSs using the entropy method. Section IV provides an illustrative example of evaluating interior landscape design in public spaces, along with a comparative analysis. Concluding remarks are presented in Section V.

II. PRELIMINARIES

The HFSs is constructed.

Definition 1 [41]. The HFSs is demonstrated:

$$V=\left\{\left\langle \theta,u_V\left(\theta\right)\right\rangle \middle| \theta\in\Theta\right\} \tag{1}$$

where $\mu_V\left(\theta\right)\subset\left[0,1\right]$ is possible membership of element $\theta\in\Theta$, $\forall\,\theta\in\Theta$. Then, $v\theta=\left(vu\right)$ is demonstrated as HFN.

Definition 2 [59]. Let $v\theta_1=\left(vu_1\right)$ and $v\theta_2=\left(vu_2\right)$ be two HFNs, the operation is demonstrated:

$$v\theta_1\oplus v\theta_2=\bigcup_{v\gamma_1\in z\theta_1,v\gamma_2\in v\theta_2}\left\{v\gamma_1+v\gamma_2-v\gamma_1v\gamma_2\right\} \tag{2}$$

$$v\theta_1\otimes v\theta_2=\bigcup_{v\gamma_1\in v\theta_1,v\gamma_2\in v\theta_2}\left\{v\gamma_1\cdot v\gamma_2\right\} \tag{3}$$

$$\lambda v\theta_1=\bigcup_{v\gamma_1\in v\theta_1}\left\{1-\left(1-v\gamma_1\right)^{\lambda}\right\},\lambda>0 \tag{4}$$

$$\lambda v\theta_1 = \bigcup_{v\gamma_1 \in v\theta_1} \left\{ \left(v\gamma_1 \right)^{\lambda} \right\}, \lambda > 0 \tag{5}$$

From Definition 2, the operation laws are built [59].

$$(1) v\theta_1 \oplus v\theta_2 = v\theta_2 \oplus v\theta_1, v\theta_1 \otimes v\theta_2 = v\theta_2 \otimes v\theta_1, \left(\left(v\theta_1 \right)^{\lambda_1} \right)^{\lambda_2} = \left(v\theta_1 \right)^{\lambda_1 \lambda_2};$$

$$(2)\ \lambda \left(v\theta_1 \oplus v\theta_2 \right) = \lambda v\theta_1 \oplus \lambda v\theta_2, \left(v\theta_1 \otimes v\theta_2 \right)^{\lambda} = \left(v\theta_1 \right)^{\lambda} \otimes \left(v\theta_2 \right)^{\lambda};$$

$$(3)\ \lambda_1 v\theta_1 \oplus \lambda_2 v\theta_1 = \left(\lambda_1 + \lambda_2 \right) v\theta_1, \left(v\theta_1 \right)^{\lambda_1} \otimes \left(v\theta_1 \right)^{\lambda_2} = \left(v\theta_1 \right)^{\left(\lambda_1 + \lambda_2 \right)}.$$

Definition 3 [59]. Let $v\theta_1 = \left(vu_1 \right)$ and $v\theta_2 = \left(vu_2 \right)$ be HFNs, the score functions of $v\theta_1$ and $v\theta_2$ is demonstrated:

$$SF\left(v\theta_1 \right) = \frac{1}{\# v\theta_1} \sum_{v\gamma_1 \in v\theta_1} v\gamma_1 \tag{6}$$

$$SF\left(v\theta_2 \right) = \frac{1}{\# v\theta_2} \sum_{v\gamma_2 \in v\theta_2} v\gamma_2 \tag{7}$$

where $\# v\theta_1$ and $\# v\theta_2$ are numbers of the elements in $v\theta_1 = \left(vu_1 \right)$ and $v\theta_2 = \left(vu_2 \right)$.

For $v\theta_1 = \left(vu_1 \right)$ and $v\theta_2 = \left(vu_2 \right)$, then

$(1)\ if\ SF\left(v\theta_1 \right) < SF\left(v\theta_2 \right),\ v\theta_1 < v\theta_2;$

$(2)\ if\ SF\left(v\theta_1 \right) = SF\left(v\theta_2 \right), AF\left(v\theta_1 \right) = AF\left(v\theta_2 \right),\ v\theta_1 = v\theta_2.$

Definition 4 [60]. Let $v\theta_1 = \left(vu_1 \right)$ and $v\theta_2 = \left(vu_2 \right)$ be HFNs, the HFN Hamming distance (HFNHD) and HFN Euclidean distance(HFNED) are demonstrated:

$$HFED\left(v\theta_1, v\theta_2 \right) = \frac{1}{\# v\theta} \sum_{k=1}^{\# v\theta} \left| v\gamma_1 \left(\sigma(k) \right) - v\gamma_2 \left(\sigma(k) \right) \right| \tag{8}$$

$$HFED\left(v\theta_1, v\theta_2 \right) = \sqrt{\frac{1}{\# v\theta} \sum_{k=1}^{\# v\theta} \left| v\gamma_1 \left(\sigma(k) \right) - v\gamma_2 \left(\sigma(k) \right) \right|^2} \tag{9}$$

where $v\gamma_1 \left(\sigma(k) \right)$ and $v\gamma_2 \left(\sigma(k) \right)$ are kth largest values in $v\theta_1 = \left(vu_1 \right)$ and $v\theta_2 = \left(vu_2 \right)$ and $\# v\theta = \# v\theta_1 = \# v\theta_2$.

The HFWA and HFWG approach is demonstrated [59].

III. HF-TODIM-TOPSIS Approach for MADM with Entropy

A. HF-MAGDM Issues

The HF-TODIM-TOPSIS approach (Fig. 1) is demonstrated for MADM. Let $VA = \left\{ VA_1, VA_2, \cdots, VA_m \right\}$ be alternatives, and the attributes set $VG = \left\{ VG_1, VG_2, \cdots, VG_n \right\}$ with weight values WV, where $wv_j \in [0,1]$, $\sum_{j=1}^{n} wv_j = 1$. Then, HF-TODIM-TOPSIS approach is demonstrated for MAGDM.

Step 1. Implement the HFN-matrix $VR = \left[v\phi_{ij} \right]_{m \times n} = \left(vu_{ij} \right)_{m \times n}$:

$$VR = \left[v\phi_{ij} \right]_{m \times n} = \begin{array}{c} \\ VA_1 \\ VA_2 \\ \vdots \\ VA_m \end{array} \begin{array}{c} \begin{array}{cccc} VG_1 & VG_2 & \cdots & VG_n \end{array} \\ \begin{bmatrix} v\phi_{11} & v\phi_{12} & \cdots & v\phi_{1n} \\ v\phi_{21} & v\phi_{22} & \cdots & v\phi_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v\phi_{m1} & v\phi_{m2} & \cdots & v\phi_{mn} \end{bmatrix} \end{array} \tag{8}$$

Step 2. Normalize the $VR = \left[v\phi_{ij} \right]_{m \times n}$ into $VN = \left[n\phi_{ij} \right]_{m \times n} = \left(nvu_{ij} \right)_{m \times n}$.

For benefit attributes:

$$n\phi_{ij} = \left(nvu_{ij} \right) = \left(vu_{ij} \right) \tag{10}$$

For cost attributes:

$$n\phi_{ij} = \left(nvu_{ij} \right) = \left(1 - vu_{ij} \right) \tag{11}$$

B. Implement the Attributes Weight through Entropy

Step 3. Implement the attributes weight through entropy.

The information entropy is employed under different environment[61-65]. Entropy [58] is used to derive weight values. The $HFNM_{ij}$ is demonstrated:

$$HFNM_{ij} = \frac{SF\left(nvu_{ij}\right)+1}{\sum_{i=1}^{m}\left(SF\left(nvu_{ij}\right)+1\right)}, \quad (12)$$

The HFN Shannon entropy $HFNSE = \left(HFNSE_1, HFNSE_2, \cdots, HFNSE_n\right)$ is demonstrated:

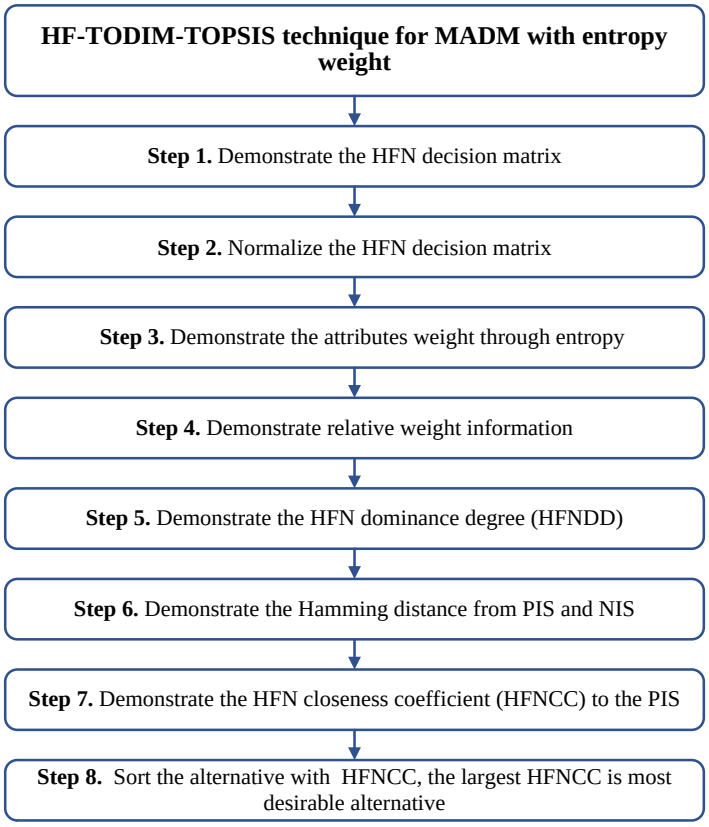


Fig. 1. HF-TODIM-TOPSIS approach for MADM with entropy weight.

$$HFNSE_j = -\frac{1}{\ln m}\sum_{i=1}^{m} HFNM_{ij} \ln HFNM_{ij} \quad (13)$$

and $HFNM_{ij} \ln HFNM_{ij} = 0$ if $HFNM_{ij} = 0$.

The weights $wv = \left(wv_1, wv_2, \cdots, wv_n\right)$ is demonstrated:

$$wv_j = \frac{1 - HFNSE_j}{\sum_{j=1}^{n}\left(1 - HFNSE_j\right)}, \quad j = 1, 2, \cdots, n. \quad (14)$$

C. HF-TODIM-TOPSIS Approach for MADM

The HF-TODIM-TOPSIS approach is demonstrated for MADM.

Step 4. Implement relative weight of VG_j as:

$$rwv_j = wv_j \Big/ \max_j wv_j, \quad (15)$$

Step 5. Illustrate the HFN dominance degree (HFNDD).

(1) The dominance degree $HFNDD_j\left(VA_i, VA_t\right)$ of VA_i over VA_t for VG_j is demonstrated:

$$HFNDD_j\left(VA_i,VA_t\right)=\begin{cases}\dfrac{rwv_j\times\left(\dfrac{HFNHD\left(n\phi_{ij},n\phi_{tj}\right)+HFEND\left(n\phi_{ij},n\phi_{tj}\right)}{2}\right)^{\alpha}}{\sum_{j=1}^{n}rwv_j} & \text{if } SF\left(n\phi_{ij}\right)>SF\left(n\phi_{tj}\right)\\ 0 & \text{if } SF\left(n\phi_{ij}\right)=SF\left(n\phi_{tj}\right)\\ -\dfrac{1}{\theta}\dfrac{\sum_{j=1}^{n}rwv_j\times\left(\dfrac{HFNHD\left(n\phi_{ij},n\phi_{tj}\right)+HFEND\left(n\phi_{ij},n\phi_{tj}\right)}{2}\right)^{\beta}}{rwv_j} & \text{if } SF\left(n\phi_{ij}\right)<SF\left(n\phi_{tj}\right)\end{cases} \tag{16}$$

The values of α,β is determined from study [66].

(2) The $HFNDD_j\left(VA_i\right)\left(j=1,2,\cdots,n\right)$ with respect to VG_j is defined:

$$HFNDD_j\left(VA_i\right)=\left[HFNDD_j\left(VA_i,VA_t\right)\right]_{m\times m}$$

$$=\begin{array}{c}\\VA_1\\VA_2\\\vdots\\VA_m\end{array}\begin{array}{c}\begin{array}{cccc}VA_1 & VA_2 & \cdots & VA_m\end{array}\\\begin{bmatrix}0 & HFNDD_j\left(VA_1,VA_2\right) & \cdots & HFNDD_j\left(VA_1,VA_m\right)\\ HFNDD_j\left(VA_2,VA_1\right) & 0 & \cdots & HFNDD_j\left(VA_2,VA_m\right)\\ \vdots & \vdots & \cdots & \vdots\\ HFNDD_j\left(VA_m,VA_1\right) & HFNDD_j\left(VA_m,VA_2\right) & \cdots & 0\end{bmatrix}\end{array}$$

(3) Implement the overall HFNDD of alternative VA_i over other alternatives for VG_j:

$$HFNDD_j\left(VA_i\right)=\sum_{t=1}^{m}HFNDD_j\left(VA_i,VA_t\right) \tag{12}$$

The overall HFNDD matrix is defined:

$$HFNDD=\left(HFNDD_{ij}\right)_{m\times n}$$

$$=\begin{bmatrix} & VG_1 & VG_2 & \cdots & VG_n\\ VA_1 & \sum_{t=1}^{m}HFNDD_1\left(VA_1,VA_t\right) & \sum_{t=1}^{m}HFNDD_2\left(VA_1,VA_t\right) & \cdots & \sum_{t=1}^{m}HFNDD_n\left(VA_1,VA_t\right)\\ VA_2 & \sum_{t=1}^{m}HFNDD_1\left(VA_1,VA_t\right) & \sum_{t=1}^{m}HFNDD_2\left(VA_1,VA_t\right) & \cdots & \sum_{t=1}^{m}HFNDD_n\left(VA_1,VA_t\right)\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ VA_m & \sum_{t=1}^{m}HFNDD_1\left(VA_m,VA_t\right) & \sum_{t=1}^{m}HFNDD_2\left(VA_m,VA_t\right) & \cdots & \sum_{t=1}^{m}HFNDD_n\left(VA_m,VA_t\right)\end{bmatrix}$$

(4) Implement the positive ideal solution (PIS) and negative ideal solution (NIS):

$$PIS=\left(PIS_1,PIS_1,\cdots,PIS_n\right) \tag{27}$$

$$NIS=\left(NIS_1,NIS_1,\cdots,NIS_n\right) \tag{28}$$

$$PIS_j=\max_{j=1}^{n}HFNDD_{ij},NIS_j=\min_{j=1}^{n}HFNDD_{ij} \tag{29}$$

Step 6. Implement the Euclidean distance from PIS and NIS.

$$ED\left(VA_i,PIS\right)=\sum_{j=1}^{n}\left|HFNDD_{ij}-PIS_j\right| \tag{30}$$

$$ED\left(VA_i,NIS\right)=\sum_{j=1}^{n}\left|HFNDD_{ij}-NIS_j\right| \tag{31}$$

Step 7. Implement the HFN closeness coefficient (HFNCC) from PIS.

$$HFNCC(VA_i, PIS) = \frac{ED(VA_i, NIS)}{ED(VA_i, PIS) + ED(VA_i, PIS)} \quad (32)$$

Step 8. Sort the alternative in line with the HFNCC, the largest HFNCC is the most desirable alternative.

IV. Numerical Example and Comparative Analysis

A. Numerical Example for Interior Design Quality Evaluation in Public Spaces

Evaluating interior landscape design in public spaces is a multifaceted process aimed at enhancing overall quality and user experience. The primary goal is to ensure the design is both aesthetically pleasing and functional while meeting sustainability requirements. Firstly, aesthetic evaluation is crucial. The visual appeal of a design directly affects users' first impressions and long-term feelings. Color coordination, material selection, and spatial layout need to be harmonious to create a pleasant environment. The design should not only align with current aesthetic trends but also possess innovation to inspire interest and curiosity. Secondly, functionality focuses on practicality and convenience. Public spaces must meet various needs, such as socializing, resting, and activities. Therefore, design should consider traffic flow, seating arrangements, and accessibility of facilities. A well-functioning design improves space efficiency, allowing users to engage in activities with ease. Sustainability is an essential element in modern design. Evaluating the environmental friendliness of materials and energy-saving features can reduce negative environmental impacts. Choosing renewable materials and energy-efficient equipment not only lowers long-term operational costs but also enhances ecological value. Designers need to consider lifecycle costs to balance economic and environmental benefits. User experience evaluation is another key aspect. By collecting and analyzing user feedback, designers can gain insights into their true feelings and needs within the space. This user-centered approach helps in making targeted improvements, increasing satisfaction and comfort. Whether through surveys, interviews, or observing behavior, this data provides crucial support for design adjustments. Finally, comprehensive evaluation results offer valuable references for future projects. By summarizing successful experiences and identifying shortcomings, designers can continuously optimize strategies and improve overall project quality. This process of ongoing improvement not only drives design innovation but also enhances the utility of public spaces.

In summary, evaluating interior landscape design in public spaces is a complex yet essential task that involves technical considerations as well as artistic and humanistic care. Through scientific evaluation methods, it is possible to create more attractive, functional, and sustainable public spaces that meet both social and environmental needs. The interior design quality evaluation in public spaces is a MADM issue. Therefore, the interior design quality evaluation in public spaces is presented to demonstrate the approach developed in this essay. Five potential interior landscape design schemes $VA_i\ (i = 1, 2, 3, 4, 5)$ are assessed with four attributes (see Table I):

TABLE I. Four Attributes for Interior Design Quality Evaluation in Public Spaces

Attribute	Description
Aesthetic Value-VG_1	Focuses on the visual appeal of the design, ensuring consistency in color, materials, and style to create a harmonious overall effect.
Functionality-VG_2	Evaluates whether the spatial layout is reasonable and supports various activity needs, as well as the convenience and accessibility of facilities.
Sustainability-VG_3	Examines the environmental characteristics of materials, use of renewable resources, and assesses the energy efficiency and long-term cost benefits.
User Experience-VG_4	Collects and analyzes user feedback to evaluate comfort, satisfaction, and whether the design meets user needs and expectations.

All attributes are beneficial. The five possible interior landscape design schemes $VA_i\ (i = 1, 2, 3, 4, 5)$ are evaluated with HFNs. The HF-TODIM-TOPSIS approach is employed to solve the interior design quality evaluation in public spaces.

Step 1. Illustrate the HFN matrix $VR = \left[v\phi_{ij} \right]_{5\times4}$ (see Table II).

TABLE II. THE $VR = \left[v\phi_{ij} \right]_{5\times4}$

	VG1	VG2
VA_1	{0.1342, 0.5621, 0.8173}	{0.2451, 0.6894, 0.9238}
VA_2	{0.2275, 0.6953, 0.0182}	{0.3184, 0.7439, 0.1347}
VA_3	{0.3526, 0.7195, 0.2834}	{0.4731, 0.8274, 0.3142}
VA_4	{0.4173, 0.8021, 0.3652}	{0.5294, 0.8903, 0.4781}
VA_5	{0.5789, 0.9134, 0.4508}	{0.6891, 0.0257, 0.5723}
	VG3	VG4
VA1	{0.3785, 0.7512, 0.8426}	{0.4923, 0.8034, 0.0159}
VA2	{0.4658, 0.8125, 0.2964}	{0.5709, 0.9142, 0.3471}
VA3	{0.5839, 0.9056, 0.4203}	{0.6912, 0.0328, 0.5784}
VA4	{0.6417, 0.0135, 0.5236}	{0.7542, 0.1267, 0.6895}
VA5	{0.7904, 0.1382, 0.6458}	{0.8916, 0.2493, 0.7341}

Step 2. Normalize the $VR = \left[v\phi_{ij} \right]_{5\times4}$ into $VN = \left[n\phi_{ij} \right]_{5\times4}$ (see able III).

TABLE III. THE $VN = \left[n\phi_{ij} \right]_{5\times4}$

	VG1	VG2
VA_1	{0.1342, 0.5621, 0.8173}	{0.2451, 0.6894, 0.9238}
VA_2	{0.0182, 0.2275, 0.6953}	{0.1347, 0.3184, 0.7439}
VA_3	{0.2834, 0.3526, 0.7195}	{0.3142, 0.4731, 0.8274}
VA_4	{0.3652, 0.4173, 0.8021}	{0.4781, 0.5294, 0.8903}
VA_5	{0.4508, 0.5789, 0.9134}	{0.0257, 0.5723, 0.6891}
	VG3	VG4
VA_1	{0.3785, 0.7512, 0.8426}	{0.0159, 0.4923, 0.8034}
VA_2	{0.2964, 0.4658, 0.8125}	{0.3471, 0.5709, 0.9142}
VA_3	{0.4203, 0.5839, 0.9056}	{0.0328, 0.5784, 0.6912}
VA_4	{0.0135, 0.5236, 0.6417}	{0.1267, 0.6895, 0.7542}
VA_5	{0.1382, 0.6458, 0.7904}	{0.2493, 0.7341, 0.8916}

Step 3. Implement the weight: $wv_1 = 0.2764, wv_2 = 0.1937$ $wv_3 = 0.3429, wv_4 = 0.1870$.

Step 4. Implement the relative weight: $rwv = \{0.8059, 5651, 1.0000, 0.5456\}$

Step 5. Implement the $HFNDD = \left(HFNDD_{ij} \right)_{5\times4}$ (see Table IV):

TABLE IV. THE $HFNDD = \left(HFNDD_{ij} \right)_{5\times4}$

	VG_1	VG_2	VG_3	VG_4
VA_1	0.7143	-0.7965	0.3553	-0.3080
VA_2	-0.2413	0.8392	-1.2242	0.4401
VA_3	-0.3098	0.0711	-0.0800	0.8909
VA_4	0.7102	-0.2481	0.3035	0.3751
VA_5	-0.6798	-0.9131	-0.7609	-0.5322

Step 6. Implement the PIS and NIS (see Table V).

TABLE V. THE PIS AND NIS

	VG_1	VG_2	VG_3	VG_4
PIS	0.7143	0.8392	0.3553	0.8909
NIS	-0.6798	-0.9131	-1.2242	-0.5322

Step 7. Implement the $\left|HFNDD_{ij} - PIS_j\right|$ and $\left|HFNDD_{ij} - NIS_j\right|$ (see Table VI to Table VII).

TABLE VI. THE $\left|HFNDD_{ij} - PIS_j\right|$

	VG_1	VG_2	VG_3	VG_4
VA_1	0.0000	1.6357	0.0000	1.1989
VA_2	0.9556	0.0000	1.5795	0.4508
VA_3	1.0241	0.7681	0.4353	0.0000
VA_4	0.0041	1.0873	0.0518	0.5158
VA_5	1.3941	1.7523	1.1162	1.4231

TABLE VII. THE $\left|HFNDD_{ij} - NIS_j\right|$

	VG_1	VG_2	VG_3	VG_4
VA_1	1.3941	0.1166	1.5795	0.2242
VA_2	0.4385	1.7523	0.0000	0.9723
VA_3	0.3700	0.9842	1.1442	1.4231
VA_4	1.3900	0.6650	1.5277	0.9073
VA_5	0.0000	0.0000	0.4633	0.0000

Step 8. Implement the $HD(VA_i, PIS)$, $HD(VA_i, NIS)$ and $CC(VA_i, PIS)$ (see Table VIII to Table IX).

TABLE VIII. THE $HD(VA_i, PIS)$, $HD(VA_i, NIS)$

	$HD(VA_i, PIS)$	$HD(VA_i, NIS)$
VA_1	2.8346	3.3144
VA_2	2.9859	3.1631
VA_3	2.2275	3.9215
VA_4	1.6590	4.4900
VA_5	5.6857	0.4633

TABLE IX. THE $HFNCC(VA_i, PIS)$ AND ORDER

	$HFNCC(VA_i, PIS)$	Order
VA_1	0.5390	3
VA_2	0.5144	4
VA_3	0.6377	2
VA_4	0.7302	1
VA_5	0.0753	5

Thus, the best interior landscape design scheme is VA_1.

B. Comparative Analysis

Then, the HF-TODIM-TOPSIS approach is compared with HFWA approach[59], HFWG approach [59], HF-MABAC approach [67], HF-CODAS approach [68], HF-EDAS approach [69] and HF-TODIM approach [70]. The comparative results are demonstrated in Table X and Fig. 2.

TABLE X. ORDER FOR DIFFERENT APPROACHES

	Order
HFWA approach [59]	$VA_4 > VA_3 > VA_1 > VA_2 > VA_5$
HFWG approach [59]	$VA_4 > VA_3 > VA_2 > VA_1 > VA_5$
HF-MABAC approach [67]	$VA_4 > VA_3 > VA_1 > VA_2 > VA_5$
HF-CODAS approach [68]	$VA_4 > VA_3 > VA_1 > VA_2 > VA_5$
HF-EDAS approach [69]	$VA_4 > VA_3 > VA_1 > VA_2 > VA_5$
HF-TODIM approach [70]	$VA_4 > VA_3 > VA_1 > VA_2 > VA_5$
HF-TODIM-TOPSIS approach	$VA_4 > VA_3 > VA_1 > VA_2 > VA_5$

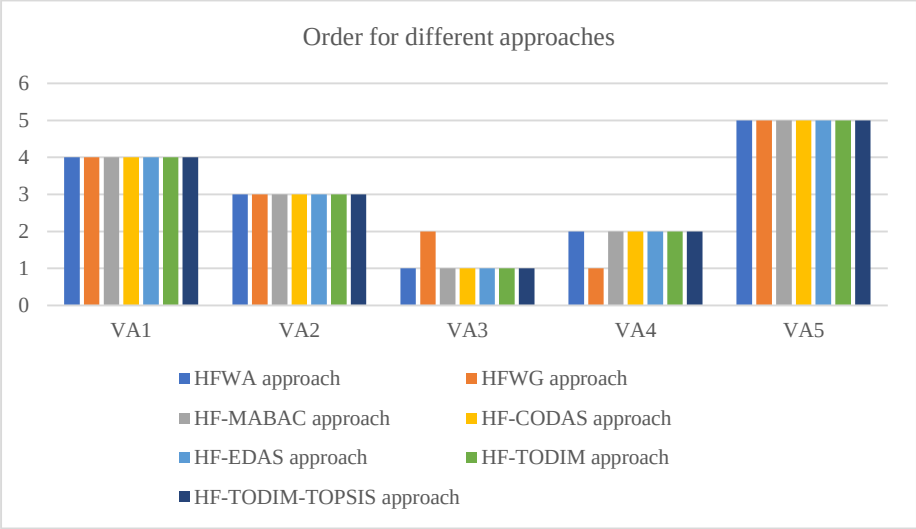


Fig. 2. Order for different approaches.

Through the above analysis, the HF-TODIM-TOPSIS method demonstrates its effectiveness and reliability for multi-attribute decision-making (MADM). The primary advantages of this approach are as follows: (1) the HF-TODIM-TOPSIS method adeptly addresses the uncertainties inherent in real-world MADM scenarios and captures the psychological behaviors of decision-makers during the evaluation of interior landscape design in public spaces; (2) it also explores the dynamics of the TODIM and TOPSIS techniques when integrated into a hybrid model specifically designed for assessing interior landscape design in public spaces. However, a significant limitation of the HF-TODIM-TOPSIS approach is its failure to address issues related to group consensus.

V. Conclusion

The evaluation of interior landscape design in public spaces is highly significant. Firstly, it ensures the beauty and functionality of the space, enhancing the overall user experience. By assessing the visual appeal and practicality of the design, it creates environments that are both pleasant and efficient. Secondly, the evaluation process promotes sustainability by emphasizing the use of eco-friendly materials and energy-efficient designs, reducing environmental impact. Additionally, it focuses on user needs and feedback, ensuring the design meets expectations and improves satisfaction and comfort. This comprehensive evaluation not only provides direction for designers to improve but also offers valuable references for future projects, helping to enhance design quality and innovation, ultimately creating better public spaces for everyone. The interior design quality evaluation in public spaces is MADM. Recently, the TODIM and TOPSIS methods have been employed to address challenges in MADM. HFSs are utilized to represent uncertain information in the evaluation of interior landscape design within public spaces. This study introduces the hesitant fuzzy TODIM-TOPSIS (HF-TODIM-TOPSIS) approach to resolve MADM issues in the context of HFSs. A numerical case study focused on the evaluation of interior landscape design in public spaces demonstrates the validity of this method.

The main conclusions and findings of this study can be summarized as follows:(1) Effectiveness of the HF-TODIM-TOPSIS method: The research demonstrated the effectiveness of the HF-TODIM-TOPSIS method in addressing multi-attribute decision-making problems, such as indoor landscape design in public spaces, through numerical case analysis. This method effectively handles uncertainty in the evaluation process and provides more comprehensive and objective evaluation results. (2) Application value of HFSs: The study indicates that the introduction of HFSs can better capture the hesitation and subjectivity of decision-makers during the evaluation process, making the evaluation results more aligned with actual conditions. (3) Weight determination using information entropy: The study utilized information entropy to determine the weights of different evaluation indicators. Compared to traditional subjective weighting methods, this approach is more objective and reduces interference from human factors. (4) Extension of TODIM and TOPSIS methods: The research extends the traditional TODIM and TOPSIS methods to the HFSs framework, providing new ideas and methods for solving more complex multi-attribute decision-making problems.

In summary, this study proposes a new and more effective multi-attribute decision-making method, HF-TODIM-TOPSIS, and validates its practical value in the evaluation of indoor landscape design in public spaces through case analysis.

References

[1] X. Li, Y. Zhang, and J. Wang, "A study on the relationship between environmental design and human behavior in public spaces," Journal of Landscape Research, vol. 5, no. 2, pp. 56-65, 2013.

[2] R. Kaplan, "The role of nature in the urban environment: Implications for landscape design," Urban Forestry & Urban Greening, vol. 13, no. 2, pp. 224-229, 2014.

[3] L. Zhao and Y. Chen, "Aesthetic evaluation of public parks: A case study in china," Landscape Architecture Journal, vol. 23, no. 1, pp. 14-26, 2015.

[4] J. Gomez, M. Smith, and T. Diaz, "Evaluating public spaces: The role of social interaction in landscape design," Journal of Urban Design, vol. 21, no. 4, pp. 1-15, 2016.

[5] H. Sun, J. Liu, and Q. Wang, "The effect of biophilic design on user experience in public spaces," Chinese Journal of Landscape Architecture, vol. 32, no. 2, pp. 45-51, 2016.

[6] D. Miller, "Sustainable practices in public space design: An evaluation framework," Sustainable Cities and Society, vol. 29, pp. 22-30, 2017.

[7] Y. Zhang and X. Li, "Cultural identity in public space design: A chinese perspective," Landscape Research, vol. 42, no. 2, pp. 135-147, 2017.

[8] S. Haq and A. Lynch, "Cross-cultural evaluation of public space design: A comparative study," International Journal of Urban Planning, vol. 34, no. 3, pp. 267-279, 2019.

[9] Y. Chen, L. Wang, and X. Liu, "Digital tools for evaluating public space design: Enhancing user feedback," Journal of Digital Landscape Architecture, vol. 5, no. 1, pp. 15-25, 2020.

[10] Y. Fang and L. Zhao, "The impact of urban green spaces on public health: Evaluation framework and design recommendations," Health & Place, vol. 68, p. 102490, 2021.

[11] F. Martin, J. Nelson, and R. Smith, "Community participation in public space design: A pathway to better evaluation," Urban Studies, vol. 59, no. 4, pp. 789-804, 2022.

[12] Q. Wang and J. Liu, "Climate-responsive design in public spaces: Evaluation and implications," Journal of Environmental Management, vol. 305, pp. 114-123, 2022.

[13] Y. Zhou, X. Chen, and L. Liu, "A comprehensive framework for evaluating user experience in public spaces: Emphasizing inclusivity," Journal of Urban Design, vol. 28, no. 1, pp. 85-102, 2023.

[14] J. Smith and R. Johnson, "Sensory experiences in public space design: A new evaluation model," Landscape and Urban Planning, vol. 226, pp. 104-119, 2023.

[15] Y. Lu, H. Wang, and D. Chen, Sustainable Cities and Society, vol. 82, p. 103934, 2023.

[16] M. Palanikumar, I. M. Hezam, C. Jana, M. Pal, and G. W. Weber, "Multiple-attribute decision-making for selection of medical robotic engineering based on logarithmic square root neutrosophic normal approach," (in English), Journal of Industrial and Management Optimization, Article vol. 20, no. 7, pp. 2405-2433, Jul 2024.

[17] J. J. Jiang, G. C. Gong, L. Wang, and Q. B. Zha, "Risk measurement of aggregation approaches in multiple attribute decision making under uncertain information," (in English), Applied Soft Computing, Article vol. 158, p. 13, Jun 2024, Art. no. 111568.

[18] H. Y. Bian, W. Y. Zeng, D. Q. Li, Z. Xie, and Q. Yin, "Pythagorean fuzzy monotonic argument dependent owa operator and its applications in multiple attribute decision making," (in English), International Journal of Fuzzy Systems, Article vol. 26, no. 3, pp. 1016-1029, Apr 2024.

[19] H. Y. Zhang, H. J. Wang, Q. Cai, and G. W. Wei, "Spherical fuzzy hamacher power aggregation operators based on entropy for multiple attribute group decision making," (in English), Journal of Intelligent & Fuzzy Systems, Article vol. 44, no. 5, pp. 8743-8771, 2023.

[20] C. Zhang, W. H. Bai, D. Y. Li, and J. M. Zhan, "Multiple attribute group decision making based on multigranulation probabilistic models, multimoora and tpop in incomplete q-rung orthopair fuzzy information systems," (in English), International Journal of Approximate Reasoning, Article vol. 143, pp. 102-120, Apr 2022.

[21] H. Sun, Z. Yang, Q. Cai, G. W. Wei, and Z. W. Mo, "An extended exp-todim method for multiple attribute decision making based on the z-wasserstein distance," (in English), Expert Systems with Applications, Article vol. 214, p. 14, Mar 2023, Art. no. 119114.

[22] T. Senapati, G. Y. Chen, R. Mesiar, and R. R. Yager, "Intuitionistic fuzzy geometric aggregation operators in the framework of aczel-alsina triangular norms and their application to multiple attribute decision making," (in English), Expert Systems with Applications, Article vol. 212, p. 15, Feb 2023, Art. no. 118832.

[23] F. Riazi, M. H. Dehbozorgi, M. R. Feylizadeh, and M. Riazi, "Enhanced oil recovery prioritization based on feasibility criteria using intuitionistic fuzzy multiple attribute decision making: A case study in an oil reservoir," (in English), Petroleum Science and Technology, Article; Early Access p. 19, 2023 Jun 2023.

[24] W. Ali et al., "Aczel-alsina-based aggregation operators for intuitionistic hesitant fuzzy set environment and their application to multiple attribute decision-making process," (in English), Aims Mathematics, Article vol. 8, no. 8, pp. 18021-18039, 2023.

[25] M. W. Zhao, G. W. Wei, Y. F. Guo, and X. D. Chen, "Cpt-todim method for interval-valued bipolar fuzzy multiple attribute group decision making and application to industrial control security service provider selection (vol 27, pg 1186, 2021)," (in English), Technological and Economic Development of Economy, Correction vol. 28, no. 2, pp. 581-582, 2022.

[26] M. Palanikumar, K. Arulmozhi, C. Jana, and M. Pal, "Multiple attribute decision-making pythagorean vague normal operators and their applications for the medical robots process on surgical system," (in English), Computational & Applied Mathematics, Article vol. 42, no. 6, p. 27, Sep 2023, Art. no. 287.

[27] A. Noori, H. Bonakdari, A. H. Salimi, L. Pourkarimi, and J. M. Samakosh, "A novel multiple attribute decision-making approach for assessing the effectiveness of advertising to a target audience on drinking water consumers? Behavior considering age and education level," (in English), Habitat International, Article vol. 133, p. 9, Mar 2023, Art. no. 102749.

[28] B. Q. Ning, R. Lin, G. W. Wei, and X. D. Chen, "Edas method for multiple attribute group decision making with probabilistic dual hesitant fuzzy information and its application to suppliers selection," (in English), Technological and Economic Development of Economy, Article vol. 29, no. 2, pp. 326-352, 2023.

[29] Y. T. Liu, S. Q. Wu, C. C. Li, and Y. C. Dong, "Exploring 2-rank strategic weight manipulation in multiple attribute decision making and its applications in project review and university ranking," (in English), Engineering Applications of Artificial Intelligence, Article vol. 117, p. 14, Jan 2023, Art. no. 105525.

[30] P. Wu, L. G. Zhou, and L. Martinez, "An integrated hesitant fuzzy linguistic model for multiple attribute group decision-making for health management center selection," (in English), Computers & Industrial Engineering, Article vol. 171, p. 15, Sep 2022, Art. no. 108404.

[31] A. Thilagavathy and S. Mohanaselvi, "A study of cubical fuzzy possibility degree measure and its applications to multiple attribute decision-making problems," (in English), Journal of Intelligent & Fuzzy Systems, Article vol. 43, no. 6, pp. 7663-7678, 2022.

[32] Y. Su, M. W. Zhao, G. W. Wei, C. Wei, and X. D. Chen, "Probabilistic uncertain linguistic edas method based on prospect theory for multiple attribute group decision-making and its application to green finance," (in English), International Journal of Fuzzy Systems, Article vol. 24, no. 3, pp. 1318-1331, Apr 2022.

[33] T. Senapati, G. Y. Chen, and R. R. Yager, "Aczel-alsina aggregation operators and their application to intuitionistic fuzzy multiple attribute decision making," (in English), International Journal of Intelligent Systems, Article vol. 37, no. 2, pp. 1529-1551, Feb 2022.

[34] J. Selvaraj, P. Gatiyala, and S. H. Zolfani, "Trapezoidal intuitionistic fuzzy power heronian aggregation operator and its applications to multiple-attribute group decision-making," (in English), Axioms, Article vol. 11, no. 11, p. 29, Nov 2022, Art. no. 588.

[35] F. Amin, A. Fahmi, and M. Aslam, "Approaches to multiple attribute group decision making based on triangular cubic linguistic uncertain fuzzy aggregation operators," (in English), Soft Computing, Article vol. 24, no. 15, pp. 11511-11533, Aug 2020.

[36] A. P. Darko and D. C. Liang, "Some q-rung orthopair fuzzy hamacher aggregation operators and their application to multiple attribute group decision making with modified edas method," (in English), Engineering Applications of Artificial Intelligence, Article vol. 87, p. 17, Jan 2020, Art. no. 103259.

[37] A. R. Mishra, A. K. Garg, H. Purwar, P. Rana, H. C. Liao, and A. Mardani, "An extended intuitionistic fuzzy multi-attributive border approximation area comparison approach for smartphone selection using discrimination measures," (in English), Informatica, Article vol. 32, no. 1, pp. 119-143, 2021.

[38] M. Tang, H. C. Liao, E. Herrera-Viedma, C. L. P. Chen, and W. Pedrycz, "A dynamic adaptive subgroup-to-subgroup compatibility-based conflict detection and resolution model for multicriteria large-scale group decision making," (in English), Ieee Transactions on Cybernetics, Article vol. 51, no. 10, pp. 4784-4795, Oct 2021.

[39] X. L. Wu and H. C. Liao, "Modeling personalized cognition of customers in online shopping," (in English), Omega-International Journal of Management Science, Article vol. 104, p. 13, Oct 2021, Art. no. 102471.

[40] L. A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, no. 3, pp. 338-353, 1965.

[41] V. Torra, "Hesitant fuzzy sets," International Journal of Intelligent Systems, vol. 25, no. 6, pp. 529-539, Jun 2010.

[42] S. Ashraf, M. Kousar, and M. S. Hameed, "Early infectious diseases identification based on complex probabilistic hesitant fuzzy n-soft information," (in English), Soft Computing, Article; Early Access p. 26, 2023 May 2023.

[43] Attaullah, N. Rehman, A. Khan, and G. Santos-Garcia, "Fermatean hesitant fuzzy rough aggregation operators and their applications in multiple criteria group decision-making," (in English), Scientific Reports, Article vol. 13, no. 1, p. 26, Feb 2023.

[44] A. H. Dolatabad, J. H. Dahooie, J. Antucheviciene, M. Azari, and S. H. R. Hajiagha, "Supplier selection in the industry 4.0 era by using a fuzzy cognitive map and hesitant fuzzy linguistic vikor methodology," (in English), Environmental Science and Pollution Research, Article vol. 30, no. 18, pp. 52923-52942, Apr 2023.

[45] M. Kamran, S. Ashraf, N. Salamat, M. Naeem, and T. Botmart, "Cyber security control selection based decision support algorithm under single valued neutrosophic hesitant fuzzy einstein aggregation information (vol 8, pg 5551, 2023)," (in English), Aims Mathematics, Correction vol. 8, no. 6, pp. 13795-13796, 2023.

[46] A. Khan, S. Ashraf, S. Abdullah, M. Ayaz, and T. Botmart, "A novel decision aid approach based on spherical hesitant fuzzy aczel-alsina geometric aggregation information (vol 8, pg 5148, 2023)," (in English), Aims Mathematics, Correction vol. 8, no. 6, pp. 13787-13788, 2023.

[47] R. M. Pattanayak, H. S. Behera, and S. Panigrahi, "A novel high order hesitant fuzzy time series forecasting by using mean aggregated membership value with support vector machine," (in English), Information Sciences, Article vol. 626, pp. 494-523, May 2023.

[48] A. Sarkar, S. Moslem, D. Esztergar-Kiss, M. Akram, L. S. Jin, and T. Senapati, "A hybrid approach based on dual hesitant q-rung orthopair fuzzy frank power partitioned heronian mean aggregation operators for estimating sustainable urban transport solutions," (in English), Engineering Applications of Artificial Intelligence, Article vol. 124, p. 23, Sep 2023, Art. no. 106505.

[49] L. Gomes and M. Lima, "Todim: Basics and apllication to multicriteria ranking of projects with environmental impacts," Foundations of Control Engineering, vol. 16, pp. 113-127, 01/01 1991.

[50] L. F. A. M. Gomes and M. M. P. P. Lima, "From modeling individual preferences to multicriteria ranking of discrete alternatives: A look at prospect theory and the additive difference model," Foundations of Computing and Decision Sciences, vol. 17, no. 3, pp. 171-184, 1992.

[51] L. Gomes and L. A. D. Rangel, "An application of the todim method to the multicriteria rental evaluation of residential properties," (in English), European Journal of Operational Research, Article vol. 193, no. 1, pp. 204-211, Feb 2009.

[52] L. Gomes, L. A. D. Rangel, and F. J. Maranhao, "Multicriteria analysis of natural gas destination in brazil: An application of the todim method," (in English), Mathematical and Computer Modelling, Article vol. 50, no. 1-2, pp. 92-100, Jul 2009.

[53] Y.-J. Lai, T.-Y. Liu, and C.-L. Hwang, "Topsis for modm," European journal of operational research, vol. 76, no. 3, pp. 486-500, 1994.

[54] K. P. Yoon and C.-L. Hwang, Multiple attribute decision making: An introduction. Sage publications, 1995.

[55] C. Y. Wang, L. X. Wang, T. T. Gu, J. Y. Yin, and E. Y. Hao, "Critic-topsis-based evaluation of smart community safety: A case study of shenzhen, china," (in English), Buildings, Article vol. 13, no. 2, p. 21, Feb 2023, Art. no. 476.

[56] X. X. Wu, Z. Y. Zhu, C. Chen, G. R. Chen, and P. D. Liu, "A monotonous intuitionistic fuzzy topsis method under general linear orders via admissible distance measures," (in English), Ieee Transactions on Fuzzy Systems, Article vol. 31, no. 5, pp. 1552-1565, May 2023.

[57] K. Zhang, X. Liang, H. Wei, S. S. Liu, and K. Su, "An improved topsis-anp composite shielding material performance evaluation method based on gray relational projection algorithm," (in English), Frontiers in Energy Research, Article vol. 10, p. 13, Jan 2023, Art. no. 1102997.

[58] C. E. Shannon, "A mathematical theory of communication," Bell System Technical Journal, vol. 27, no. 4, pp. 379-423, 1948.

[59] M. M. Xia and Z. S. Xu, "Hesitant fuzzy information aggregation in decision making," International Journal of Approximate Reasoning, vol. 52, no. 3, pp. 395-407, Mar 2011.

[60] Z. S. Xu and M. M. Xia, "Distance and similarity measures for hesitant fuzzy sets," Information Sciences, vol. 181, no. 11, pp. 2128-2138, Jun 2011.

[61] Tehreem, A. Hussain, A. Alsanad, and M. A. A. Mosleh, "Spherical cubic fuzzy extended topsis method and its application in multicriteria decision-making," (in English), Mathematical Problems in Engineering, Article vol. 2021, p. 14, Jun 2021, Art. no. 2284051.

[62] R. P. Tan, W. D. Zhang, and S. Q. Chen, "Decision-making method based on grey relation analysis and trapezoidal fuzzy neutrosophic numbers under double incomplete information and its application in typhoon disaster assessment," (in English), Ieee Access, Article vol. 8, pp. 3606-3628, 2020.

[63] J. H. Kim and B. S. Ahn, "The hierarchical vikor method with incomplete information: Supplier selection problem," (in English), Sustainability, Article vol. 12, no. 22, p. 15, Nov 2020, Art. no. 9602.

[64] M. S. A. Khan, F. Khan, J. Lemley, S. Abdullah, and F. Hussain, "Extended topsis method based on pythagorean cubic fuzzy multi-criteria decision making with incomplete weight information," (in English), Journal of Intelligent & Fuzzy Systems, Article vol. 38, no. 2, pp. 2285-2296, 2020.

[65] P. D. Liu and W. Q. Liu, "Multiple-attribute group decision-making method of linguistic q-rung orthopair fuzzy power muirhead mean operators based on entropy weight," International Journal of Intelligent Systems, vol. 34, no. 8, pp. 1755-1794, Aug 2019.

[66] A. Tversky and D. Kahneman, "Prospect theory: An analysis of decision under risk," Econometrica, vol. 47, no. 2, pp. 263-291, 1979.

[67] P. D. Liu and P. Zhang, "A normal wiggly hesitant fuzzy mabac method based on ccsd and prospect theory for multiple attribute decision making," (in English), International Journal of Intelligent Systems, Article vol. 36, no. 1, pp. 447-477, Jan 2021.

[68] X. D. Peng and W. Q. Li, "Algorithms for hesitant fuzzy soft decision making based on revised aggregation operators, wdba and codas," (in English), Journal of Intelligent & Fuzzy Systems, Article vol. 36, no. 6, pp. 6307-6323, 2019.

[69] X. M. Mi and H. C. Liao, "An integrated approach to multiple criteria decision making based on the average solution and normalized weights of criteria deduced by the hesitant fuzzy best worst method," (in English), Computers & Industrial Engineering, Article vol. 133, pp. 83-94, Jul 2019.

[70] X. L. Zhang and Z. S. Xu, "The todim analysis approach based on novel measured functions under hesitant fuzzy environment," Knowledge-Based Systems, vol. 61, pp. 48-58, May 2014.

ARO-CapsNet: A Novel Method for Evaluating User Experience in Immersive VR Furniture Design

Yin Luo, Jun Liu*, Li Zhang
College of Fine Arts and Design, WenZhou University, WenZhou 325035, ZheJiang, China

***Abstract*—Immersive virtual reality (VR) technology has become an essential tool in enhancing user experience across industries, particularly in furniture design. With the ability to provide realistic, interactive, and immersive environments, it significantly improves user engagement and decision-making in product design. However, existing analysis methods lack precision in evaluating user experience within VR environments. This study aims to develop a more accurate and efficient model for analyzing the application of immersive VR in future furniture design. By integrating the Artificial Rabbit Optimization (ARO) algorithm with Capsule Networks (CapsNet), this research enhances the evaluation of user experience in immersive VR environments. The proposed method uses the ARO algorithm to optimize the parameters of CapsNet, which maps the relationship between the analysis indicators of furniture design and user experience. This model is tested against traditional methods such as CNN and CapsNet alone. The analysis focuses on key factors such as visual elements, interaction, and system performance, with performance metrics like root mean square error (RMSE) and R^2 value used for evaluation. Experimental results show that the ARO-CapsNet model achieves a RMSE of 0.17 and an R^2 value of 0.988, outperforming both CNN and CapsNet in terms of accuracy and efficiency. Additionally, the proposed model improves the immersive VR system's ability to deliver accurate user experience evaluations, making it a superior method for analyzing future furniture design applications. The integration of the ARO algorithm with CapsNet significantly enhances the precision of immersive VR user experience evaluations in furniture design. The ARO-CapsNet model not only improves evaluation accuracy but also increases system efficiency, providing a robust framework for future applications of VR in product design.**

Keywords*—Immersive virtual reality; furniture design; application analysis; artificial rabbit optimisation algorithm

I. Introduction

Due to advancements in science and technology, the production of furniture has consistently risen, leading to heightened rivalry among furniture companies. Additionally, consumer attitudes towards consumption have shifted, resulting in increasingly high expectations for user experience [1]. The technology used for furniture presentation has inherent biases and constraints, resulting in a passive role for the buyer and directly impacting the consumer experience [2]. With the progressive advancement and enhancement of virtual reality technology in recent years, significant achievements have been made. Its interactive capabilities have greatly enhanced the user experience and expanded the scope of research in the domestic furniture virtual display field. This has a significant impact on the development direction of furniture enterprises [3]. Virtual display technology utilizes computer technology to create three-dimensional models of furniture products, which can be accessed and interacted with by users through computers or networks. This technology enables users to have a realistic sensory and emotional experience with furniture products.

The integration of advanced virtual reality technology in furniture design and user experience research enables users to fully immerse themselves in virtual displays, enhancing the depth of information, realism, and overall user experience [4]. This has significant practical applications. At now, immersive virtual reality technology is being used to study several areas of future furniture design, user experience, and application analysis [5]. Svalina et al. [6] examined the use of immersive virtual reality technology to create a virtual exhibition hall. Jafarifiroozabadi et al. [7] developed a virtual reality technology specifically for train driving simulations, which includes realistic acoustic sounds to enhance the user's auditory immersion. Zhang et al. [8] combined virtual reality technology with furniture display design to create a furniture virtual display system that offers users an intuitive and realistic interactive experience. Potseluyko et al. [9] used the LSSVM model to construct an application analysis system for virtual reality technology in future furniture design, using the case of ancient towns in Sichuan and Chongqing for performance analysis. Lastly, Ji et al. [10] proposed a user experience analysis method for future furniture virtual display, utilizing an intelligent optimization algorithm to improve the neural network model. Based on extensive literature study and survey analysis, it can be stated that immersive virtual reality technology and furniture design analysis application has the following features [3]: a. The study on the future furniture virtual display system solely focuses on qualitative analysis and lacks quantitative analysis. The current furniture virtual display system lacks a comprehensive examination of the user experience and performance metrics. Current machine learning algorithms that analyze the use of virtual reality technologies lack adequate accuracy in their evaluation models. The use of intelligent optimization algorithms has led to the creation of a model optimization approach for analyzing the application of virtual reality technology. This approach aims to enhance the accuracy of virtual reality technology analysis [11].

This study presents a way for analyzing and using immersive virtual reality technology in furniture design. The approach is based on intelligent optimization algorithms and deep learning algorithms. The method examines the challenges of using virtual reality in furniture design from a user experience perspective. It identifies key analysis factors and utilizes the efficient optimization capabilities of the artificial rabbit optimization algorithm [12] to optimize the parameters of the capsule network

*Corresponding Author.

model [13]. Additionally, it constructs a design application analysis algorithm based on the ARO-CapsNet model. Through comparative analysis validation, the proposed method in this paper demonstrates superior performance.

II. Immersive Virtual Reality in Furniture Design-User Experience

A. Immersive Virtual Reality in Furniture Design-User Experience Application Issues in Analysis

1) Immersive virtual reality: Immersive Virtual Reality (Immersive VR) technology [14] refers to the utilization of three-dimensional input and output devices and software systems to create virtual simulation environments on computers. These environments are designed to be interactive and immersive, providing the user with a multi-channel sensory experience that gives the illusion of being in a virtual environment, as depicted in Fig. 1.

An immersive VR system usually consists of three parts: a reality system, a processing control system, and a motion capture system [15], and its composition is shown in Fig. 2.

Immersive virtual reality technology as a virtual reality technology in the more advanced, more complex a comprehensive technology, its system and table and virtual reality system, AR system and distributed virtual reality system, compared with the following characteristics [15]: 1) immersive; 2) follow the movement; 3) real-time, specific as Fig. 3.

Fig. 1. Effect of immersive virtual reality technology.

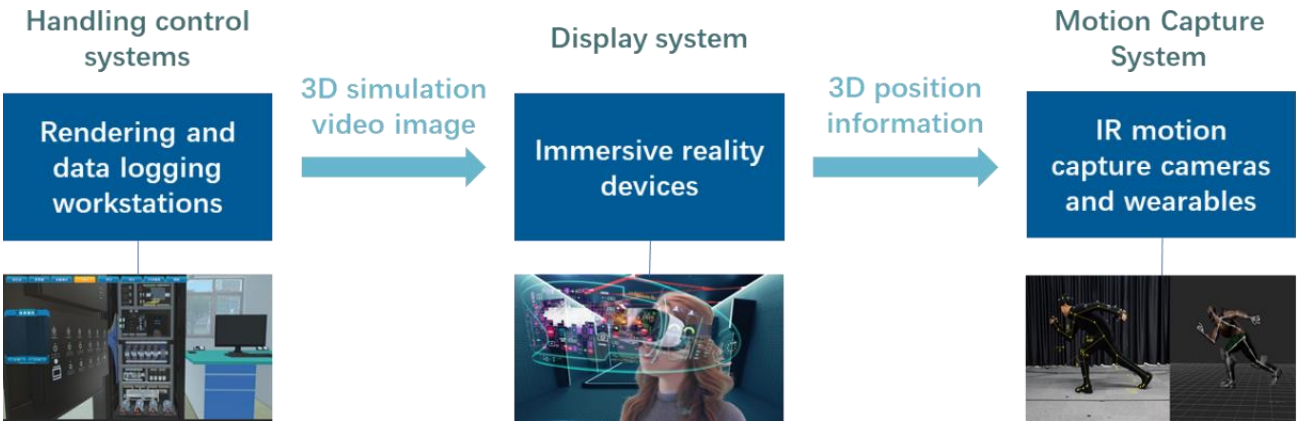


Fig. 2. Immersive virtual reality system composition.

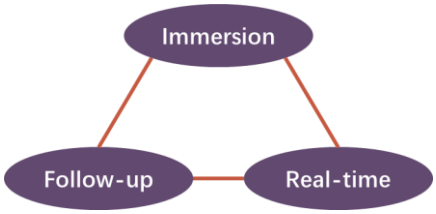


Fig. 3. Characteristics of immersive virtual reality technology.

2) Immersive VR technology in furniture design-user experience: The use of immersive virtual reality (VR) technology in furniture design and user experience is progressively intensifying. This enables consumers to have a comprehensive experience prior to making a purchase by offering an immersive environment, as seen in Fig. 4. The applications of immersive virtual reality (VR) technology in furniture design-user experience encompass various features such as virtual reality roaming, real-time design interaction, home atmosphere simulation, customized experience, cost and resource saving, panoramic home display, integration of virtual and reality, optimization of user experience, remote observation, and multimedia embedding [16].

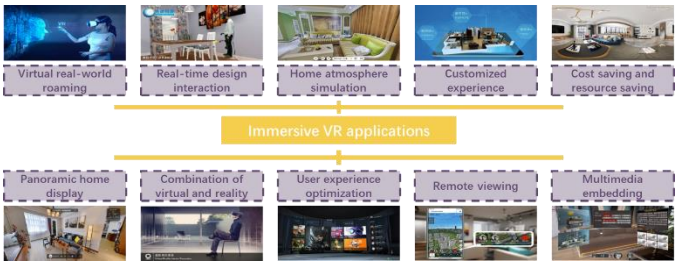


Fig. 4. Analysis of immersive virtual reality technology applications.

B. Extraction and Construction of Indicators for Applied Analysis

1) Immersive VR technology application process: The steps of immersive VR technology application in furniture design-user experience are shown in Fig. 5, and the specific steps include 3D furniture scene design, scene furniture modelling, adjusting lighting, scene roaming, adding detail display, furniture attribute replacement, and system release, etc. [17].

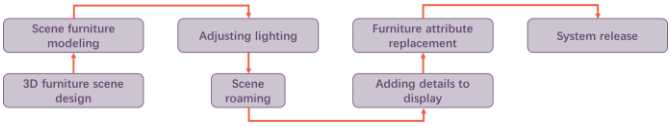


Fig. 5. Steps in the application of immersive virtual reality technology.

2) Application analysis indicator extraction: According to the analysis of the application of immersive VR technology in furniture design-user experience, this paper analyses the visual elements, psychological elements, creating space, colour design, etc., and the construction of the specific indicator set is shown in Fig. 6.

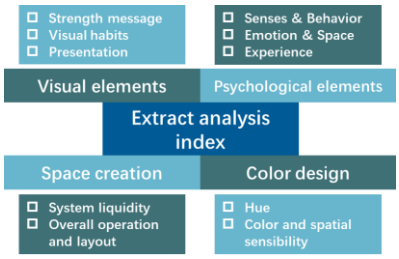


Fig. 6. Extraction and construction of indicators for analysing the application of immersive virtual reality technology.

C. Application Analysis Programme Design

This paper proposes a method for analyzing the application of immersive VR technology in furniture design, specifically focusing on user experience issues. The method is based on intelligent optimization algorithms and deep learning. The detailed design scheme is illustrated in Fig. 7. The immersive VR technology application analysis research technique encompasses several essential technologies, including VR application analysis, application analysis scheme design, application analysis model construction and optimization, and case design analysis.

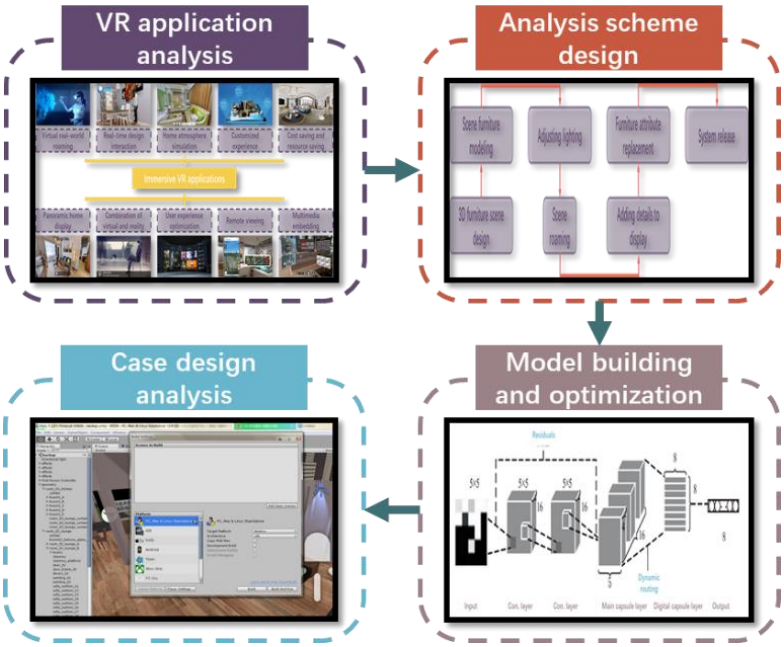


Fig. 7. Immersive virtual reality technology application analysis programme.

III. Application of Virtual Reality Furniture Design

A. ARO Algorithm

Artificial rabbits optimization (ARO) [18] is a nature-inspired swarm intelligence optimisation algorithm. The ARO algorithm is inspired by the survival strategies of rabbits in nature (Fig. 8), including meandering foraging and random hiding. The meandering foraging strategy forces a rabbit to eat grass near other rabbits' nests, which prevents its nest from being discovered by predators. The random hiding strategy allows the rabbit to choose a random burrow among its own to hide in, which reduces the likelihood of being captured by an enemy. In addition, the rabbit's energy contraction causes it to shift from a meandering foraging strategy to a random hiding strategy. The algorithm mathematically models this survival strategy to develop a new optimiser.

Fig. 8. ARO algorithm inspired behaviour.

In the phase of initialising the artificial rabbit population, a certain number of individual rabbits are randomly generated in the space of the defining domain, and each rabbit represents a possible solution in the problem space. And then, the function values of these individuals are calculated based on their locations.

1) Bypass foraging (exploration): When foraging, rabbits will search far away and ignore what is close by. They only eat grass from other areas and not from their own area, a foraging behaviour known as meandering foraging.ARO's meandering foraging behaviour suggests that each searching individual tends to update its position to another randomly selected searching individual in the group with an added perturbation. The specific model is as follows:

$$X_i(t+1)=X_j(t)+R\cdot\left(X_i(t)-X_j(t)\right)+round\left(0.5\cdot\left(0.05+r_1\right)\right)\cdot r_2 \quad (1)$$

$$R=L\cdot c \quad (2)$$

$$L=\left(e-e^{\left(\frac{t-1}{T}\right)^2}\right)\cdot\sin\left(2\pi r_3\right) \quad (3)$$

$$c(k)=\begin{cases}1 & if\ k==g(l)\\ 0 & else\end{cases}\quad k=1,\cdots,d\ and\ l=1,\cdots,\lceil r_3\cdot d\rceil \quad (4)$$

$$g=randperm(d) \quad (5)$$

$$n_1 \sim N(0,1) \quad (6)$$

Where $X_i(t+1)$ denotes the position of the ith rabbit; R denotes the moving step; T is the maximum number of iterations; $\lceil\cdot\rceil$ denotes the ceil function; $randperm$ denotes a random integer from 1 to d; r_1 , r_2 and r_3 are random numbers; n_1 denotes that it obeys a normal distribution. Fig. 9 gives the curve of the step size L with the number of iterations.

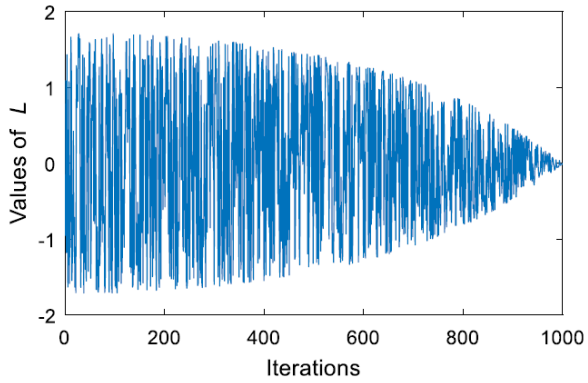


Fig. 9. Curve of step size with number of iterations.

2) Random concealment (exploitation): In order to hide from predators, rabbits usually dig a number of different burrows around their nests. In each iteration of the ARO algorithm, the rabbit always generates a number of burrows around it along each dimension of the search space, and always chooses one randomly from all the burrows to hide, in order to reduce the probability of being predated. The specific model is as follows:

$$X_i(t+1)=X_j(t)+H\cdot g\cdot X_i(t) \quad (7)$$

$$H=\frac{T-t+1}{T}\cdot r_4 \quad (8)$$

$$n_2 \sim N(0,1) \quad (9)$$

$$g(k)=\begin{cases}1 & if\ k==j\\ 0 & else\end{cases}\quad k=1,\cdots,d \quad (10)$$

In order to determine the next behaviour of the rabbit group, its energy factor needs to be calculated, which in turn determines the next behaviour of the individual, i.e. the choice of meandering foraging or random hiding. For the rabbit population, its energy factor at the tth iteration is calculated as shown in Eq. (11):

$$A(t)=4\left(1-\frac{t}{T}\right)\ln\frac{1}{r} \tag{11}$$

where r is a random number. Fig. 10 gives the curve of the energy factor A with the number of iterations, and Fig. 11 gives the schematic diagram of the search mechanism of the energy factor. Fig. 12 gives a schematic diagram of the calculation of the probability of bypass foraging.

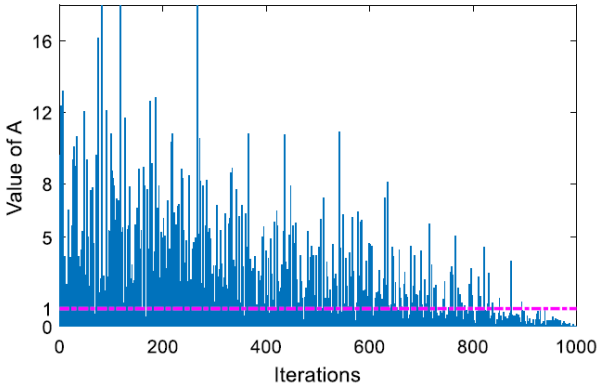


Fig. 10. Curve of energy factor A with number of iterations.

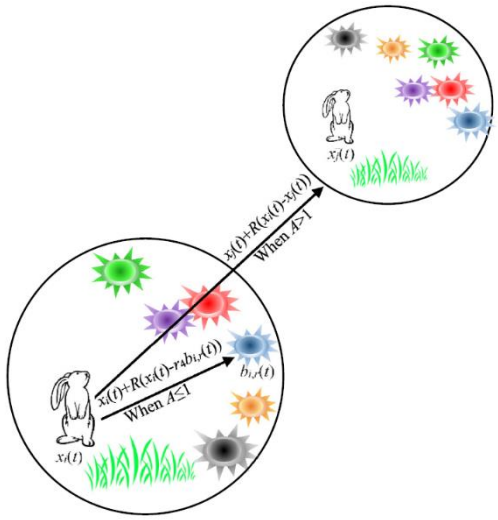


Fig. 11. The curve of step length with a number of iterations.

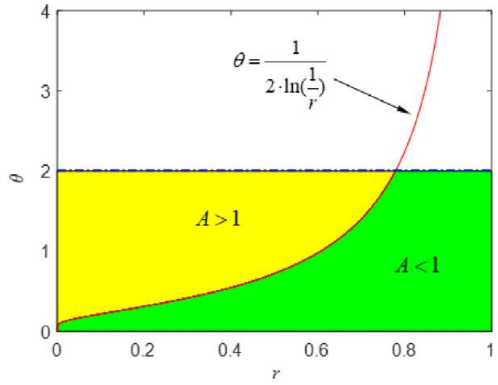


Fig. 12. Calculating the probability of foraging bypasses.

3) ARO process steps: According to the optimization behaviour of the ARO algorithm, the ARO flowchart is shown in Fig. 13, with the following steps: a. set the parameters of the ARO algorithm, including the number of populations, the maximum number of iterations, and other parameters; b. randomly initialize rabbit populations and evaluate the population position to obtain the optimal rabbit position; c. calculate the energy factor A; d. if A<1, update the populations by using a detour foraging strategy, or else use a random hiding strategy to update the population; e. Calculate the updated population position and obtain the optimal rabbit position; f. Determine whether the number of iterations reaches the maximum and output the final optimal solution.

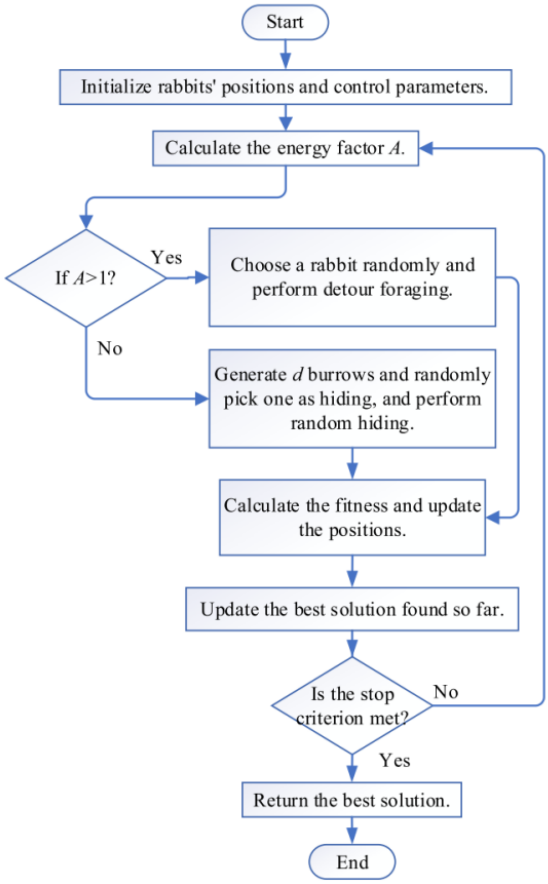


Fig. 13. Flowchart of ARO algorithm.

B. Capsule Network Model

Capsule Networks (CNNs) [19] are a novel deep learning model designed to overcome some of the limitations of traditional Convolutional Neural Networks (CNNs) [20] in processing images, especially in recognising the pose and spatial layout of objects. The core idea of capsule networks is to use so-called "capsules" instead of traditional neurons (as shown in Fig. 14), which are a collection of neurons that collectively represent the instantiated parameters of an object, such as position, size, and orientation. The capsule network learns the relationships between different capsules through a dynamic routing algorithm that allows the network to adaptively focus on relevant features and suppress irrelevant information.

The residual block structure is introduced in the capsule network [21], in order to reduce the number of parameters in the model and improve the robustness of the model. The improved capsule network structure is shown in Fig. 15.

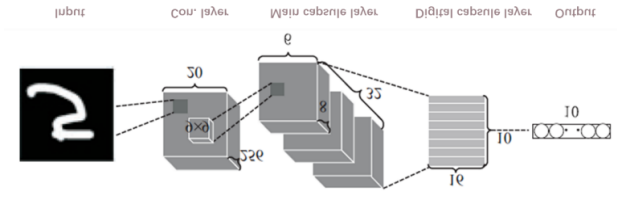


Fig. 14. CapsNet network structure.

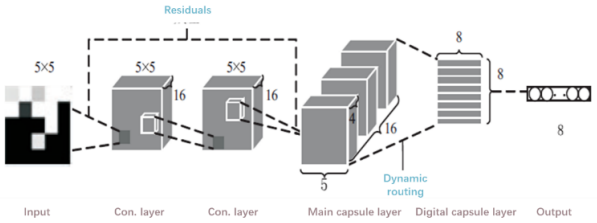


Fig. 15. Improved CapsNet network structure.

The core of a capsule network is a capsule, which is a collection of neurons that together represent a feature vector in the input data, which has the advantage over CNN in that it can better deal with spatial relationships in the data. The core idea of dynamic routing algorithm in capsule network is to adjust the routing weights from the low-level capsule to the high-level capsule through iteration, so that the output vector of the low-level capsule can focus on the high-level capsule associated with it. The iterative process of dynamic routing algorithm in capsule network is described as follows:

$$c_{ij} = \frac{\exp\left(b_{ij}\right)}{\sum_{i} \exp\left(b_{ij}\right)} \tag{12}$$

$$u_{j|i} = W_{i|j} \times u_i \tag{13}$$

$$s_j = \sum_{j} c_{ij} \times u_{j|i} \tag{14}$$

$$v_j = \frac{\left\|s_j\right\|^2}{1+\left\|s_j\right\|^2} \times \frac{s_j}{\left\|s_j\right\|} = squash\left(s_j\right) \tag{15}$$

$$b_{ij} \leftarrow b_{ij} + u_{j|i} v_j \tag{16}$$

where b_{ij} denotes the prior probability that capsule i is connected to capsule j; $W_{i|j}$ is the transformation matrix; u_i is the output vector of low-level capsule i; $u_{j|i}$ is the predicted capsule; s_j is the total input of high-level capsules; and v_j is the output vector of high-level capsule j.

C. ARO-CapsNet Model Application Methodology

1) ARO-CapsNet model: In order to improve the analysis accuracy and design efficiency of the application of immersive VR technology in future furniture design and user experience, this paper adopts the CapsNet model to construct the application analysis model, and at the same time adopts the ARO algorithm to optimise the application analysis model. The ARO-CapsNet model takes the CapsNet network structural parameters as the optimisation variables, and takes RMSE as the fitness value function value, and adopts the ARO algorithm optimisation strategy to optimally find the CapsNet network structure parameters, as shown in Fig.16.

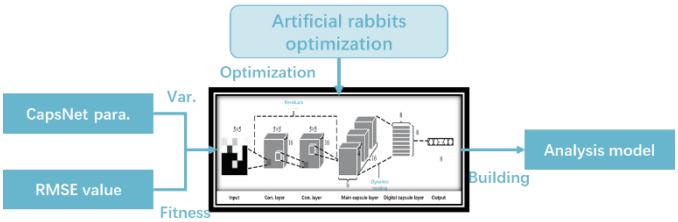


Fig. 16. ARO-CapsNet network model.

2) ARO-CapsNet application process: Based on the ARO-CapsNet model immersive VR technology in the future furniture design and user experience application analysis method by analysing the immersive virtual reality in furniture design-user experience application problems, extracting the application analysis indexes, constructing the index system, using the ARO-CapsNet model to construct the mapping relationship between the application analysis indexes and the assessment value, and obtaining the future furniture design and user experience application analysis model, the specific flow chart is shown in Fig.17.

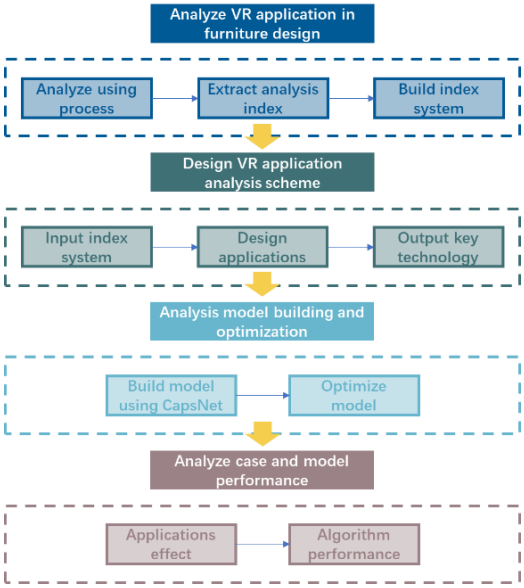


Fig. 17. ARO-CapsNet network model application process.

IV. Experiments and Analysis of Results

A. Experimental Set-up

For the future furniture design problem, this paper adopts Unity3D, 3Dmax and CAD software to develop and design [22], the specific development process is shown in Fig. 18.

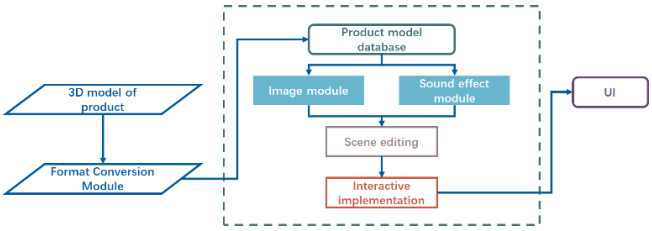


Fig. 18. System development process.

For the immersive VR technology application analysis problem, this paper uses CNN [23], CapsNet [19], ARO-CapsNet model for comparative analysis. The parameters of ARO algorithm are set as follows: the number of populations is 100, and the number of iterations is 1,000; the CNN network is set as follows: the convolutional layer is 100 nodes.

B. Analysis of Results

In order to analyse the application of immersive VR technology in future furniture design, this paper analyses the effect from three aspects: 3D modelling, interaction design and system release [24]. The effect diagram of the showroom is shown in Fig. 19. In Fig. 20, we add the design effect after adding relevant interaction elements. At the same time, the virtual system released on PC, IOS system and Android system is embedded in Fig. 21 to show the effect.

Fig. 19. 3D modelling effect.

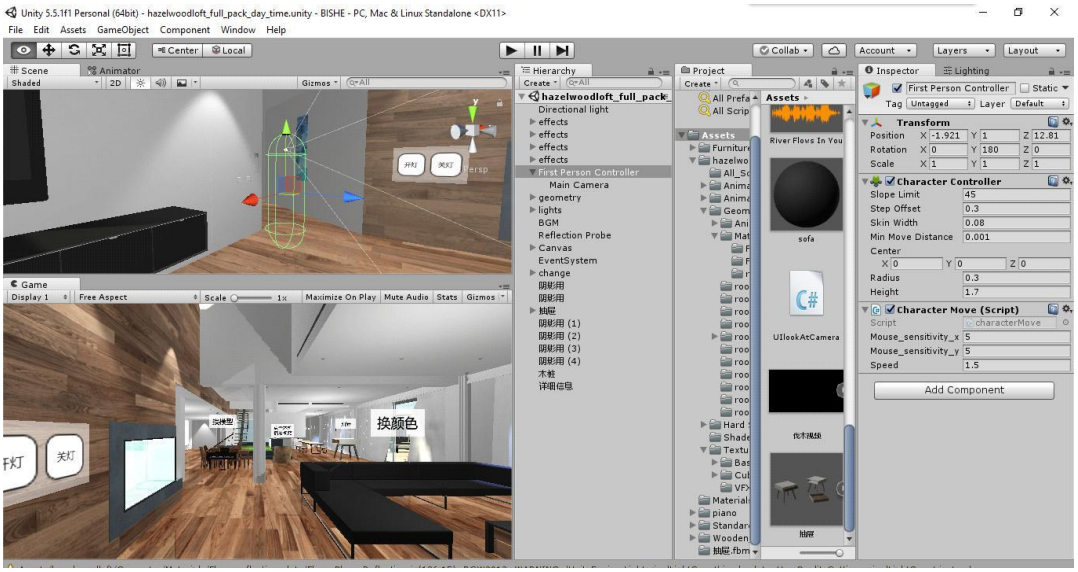


Fig. 20. Interaction design diagram.

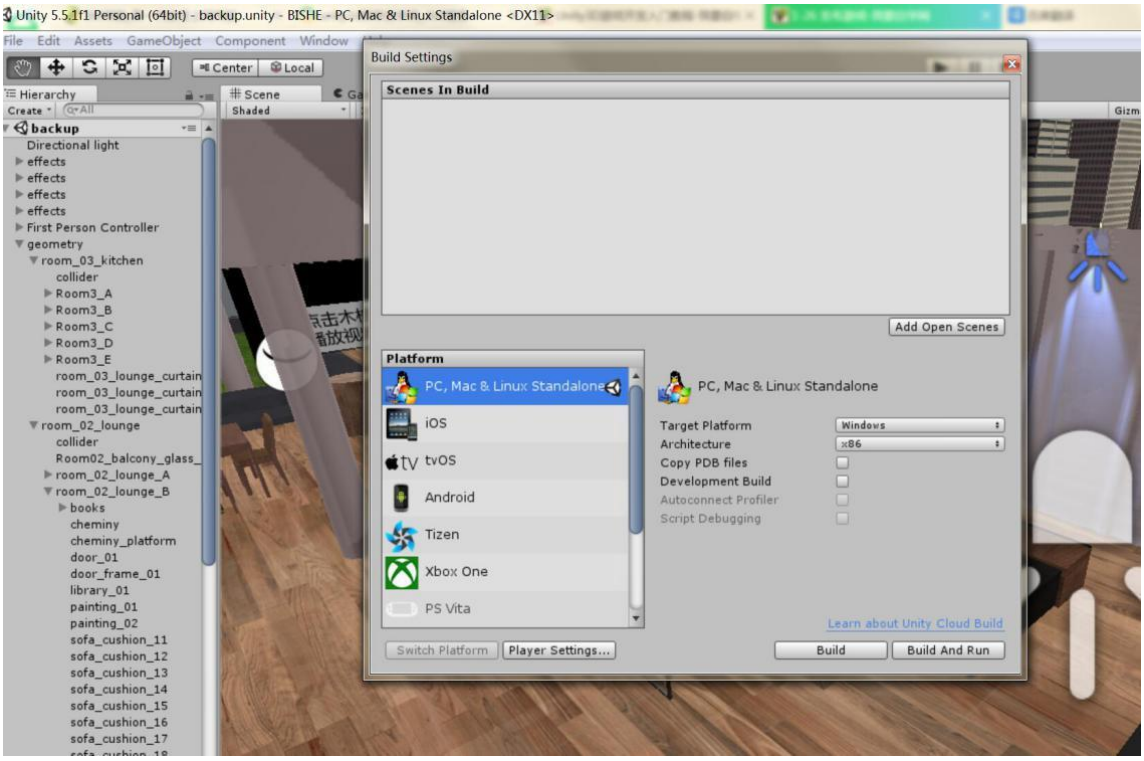


Fig. 21. Schematic system development.

To confirm the efficiency and superiority of the immersive VR future furniture design experience application analysis approach based on the ARO-CapsNet model, we compared and analyzed ARO-CapsNet with CNN and CapsNet. The findings are shown in Fig. 22 and Fig. 23.

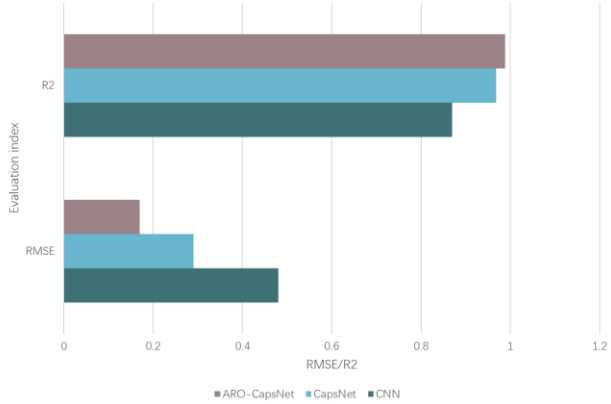


Fig. 22. Comparative analysis of application analytics model performance.

The performance of the application analysis models, namely ARO-CapsNet, CNN, and CapsNet, may be seen in Fig. 22 located in the center of our document. According to the figure. Based on the RMSE and R2 values, it is evident that the ARO-CapsNet model outperforms the other models in predicting application analysis. The RMSE for ARO-CapsNet is 0.17, which is the smallest among all models. Additionally, the R2 value for ARO-CapsNet is 0.988, indicating the highest level of accuracy compared to the other models. Figure The table displays the outcomes of the application analysis for each model in the comparison. Fig. 23 demonstrates that the application analysis technique of immersive VR future furniture design experience, which is based on the ARO-CapsNet model, accurately analyzes the value, bringing it closer to the actual value.

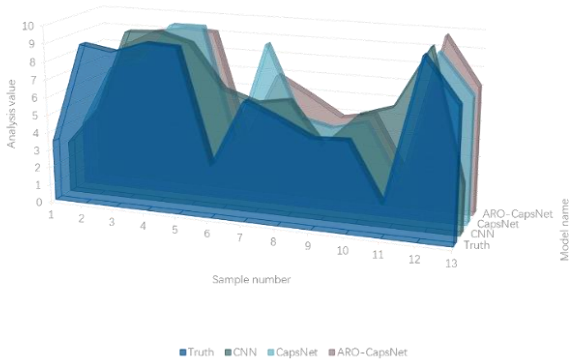


Fig. 23. Application analysis results of each algorithm.

V. CONCLUSION

To address the issues of poor accuracy and low design efficiency in the study of immersive VR technology applications, a novel technique is given. This method utilizes ARO and CapsNet to develop an immersive VR future furniture design experience application analysis method. The technique examines the indications of immersive VR technology application and formulates an application analysis scheme by analyzing the challenges faced in applying immersive virtual reality to furniture design from a user experience perspective.

The ARO algorithm is used to optimize the parameters of CapsNet in the analysis model for immersive VR technology application. Additionally, a new analysis model is developed for the future furniture design experience application in immersive VR, which is based on ARO-CapsNet. By doing experimental analysis and comparing it with other models, the suggested model demonstrates superior performance in application analysis. This further confirms that the model has more flexibility for future furniture design experiences.

REFERENCES

[1] Grand A , Dittrich R , Francis B , Hinde J. Modelling changes over time in a multivariate paired comparison: An application to window display design:[J].Statistical Modelling, 2022, 22(1-2):95-106.

[2] Chung S E , Ryoo H Y .User Experience Factors and attributes on the Stretchable Display applied Automotive[J].International Journal of Asia Digital Art and Design Association, 2022, 26(1):1-11.

[3] Azadmanjir Z , Sadeghi-Naini M , Dashtkoohi M , Moradi-Lakeh M, Arabkheradmand J, Harrop J S. The design of a quality improvement dashboard for monitoring spinal cord and column injuries[J].Informatics in Medicine Unlocked, 2024, 47.

[4] Zhang J .User Experience Perspectives on the Application of Interactivity Design Based on Sensor Networks in Digital Museum Product Display[J].Journal of Sensors, 2022.

[5] Ortiz-Toquero S , Sanchez I , Serrano A , Martin R.Prevalence of Computer Vision Syndrome and Its Risk Factors in a Spanish University Population[J].Eye & Contact Lens: Science & Clinical Practice, 2024, 50(8):333-341.

[6] Svalina A , Pibernik J , Dolic J M L .Assessing the Design of Interactive Radial Data Visualizations for Mobile Devices[J].journal of imaging, 2023, 9(5).

[7] Jafarifiroozabadi R , Joshi R , Joseph A , Wingler D.Perceived Usability of Seating in an Outpatient Waiting Area: A Combined Approach Utilizing Virtual Reality and Actual Seating Prototypes:[J].HERD: Health Environments Research & Design Journal, 2022, 15(2):248-261.

[8] Zhang Y , Wang J , Ahmad R , Li X. Integrating lean production strategies, virtual reality technique and building information modeling method for mass customization in cabinet manufacturing[J].Engineering construction & architectural management, 2022.

[9] Potseluyko L , Rahimian F P , Dawood N , Elghaish F, Hajirasouli A. Game-like interactive environment using BIM-based virtual reality for the timber frame self-build housing sector[J].Automation in construction, 2022.

[10] Ji G , Sawyer A O , Narasimhan S G .Virtual home staging and relighting from a single panorama under natural illumination[J].Machine Vision and Applications, 2024, 35(4).

[11] Gong C., Xiang W., Chen Y. Optimization of process parameters for injection moulding products based on machine learning and genetic algorithms [J]. Machinery Manufacturing, 2024, 62(05): 60-65.

[12] Luo Jianfu. Adaptive diversity golden sine search improved artificial rabbit optimization algorithm [J]. Journal of Hulunbeier College, 2024, 32(03): 91-99.

[13] Zhang Huimin, Xie Zeqi. A method for identifying rice pests based on multi-scale hollow capsule twin networks [J]. Jiangsu Agricultural Sciences, 2024, 52(11): 231-237.

[14] Mazza T .Unity virtual reality development with VRTK4: a no-coding approach to developing immersive VR experiences, games, & apps[J].Computing reviews, 2023.

[15] Kablitz D , Conrad M , Schumann S .Immersive VR-based instruction in vocational schools: effects on domain-specific knowledge and wellbeing of retail trainees[J].Empirical Research in Vocational Education and Training, 2023, 15(1).

[16] Modoni G E , Sacco M .A Human Digital-Twin-Based Framework Driving Human Centricity towards Industry 5.0[J].sensors, 2023, 23(13).

[17] Li B , Zhou M , Bai Y .The relationships and trends of interregional virtual water trade based on an MRIO model[J].Water science & technology: Water supply, 2022, 22(3):2395-2406.

[18] Lam M C , Nizam S S M , Arshad H , Suwadi N A.Tangible interaction technique with authoring capability for kitchen design[J].Multimedia Tools and Applications, 2023, 82(19):30125-30150.

[19] Li Qi, Liu Chunxia, Gao Gaimei. Industrial Internet intrusion detection method based on CapsNet and SRU [J]. Computer Technology and Development, 2024, 34(07):93-99.

[20] Hashmi H , Dwivedi R K , Kumar A .Comparative Analysis of CNN-Based Smart Pre-Trained Models for Object Detection on Dota[J].Journal of Automation, Mobile Robotics and Intelligent Systems, 2024, 18(2):31-45.

[21] Zhang Hongying, Tian Penghua. A gait recognition method combining residual networks and multi-level block structures [J]. Journal of Electronic Measurement and Instruments, 2022(6):66-72.

[22] Yu Jin, Yan Shuguang, Lv Tong. Design and implementation of a virtual magnetic separation laboratory system based on Unity3D [J]. Software Engineering and Application, 2024, 13(3):8.

[23] Lin Wei, Chen Yan. Chinese microblog sentiment analysis based on BERT-BiGRU and multi-scale CNN [J]. Journal of China Electronics Technology Group Corporation, 2023, 18(10):939-945.

[24] Joakim V , Barbara W .Constructing hermeneutical relations: a postphenomenological inquiry into immersive VR memory palaces[J].Virtual reality, 2023, 27(4):3239-3258.

Application Pigeon Swarm Intelligent Optimisation BP Neural Network Algorithm in Railway Tunnel Construction

Feng Zhou[1]*, Hong Ye[2], Jie Song[3], Hui Guo[4], Peng Liu[5]
Zhejiang Deqing County Transportation and Water Resources Investment Group Co., Ltd Huzhou 313200, Zhejiang, China[1, 2]
China Railway First Group Second Engineering Co., Ltd, Tangshan 063000, Hebei, China[3, 4, 5]

***Abstract*—Due to the uncertainty and complexity of the risk factors of the urban railway tunnel project to increase the difficulty of risk analysis, so that the traditional risk assessment methods can not accurately assess the construction risk of the urban railway tunnel project. Aiming at the problems of the existing risk assessment algorithms, the construction risk assessment method of an urban railway tunnel project based on intelligent optimisation algorithm and machine learning algorithm is proposed. Firstly, for the problem of construction risk identification and assessment of municipal railway tunnel project, a tunnel construction risk identification and assessment scheme using a combination of intelligent optimization algorithm and machine learning algorithm is designed, and the principles and functions of each module of the risk assessment system are introduced; then, for the problem of risk assessment construction, a risk assessment algorithm based on the swarm intelligent optimization algorithm to improve the BP neural network is proposed; secondly, relying on the Hangzhou Secondly, relying on Xinfeng Road underground passage close to cross the underground line 9 tunnel and the side through the Hanghai intercity tunnel project in Hangzhou, the effectiveness of the construction risk assessment algorithm is verified from monitoring data and numerical simulation, and the risk control scheme is proposed in turn. The experimental results show that the risk assessment algorithm proposed in this paper effectively solves the problem of construction risk assessment of the urban railway tunnel project, and improves the prediction performance of the risk assessment algorithm, and verifies that the risk control scheme meets the construction safety requirements.**

Keywords*—Municipal railway tunnel construction optimization; scenario risk assessment; machine learning; pigeon flock optimisation algorithm

I. INTRODUCTION

With the rapid development of national economy as well as the improvement of information technology, the pace of urbanisation in China is getting faster and faster, which makes the city scale and population grow dramatically [1], and brings a lot of dilemmas to the urban traffic, including traffic congestion, air pollution, and high energy loss [2]. In order to alleviate this development trend, the development of urban underground space to alleviate the surface eyes, improve urban transport, less urban environmental pollution, and achieve carbon neutrality [3]. In addition to making full use of urban space, underground rail transport has the advantages of fast running speed, large passenger capacity, safety and comfort, punctuality, energy saving and environmental protection, but there are also frequent phenomena of accidents in underground tunnel engineering, such as ground subsidence, sand gushing out, and river water backing up [4].

The risk assessment of the optimisation scheme for urban railway tunnel construction not only provide a more accurate, professional and simplified decision-making basis for the decision-makers of the project, but also help to formulate effective risk countermeasures, and is also conducive to the improvement of the risk management level of urban railway tunnel construction [5]. Therefore, the study of risk assessment algorithms for the construction of urban railway tunnel projects is of great theoretical significance and practical problem-solving significance. Risk assessment algorithm generally includes risk mechanism analysis, risk identification, risk assessment and risk evaluation steps [6]. Risk mechanism is generally analysed from a systematic and professional point of view [7], risk identification is mainly to select and classify the uncertain factors that cause adverse consequences of engineering construction [8], risk assessment is mainly to estimate the identified risks, and risk evaluation is to determine the level of risk through qualitative analysis, quantitative analysis or other methods [9]. The risk assessment research of the tunnel engineering construction optimisation scheme for the city railway mainly includes the tunnel engineering construction risk assessment index system and model construction. The index system research generally adopts SWOT analysis method, flow chart method, cause and effect analysis diagram, work decomposition structure method, accident tree method, etc. [10]. Risk assessment model construction research generally uses fuzzy logic method, grey model, machine learning and other methods [11]. With the development of artificial intelligence technology, risk assessment based on machine learning algorithms has entered the field experts and scholars [12]. Due to the uncertainty, hidden nature and complex structure of the construction risk of the municipal railway tunnel project, which makes the non-linear relationship between the risk assessment indicators and the evaluation level, the machine learning method is not only convenient and effective in constructing the mapping relationship between the risk assessment indicators and the evaluation level, but also improves the efficiency of the risk identification and assessment [13]. Risk assessment methods based on machine learning algorithms for the construction of municipal railway tunnel projects include BP neural networks, support vector machines, decision trees, clustering and other

* Corresponding Author

algorithms [14]. Although the research on construction risk assessment of municipal railway tunnel projects has achieved certain results, research and analysis are still needed in the area of construction risk assessment of cross operation tunnels on top of the pipe. Although the pipe jacking method has been used more often in underground engineering construction, it faces the problem of construction control that threatens the structural safety when the pipe jacking crosses the existing structure [15]. The construction of pipe jacking will cause disturbances such as loading and unloading, changing pore water pressure, and changing stratum compactness to the soil body, destroying the state of stress equilibrium, and in the long term, it will cause deformation of stratum consolidation, which will result in the synergistic deformation of the existing structure and the stratum [16], so it is very meaningful to study the construction risk identification and assessment methods, and the optimal control of the construction risk of the tunnel spanning over the operation of the jacking pipe. Through the domestic and foreign literature research and analysis, there is a certain accumulation of construction risk assessment research for the top tube of urban railway cross operation tunnel, but there are still many problems [17]:

- Less risk research and more construction technology research, and lack of construction overall risk research;
- Lack of reliability of the risk identification process;
- Quantitative analysis of the risk assessment is not in-depth enough;
- Application of the results of the risk assessment is low. The applicability of the results is low.

This paper focuses on the risk assessment of tunnel construction on top of pipe, combines machine learning algorithm and pigeonhole optimisation algorithm, and constructs a risk assessment method based on pigeonhole optimisation algorithm and improved BP neural network. Aiming at the characteristics of the risk assessment problem of tunnel construction above the top tube, a risk assessment scheme for tunnel construction is designed, and the roles of each module of the risk assessment system and its principle are introduced in detail. Combined with the risk assessment scheme and the assessment model construction algorithm, the effectiveness of the risk assessment model is studied and the performance impact of the risk control measures is analysed for the case of the operation tunnel project of Metro Line 9 in the silt stratum of Linping District, Hangzhou City.

II. Design of a Risk Identification and Assessment Programme for Tunnel Construction

A. Programme Design

In order to improve the reliability of the risk identification and assessment method of the construction risk of the pipe jacking up and across the operation tunnel and optimise the feasibility of the risk control scheme, this paper studies the tunnel construction risk identification and assessment scheme using a combination of intelligent optimisation algorithms and machine learning algorithms [18], which is shown in Fig. 1.

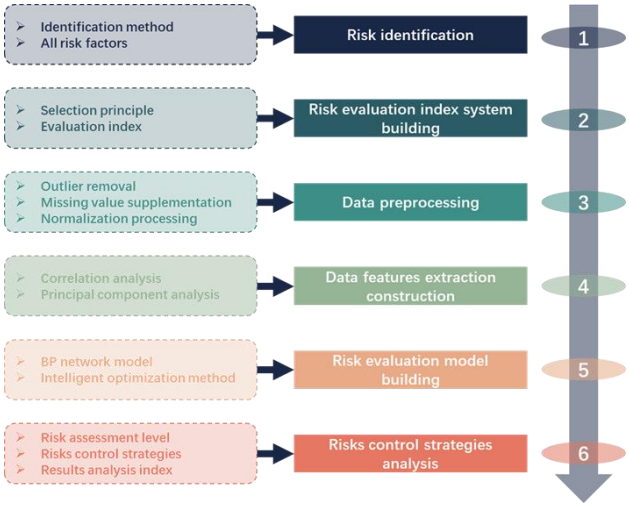


Fig. 1. General scheme of risk assessment for tunnel construction.

From Fig. 1, in the construction risk assessment scheme of the top tube over operation tunnel based on the intelligent optimization algorithm combined with the machine learning algorithm, the mechanism of the analysis of the construction process of the top tube over operation tunnel is analysed, and the sources of risk faced by the construction process are identified by combining with the method of the decomposition structure of the work; in order to further improve the accuracy of the construction risk assessment model of the top tube over operation tunnel, the raw data continue to be pre-processed, and the operations of outliers elimination, missing values supplementation and normalization are carried out. In order to further improve the accuracy of the construction risk assessment model, the raw data are preprocessed, and operations such as outlier removal, missing value supplementation, and normalisation are carried out. In addition, in order to reduce the redundancy of the indicator system and improve the efficiency of the model construction, correlation analysis and dimensionality reduction analysis are carried out for the input indicators; on the basis of the data preprocessing and analysis, the intelligent optimisation algorithm proposed in this paper is combined with the improvement of machine learning algorithm to realise the construction and optimisation of the risk assessment model of the construction of the roof tube above the operating tunnels; According to the risk assessment level and risk probability and control measures, numerical analysis and monitoring analysis are carried out on the proposed deformation control scheme for the construction of roof tube over operation tunnel.

B. Module Analysis

The research on construction risk assessment method of header tube over operation tunnel based on intelligent optimization algorithm and improved machine learning algorithm mainly includes construction risk identification of header tube over operation tunnel, establishment of construction assessment index system of header tube over operation tunnel, processing and analysis of measurement value of header tube over operation tunnel construction risk assessment index, optimization of construction risk assessment model of header tube over operation tunnel and analysis of the results of the risk

control scheme. technical research [19], the specific research composition framework is shown in Fig. 2. In Fig. 2, the construction risk assessment system of top tube over operation tunnel based on intelligent optimization algorithm and improved machine learning algorithm is mainly composed of risk identification, indicator system, risk level, data processing, risk assessment, risk control and other modules in order to accurately and objectively and systematically assess the construction risk of top tube over operation tunnel and deformation control scheme.

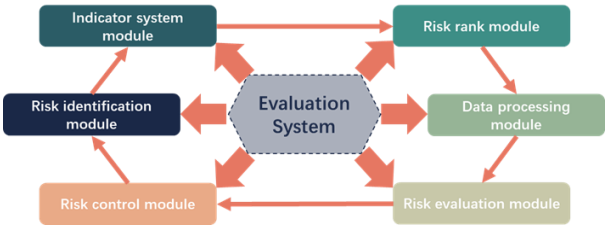


Fig. 2. Risk assessment system building blocks.

1) Risk identification module: The risk identification module identifies and categorises the uncertainties that may cause adverse consequences during the construction of the tunnel, and then screens out the uncertainties that may cause risky accidents. As an important basis for risk management, the risk identification module can determine the impact of different risk factors on the construction of the tunnel above the pipe, and then classify the different risk factors into categories, and the process of line identification is demonstrated in Fig. 3. The inputs of the risk identification module of the construction project of the roof tube over operation tunnel are investigation data analysis, expert consultation, experimental demonstration, and work decomposition structure method, and the outputs are risk code, risk factors, risk events, and risk consequences, and the specific input-output relationship diagram is presented in Fig. 4.

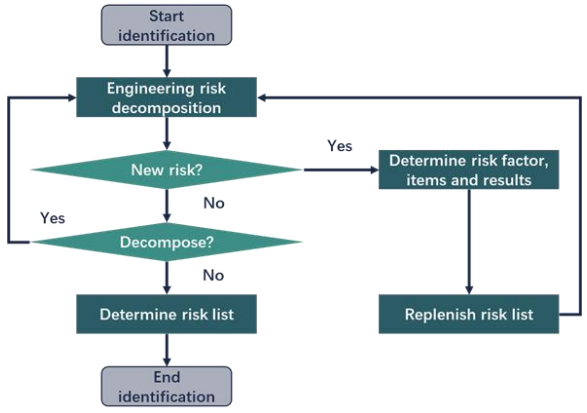


Fig. 3. Risk assessment system building blocks.

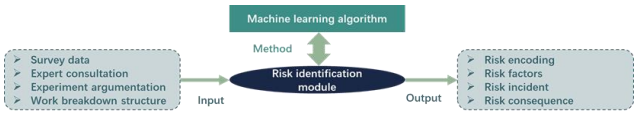


Fig. 4. Risk identification input-output relationship.

2) Indicator system module: When constructing the construction risk assessment index system of the roofed pipe upper span operation tunnel, it is necessary to follow some basic principles, including the principles of systematicity, scientificity, operability, comparability, etc., as shown in Fig. 5.

Fig. 5. Principles for the selection of risk assessment indicators.

On the basis of the identification and classification results of the construction risk of the top tube over operation tunnel, the index system module integrates the field survey and the research of the field research experts, and adopts the methods of quantitative analysis, qualitative analysis, and case study, etc., and constructs the construction risk of the top tube over operation tunnel from the aspects of engineering geological risk A, investigation and design risk B, construction technology risk C, tunnel engineering risk D, management risk E, and environmental factor risk F. Assessment index system, the specific system structure is shown in Fig. 6. As can be seen from Fig. 6, the input of the indicator system module is the selection principle and risk identification results, and the output is the risk assessment indicator system, and the input-output relationship is shown in Fig. 7.

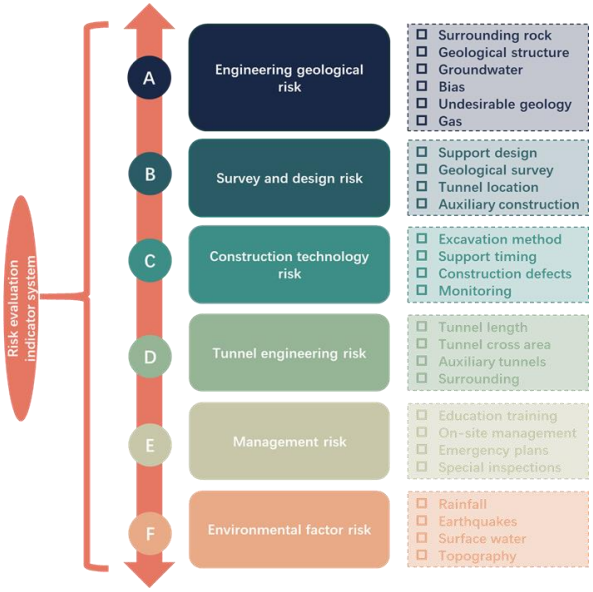


Fig. 6. Risk assessment index system for construction of pipe jacking over operational tunnels.

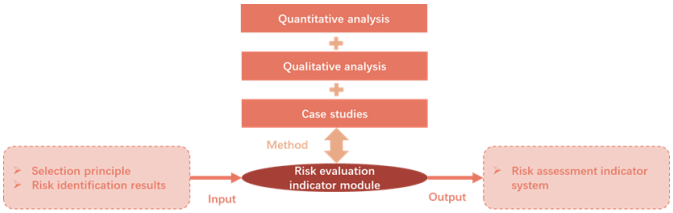


Fig. 7. Principles for the selection of risk assessment indicators.

3) Data processing module: The data processing module includes processes such as outlier removal, missing value supplementation, normalisation, indicator feature correlation analysis, feature dimensionality reduction, etc., as shown in Fig. 8.

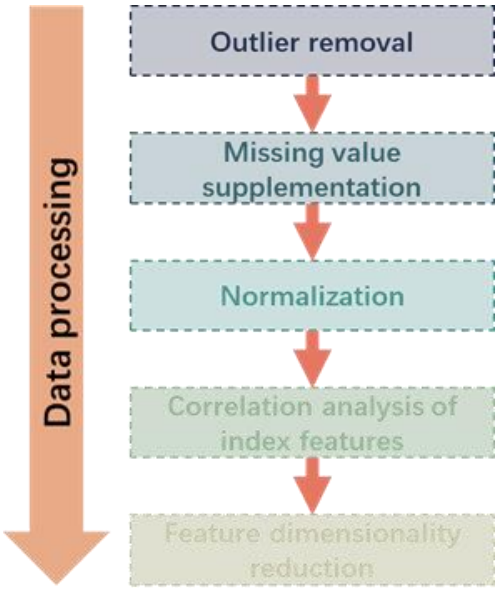


Fig. 8. Data pre-processing flow.

As an important step in data preprocessing, outlier removal removes data points that significantly deviate from other values in the data set. In this paper, we use the outlier processing method based on the 3σ criterion [20], which determines any data point in the data that is outside the range of the mean ± 3 standard deviations as an outlier, and the principle is shown in Fig. 9.

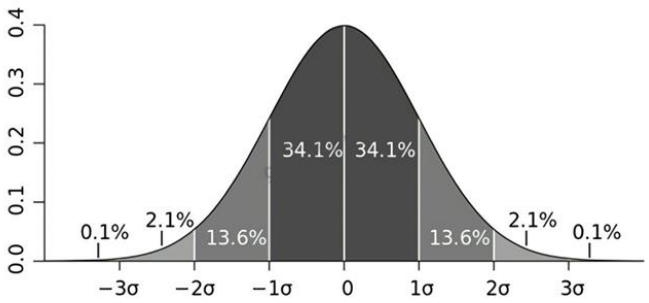


Fig. 9. Outlier rejection algorithm based on 3σ criterion.

In the case of missing data, the missing value supplementation can fill in the data, make the data conform to the pattern, and improve the data quality to improve the performance of the subsequent evaluation model. In this paper, we adopt the proximity filling method, i.e., we use the observations before or after the missing values to fill in the missing values, as shown in Fig. 10.

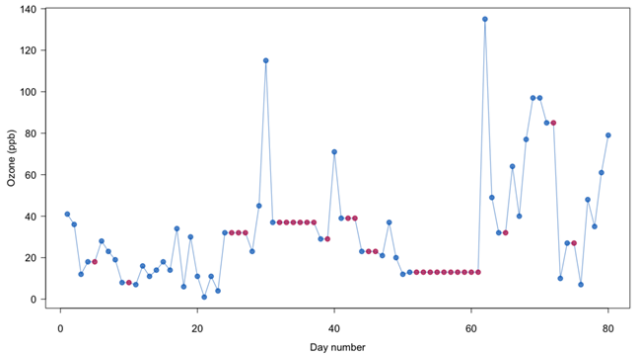


Fig. 10. Algorithm for missing value filling method.

In order to eliminate the variance over the limit brought about by the data magnitude, the normalisation process is to scale the data so that it falls into a small specific interval. For the data characteristics occurring in the construction of the top tube up-span operation tunnel, this paper adopts the *Z*-score normalisation method, i.e., all data are normalised to the range of normal distribution with mean 0 and variance 1, and the calculation formula is as follows Eq. (1):

$$x' = \frac{x - \overline{x}}{\sigma} \tag{1}$$

Where x' denotes the data after normalisation, x is the data before normalisation, $\overline{x}$ is the mean and σ is the standard deviation.

In order to analyse the redundancy of the risk assessment indicators for the construction of the roof-tube up-and-over operational tunnels, Pearson is used in this paper to calculate the correlation coefficients, which are calculated as follows, Eq. (2):

$$\rho(x,y) = \frac{\operatorname{cov}(x,y)}{\sigma(x)\sigma(y)} = \frac{E\left[(x-\mu_x)(y-\mu_y)\right]}{\sigma(x)\sigma(y)} \tag{2}$$

Where $\operatorname{cov}(x,y)$ is the covariance coefficient and $\sigma(x)$ and $\sigma(y)$ are the standard deviations.

In order to reduce the dimensionality of the construction risk assessment indexes of the roof-tube up-and-over operation tunnels and extract the principal components, this paper adopts the Kernel Principal Component Analysis (KPCA) [21] method to extract features and reduce the dimensionality of the input construction risk assessment indexes. The KPCA is an improvement of the Principal Component Analysis (PCA) method, which uses the kernel function to construct complex nonlinear classifiers. The core idea of KPCA is to use the kernel function to map the original data to a high-dimensional feature space, and then perform PCA in that space. The specific principle is shown in Fig. 11.

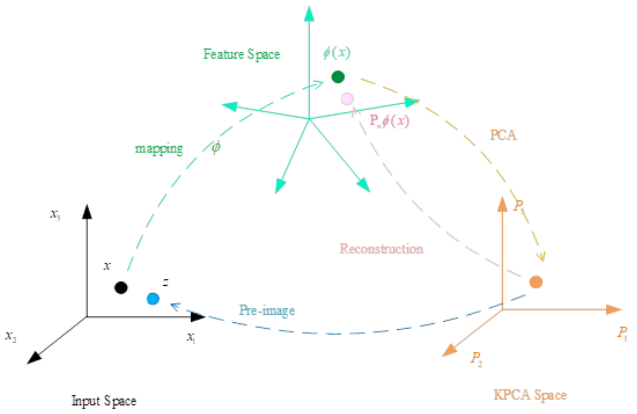


Fig. 11. Principle of KPCA method.

According to the introduction of the principles and mechanisms of the above methodology, the input to the data processing module consists of the original values of the construction risk assessment indicators for the jacked-up cross operational tunnels, and the output is the standardised values of the downgraded assessment indicators.

4) Risk level module: According to the risk assessment index system of the construction risk of pipe jacking up and across the operation tunnel, including engineering geological risk A, investigation and design risk B, construction technology risk C, tunnel engineering risk D, management risk E and environmental factors risk F and other six aspects of the 26 assessment indicators, this paper adopts the AHP to initially determine the weight of the indicators, and the specific process is shown in Fig.12.

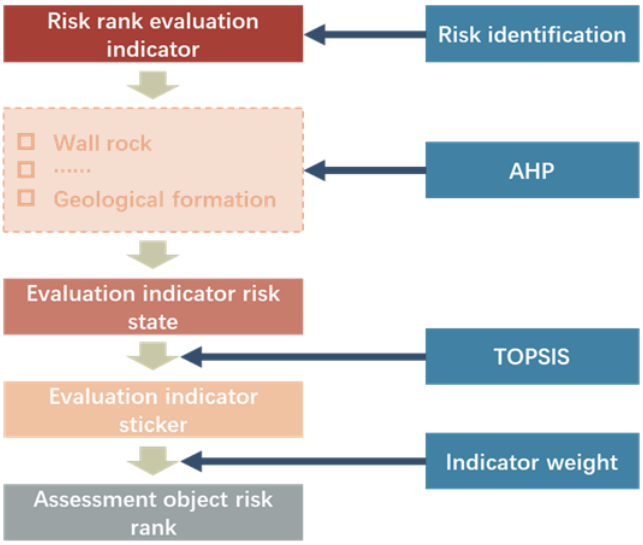


Fig. 12. Flowchart for the initial determination of the overall risk level based on the hierarchical analysis method.

In order to determine the degree of risk impact based on the risk level, so as to determine the risk control strategy, this paper classifies the risk level of the construction of pipe jacking up and across the operation tunnel into five types, which are high risk, higher risk, medium risk, lower risk and low risk, and the scores corresponding to the different risk levels are shown in Table I.

TABLE I. DIFFERENT RISK LEVELS AND CORRESPONDING LEVEL SCORES

Risk level	High	Higher	Moderate	Lower	Low
Score	≥20	15-20	10-15	5-10	0~5

The inputs to the risk level module are the hierarchical analysis method, the indicator system, and the outputs are the classification of the levels and the determination of the level scores.

5) Risk assessment module: According to the risk analysis data of the construction risk of the top tube over the operation tunnel, the machine learning algorithm is used to determine the mapping relationship between the value of the construction risk assessment indexes of the top tube over the operation tunnel and the value of the risk assessment level, so as to construct the risk assessment model of the construction risk of the top tube over the operation tunnel. With the increase of data volume, the machine learning model structure optimisation and parameter optimisation are prone to problems such as premature maturity, falling into local optimum, and slow convergence speed. In order to improve the performance of the machine learning algorithm, an intelligent optimisation algorithm is used to optimise it [22], and the improved paradigm is shown in Fig. 13.

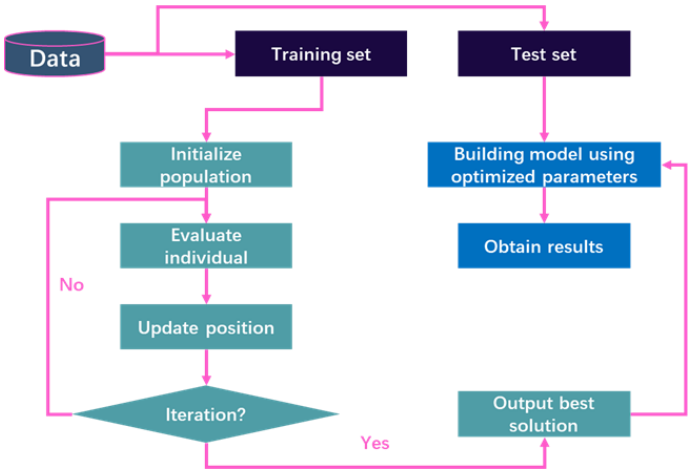


Fig. 13. Machine learning algorithm optimisation.

In Fig. 13, the first step is to determine whether the machine learning algorithm needs to optimise the structural parameters or the control parameters, and the machine learning algorithm chosen in this paper is the BP neural network, so the variables to be optimised are the structural parameters, i.e., the BP neural network weights and biases. According to the initialisation strategy to initialise the BP neural network weights and bias, with the training error as the value of the fitness value function value, the optimisation strategy of the intelligent optimisation algorithm is used, and after iteration, the BP neural network weights and bias with the smallest error are obtained.

The inputs to the risk assessment module are BP neural networks, intelligent optimisation algorithms, risk analysis data for the construction of a roof-tube up and over an operational tunnel, and the outputs are the predicted risk level scores as well as the levels.

6) Risk control module: The risk control module will remove accident risk control measures from engineering geology, construction technology, engineering management and other aspects according to the risk assessment results and risk acceptance criteria. In view of the construction risk problem of pipe jacking up and across operation tunnels, this paper analyses the deformation risk of pipe jacking through operation tunnels, and gives the deformation control method, i.e., the risk control measures are given from the engineering technology level.

III. Improved Machine Learning Algorithms for Risk Assessment Problems

A. Machine Learning Algorithms

Machine learning algorithms are a subfield of artificial intelligence that allow computers to learn from data and improve their performance without the need for explicit programming instructions. These algorithms can be categorised into three types, including supervised learning, unsupervised learning and reinforcement learning, as shown in Fig. 14. Since the problem of risk assessment for the construction of a roofed pipe up and over operational tunnels is a supervised learning problem, machine learning algorithms in the supervised learning category are used in this paper.

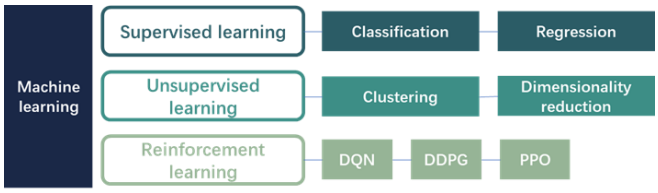


Fig. 14. Machine learning algorithm classification.

Common machine learning algorithms include linear regression, logistic regression, decision trees, random forests, K-nearest neighbours, Bayesian networks, neural networks, support vector machines, and integrated learning [23], as shown in Fig. 15.

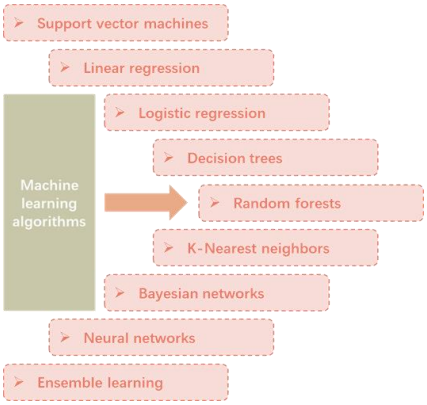


Fig. 15. Types of machine learning algorithms.

B. BP Neural Network

1) Principles and mechanisms: BP neural network [24] consists of three layers: input layer, hidden layer and output layer. W_{mi}, W_{in} The connection weights from the input layer x_m to the hidden layer k_i and the connection weights from the hidden layer k_i to the output layer y_n are represented respectively.

Define the actual output of the network as Eq. (3):

$$\boldsymbol{Y}(s) = (v_N^1, v_N^2, \ldots, v_N^N) \tag{3}$$

Its desired output is Eq. (4):

$$\boldsymbol{d}(s) = (d_1, d_2, \ldots, d_N) \tag{4}$$

a) Positive propagation of the input signal

The output of the m th neuron of layer I can be expressed as Eq. (5):

$$v_M^m(s) = x(s) \tag{5}$$

The inputs u_I^i and outputs v_I^i of the i th neuron of layer H are defined respectively as

$$u_I^i(s) = \sum_{m=1}^{M} w_{mi}(s) v_M^m(s) \tag{6}$$

$$v_I^i(s) = f\left(u_I^i(s)\right) \tag{7}$$

In Eq. (6) and Eq. (7), where $f(\square)$ denotes the H-layer transfer function.

Then the input u_N^n and output v_N^n of the n th neuron of layer O can be expressed as Eq. (8) and Eq. (9):

$$u_N^n(s) = \sum_{n=1}^{N} w_{in}(s) v_I^i(s) \tag{8}$$

$$v_N^n(s) = g\left(u_N^n(s)\right) \tag{9}$$

where $g(\square)$ denotes the output layer transfer function.

Then the overall error of the network can be expressed as Eq. (10):

$$e(s) = \frac{1}{2}\sum_{n=1}^{N} e_n^2(s), e_n(s) = d_n(s) - v_N^n(s) \tag{10}$$

b) Error signal back propagation

When the overall system error is greater than a threshold, the weights need to be adjusted so that the error gradually decreases.

$$w_{in}(s+1) = w_{in}(s) + \Delta w_{in}(s) \tag{11}$$

$$w_{mi}(s+1) = w_{mi}(s) + \Delta w_{mi}(s) \tag{12}$$

In Eq. (11) and Eq. (12), Where, $\Delta w_{in}(s)$ denotes the weight adjustment value of H layer and O layer, and $\Delta w_{mi}(s)$ denotes the weight adjustment value of I and H layers.

2) BP network applications: BP networks are able to mimic the learning and memory mechanisms of the human brain to learn and predict input data.BP networks are widely used in a variety of scenarios [25] due to their ability to learn to train nonlinear mapping laws, including but not limited to:

- BP networks are widely used in the field of pattern recognition;
- BP networks can be used to predict future outcomes or to make optimal decisions, such as in finance for predicting stock prices or developing risk management strategies;
- Train neural networks to control the actions of robots or to optimise production processes to improve efficiency;
- In the field of machine translation, BP networks are used to generate high quality translated texts;
- BP networks also perform very well in the field of speech recognition, such as speech to text and voice command recognition.

3) Problems with BP: Although BP networks have a wide range of applications in many fields, it has some problems and challenges:

- Overfitting the training data leads to performance degradation on the test data;
- The optimisation process may fall into local minima without reaching the global optimal solution;
- In deep networks, gradients may fade away during backpropagation, making it difficult for the network to learn.

C. Pigeon Swarm Optimisation Algorithm

Pigeon-Inspired Optimization (PIO) is a novel population intelligence optimization algorithm [26], which is inspired by the autonomous homing behaviour of domestic pigeons in nature. This algorithm is mainly implemented by map and compass operators and landmark operators to update the position and velocity of pigeon flocks, so as to simulate the homing behaviour of domestic pigeons and find the optimal solution.

4) Algorithmic principles

a) Map and compass calculator: In the flock optimisation algorithm, map and compass operators are used to model the behaviour of domestic pigeons that use the geomagnetic field to determine the approximate direction. The velocity and position of each pigeon is updated based on the previous generation's velocity and current optimal position, as shown in Fig. 16. Specifically, the equations for updating the pigeon's velocity is as follows Eq. (13) and Eq. (14):

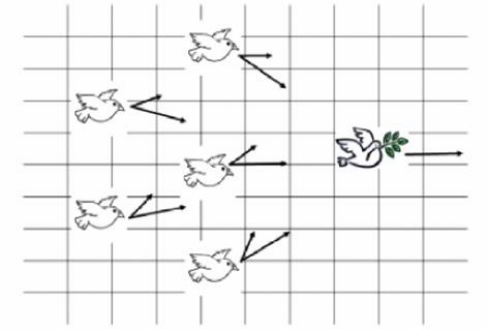


Fig. 16. Map core guide operator.

$$V_i^t = V_i^{t-1} e^{-R \times t} + rand \cdot \left(X_{gbest} - X_i^{t-1} \right) \quad (13)$$

$$X_i^t = X_i^{t-1} + V_i^t \quad (14)$$

Where X_i^t denotes the position information of the i^{th} individual of the flock in the tth iteration, V_i^t denotes the individual velocity information, X_{gbest} denotes the optimal individual position, R denotes the map kernel compass factor, and $rand$ is a random number. When the number of iterations reaches a certain number of iterations, the execution of the map and compass operator stops and enters the landmark operator.

5) Pseudo-code and flowchart: According to the basic principle and optimisation strategy of the pigeon flocking optimisation algorithm, the flowchart of the pigeon flocking optimisation algorithm is shown in Fig. 17 respectively.

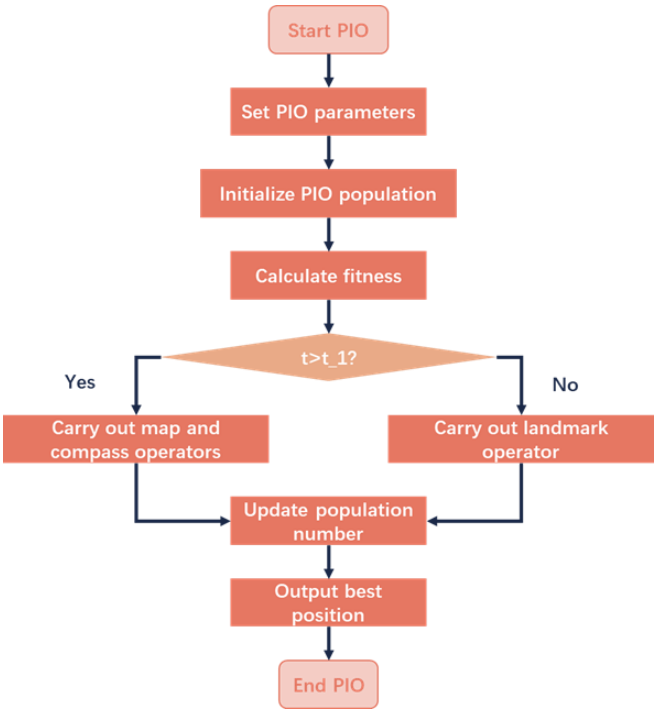


Fig. 17. Flowchart of the PIO algorithm.

D. PIO-BP Neural Network

In this paper, we use real number coding to encode the BP hidden layer weight values and hidden layer bias with the coding dimension of $(m_1 \times l_1 + l_1) + (m_2 \times l_2 + l_2)$, and also use MAE as the adaptation function Eq. (19):

$$MAE = \frac{1}{M}\sum_{i=1}^{M}|\hat{y}_i - y_i| \quad (19)$$

Where, $\hat{y}_i$ denotes the predicted value based on the proposed algorithm, y_i denotes the true value and M is the number of test samples.

The steps of the PIO-BP neural network prediction method (Fig. 18) are as follows:

- PIO algorithm encodes the initial parameters;
- Calculates the value of the fitness function;
- Updates the position and speed of the PIO population by using the map and compass operator and landmark operator;
- Calculates the value of the fitness function and updates the global optimal solution;
- Determines whether or not the termination conditions are satisfied;
- Decodes the PIO algorithm-optimised BP network structure parameters;
- Constructing a tunnel construction risk assessment model based on PIO-BP neural network.

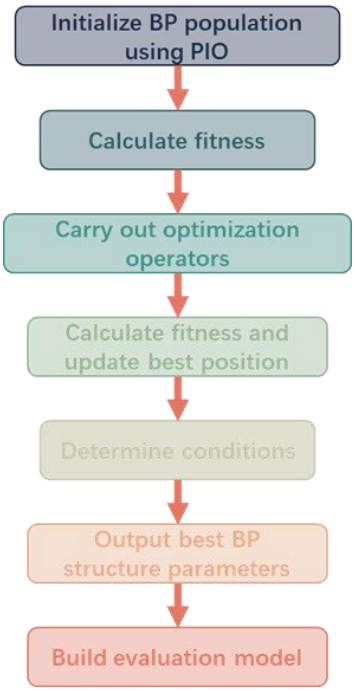


Fig. 18. Tunnel construction risk assessment based on PIO-BP neural network.

- Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as “3.5-inch disk drive”.
- Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
- Do not mix complete spellings and abbreviations of units: “Wb/m^2” or “webers per square meter”, not “webers/m^2”. Spell out units when they appear in text: “. . . a few henries”, not “. . . a few H”.
- Use a zero before decimal points: “0.25”, not “.25”. Use “cm^3”, not “cc”. (*bullet list*)

IV. Algorithmic Applications

In order to verify the performance of the risk assessment algorithm for the construction engineering of the city railway tunnel project, this paper relies on the construction risk analysis of the tunnel of Xinfeng Road underground passage close to the upper crossing of Metro Line 9 in Hangzhou and the side penetration of Hanghai Intercity Tunnel Project, constructs the risk assessment model, and puts forward the effective risk control measures.

A. Project Description

Xinfeng Road Underpass in Linping District, Hangzhou is located in the north side of the intersection of Xinfeng Road and Wenzheng Street in Linping District, and there are many existing structures within the new construction scope. The channel passes through Xinfeng Road, the main road (roof pipe depth 2.3m), and close to cross (roof pipe and tunnel structure minimum vertical clearance 2.5m) existing operation Hangzhou Metro Line 9, Yuhang high-speed rail station ~ Nanyuan station interval two-line tunnel, and parallel side through (roof pipe and tunnel horizontal clearance 15.6m) existing Hanghai intercity two-line tunnel. The total length of the underpass is 136.5m, which is constructed by pipe jacking method and open cut method, of which the starting shaft and receiving shaft open cut section are 34.9m and 26.6m long respectively, with the depth of the shaft being about 8~9m. The crossing section of the underpass is constructed by pipe jacking method from west to east, with a length of 75m. the standard rectangle pipe jacking section is adopted, with the internal dimensions of 6.0m×3.3m, the wall thickness of the jacking pipe is 0.45m, and the length of the pipe section is 1.5m, and the socket joint is adopted. The length of the pipe section is 1.5m, and the socket joints are adopted.

B. Construction Risk Assessment

For the factors that may lead to excessive deformation of the existing tunnel during the jacking construction process of the pipe jacking section, the main focus is on the silt layer and the close proximity through the existing tunnel in two aspects: (1) the project is located in the silt layer, with high compressibility, high sensitivity and thixotropy, poor engineering properties, and unfavourable control of deformation of the ground layer

disturbed by the construction. At the same time belongs to the low to medium permeability stratum, and this project is adjacent to East Lake, rich groundwater recharge, strata water content is large, jacking process is prone to groundwater gushing, resulting in over-excavation of tunnels and triggering the risk of construction safety; (2) jacking pipe with a vertical clearance of 2.5m through the operating tunnel in the vicinity of the top, jacking process in the front of the strata by the construction of the influence of the stress of the disturbance is serious, resulting in the unloading of the lower part of the front disturbed area as well as the pipe section of the ground below shear disturbance zone During the jacking process, the ground strata in front is severely disturbed by the impact of the application, which causes the unloading disturbance zone in front and the shear disturbance zone in the lower part of the pipe section to be relaxed, and the structure of the operating tunnel in the lower part of the pipe section is uplifted along with the surrounding strata, which has a great impact on the deformation of the existing tunnel before and after jacking. At the same time, the soil cover above the jacking tube is shallow, only 2.3m, and the jacking has a strong influence on the deformation of the ground surface, and the deformation effect of the shallow soil cover will increase the deformation of the tunnel in the unprotected condition.

Aiming at the above key risks, this paper carries out construction risk assessment from engineering geological risk A, investigation and design risk B, construction technology risk C, tunnelling risk D, management risk E and environmental factor risk F. Risk assessment indexes of the six aspects are taken as inputs, and risk level score values are taken as outputs, where the risk index values need to be extracted by downscaling features. According to the risk level score value, the risk level is obtained by combining the correspondence between the risk assessment value and the level grade in the risk level module.

C. Risk Control Programme

The deformation control of pipe jacking through operational tunnels includes deformation monitoring control and factor-specific control. Deformation monitoring and control includes the development of deformation control standards and automated monitoring measures; factor-specific control includes MJS portal-type ground reinforcement measures for the chalky sand stratum close to the underpass and surface hardening measures for shallow overburden.

Standard measures for deformation control were developed as shown in Table II.

TABLE II. DEFORMATION CONTROL STANDARDISATION

Structural safety control indicator control values	metric
Horizontal displacement (mm)	<5
Vertical displacement (mm)	<5
Relative convergence (mm)	<5
Differential settlement at station and zone junction (mm)	<5
Radius of deformation curvature (m)	>15000
relative curvature of deformation	<1/2500
Tube sheet seam opening (mm)	<1
Additional load on outer wall (kPa)	≤10
Crack width (mm)	≤0.1
Contact net guide height (mm)	<20
Roadbed and track displacement (mm)	<5

Aiming at the characteristics of large compressibility, poor engineering properties and large water content of the silt layer, and the large influence of groundwater on the slagging process of the pipe jacking and the stability of the thixotropic mud on the outside of the pipe joints, the all-around high-pressure rotary injection grouting method (MJS) is adopted in the silt layer crossed by the pipe jacking to carry out gated reinforcement in advance in the area of the pipe jacking crossing over the operation tunnel.

V. EXPERIMENTAL ANALYSIS

A. Experimental Set-Up

In order to verify the effectiveness of the risk assessment algorithm for tunnel construction proposed in this paper and the feasibility of taking risk control measures, this paper takes the data of the project of Hangzhou Xinfeng Road underground passage close to crossing the metro line 9 tunnel and side through Hanghai intercity tunnel as the data for analysis, and selects SVM, Decision Tree, and BP as the comparative algorithms of the analysis and assessment algorithms of the PIO-BP neural network, and at the same time analyses the risk control measures from the on-site monitoring and numerical simulation. Two aspects of risk control measures are analysed.

The algorithm setup is shown in Table III. The algorithm used in this paper is PIO-BP neural network and the comparison algorithms are SVM, Decision Tree and BP neural network.

TABLE III. PARAMETER SETTINGS FOR THE COMPARATIVE RISK ASSESSMENT ALGORITHM

Arithmetic	Parameterisation
Support Vector Machine (SVM)	C=100,σ=0.1
Decision Tree	The maximum number of divisions is 4
BP neural network	Hidden layer node is 50, activation function is radial basis function
PIO-BP neural network	Hidden layer nodes are 50, activation function is radial basis function, population size is 50, maximum number of iterations is 100

The experimental simulation environment is Windows 10, the risk assessment algorithm programming language Python 3.7, and the Midas GTS finite element software is used for the risk control measures.

The experimental finite element calculation model for numerical analysis of risk control measures is shown in Fig. 19. *x* is the direction of pipe jacking and *z* is the direction of model elevation. The relevant calculation parameters of each soil layer are shown in Table IV The pipe jacking sheet and tunnel structure, station wall panel structure, enclosure structure and support adopt linear elastic principal structure, and the values of structural parameters are shown in Table V.

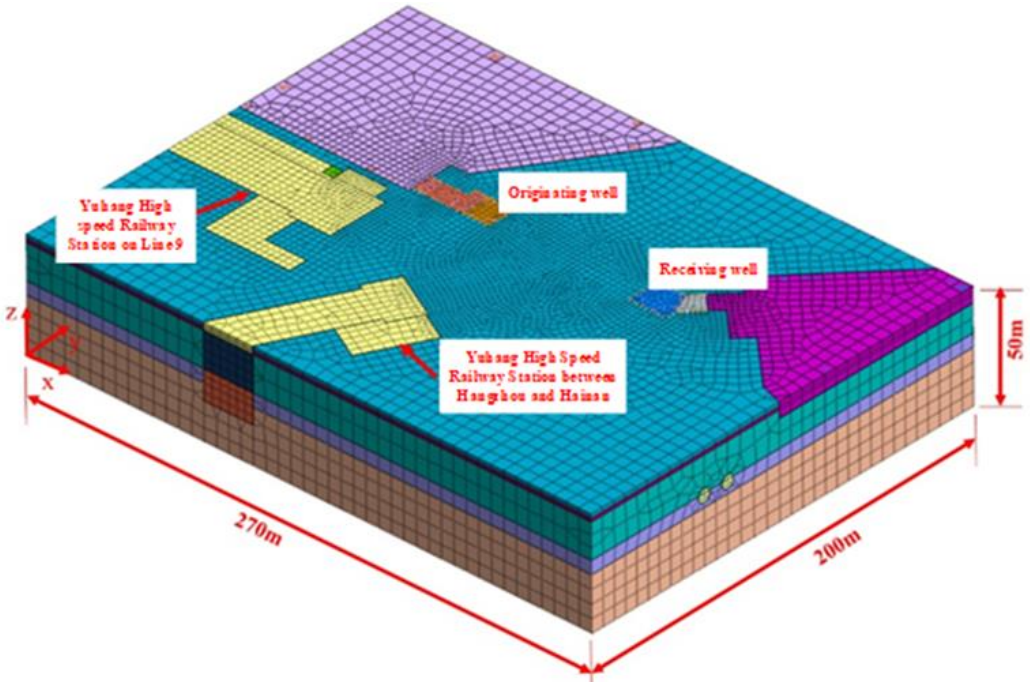


Fig. 19. Schematic diagram of finite element calculation model.

TABLE IV. CALCULATED PARAMETERS FOR SOIL LAYERS

Stratigraphic name	Triaxial loading stiffness E_{50} (MPa)	Triaxial unloading stiffness E_{ur} (MPa)	Consolidator loading stiffness E_{ord} (MPa)	Initial small strain modulus G_0 (MPa)	Modulus stress related power index(m)	Shear strain level $\gamma^{0.7}$
miscellaneous fillings	3.0	15.0	3.0	50.0	0.5	1.0×10^{-4}
clayey silt	7.0	28.0	7.0	112.0	0.5	2.0×10^{-4}
sandy silt	8.5	34.0	8.5	136.0	0.5	2.0×10^{-4}
silt sand	10.0	40.0	10.0	160.0	0.5	2.0×10^{-4}
clays	6.5	27.0	5.4	108.0	0.7	2.0×10^{-4}

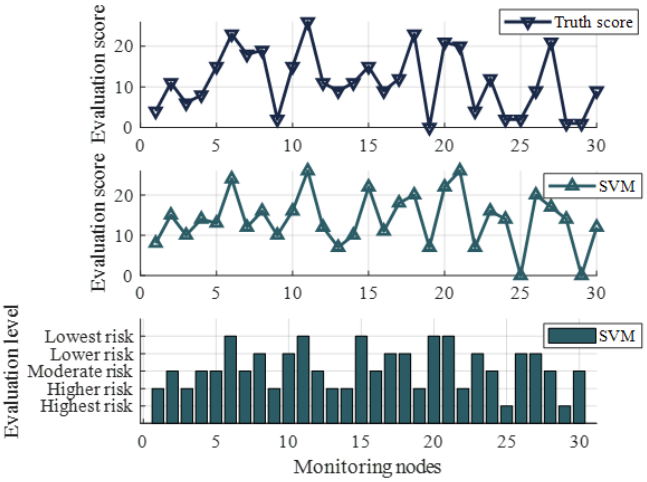
TABLE V. STRUCTURAL CALCULATION PARAMETERS

Typology	Serious $(kN/m)^3$	Modulus of elasticity (Mpa)	Poisson's ratio	Cohesion(kPa)	Angle of internal friction(°)
MJS plus solids	18.0	400	0.2	1000	23
pipe jacking slice	25.0	34500	0.25	-	-
shield	25.0	34500	0.25	-	-
Station wall panels, enclosures and internal supports	24.0	30000	0.2	-	-
steel support	78.0	200000	0.2	-	-

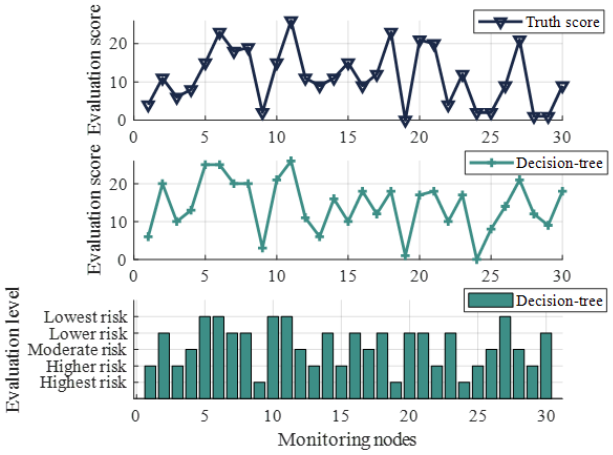
B. Analysis of Evaluation Test Results

In order to verify the effectiveness of the PIO-BP neural network based risk assessment algorithm for tunnel construction, this subsection compares the performance of SVM, Decision-tree, BP, and PIO-BP methods using a test set.

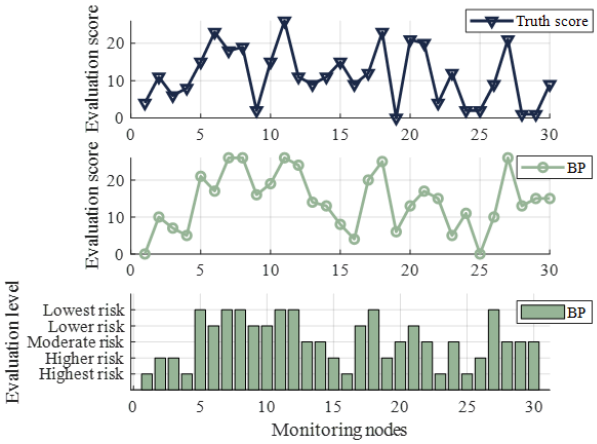
The results of risk assessment of 26 monitoring sections in tunnel construction based on different algorithms are given in Fig. 20. As can be seen from Fig. 20(a) – Fig. 20(d), the accuracy of the risk assessment algorithm of the PIO algorithm optimised BP neural network is better than the other algorithms. The statistical results show that the risk assessment model based on the PIO-BP algorithm is closer to the real value of the test set data than the assessment results of other modelling methods, which demonstrates the high assessment accuracy of the model.



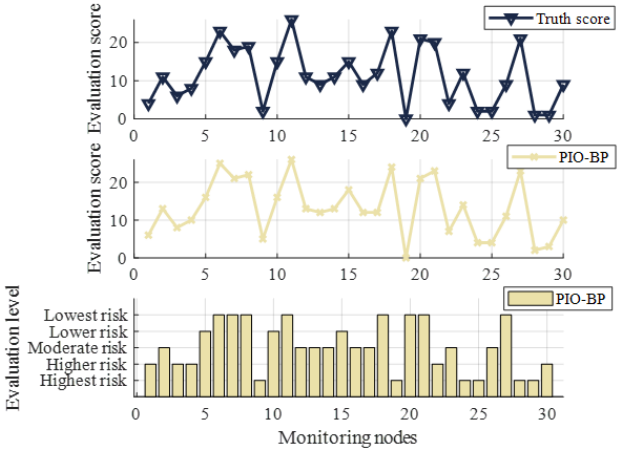
(a) SVM



(b) Decision-tree



(c) BP

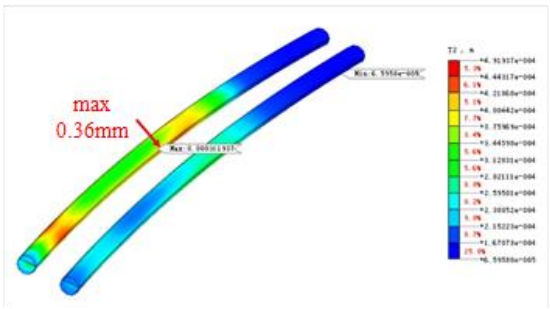


(d) PIO-BP

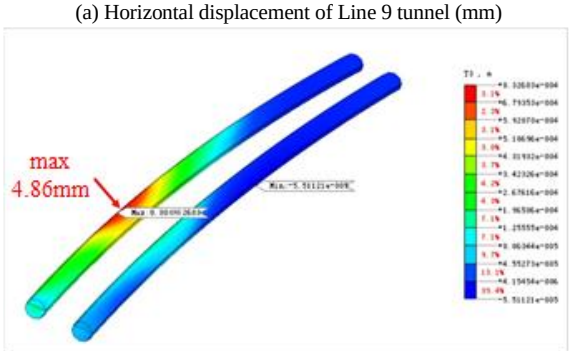
Fig. 20. Test results of different risk assessment model algorithms.

C. Analysis of the Results of the Testing of Risk Control Measures

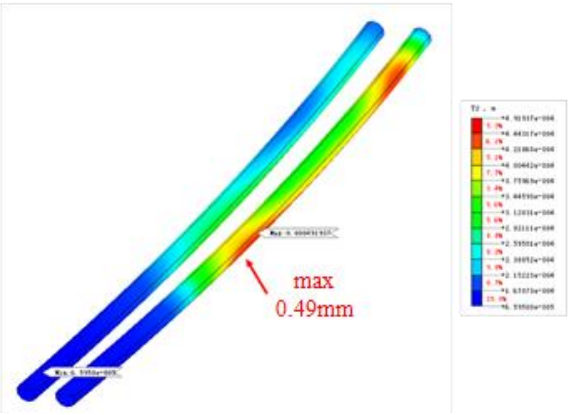
6) Tunnel structural displacement: The software is used to simulate the pipe jacking construction, and the calculation results after the advancement of the pipe jacking in the characteristic working condition are shown in Fig. 21. It can be seen from Fig. 21 that the deformation values of the two operating tunnels satisfy the control requirement of 5mm. The difference settlement at the junction between the tunnel section and the station is small.



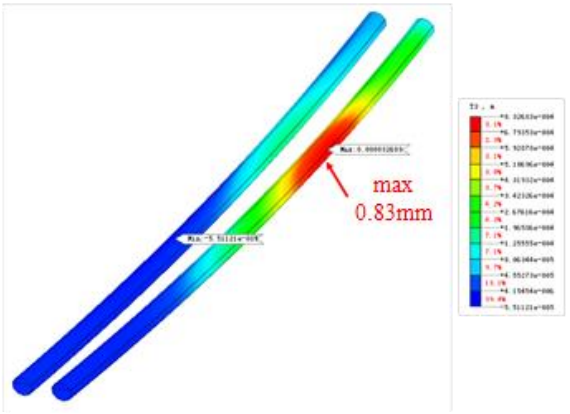
(a) Horizontal displacement of Line 9 tunnel (mm)



(b) Vertical displacement of Line 9 tunnel (mm)



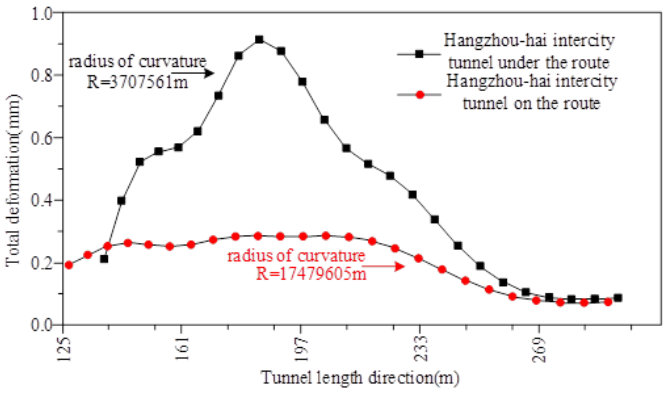
(c) Horizontal displacement of intercity tunnels (mm)



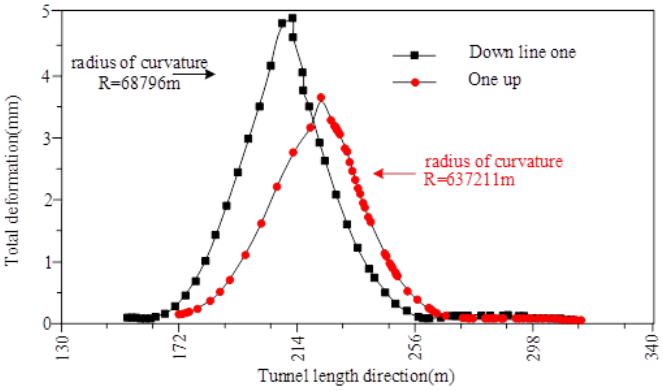
(d) Vertical displacement of intercity tunnels (mm)

Fig. 21. Pipe jacking to complete the upper span construction results.

7) Tunnel structural curvature: According to the maximum deformation results of the two tunnels, the additional radius of curvature of the tunnels caused by the jacking is calculated, and the results are shown in Fig. 22. It can be seen that the additional radius of curvature of the two operation tunnels caused by the jacking construction is much larger than the control requirements of 15,000m, which meets the requirements, and the jacking pipe is directly above the close up penetration of the structural deformation of the operation tunnels is more influential.



(a) Line 9 underground tunnel



(b) Hang Hai Intercity Tunnel

Fig. 22. Additional radius of curvature of operational tunnels.

VI. Conclusion

The research successfully develops a risk assessment algorithm based on a combination of machine learning technology and pigeon-inspired optimization (PIO) algorithm to address the construction risks associated with urban railway tunnel projects. This PIO-BP neural network-based risk assessment model effectively identifies and assesses risks, leading to improved prediction accuracy. The study also provides a corresponding risk control scheme, which has been validated using monitoring data and numerical models, confirming the feasibility of the proposed risk assessment and control measures. The algorithm and approach provide a solid foundation for risk management in complex urban railway tunnel projects.

While acknowledging the contributions of this study, there are three key limitations that cannot be overlooked: Firstly，the risk identification process primarily relies on expert consultations and qualitative analysis, lacking quantitative automation support, which may impact the comprehensiveness and accuracy of risk identification. Then, while machine learning algorithms improve accuracy, the risk assessment indicator system could benefit from deeper quantitative analysis, leveraging big data technologies to enhance the granularity of risk predictions. Finally, the proposed risk assessment model is validated on specific projects but lacks clarity on its adaptability under different geological and environmental conditions, limiting its feasibility for broader applications.

References

[1] Song M , Yang D , Ramu A G , Choi D. An onsite risk assessment of water quality and heavy metal contamination in Kandal Kampong Speu and Kampong Chhnang Province of Cambodia[J].Chemical Papers, 2024, 78(7):4239-4247.

[2] Zhao D , Wu Q , Zeng Y ,Zhang J, Mei A, Zhang X. Contamination and human health risk assessment of heavy metal(loid)s in topsoil and groundwater around mining and dressing factories in Chifeng,North China[J]. International Journal of Coal Science and Technology:English Edition, 2023, 10(1):33-47.

[3] Sevin S , Tutun H , Yipel M , Alu Y, Hüsamettin E. Concentration of essential and non-essential elements and carcinogenic / non-carcinogenic health risk assessment of commercial bee pollens from Turkey[J].Journal of trace elements in medicine and biology : organ of the Society for Minerals and Trace Journal of trace elements in medicine and biology : organ of the Society for Minerals and Trace (GMS), 2023, 75:127104.

[4] Wu S , Dong H , Zhang L .Formation Characteristics and Risk Assessment of Disinfection By- Products in Drinking Water in Two of China's Largest Basins. Yangtze River Basin Versus Yellow River Basin[J].ACS ES&T Water, 2024(1):4.

[5] Zhang J , Guan Y , Lin Q , Wang Y, Wu B, Liu X. Spatiotemporal Differences and Ecological Risk Assessment of Heavy Metal Pollution of Roadside Plant Leaves in Baoji City, China[J].Sustainability, 2022, 14.

[6] Tuncel S , Oskouei M Z , Seker A A .Risk assessment of renewable energy and multi-carrier energy storage integrated distribution systems[J]. International journal of energy research, 2022.

[7] Pan W .Research on power system risk assessment considering large-scale wind and solar access[J].Journal of Physics: Conference Series, 2022, 2215 (1):012024-.

[8] Yu J , Hou J , Xu Z .Dissipation behaviour and dietary risk assessment of cyclaniliprole and its metabolite in cabbage under field conditions[J]. Environmental Science and Pollution Research, 2023(60):30.

[9] Zhou A , Yu S , Deng S .Enrichment characteristics and environmental risk assessment of heavy metals in municipal sludge pyrolysis biochar[J]. Journal of the Energy Institute, 2023:111.

[10] Arjhan W , Thephamongkhol K , Setakornnukul J , Samarnthai N, Pisarnturakit P. 99P Development of a risk assessment and prediction model for DCIS recurrence: insights from analysis of 600 patients[J].ESMO Open, 2024, 9.

[11] Donthamsetty S , Forreryd A , Sterchele P , Huang X, Gradin R, Johansson H.GARDskin dose-response assay and its application in conducting Quantitative Risk Assessment (QRA) for fragrance materials using a Next Generation Risk Assessment (NGRA) framework[J].Regulatory Toxicology and Pharmacology, 2024, 149.

[12] Sarwar M , Gulzar W , Ashraf S .Improved risk assessment model based on rough integrated clouds and ELECTRE-II method: an application to intelligent manufacturing process[J].Granular Computing, 2023(6):8.

[13] Ferreira S L C , Porto I S A , Dantas S V A , Felix C S A, Cunha F A S, Junior J B P. Evaluation of contamination of chemical elements in fish samples using human health risk assessment indices[J].Microchemical Journal, 2024, 202.

[14] Rhouma M , Gaucher M L , Badredine S , Bekal S, Sanders P. Food risk assessment in the farm-to-table continuum: report from the conference on good hygiene practices to ensure food safety[J].Agriculture & Food Security, 2024, 13(1).

[15] ZHANG Qinghe, ZHU Zhonglong, YANG Junlong, ZHU Jiwen. Theoretical analysis and experimental study on soil disturbance caused by shield propulsion[J]. Journal of Rock Mechanics and Engineering,1999,(06):699-703.

[16] Lin Hangchen. Development and prospect of China's tunnelling and underground engineering technology[J]. Construction Technology Development,2020,47(03):107-108.

[17] Fekri M , Nikoukar J , Gharehpetian G B .Vulnerability risk assessment of electrical energy transmission systems with the approach of identifying the initial events of cascading failures[J].Electric Power Systems Research, 2023(Jul.):220.

[18] Bouchagiar G .Risk Assessment Technologies ('RATs') in Criminal Justice: Time to Recognise the Legal Status of RATs?[J].SSRN Electronic Journal, 2023.

[19] Halder P , Jeer G , Nongkynrih B .Risk assessment of type 2 diabetes mellitus using Indian diabetes risk score among females aged 30 years and above in urban Delhi[J].Indian Journal of Medical Sciences, 2023.

[20] SHAO-MING XU, YU LI, QING-LONG YUAN. A combinatorial pruning method based on reinforcement learning and 3σ criterion[J]. Journal of Zhejiang University (Engineering Edition),2023,57(03):486-494.

[21] P. Zhao,Y. Hong. Chemical process fault detection based on improved dynamic kernel principal element analysis algorithm[J]. Chemical Automation and Instrumentation,2024,51(03):403-409.

[22] Chen Yinwei, Wang Anqi, Li Fengsen. Application of population intelligence optimisation algorithm in medical field[J]. Chinese Journal of Medical Physics,2024,41(05):646-656.

[23] FU Yonghao, LI Weipo, ZHANG Aijun. Application of object-oriented and integrated learning algorithms in remote sensing estimation of forest stock[J]. Journal of Northeast Forestry University,2024,52(06):64-69+78.

[24] WANG Tianqi, MENG Kaiquan, WANG Chuanrui. Prediction and optimisation of multi-layer multi-pass welding process based on GA-BP neural network[J]. Journal of Welding,2024,45(05):29-37.

[25] LU Lei, YU Xinyu, RONG Ziqi. Electricity prediction and tariff scheme analysis based on BP neural network[J]. Low Carbon World,2024,14(05):109-111.

[26] Duan Haibin,Ye Fei. Research progress of pigeon flock optimisation algorithm[J]. Journal of Beijing Institute of Technology,2017,43(01):1-7.

A Data-Driven Deep Machine Learning Approach for Tunnel Deformation Risk Assessment

Fusheng Liu
China Railway Siyuan Survey and Design Group Co., LTD. Hangzhou 310000, Zhejiang, China

Abstract*—The shallow overburden pipe jacking over operation tunnel construction project in chalk stratum has the risk of deformation of the soil layer and the existing tunnel, which increases the difficulty of pipe jacking over construction, and the risk assessment and control become the key technology for the safe and successful completion of the construction. Aiming at the problems of the current deformation risk assessment and control method, such as the assessment system is not comprehensive, systematic and objective enough, the prediction accuracy is not efficient enough, and there is a lack of quantitative analysis, etc., a deformation risk assessment and control method is proposed to combine the heuristic optimization algorithm of human behaviour and deep machine learning algorithm for pipe jacking up to and across operation tunnels on shallow overburden of chalky sand stratum. Firstly, by analyzing the construction process of pipe jacking tunnel, the deformation risk factors of the construction process and the deformation risk control scheme are given; then, a deformation risk assessment and control algorithm with improved deep limit learning machine is proposed by combining human heuristic optimization algorithm; finally, the proposed deformation assessment and control model is applied to the deformation risk assessment and control problem of pipe jacking over operation tunnel on shallow overburden of pulverised sand stratum, and a finite element computational model is used to construct the data. Finally, the proposed deformation assessment and control model is applied to the problem of deformation risk assessment and control in a tunnel with shallow overburden in chalky sand stratum by using finite element computational model to construct the data set, training the deformation risk assessment and control model, and using the monitoring data as the test set to validate the validity of the proposed model algorithm, and solving the problem of the poor prediction accuracy of the control algorithm for deformation risk assessment and control of a tunnel with shallow overburden in a tunnel with shallow overburden in chalky sand stratum.

Keywords*—Pipe jacking up and over operational tunnel construction; tunnel deformation risk assessment; deep limit learning machine; hybrid leader optimisation algorithm; control strategy

I. INTRODUCTION

Due to the rapid development of economic technology and science and technology, the urbanisation process in China has been increasing, which has led to many problems in cities, such as traffic congestion, environmental pollution, population increase, and huge energy depletion [1]. In order to alleviate the increasingly serious pressure on urban space, the construction and development of underground space has gradually become an important way for major cities to solve the problems arising from urbanisation [2]. The construction of urban underground space includes the construction of underground tunnels, and its construction methods mainly include shield method and pipe jacking method, two urban tunnel construction methods [3]. The pipe jacking tunnel construction method, as a kind of no-excavation construction technology, achieves the construction of tunnels by setting up work shafts on the ground, and then using pipe jacking machines to push the pipeline or tunnel structure from one work shaft to another work shaft [4]. The pipe jacking tunnel construction technology has the characteristics of reducing damage to the surrounding environment, ensuring construction safety, fast construction speed, controllable quality and strong adaptability [5]. Although there are many advantages in the process of jacking tunnel construction, it is still affected by the geological environment, nearby buildings and other influences, and there is the phenomenon of frequent accidents in underground tunnel engineering, such as ground subsidence, sand and soil gushing out, and river water backing up and other problems [6]. Therefore, it is of great practical significance to study the comprehensive and systematic quantitative risk assessment and control method of tunnel deformation during the construction of pipe jacking tunnels.

Accurate and effective risk assessment methods for deformation of tunnel operating in jacked tube construction not only improve the safety of jacked tube tunnel construction, but also improve the risk management level of tunnel engineering construction [7]. Risk assessment generally includes the steps of risk mechanism analysis, risk identification, risk assessment and risk control [6]. The deformation risk assessment of roof-tube construction and operation tunnel is to analyse and identify the risk factors of roof-span jacking construction in the process of roof-tube top-span operation tunnel construction, use the risk assessment model to construct the complex law relationship between the tunnel deformation risk indexes and the value of the control strategy, and obtain the deformation control strategy of the roof-tube construction and operation tunnel based on the specific deformation situation of the tunnel [7]. Risk assessment algorithm, as one of the key technologies for deformation risk assessment of top tube over spanning operation tunnels, should not only analyse the risk of tunnel changes in the construction process from the perspective of top tube over spanning operation tunnels, but also put forward risk assessment algorithms that can describe the law according to the specificity of the problem. Currently, the research on the top tube over operational tunnels mainly focuses on the deformation of the soil layer around the top tube method and the deformation of the existing tunnel structure, and usually adopts the empirical formula method [8], the theoretical analysis method [9], and the finite element analysis method [10], etc. Literature [8] has shown that the deformation of the soil layer around the top tube method and the deformation of the tunnel structure is the main cause of the risk

of tunnel changes during the construction process; Literature in [9] used random medium method and peck formula method to analyse the difference of surface settlement caused by pipe jacking construction; Literature in [10] for the problem of rectangular pipe jacking construction of large cross-section, the use of finite element software to analyse the disturbance of the soil body, and at the same time put forward the relevant construction control scheme. For the problem of risk assessment model construction, the current more popular assessment algorithms include fuzzy logic method, grey model, machine learning and other methods [11]. Due to the deformation of the top tube over operation tunnel is affected by the uncertainty and complexity of the construction risk, and at the same time, there is a nonlinear relationship between the deformation risk and the control strategy, the deformation risk assessment method of the top tube over operation tunnel based on machine learning algorithms can use the data to quickly construct an accurate model, which is paid special attention to by experts in the field, and has also become one of the directions of the development of the deformation risk intelligent analysis of the top tube construction and operation tunnel [12]. Risk assessment methods based on machine learning algorithms include BP neural networks, support vector machines, decision trees, clustering and other algorithms [13]. Although the research on deformation risk assessment algorithms for roof-tube up-and-over operation tunnels has achieved certain qualitative theoretical results, there are still some problems [14]: 1) the identification of deformation risk of roof-tube up-and-over operation tunnels is not comprehensive and systematic enough; 2) the quantitative research on the deformation control strategy of roof-tube up-and-over operation tunnels is relatively small; and 3) the precision of the deformation risk assessment model needs to be improved.

For groundwater-rich chalk strata, pipe jacking is prone to the risk of over-excavation due to gushing, which affects the stability of the surrounding strata. Compared with general clay and weathered rock strata, there are fewer construction practices in the engineering community for pipe jacking across highly sensitive soils such as chalk strata, and there is a lack of deformation control measures for existing structures that are compatible with such strata [15]. In order to analyse the deformation risk mechanism of pipe jacking across operational tunnels in shallow overburden in chalky sand strata and to quantify the precise deformation risk control measures, machine learning algorithms are used to construct a deformation risk assessment and control model for pipe jacking across operational tunnels in shallow overburden in chalky sand strata.

In order to solve the problems of deformation risk assessment and control method of pipe jacking over operation tunnel, this paper proposes a risk assessment and control method based on hybrid leader optimisation algorithm to improve the depth limit learning machine. In view of the deformation risk problem of shallow overburden pipe jacking over operation tunnel in chalk stratum, the deformation risk mechanism is analysed, and the deformation risk factors and control indexes in the construction process are introduced; in view of the deformation risk assessment and control problem of the tunnel, the hybrid leader optimization algorithm is used to optimize the network of the deep limit learning machine, and the proposed general application is applied to the specific problems. The effectiveness and robustness of the proposed algorithm is verified by analysing the structural numerical simulation data with the case of a close-range up-span underground operation tunnel in chalky sand formation.

The paper's framework begins with an analysis of the deformation mechanisms involved in pipe-jacking tunnel construction within chalky sand strata, focusing on key factors that influence deformation risk and stability control. Following this, it introduces a hybrid machine learning model that combines a Deep Limit Learning Machine (DELM) with a Hybrid Leader-Based Optimization (HLBO) algorithm to enhance prediction accuracy and model robustness. This model is then applied to a case study in Hangzhou, China, where pipe-jacking occurs near existing metro tunnels, with simulations and field measurements used to test accuracy. Comparative experiments validate the model's effectiveness against other methods, presenting detailed parameter evaluations and monitoring data. The paper concludes by discussing the model's contributions to improving deformation risk assessment in tunnel engineering, noting its limitations and proposing areas for further research to increase predictive accuracy and computational efficiency.

II. Analysis of Deformation Risks and Control Options for Pipe Jacking

A. Pipe Jacking Tunnel Construction Process

Pipe jacking tunnelling is a trenchless construction technique, which is mainly used for the construction of urban underground pipelines, subways, pedestrian passages and other projects. This technology achieves tunnel construction by setting up work shafts on the ground and then using pipe jacking machines to push the pipeline or tunnel structure from one work shaft to another, as shown in Fig. 1. Pipe jacking construction technology has the characteristics of reducing damage to the surrounding environment, ensuring construction safety, fast construction speed, controllable quality and strong adaptability.

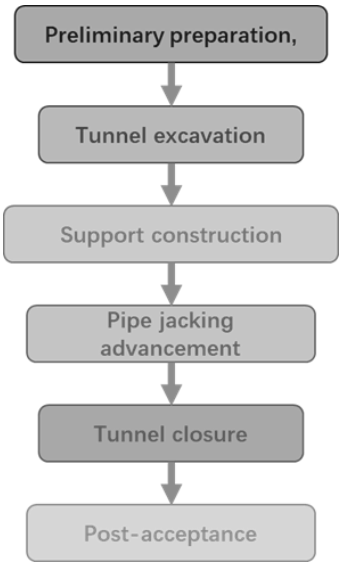


Fig. 1. Construction process of pipe jacking tunnelling.

As shown in Fig. 1, it can be seen that the process of pipe jacking tunnel construction includes pre-preparation, tunnel excavation, support construction, pipe jacking advancement, tunnel closure, and post-acceptance [16].

1) Pre-preparation: Determine the tunnel construction area, carry out geological survey and design, and formulate detailed construction plan, including propulsion path and propulsion machinery selection.

2) Tunnel excavation: traditional tunnel excavation methods, such as blasting or roadheader method, are used to open up a large enough tunnel space for pipe jacking construction.

3) Support construction: choose the appropriate support method according to the geological condition, such as steel frame support, spray anchor support, etc., to ensure the stability and safety of the tunnel.

4) Pipe jacking advancement: choose suitable pipe jacking machinery to carry out the advancement operation, and support the tunnel wall during the advancement process to prevent collapse and instability.

5) Tunnel closure: When the jacking pipe advances to the target position, the pipe closure and connection work is carried out to ensure the sealing and use function of the tunnel.

6) Post-acceptance: acceptance of construction quality, check whether pipe jacking construction meets the requirements to ensure the quality of the project.

B. Project Orientated Risk Analysis of Deformation during the Construction Process

1) Introduction to the project: In order to verify the effectiveness of the deformation risk assessment and control method of the pipe jacking across the operation tunnel, this paper adopts the pipe jacking construction project of Xinfeng Road underground passage in Linping District of Hangzhou City as an analysis sample.

Xinfeng Road Underpass in Linping District, Hangzhou is located in the north side of the intersection of Xinfeng Road and Wenzheng Street in Linping District, and there are many existing structures within the new construction scope. The underpass passes through Xinfeng Road, a main road (header pipe depth 2.3m), and crosses (minimum vertical clearance between header pipe and tunnel structure 2.5m) the existing Hangzhou Metro Line 9 Yuhang High Speed Railway Station to Nanyuan Station double line tunnel, and passes through the existing Hanghai Intercity Double Line Tunnel in parallel (horizontal clearance between header pipe and tunnel 15.6m). The relative position of the underpass and the existing structure is shown in Fig. 2.

The pipe jacking section of the underpass passes through the shield tunnel of Metro Line 9 (inner diameter 5.5m, wall thickness 350mm) and the shield tunnel of Hanghai Intercity (inner diameter 6.0m, wall thickness 350mm).

According to the results of ground investigation, the pipe jacking section is mainly located in ②2 sandy silt and ④ silt stratum, the upper layer is ① miscellaneous fill and ②1 clayey silt stratum, and the layer where the tunnel is located in the lower zone is ④ silt and ⑥ clay stratum, and the physico-mechanical parameter of the soil stratum is shown in Table I.

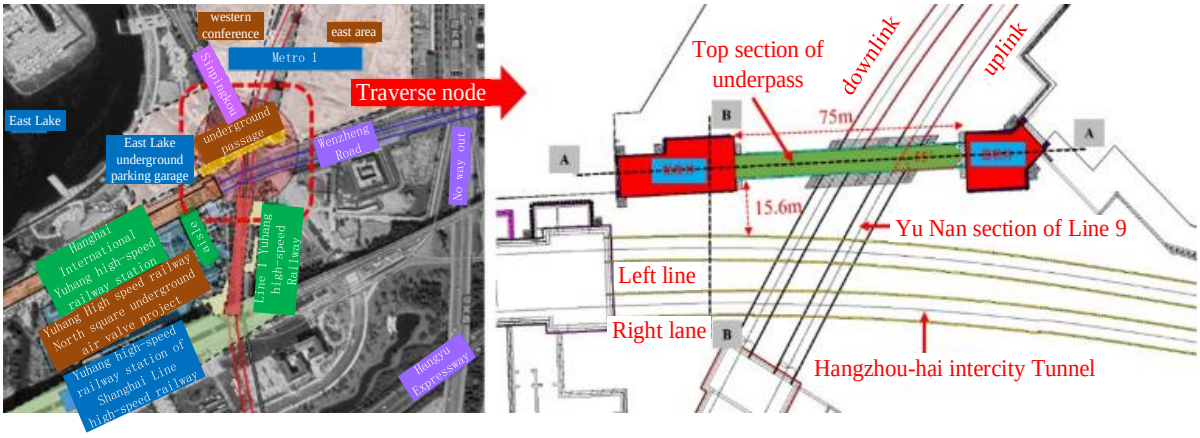


Fig. 2. Relationship between the plan position of the underground passage and the existing structure.

TABLE I. PHYSICAL-MECHANICAL PARAMETERS OF LANDMARKS

Layer number	Stratum	Water content/%	Pore ratio/%	Natural gravity/(kN/m^3)	Cohesion/kPa	Angle of internal friction/°	Horizontal permeability coefficient k/(×10^{-4}cm/s)	Vertical permeability coefficient k /(×10^{-4}cm/s)
①	mixed soil	(30.0)		(19.0)	(7.0)	(15.0)		
②$_1$	clayey silt	25.5	0.731	19.09	5.6	17.6	0.63	0.49
②$_2$	sandy silt	24.6	0.693	19.25	3.0	21.6	7.4	6.1
④	siltstone	24.2	0.677	19.28	3.3	23.4	53.4	37.8
⑥	clays	27.6	0.811	18.88	34.4	14.4		

2) Deformation analysis of pipe jacking construction process: The pipe jacking method of construction generally causes deformation of the ground and the existing tunnel [17].

The deformation of the ground includes ground loss and reconsolidation of disturbed soil. The deformation of stratum mainly refers to the difference between the actual soil volume and the completed tunnel volume during the pipe jacking construction process, and the factors that cause the loss of stratum include soil excavation, pipe section size, tool pipe dragged with soil, pipe jacking correction, pipe section rebound and so on. Re-consolidation of disturbed soil refers to the re-consolidation of disturbed soil after the end of pipe jacking construction, resulting in deformation of the soil layer again, and the main factors include the decrease of void pressure and the disappearance of super pore water pressure.

The deformation of an existing tunnel includes both lateral and vertical deformation [18].

In order to construct an accurate tunnel deformation risk assessment and control model, the tunnel deformation risk factor set is firstly established from two perspectives: ground deformation and existing tunnel deformation, as shown in Fig. 3.

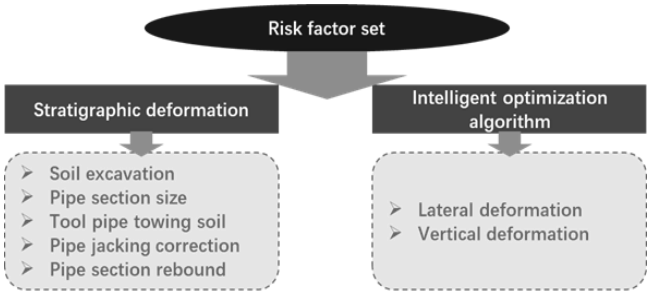


Fig. 3. Tunnel deformation risk factor set.

3) Specific analysis of deformation risk: In this project, there was excessive deformation of the existing tunnel during the jacking construction of the pipe jacking section, mainly focusing on two aspects.

a) Aspects of deformation in chalk strata: Firstly, the project is located in the stratum of silt sand stratum, with high compressibility, high sensitivity and thixotropy, and unfavourable deformation control after stratum construction; secondly, the project is adjacent to the East Lake, with large water content in the stratum, and easy to occurrence of groundwater gushing in the process of jacking.

b) Deformation of existing tunnels: The jacking pipe penetrates the operation tunnel with a vertical clearance of 2.5m, which causes the ground stress relaxation in the unloading disturbance area and the shear disturbance area, and the structure of the operation tunnel near the bottom rises upwards with the surrounding strata; the soil overlay above the jacking pipe is relatively shallow, and the jacking construction has a large impact on the ground surface deformation, as shown in Fig. 4.

C. Deformation Risk Control Programme

In order to analyse the impact of the construction process of the pipe jacking project on the deformation of the operation tunnel, in order to minimise the project risk, the existing tunnel inspection situation is taken into account to determine the structural and surface deformation control scheme of the existing tunnel in the area during the construction process of the pipe jacking project. The existing tunnel structure and surface deformation control program during the construction process of the pipe jacking project is mainly expressed in the form of safety control indicators.

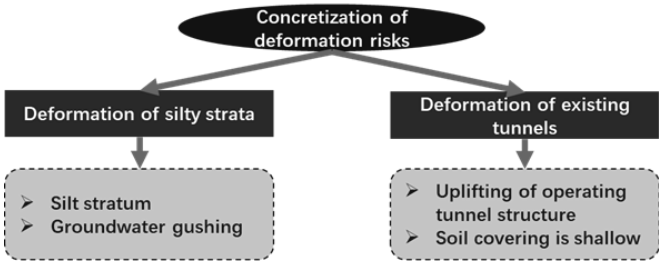


Fig. 4. Schematic diagram for specific analysis of tunnel deformation risk.

The deformation control index of the interval during the construction process of the pipe jacking upper span project is designed from the deformation control of the existing tunnel structure and the surface deformation control in two aspects of the index value [19], in which the deformation control of the existing tunnel structure includes the safety control index and the deformation rate control index [20], as shown in Table. II

TABLE II. SCHEMATIC DIAGRAM OF DEFORMATION CONTROL INDICATORS

Items	Indicators
Existing tunnels	Horizontal displacement of the tunnel
	Vertical displacement of the tunnel
	Tunnel differential settlement
	Tunnel radial convergence
	Rail transverse height difference
	Shield segment joint opening
	Settlement of tunnel structures
	Tunnel structure floats upward
	Horizontal displacement of structure
Surface	Surface uplifting
	Surface subsidence

In view of the shallow soil cover above the jacking tube, 300mm thick reinforced concrete slabs are used for road hardening on the surface above the jacking section of the channel to reinforce the strength of the ground surface, reduce the surface uplift in the jacking process, slow down the effect of shallow soil cover on the deformation of the operation tunnel and act as counterweights above the jacking tube.

III. IMPROVED DEEP LIMIT LEARNING MACHINE MODEL

Deep Extreme Learning Machine is a deep neural network stacked by multiple Extreme Learning Machine self-encoders with fast training speed and good generalisation performance [21]. In order to overcome the problem that the random input weights and biases of deep extreme learning machine affect the

training effect, this paper proposes a deep extreme learning machine model based on hybrid leader optimisation algorithm.

A. Deep Limit Learning Machine

The limit learning machine [22] is denoted as

$$f_{ELM}\left(x_i\right)=\sum_{j=1}^{l}\beta_j g\left(a_j x_i+b_j\right), i=1,2,\cdots,N \quad (1)$$

Where $\beta_j=\left[\beta_{j1},\beta_{j2},\cdots,\beta_{jn}\right]$ denotes the output weights, $a_j=\left[a_{j1},a_{j2},\cdots,a_{jm}\right]$ denotes the input weights, b_j denotes the bias, and $g\left(\cdot\right)$ denotes the activation function.

The ELM output error is

$$\begin{aligned}E&=\sum_{i=1}^{N}\left\|f_{ELM}\left(x_i\right)-y_i\right\|\\&=\left\|\boldsymbol{H}\left(\boldsymbol{a},\boldsymbol{b}\right)\cdot\beta-\boldsymbol{y}\right\|\end{aligned} \quad (2)$$

Where, $\boldsymbol{H}$ denotes the output, β denotes the output weights and $\boldsymbol{y}$ denotes the desired output. In ELM algorithm, by determining $\boldsymbol{a}$ and $\boldsymbol{b}$, $\boldsymbol{H}$ is uniquely determined. The output weights are solved by the formula

$$\boldsymbol{\beta}^{*}=\boldsymbol{H}^{-1}\cdot\boldsymbol{y} \quad (3)$$

where $\boldsymbol{H}^{-1}$ denotes the Moore-Penrose generalised inverse matrix of the matrix $\boldsymbol{H}$.

Deep extreme learning machine (DELM) output weights are

$$\boldsymbol{\beta}^{*}=\boldsymbol{H}^{-1}\left(\frac{1}{C}+\boldsymbol{H}\boldsymbol{H}^{T}\right)^{-1}\cdot\boldsymbol{y} \quad (4)$$

Where, C tables the regular term coefficients.

B. Hybrid Leader Optimisation Algorithm

In intelligent optimisation algorithms, the individuals of the population act as searchers in the problem space, which are candidates for solving the problem, and update the position information through continuous iterative optimisation and comparison to provide a better solution. In this paper, we propose a leader-inspired intelligent optimisation algorithm, Hybrid leader based optimization (HLBO), which uses the best member, a random member, and the corresponding member to update and guide the position information of the population [23].

Like other heuristic algorithms, the population representation of the HLBO algorithm is as follows:

$$X=\begin{bmatrix}X_1\\X_2\\\vdots\\X_N\end{bmatrix}_{N\times m}=\begin{bmatrix}x_{11}&x_{12}&\cdots&x_{1m}\\x_{21}&x_{22}&\cdots&x_{2m}\\\vdots&\vdots&\cdots&\vdots\\x_{N1}&x_{N2}&\cdots&x_{Nm}\end{bmatrix}_{N\times m} \quad (5)$$

At the beginning of the optimisation process, the population, N individuals are randomly initialised with the following initialisation formula:

$$x_{ij}=lb_j+rand\times\left(ub_j-lb_j\right), j=1,2,\cdots,m \quad (6)$$

In HLBO, two search phases are proposed based on leader behaviour: an exploration (global) phase and an exploitation (local) phase.

1) Exploration (global) phase: The exploration phase usually allows the population individuals to precisely search different spaces to reach the original optimal region. Continuous dependence on population-specified individuals can prevent global search and reduce the exploration operation of the algorithm, which results in the population individuals falling into a local optimum. In the HLBO algorithm, a hybrid leadership strategy is used to update the population, and its strategy mainly depends on the current individual, optimal individual, and random individual position information.

The participation factors of current individual, optimal individual, and random individual make the calculation based on individual quality, and the specific formula of individual quality is as follows:

$$q_i=\frac{F_i-F_{worst}}{\sum_{j=1}^{N}\left(F_i-F_{worst}\right)}, i\in\left\{1,2,\cdots,N\right\} \quad (7)$$

The participation factor for each member is calculated as follows:

$$PC_i=\frac{q_i}{q_i+q_{best}+q_k} \quad (8)$$

$$PC_{best}=\frac{q_{best}}{q_i+q_{best}+q_k} \quad (9)$$

$$PC_k=\frac{q_k}{q_i+q_{best}+q_k} \quad (10)$$

Where q_i denotes the individual quality, F_i denotes the fitness value, F_{worst} denotes the fitness value of the worst solution, and PC_i , PC_{best} and PC_k denote the participation factors of the *ith* candidate solution, the optimal solution, and the *kth* candidate solution, respectively.

Based on the calculation of the participation factor, the hybrid leader location information is:

$$HL_i=PC_i\cdot X_i+PC_{best}\cdot X_{best}+PC_k\cdot X_k \quad (11)$$

where HL_i denotes the hybrid leader generated by the *ith* candidate solution and X_k denotes a randomly selected

individual. The *ith* individual position update is based on the guidance of the hybrid leader.

$$x_{ij}^{new,p1}=\begin{cases} x_{ij}+r\left(HL_{ij}+I\,x_{ij}\right) & F_{HL_i}<F_i \\ x_{ij}+r\left(x_{ij}-HL_{ij}\right) & otherwise \end{cases} \quad (12)$$

The HLBO algorithm uses an elite strategy to select individuals as follows:

$$X_i=\begin{cases} X_i^{new,p1} & F_i^{new,p1}<F_i \\ X_i & otherwise \end{cases} \quad (13)$$

Where, $X_i^{new,p1}$ denotes the new position of the *ith* candidate solution, $F_i^{new,p1}$ is the fitness value of $X_i^{new,p1}$, r denotes the random number between $[0,1]$, I is a randomly selected integer from the integer set $\{1,2\}$, and F_{HL_i} denotes the mixed leader fitness value of the *ith* candidate solution.

2) Development (partial) phase: The development phase is a localised search to obtain better solutions in the vicinity of the solution. In the HLBO algorithm, each individual neighbourhood region can allow an individual search to find a better candidate solution. In the development phase, the local search strategy is modelled as follows:

$$x_{ij}^{new,p2}=x_{ij}+(1-2r)\,R\left(1-\frac{t}{T}\right)x_{ij} \quad (14)$$

$$X_i=\begin{cases} X_i^{new,p2} & F_i^{new,p2}<F_i \\ X_i & otherwise \end{cases} \quad (15)$$

Where, $X_i^{new,p2}$ denotes the new position of the local phase of the *ith* candidate solution, $F_i^{new,p2}$ is the fitness value of $X_i^{new,p2}$, R is a constant set to 2, t denotes the current number of iterations, and T is the maximum number of iterations.

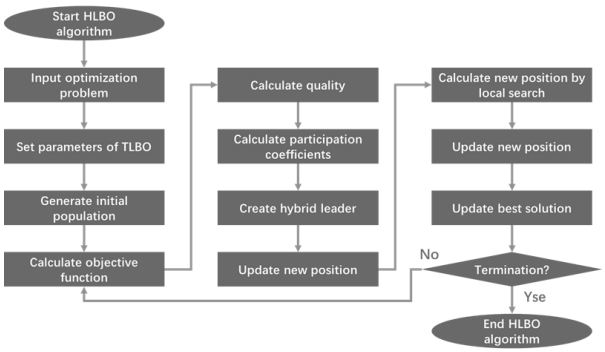


Fig. 5. Flowchart of HLBO algorithm.

3) Process steps: Based on the analysis and description of the above strategies and mechanisms, the flow of the KOA algorithm is shown in Fig. 5.

C. DELM Model based on HLBO Algorithm

1)Coding method: In this paper, the real number coding method is used to encode the hidden layer parameters, which is shown in Fig. 6.

Fig. 6. Encoded DELM parameters.

2) Adaptation function: In this paper, RMSE [24] is used as the adaptation function:

$$RMSE=\sqrt{\left(\sum_{i=1}^{M}\left(\hat{y}_i-y_i\right)^2\right)\Big/M} \quad (16)$$

3) HLBO-DELM methodology: According to the encoding method and fitness function, the flowchart of the deep limit learning machine model step method based on the HLBO algorithm is shown in Fig. 7.

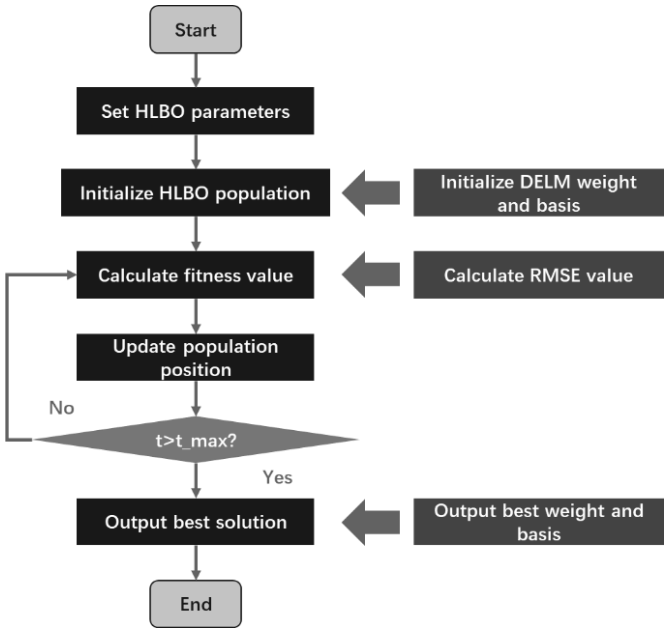


Fig. 7. HLBO-DELM methodology.

D. Application of the HLBO-DELM Model

In order to construct a deformation risk control model for shallow overburden pipe jacking operation tunnels in chalky sand strata, this paper adopts the HLBO-DELM model, by analysing the tunnel deformation risk factors and control indexes, taking the weights and biases of the DELM as the optimisation variables, and taking the RMSE values between the analytical tunnel deformation risk control indexes and the predicted values and the simulated values as the fitness value function, the optimisation strategy of the HLBO algorithm is used to find out the optimal weights and biases of the DELM. The HLBO-DELM model application principle and framework structure are shown in Fig. 8.

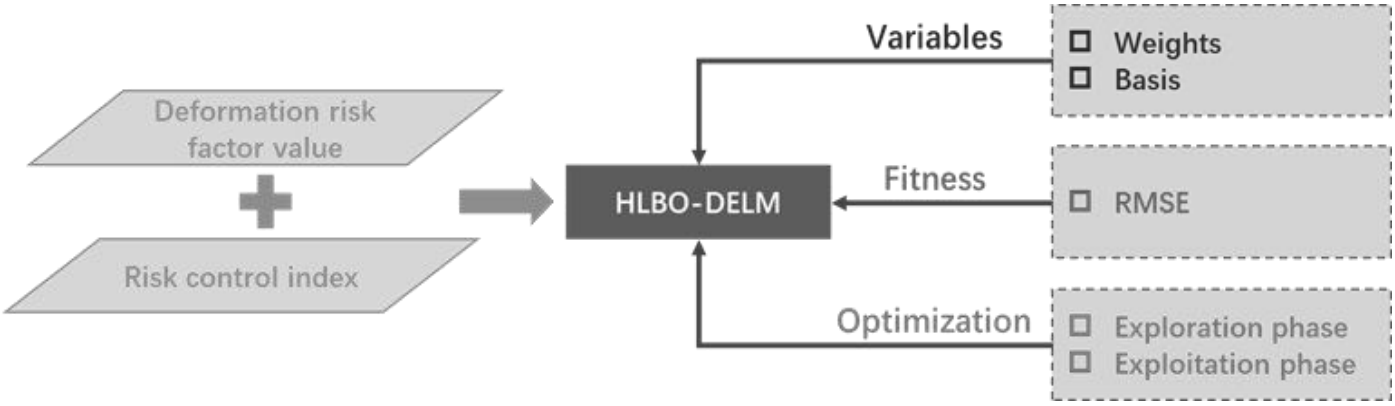


Fig. 8. HLBO-DELM application analysis.

IV. Tunnel Deformation Risk Assessment and Control Process Methodology

Combined with the HLBO-DELM model oriented to the tunnel deformation risk assessment and control problem, this subsection analyses the mapping relationships that need to be constructed in the HLBO-DELM model and gives the tunnel deformation risk assessment and control method flow.

A. Analysis of Model Mapping Relationships

The deformation risk assessment factors of the operation tunnel over shallow cope pipe in chalk stratum are set up from the perspective of ground deformation and existing tunnel deformation, and the deformation control indexes of the operation tunnel over shallow cope pipe in chalk stratum are mainly designed from the control of structural deformation of the existing tunnel and the control of ground surface deformation. The specific construction results are shown in Fig. 9.

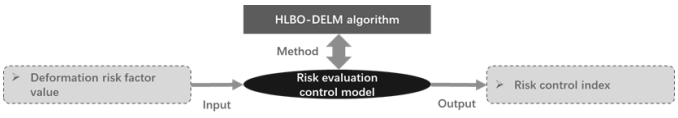


Fig. 9. Schematic diagram of model mapping relationship analysis.

B. Methodological Process

In order to improve the deformation risk assessment and control of the roof-tube up-and-over operation tunnel, this paper investigates the tunnel deformation risk assessment and control method using a combination of intelligent optimisation algorithm and machine learning algorithm, and the specific process is shown in Fig. 10.

As can be seen from Fig. 10, in the construction risk assessment and control scheme of the top tube over operation tunnel, through analysing the deformation risk factors and risk control index set of the top tube over operation tunnel, pre-processing the raw data, combining with HLBO-DELM, constructing the deformation risk assessment and control model of the top tube over operation tunnel, predicting and analysing the amount of deformation control, and improving the precision and accuracy of risk control.

Step 1: Identify and analyse the deformation risk factors of the top tube over the operational tunnel by using expert consultation, experimental demonstration and work breakdown structure method;

Step 2: Analyse and design a set of deformation risk control indicators for the top tube over operational tunnels in terms of both deformation of existing tunnels and deformation of the ground;

Step 3: Construct a sample set of labelled deformation risk factor-risk control indicators;

Step 3: Normalise the original data samples using techniques such as outlier removal, missing value supplementation, normalisation, etc., and perform feature extraction and dimensionality reduction of the input vectors using the Kernel Principal Component Analysis (KPCA) [25] method;

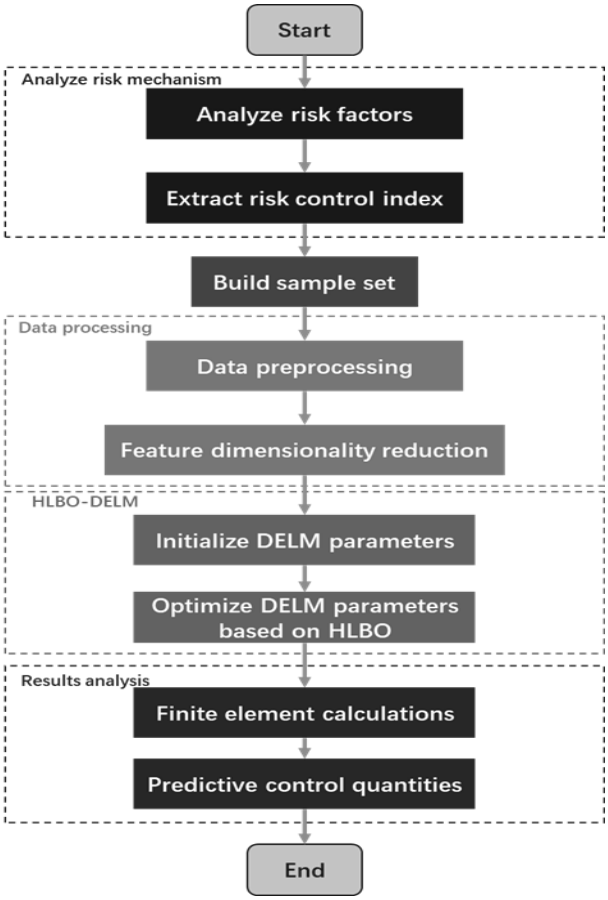


Fig. 10. Flow of tunnel deformation risk assessment and control method.

Step 4: Combine the HLBO-DELM algorithm to construct a deformation risk assessment and control model for the top tube over operation tunnel;

Step 5: Numerical Analysis of Risk Control Measures Experimental Finite Element Computational Models [26] A certain number of samples are constructed and divided into training set, validation set, and testing set;

Step 6: Train the model, analyse the results of the test set, and at the same time collect the project engineering risk factors and input them into the assessment and control model to obtain the deformation risk control index value of the top tube over the operational tunnel.

V. Analysis of Numerical Experiments

A. Experimental Setup

In order to verify the effectiveness and feasibility of the deformation risk assessment and control algorithm of the pipe jacking over operation tunnel proposed in this paper, this paper takes the project of close crossing over Metro Line 9 tunnel and side crossing over Hanghai Intercity Tunnel of Xinfeng Road Underpass in Hangzhou as an analysis sample, and selects DELM, PSO-DELM, GWO-DELM, HHO-DELM, WOA-DELM and HLBO-DELM to compare with the algorithms. algorithms for comparison.

1) Algorithm parameter setting: In Table III, DELM uses Moore-Penrose generalised inverse matrix to solve the optimal structural parameters, PSO-DELM, GWO-DELM, HHO-DELM, WOA-DELM and HLBO-DELM use intelligent optimisation algorithm to solve the optimal structural parameters, the maximum number of iterations of intelligent optimisation algorithm is 100, the number of population counts is 50, and the number of hidden layers is 2.

TABLE III. Comparison Algorithm Parameter Settings

Arithmetic	Parameterisation
DELM	Two hidden layers with 30, 30 nodes in each layer
PSO-DELM	Vmax=30, Vmin=-30, r=0.5
GWO-DELM	GWO algorithm a control parameters using a linear decreasing strategy
HHO-DELM	E0 in the range (-1, 1)
WOA-DELM	The WOA algorithm a decreases from 2 to 0, and the spiral shape parameter is 1.
HLBO-DELM	r denotes a random number between 0 and 1 and I denotes a randomly chosen integer of {1,2}

2) Environmental settings: The experimental simulation environment is Win 10, the risk assessment algorithm programming language Python 3.8, and the structural numerical analyses are performed using Midas GTS finite element software.

B. Analysis of Results

1) Numerical analysis of structures: Using the software for pipe jacking construction simulation, the calculation results after the jacking advancement in the characteristic working condition are shown in Table IV. As can be seen from Table IV, the largest vertical deformation in the deformation of the tunnel structure of Line 9 is the bulge of 4.86mm when completing the construction of the upper span, which occurs in the tunnel tube sheet of the downstream line of Line 9, as shown in Fig. 15. Since the final bulge deformation in this case is due to ground loss and subsequent deformation of the ground, the tunnel bulge deformation will be smaller than the final deformation of 4.86mm when the roof tube is jacked through the tunnel directly above the Line 9 tunnel. The maximum horizontal deformation of the metro tunnel is 0.70mm, while the deformation of the Hanghai Intercity Tunnel is very small compared with that of the metro tunnel, with the maximum horizontal deformation and vertical uplift of 0.49mm and 0.83mm, respectively. according to the results of the calculation, the deformation of the two operating tunnels meets the control requirement of 5mm. The difference settlement at the junction between the tunnel section and the station is small.

2) Parametric analysis: The specific results of the analysis of the number of network hidden layer nodes parameter are shown in Fig. 11 and Fig. 12. From Fig. 11, it can be seen that the number of network hidden layer nodes increases, the accuracy of deformation risk assessment and control increases,

and when the number of network hidden layer nodes increases to 100, the deformation risk assessment and control algorithm RMSE is minimum. From Fig. 12, it can be seen that the number of network hidden layer nodes of DELM increases, and the control time of each algorithm increases; the assessment and control prediction time of the HLBO-DELM model is smaller than that of other models. In summary, the number of hidden layer nodes of DBN network selected in this paper is 100.

3) Example analysis: This subsection compares the performance of the DELM, PSO-DELM, GWO-DELM, HHO-DELM, WOA-DELM and HLBO-DELM methods using the numerical simulation test set.

Firstly, continuous automated monitoring of the Metro Line 9 tunnel was carried out during the implementation of the jacking crossing site and subsequent deformation stabilisation, and the structural deformation of the tunnel after completion of the jacking upper span construction is shown in Fig. 18.

TABLE IV. STRUCTURAL DEFORMATION RESULTS OF OPERATIONAL TUNNELS DURING THE CONSTRUCTION PROCESS

working condition	Line 9 tunnel/mm		Hanghai Intercity Tunnel/mm		Differential settlement at junction/mm	
	horizontal	vertical	horizontal	vertical	Line 9 Interval	Hang Hai District
Shaft Phase 1	0.34	0.22	0.32	0.14	-	-
pipe jacking	0.36	4.86	0.49	0.83	-	-
Shaft Phase 2	0.70	4.64	0.40	0.51	0.02	0.02

Fig. 13 and Fig. 14 give the monitoring results of the roadbed displacement in the tunnel. From Fig. 13 and Fig. 14, it can be seen that the maximum value of vertical displacement in the metro tunnel is 4.0mm, which occurs in the bed measurement point of the downstream line, and the displacement of the downstream line traversed by the jacking tube first is generally larger than that of the upstream line; the maximum value of horizontal displacement is 2.7mm, which occurs in the bed measurement point of the upstream line. The maximum horizontal displacement was 2.7mm, which appeared at the upstream line bed measurement point. The larger values of vertical and horizontal displacements in the upstream and downstream lines were distributed in the area where the jacking pipe traversed, which indicated that the jacking pipe's close spanning construction had a greater impact on the operation tunnel, and the area within 25m directly below the crossing belonged to the strong impact area; the distance from this boundary to 50m had a weaker impact and belonged to the weak impact area; and the area outside of 50m belonged to the non-influence area.

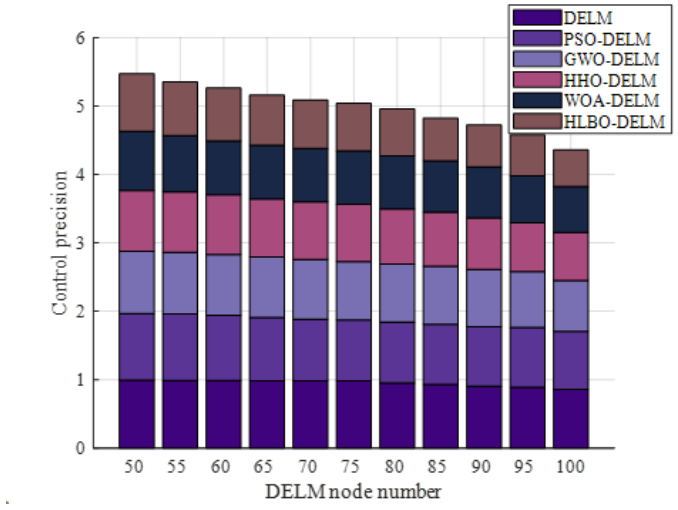


Fig. 11. Effect of different number of hidden layer nodes on the accuracy of control algorithm for deformation risk assessment.

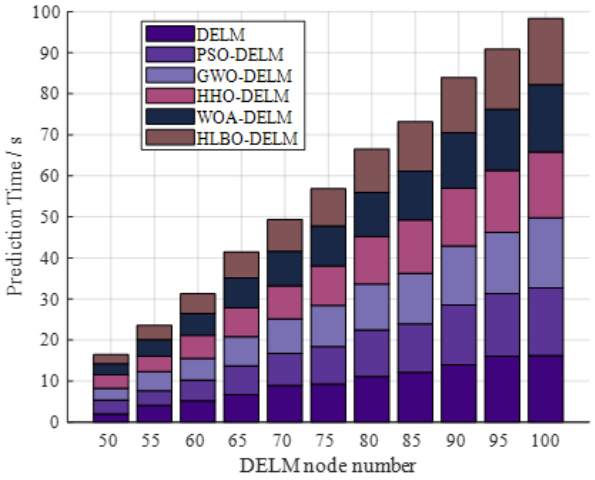


Fig. 12. Effect of different number of hidden layer nodes on control algorithm time for deformation risk assessment.

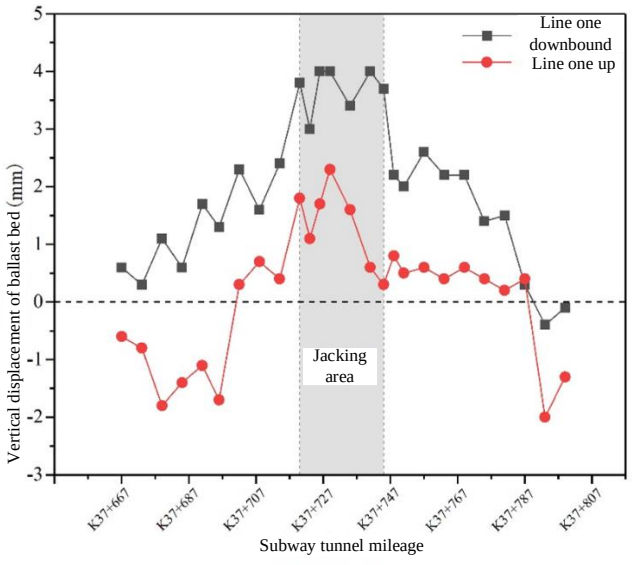


Fig. 13. Vertical displacement of tunnel bed of Line 9 metro tunnel.

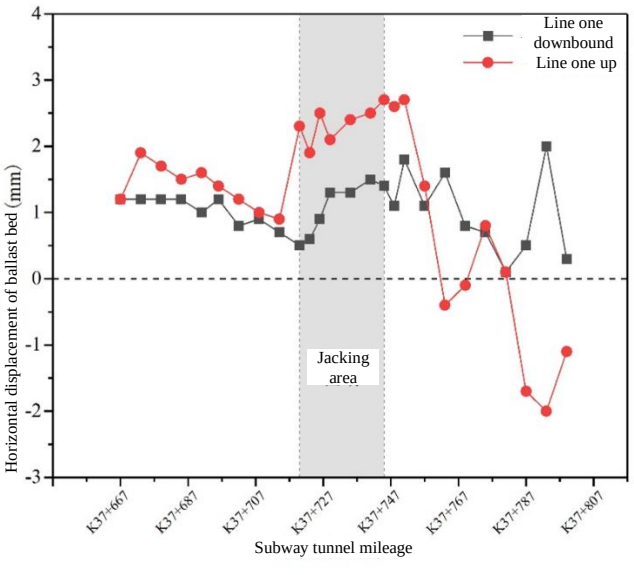


Fig. 14. Horizontal displacement of tunnel bed of Line 9 metro tunnel.

VI. Conclusion and Outlook

As the key technology of deformation risk assessment-control in the construction of roof-tube span, the deformation risk assessment-control algorithm not only reduces the subjectivity and empirical nature of the human-designed control scheme, but also constructs a complex mapping relationship between the risk identification factors and the risk control strategy. In this paper, a deformation risk assessment and control scheme is designed by analyzing the construction process of pipe jacking tunnels and the deformation risk mechanism. Meanwhile, a deformation risk assessment and control algorithm based on TLBO-DELM is proposed for the mapping relationship of the deformation risk assessment and control model, which is applied to the deformation risk and control scheme of pipe jacking up and over operation tunnels with shallow overburden in chalky sand layer, and the effectiveness of the proposed TLBO-DELM model algorithm is analyzed, and the effectiveness of the proposed TLBO-DELM model algorithm is compared with that of the other models. The effectiveness of the proposed TLBO-DELM model algorithm is analysed, and by comparing other model algorithms, it is verified that the deformation risk assessment and control model based on the TLBO-DELM algorithm has a high control prediction accuracy.

While the HLBO-DELM model has shown promise, several limitations remain. Firstly, its generalizability across different geological conditions, such as expansive soils or hard rock layers, requires further validation; performance may vary significantly in these settings. Additionally, the current study relies primarily on simulated data for model training, with limited use of real-world engineering data, which may reduce the model's robustness when applied to diverse tunnel construction projects. The algorithm's computational efficiency and real-time application also pose challenges, particularly in high-dimensional data processing and timely monitoring feedback.

To address these issues, future research should prioritize expanding the dataset by incorporating monitoring data from diverse geological contexts and construction projects, improving the model's adaptability and prediction accuracy. Enhancements in the algorithm's structure—potentially through hybridization with other optimization methods like genetic algorithms or particle swarm optimization—could strengthen its global search capability and computational speed. Moreover, integrating the HLBO-DELM model within a real-time monitoring and alert system would allow for proactive risk detection and control, facilitating automated responses to potential deformation risks in active construction sites.

References

[1] Liu Y , Song H L , Sun X D , Xing H P, Feng C Y, Zhao G. T. Characteristics of rail deformation caused by tunnel floor heave and corresponding running risk of high-speed train[J].Construction and Building Materials, 2022.

[2] Yu C .Risk Assessment of Tunnel Face Instability under Multi Factor Coupling Based on Conditional Probability and Tunnel Construction Mechanics[J]. .Applied Sciences, 2022, 12.

[3] Zheng X , Wu K , Shao Z , Yuan B, Zhao N. Tunnel Squeezing Deformation Control and the Use of Yielding Elements in Shotcrete Linings: a Review[J]. Materials (Basel, Switzerland), 2022, 15(1).

[4] Manouchehrian A , Kulatilake P .Numerical study on rock failure around a tunnel destressed by a conceptualized notched technique[J].Underground Space, 2022.

[5] Ding Z , Zhang M B , Zhang X , Wei X J. Theoretical analysis on the deformation of existing tunnel caused by under-crossing of large-diameter slurry shield considering construction factors[J].Tunnelling and Underground Space Technology, 2023, 133:104913-.

[6] Ansari A , Rao K S , Jain A K .Application of Microzonation Towards System-Wide Seismic Risk Assessment of Railway Network[J].Transportation Infrastructure Geotechnology, 2024, 11(3):1119-1142.

[7] Han X , Oreste P , Ye F .The important role of stiffnesses values of circular joints on the stress state developed in the tunnel segmental lining[J]. Geomechanics and Geophysics for Geo-Energy and Geo-Resources, 2023, 9(1).

[8] LI Zhongchao, CHEN Renpeng, MENG Fanyan, YE Junneng. Relationship between ground deformation and boring parameters for shield tunneling in soft clay[J]. Journal of Zhejiang University (Engineering Edition), 2015, 49(7): 1268-1275.

[9] Shi Chenghua, Huang Linchong. Calculation of soil deformation in disturbed area of tunnel for pipe jacking construction[J]. Journal of Central South University (Natural Science Edition),2005,(02):323-328.

[10] Jin Xin. Soil Disturbance Law and Control Technology of Large Section Rectangular Pipe Jacking Under the Beijing-Hangzhou Grand Canal [D]. China University of Mining and Technology,2020.

[11] Zhang B , Tao Z , Guo P . Model test on deformation and failure mechanism of tunnel support with layered rock mass under high ground stress[J].Engineering failure analysis,. 2023.

[12] Wu P , Lin F , Huang J , Xu Y. Multiscale evaluation of tunnel construction safety risk: a case study of an offshore tunnel construction in Ningbo[J]. Journal of Engineering and Applied Science, 2024, 71(1).

[13] Rautioaho E , Korkiala-Tanttu L .Bentomap: Survey of bentonite and tunnel backfill knowledge - State-of-the-art[J].Tanttu, 2022.

[14] Shi J , Chen Y , Kong G ,Lu H, Chen G, Shi C. Deformation mechanisms of an existing pipeline due to progressively passive instability of tunnel face. Physical and numerical investigations[J].Tunnelling and Underground Space Technology incorporating Trenchless Technology Research, 2024, 150.

[15] Fogang P M , Liu Y , Zhao J , Ka T A, Xu S. Analytical Prediction of Tunnel Deformation Beneath an Inclined Plane: Complex Potential Analysis[J].Applied Sciences, 2023.

[16] Qi X .Three-dimensional inversion of controlled-source electromagnetic data for surveying the Jiutianshan high-speed railway Tunnel, China [J] .Journal of Applied Geophysics, 2023, 209:104901-.

[17] Su D , Chen W , Wang X , Huang M, Pang X, Chen X. Numerical study on transverse deformation characteristics of shield tunnel subject to local soil loosening[J].Underground Space, 2022, 7(1):106-121.

[18] Yasuda N , Cui Y .Deformation estimation of a circular tunnel from a point cloud using elliptic Fourier analysis[J].Tunnelling and underground space technology, 2022(7):125.

[19] Xu X , Wu Z , Liu Q .An improved numerical manifold method for investigating the mechanism of tunnel supports to prevent large squeezing deformation hazards in deep tunnels[J].Computers and geotechnics, 2022.

[20] Zhang Q , Zhang X P , Wang H J , Zhang X Y, Li F Y, Xu D. Ground deformation induced by a shallow-buried twin-tunnel with small spacing: a case study of Guangzhou Metro Line 18 excavated by earth-pressure balance TBM[J].Environmental earth sciences, 2023.

[21] Boyang Zhang,Su-Mei Li. Stereoscopic image quality evaluation method applying deep limit learning machine[J]. Small Microcomputer Systems, 2017, 38(11):5.

[22] Li Shiyao,Zhou Liang,Liu Hu. Hazard source identification algorithm HIELM based on deep extreme learning machine[J]. Computer Science, 2017, 44(5):6.

[23] Dehghani M , Trojovsk P .Hybrid leader based optimization: a new stochastic optimization algorithm for solving optimisation applications[J]. Scientific Reports, 2022, 12(1):1-16.

[24] Yang Shuo, Luo Mingliang, Lin Yebin, Huang Jin, Jiang Jiayan. Quantitative study of factors affecting the interpolation accuracy of temperature data[J]. Shaanxi Meteorology, 2023(5):67-73.

[25] Thakur R , Rohilla R .An effective framework based on hybrid learning and kernel principal component analysis for face manipulation detection[J]. Signal, Image and Video Processing, 2024, 18(5):4811-4820.

[26] Yang J , Shen K , Pan S , Wang S, Zou Z. Study on the Deformation Mechanism of a Soft Rock Tunnel[J]. Fluid Mechanics and Materials Processing(English), 2022(002):018.

Scalp Disorder Imaging: How Deep Learning and Explainable Artificial Intelligence are Revolutionizing Diagnosis and Treatment

Vinh Quang Tran[1], Haewon Byeon[2]*
Department of Digital Anti-Aging Healthcare (BK21), Inje University, Gimhae 50834, South Korea[1]
Department of Medical Bigdata, Inje Medical Big Data Research Center, Inje University, Gimhae 50834, South Korea[2]

***Abstract*—Scalp disorders, affecting millions worldwide, significantly impact both physical and mental health. Deep learning has emerged as a promising tool for automated diagnosis, but ensuring model transparency and reliability is crucial. This review explores the integration of explainable AI (XAI) techniques to enhance the interpretability of deep learning models in scalp disorder diagnosis. We analyzed recent studies employing deep learning models to classify scalp disorders from image data and used XAI methods to understand the models' decision-making processes and identify potential biases. While deep learning has shown promising results, challenges such as data quality and model interpretability persist. Future research should focus on expanding the capabilities of deep learning models for real-time detection and severity prediction, while addressing limitations in data diversity and ensuring the generalizability of models across different populations. The integration of XAI techniques is essential for fostering trust in AI-powered scalp disease diagnosis and facilitating their widespread adoption in clinical practice.**

***Keywords*—Scalp disorders; artificial intelligence; explainable artificial intelligence; deep learning; interpretability**

I. Introduction

In recent times, the integration of AI in healthcare has transitioned from theoretical research to practical implementations in clinical settings. This includes areas such as telemedicine, the utilization of robots in surgical settings, and the management of electronic health records. Medical imaging stands out as one of the most recognized applications, constituting 90% of all healthcare data [1]. AI demonstrates promising capabilities in diagnosing and classifying various diseases, particularly in dermatological conditions, where it assists in the identification and categorization of skin issues, including conditions related to the scalp and hair.

Despite these advances, a significant gap in research remains regarding the deployment of deep learning (DL) models in medical imaging, particularly in clinical settings. While current DL models, inspired by neural networks in the human brain, include notable architectures such as Faster R-CNN [2], VGG-net [3], and those based on ImageNet [4] offer impressive accuracy in tasks such as image recognition and classification. their lack of interpretability presents a major challenge, especially in complex areas like dermatology and scalp and hair disorder diagnostics [5]. This issue has spurred growing interest in the role of eXplainable AI (XAI), which aims to make the decision processes of DL models transparent. XAI is not only beneficial for machine learning (ML) researchers but is also vital for clinicians and patients who rely on these models to make informed healthcare decisions. By making AI more interpretable, XAI fosters trust in clinical applications, addressing a crucial need for greater transparency in AI-driven diagnostics.

This review aims to comprehensively examine the progress and challenges in utilizing XAI and DL methodologies for analyzing medical imaging data, specifically for scalp and hair disorder diagnostics. Through an extensive review of existing studies, this paper will highlight the contributions and limitations of various DL models applied to dermatological imaging and evaluate the effectiveness of XAI techniques in enhancing their interpretability and clinical relevance. This examination includes an analysis of how XAI techniques can improve transparency in AI-based diagnostics, particularly for non-expert stakeholders, such as clinicians and patients, who require comprehensible insights into AI-driven assessments.

The significance of this review lies in addressing the critical need for interpretable AI systems in dermatology, with a focus on the largely unexplored domain of scalp and hair disorder imaging. By synthesizing existing findings, this paper aims to provide a reference for developing clinically applicable AI frameworks that enhance both accuracy and interpretability. Ultimately, this review not only consolidates current knowledge but also serves as a foundation for future research aimed at creating trustworthy and effective AI-driven diagnostic tools across dermatological and broader medical applications.

The structure of this paper is organized as follows: Section II details the materials and methods applied in various studies, specifically focusing on the deep learning and XAI techniques employed in scalp and hair disorder diagnostics. Section III presents the results gathered from these studies, offering insights into the effectiveness of each approach. Section IV provides a discussion that highlights both the strengths and limitations of the reviewed studies, analyzing their contributions and identifying potential gaps. Finally, Section V concludes the paper, summarizing key findings and suggesting directions for future research.

* Corresponding Author

II. Materials and Method

A. Artificial Intelligence in Scalp Disorder Diagnosis

Scalp disorders are recognized as dermatological or medical issues associated with the well-being of the scalp and hair, attributed to the abundance of hair follicles and elevated sebum production. These disorders may include dandruff, seborrheic, folliculitis, tinea capitis, psoriasis, are widespread conditions affecting adults globally. Scalp psoriasis, impacting approximately 2% of the Western population [6], and dandruff, with a global prevalence of around 50% [7], contribute significantly to these concerns. These conditions not only affect physical health but also exert a substantial influence on mental well-being, contributing to stress, anxiety, or depression [8], [9]. This impact is particularly noticeable in societies where significant of appearance holds considerable weight, as observed in places like South Korea, where lookism can have implications for health [10].

Therefore, the diagnosis and classification are crucial, as scalp disorders frequently exhibit similar clinical manifestations [11]. The way to diagnosis scalp related-problems could be use various data type, including: medical imaging, clinical notes, and scalp biopsy laboratory test result; however, scalps biopsies can cause risk such as bleeding, pain, and infection meanwhile clinical notes may be subjective and vary in quality, potentially leading to biases or inaccuracies in the diagnostic process among these approaches, scalp imaging stands out as it offers a non-invasive and direct visualization of the scalp. Advanced imaging technologies like dermoscopy (trichoscopy) and optical coherence tomography (OCT), enhance the diagnostic capabilities by providing magnified insights into structural and morphological changes at a microscopic level [12]. For dermatologists, this means enhanced diagnostic capabilities without the associated risks of scalp biopsies. On the patient's side, the non-invasiveness and direct visual feedback contribute to a more comfortable and accessible diagnostic experience. However, a concerning trend is observed, where people frequently seek diagnoses from non-professionals in hair salons rather than consulting dermatologists. This trend has contributed to a worsening state in the overall condition of scalp problems.

In order to overcome these challenges, the advances of AI applications in dermatology have introduced a transformative model shift, revolutionizing how we approach the diagnosis and treatment of scalp hair-related problems. AI, including ML and DL, has become widespread components in any medical analysis workflows and facilitating the path for the real-world diagnostic integration of solutions based on AI [13]. In the context of scalp health, the application of AI holds the promise of not only enhancing precision in identifying and classifying various scalp conditions but also revolutionizing the therapeutic strategies employed, such as providing an opportunity for patients to engage in self-diagnosis [14]. This intersection of AI and dermatology prompts a renewed research interest, particularly in the early detection and diagnosis of scalp hair diseases.

However, complex ML algorithms pose challenges in comprehending their decision-making processes, specifically in complicated tasks such as scalp hair imaging classification. In order to effectively tackle this issue, the implementation of XAI presents a distinctive opportunity, benefiting not only AI experts but also non-experts like medical doctors and patients [15].

B. Advanced Machine Learning in Scalp Imaging

Scalp imaging can be categorized into various modalities, each offering unique insights into different aspects of scalp health. Dermoscopy, or surface microscopy [16], utilizes a handheld device with magnification and lighting to visualize pigmented cutaneous lesions and assess hair follicles, patterns of hair loss, and various scalp conditions. OCT captures high-resolution, cross-sectional images of biological tissues, revealing structural changes in the skin and hair follicles. In Vivo Reflectance Confocal Microscopy (RCM) provides live visualization [17] of cellular structures in the scalp at a high resolution, generated high-quality images of the hair shaft junctions at 1µm spacing, facilitating a comprehensive analysis of the hair structure. In the field of ML and DL, several studies have predominantly utilized portable magnification imaging microscopes [2], [18], [19], [20] or dermoscopy data [21], [22], [23], in comparison to OCT studies [24] and RCM, due to higher costs and challenges in obtaining data. Additionally, limited training programs for RCM [25] contribute to subjective variability in diagnoses.

C. Limitations of Machine Learning in Scalp Disorder Imaging

Since 2014, studies employing ML for scalp imaging classification have evolved, transitioning from unsupervised learning approaches [26], [27] to more complex deep-learning based method [3], [18], [28]. These studies have utilized datasets ranging from small to mid-size, achieving accuracies typically in the mid-80s to low 90s. However, the domain of scalp disorder imaging still faces persistent challenges. Notably in contrast to research studies focused on other skin areas. In these areas, datasets commonly surpass 100,000 images [29], [30]. Moreover, the datasets within scalp disorder imaging exhibit imbalances, further compounded by a deficiency in interpretability and explainability.

As a result, these challenges make it difficult to smoothly apply these technologies in a clinical setting. To address these issues, there is a pressing need to explore new research avenues, particularly in comparison to the advancements made in skin disease classification within the dermatology realm.

D. Advancements in Integrating Deep Learning Models and Explainable AI for Scalp Disorder Imaging

Numerous researchers have dedicated their efforts to advance the deployment of ML models for the classification of scalp hair disorders. The evolution of ML into DL models, including the integration of XAI has been revolutionary. This commitment involves implementing XAI to make it possible to identify and address any potential biases in the model's decision-making process, aiming to increase trust for clinical applications. The following showcases how these advancements can be presented:

1) Convolutional neural network variations model: With the increasing use of DL models in imaging classification tasks,

the foundational technique of Convolutional Neural Networks (CNNs) plays a pivotal role in developing recent models. CNNs consist of various layers, such as convolutional, activation, and pooling layers. The inclusion of one or more Fully-Connected layers (FC) in the network is essential for generating final output predictions. Additionally, dropout layers have been incorporated into the architecture to address the overfitting issue and enhance the model's robustness. The strategic use of dropout layers aids in preventing the network from relying too heavily on specific connections during training, promoting a more generalized and resilient model.

To demonstrate how different models respond to scalp imaging disorder classification tasks, well-known models have been applied. These models can be categorized into two main architectures: one-stage architecture and two-stage architecture. In the two-stage approach, exemplified by Faster R-CNN (Region-based Convolutional Neural Network) [31], the Region Proposal Network (RPN) represents a significant advancement. By sharing convolutional layers with the object detection network, the RPN efficiently generates region proposals directly from the convolutional feature maps, avoiding the need for external proposal generation methods. The RPN evaluates a set of anchor boxes at different scales and aspect ratios, predicting their likelihood of containing an object and refining their coordinates.

On the other hand, one-stage CNNs follow a more streamlined approach, performing simultaneous object detection and localization without a separate region proposal stage. These models directly predict object localization and classification within an image, making them efficient for real-time object detection. However, it's essential to note that they may not always achieve the same level of accuracy as two-stage models in certain situations. One example of one-stage CNNs is the Single Shot MultiBox Detector (SSD) [32].

2) Vision transformers (ViTs): Traditional CNN architectures rely on convolutional layers to extract features from images. These layers progressively learn to identify low-level features like edges and textures, ultimately building towards higher-level features for classification. However, a recent advancement in image classification is the emergence of Vision Transformers (ViTs) [33]. Unlike CNNs, ViTs forego convolutional layers entirely. Instead, they split the image into patches, process them using self-attention mechanisms, and progressively learn relationships between different image regions. This approach allows ViTs to potentially capture long-range dependencies within images that might be missed by CNNs with localized filters. Fig. 1 represents the concept of ViT proposed in Dosovitskiy et al.'s study [33].

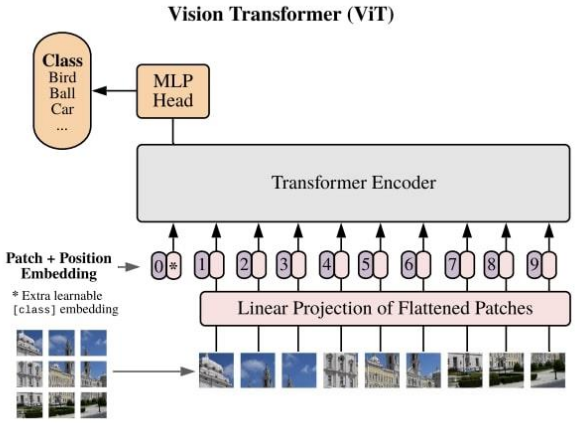


Fig. 1. The concept of vision transformers.

3) Gradient-weighted class activation mapping (Grad-CAM): Ramprasaath and his team [34] introduced a technique aimed at providing visual representations of the decision-making process of deep neural networks, particularly convolutional network. At a high level, the approach involves processing an image as input data and creating a model that is truncated at a specific layer to generate visual representations of the areas in input images that have the most impact on the network's predictions.

Operationally, the method conducts a forward pass of the input image through the network, and the subsequent prediction triggers a backward pass to the sensitivity of the predicted class score to changes in the feature maps. Global Average Pooling (GAP) is then applied to globally average these gradients across each feature map, generating a class-discriminative localization map. This map is utilized as weights to compute a weighted sum of the feature maps, emphasizing regions crucial for the prediction. Following a Rectified Linear Unit (ReLU) activation and up-sampling to match the input image's dimensions, the final heatmap is produced, producing visual maps to show important zones influencing the network's decision.

Nevertheless, Grad-CAM faces limitations in highlighting fine-grained features due to its inability for pixel-level gradient visualization. The down-sampling during convolution and the subsequent need for up-sampling via bilinear interpolation result in a loss of resolution, impacting the accuracy of explanation results. Additionally, inconsistencies between Grad-CAM and the actual model behavior diminish the reliability of its interpretations. These challenges underscore the necessity for improvements in Grad-CAM to enhance precision and alignment with the intricacies of the original model. Fig. 2 represents the concept of Grad-CAM proposed in Ramprasaath et al.'s study [35].

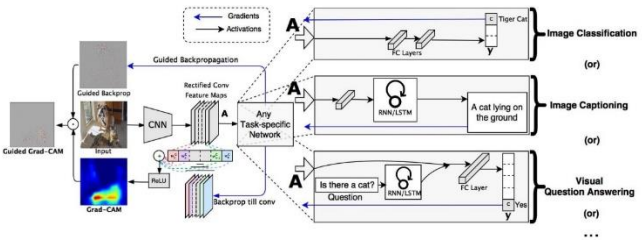


Fig. 2. The overview concept of Grad-CAM by Ramprasaath et al. [34].

4) Locally interpretable model-agnostic explanation (LIME): Local Interpretable Model-agnostic Explanations (LIME) was introduced in 2016 by Ribero et al. [35]. In the pursuit of model-agnostic interpretability, LIME adopts a unique approach by perturbing the input and observing how the predictions change. The essence of LIME lies in approximating the black-box model locally, in the vicinity of the prediction to be explained, by constructing an interpretable model (e.g., a linear model with only a few non-zero coefficients). This is achieved by generating perturbations of the original instance, such as removing words or hiding parts of an image.

The key intuition behind LIME is rooted in the understanding that it is more suitable to approximate a black-box model locally than globally. This involves weighting the perturbed instances based on their similarity to the instance being explained. Consider the scenario of explaining predictions in an image. LIME transforms the image into interpretable components, such as contiguous super-pixels. A collection of manipulated instances is created by switching off certain interpretable components. For each perturbed instance, the model's prediction is obtained. A locally weighted, simple (linear) model is then learned on this dataset, prioritizing instances that possess a greater similarity to the original image. The produced explanation highlights the interpretable components that contribute most heavily to the model's predictions, simultaneously downplaying the prominence of less relevant features. The illustration of the LIME concept is presented in Fig. 3.

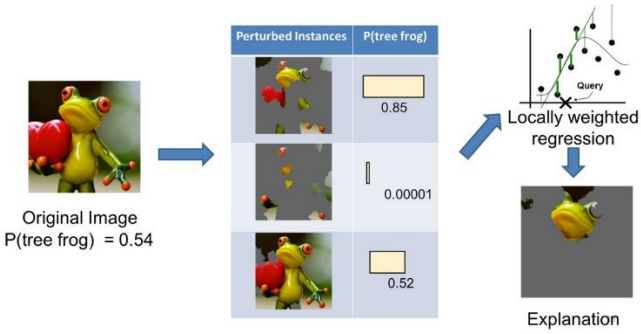


Fig. 3. LIME prediction explained by Ribero et al.

5) Occlusion sensitivity: Occlusion Sensitivity, as introduced by Zeiler and Fergus [36] in their paper on visualization techniques for conventional neural networks, is a method centered around systematically occluding or blocking individual regions of an input image to determine their influence on the model's prediction. The primary concept involves assessing how the probability score of the network changes when specific regions of the image are obscured.

By occluding various portions of the input image and observing corresponding shifts in the model's response, this technique facilitates the exploration of the model's reliance on particular regions or features for accurate predictions. If blocking certain areas significantly influences the model's accuracy, it suggests the importance of the occluded regions in the model's comprehension of the input. However, occlusion sensitivity might be computationally intensive, especially when evaluating multiple occlusions and it may not capture complex non-linear relationships.

6) Attention rollout: Similar to occlusion sensitivity, attention rollout offers a window into the decision-making process of ViT models. However, unlike occlusion sensitivity which physically blocks parts of the image, attention rollout delves deeper into the model's internal computations. Central to the functionality of ViT models are "attention" mechanisms, which enable the model to assign importance scores to various image regions. Attention allows the model to understand the relationships between different parts of an image, assigning importance scores to various regions. Attention rollout builds upon this by iteratively analyzing these attention scores.

Attention rollout starts with the final layer's attention maps, highlighting crucial image regions for the prediction. It then uses these maps to "roll back" through the network, revealing lower-level features (like edges or textures) that ultimately contributed to the final scores. By analyzing these intermediate maps, we gain insights into how the model builds its understanding of the image. Attention rollout offers advantages over occlusion sensitivity: it's computationally efficient and can capture intricate relationships between image regions. However, it doesn't provide a definitive explanation for the model's reasoning process.

III. Results

A. Studies of Scalp Disorder Diagnosis based on XAI and Deep Learning

Although the integration of DL and XAI has found extensive application in various healthcare research domains, its utilization in scalp imaging remains a gap in research. There is a clear necessity for additional research on the implementation of XAI in scalp imaging to advance its capabilities. As outlined in Table I, recent studies demonstrate a comparative analysis with conventional models, emphasizing the potential for enhancement and innovation in the domain of scalp disorder imaging. Table II illustrated Heng et al. research [37] based on two experiments. Tables III and IV display the results of the research conducted by Jeong et al. and Ha et al., respectively.

IV. Discussion

The Shih et al.'s seminal study [26] introduces a pioneering system for automated hair counting in scalp images, addressing challenges such as oily spots, wavy or curly textures, and overlapping hairs through a morphology-based approach, multi-scale line detection, and relaxation labeling. Their

approach leverages a combination of techniques: morphology-based filtering, multi-scale line detection, and relaxation labeling. While evaluated on a limited dataset of 40 images, the system achieves remarkable results with an average precision of 98.0% and recall of 85.6%. Despite the limitations in data size and algorithmic complexity, this study represents a significant pioneering effort in the field of medical image analysis using ML. It paves the way for further advancements in automated hair analysis.

With more focus on telehealth as an application of scalp hair diagnosis, Su et al.'s study [3] introduces a system to automatically identify scalp conditions. The system offers potential benefits like faster diagnosis and utilizes a cloud platform for data collection and analysis, potentially improving accuracy over time. However, some limitations need to be addressed. The system focuses on surface-level conditions like dandruff and doesn't delve into potentially linked medical issues. Additionally, details about the training data used for the DL model are missing. Future work should explore incorporating analysis of potentially linked medical problems, increasing transparency in the system's decision-making process, and integrating with telehealth platforms for wider accessibility.

In a simultaneous effort, Wang et al. utilized a dataset comprising 1000 images, with 880 designated for training and 220 for testing. The scalp images were captured using a 200x magnification camera and categorized into four types of diseases. The researchers also introduced a novel model named ImageNet-VGG-f Bag of Words (BOW), which employ ImageNet-VGG pre-trained model[42] to evaluate its predictive capabilities in comparison to other ML classification algorithms. The achieved accuracy for this model was reported at 89.77%. This accuracy significantly outperforms other ML-based methodologies in the research, such as BOW with support vector machines (SVM) at 80.50% and pyramid histogram of oriented gradients (PHOG) with SVM at 53.0%. These findings underscore the promising potential of integrating hybrid DL approaches in the field of scalp hair imaging diagnosis over conventional ML methods.

Chang et al. introduced ScalpEye [2], a comprehensive system for scalp analysis that represents a significant advancement in scalp imaging. ScalpEye integrates medical imaging with AI analysis, offering a user-friendly mobile app for image capture, a cloud server for model improvement, a centralized platform for system management, and a portable microscope for high-quality image acquisition. The study utilized nearly 2200 scalp images from the COCO dataset, categorized into four common scalp conditions. Three deep learning models were employed for analysis: Faster R-CNN Inception_v2, SSD Inception_v2, and a novel model called Faster R-CNN Inception_ResNet_v2_Atrous. This new model combines Faster R-CNN with Inception_ResNet_v2_Atrous, which utilizes Atrous convolution for a stable receptive field size. This stability allows for better fine-tuning and more accurate predictions. Consequently, the Faster R-CNN Inception_ResNet_v2_Atrous achieved an impressive mean Average Precision (mAP) of 91.75%. While ScalpEye prioritizes both data quality and DL models within a cloud-based telehealth system, a key challenge remains. Annotating large datasets requires significant manpower and expertise. This raises the question of how the system will handle future large-scale datasets.

In Chow et al.'s research [38], the application of the CNN in the last run achieved an impressive accuracy of 96.30%. To gain a more profound insight into the factors that influence the model's classification of hair health, the researchers employed the LIME technique. Upon the analyzing of LIME, several observations were made. For instance, in the case of alopecia areata, a patchy bald condition, the heatmap coincided with the bald patches, although there were some inexplicable identifications in the right corner. The study concluded that despite achieving a remarkable accuracy of 96.30%, the application of LIME highlighted potential biases in the model's decision-making process, suggesting the need for further investigation and refinement. Further studies are crucial to identify and eliminate potential biases that could affect the model's biases and generalizability, potentially through image binarization and randomization techniques.

In the study conducted by Heng et al. [37], two experiments were conducted to assess the performance of dermatological image classification. The first experiment utilized the Dernet dataset, comprising 240 images with categories such as acne keloidalis, alopecia, and others. The second experiment involved a combination of Dermnet and Figaro-1k datasets[43], totaling 485 images, categorized as healthy and unhealthy. Two pre-trained models, Inception-v3[44] and SqueezeNet [45], using the RMSProp optimizer, were employed for these experiments. For the first experiment using Inception-v3, the model achieved an accuracy of 63.9%. In the second experiment, SqueezeNet was utilized, resulting in an impressive accuracy of 100%. However, despite this high accuracy, the integration of three XAI techniques, Grad-CAM, LIME, and occlusion sensitivity, revealed some noteworthy findings. In the second experiment, the classification was influenced by unrelated areas, casting doubt on the reliability of the 100% accuracy. On the other hand, the first experiment suggested that the model's predictions were primarily affected by the forehead area, highlighting the importance of specific regions in making final decisions. However, despite this emphasis, the accuracy achieved was only 63.9%.

TABLE I. SUMMARIZING AI STUDIES IN SCALP DISORDER DIAGNOSIS

Article	Dataset	Model	Results
Shih et al. (2015)[26]	40 scale images	Hair-bundling algorithm	98.0% of precision 85.56% of recall
Su et al (2018)[3]	Not mentioned	VGG-net	90.9% of accuracy
Wang et al. (2018)[4]	1000 images (880 training images/ 220 testing images)	ImageNet-VGG-f model Bag of Words	89.77% of accuracy
Chang et al. (2020)[2]	2198 images	Faster R-CNN based model	91.75% in mAP
Chow et al. (2022)[38]	1079 images (864 training image, 215 validation image)	LIME, CNN	96.63% of accuracy
Heng et al. (2023)[37]	DermNet dataset: 240 images Figaro-1k dataset: 245 images	Integrating Grad-CAM/LIME/Occlusion Sensitivity with multiple DL models	Illustrated in Table II
Jeong et al. (2023)[39]	100,000 images (x60)	EfficientNet-B6	Illustrated in Table IV
Roy et al. (2023)[40]	150 images	CNN	91.1% of accuracy
Ha et al. (2024)[41]	100,000 images (x60)	Attention rollout with ViT-B/16	Illustrated in Table III

TABLE II. HENG ET AL. RESULT [37] BASED ON TWO EXPERIMENTS

Scalp Symptoms	Number of images	Accuracy (%)
Dryness	17,434	91.3
Oiliness	80,416	90.5
Erythema	4,592	89.6
Folliculitis	4,592	87.6
Dandruff	40,482	87.3
Hair loss	25,682	89.0

In Roy et al.'s concurrent research [40], a dataset comprising scalp images from multiple sources was collected, consisting of 150 images depicting three different diseases: alopecia, psoriasis, and folliculitis. The research employed CNN, and after experimenting with 25 different combinations, a neural network architecture with three hidden layers, one input layer, and one output layer was chosen as the final design. The training process used a batch size of 16 for each batch over 50 epochs, and the preprocessed data was divided into a 70-30 train-test split for training and validation purposes. The model was constructed with 256 inputs, a 3x3 square kernel, 3 output units, and a Softmax output layer. The model achieved a training accuracy of 96.2% and a validation accuracy of 91.1%. This approach demonstrates a careful exploration of model architecture variations, leading to the selection of an optimal configuration. The high training and validation accuracies indicate the effectiveness of the chosen model in learning and generalizing from. However, it is essential to consider the potential impact of overfitting and the model's performance on unseen data.

TABLE III. RESULTS OF JEONG ET AL.'S RESEARCH UTILIZING EFFICIENT NET-B6 MODEL

Dataset and Model	DermNet and Inception-V3	Figaro-1k and SqueezeNet
Training accuracy (%)	98.4	100.0
Validation accuracy (%)	63.9	100.0
Validation sensitivity (%)	88.9	100.0

TABLE IV. RESULTS OF HA ET AL.'S RESEARCH UTILIZING THE VIT-B/16 MODEL

Scalp Symptoms	Number of images	Accuracy (%)	F1-Score (%)	Precision (%)	Recall (%)
Dryness	17,434	77.7	76.7	77.0	76.9
Oiliness	80,416	69.0	70.1	69.7	70.6
Erythema	4,592	81.4	81.6	81.5	81.7
Folliculitis	4,592	82.3	82.5	82.3	82.6
Dandruff	40,482	77.1	79.3	79.3	79.3
Hair loss	25,682	82.3	83.1	83.0	83.0

AI-ScalpGrader [39], a DL system designed for scalp diagnosis, offers promise with its detailed classification scheme. Analyzing ten scalp conditions based on seven dermatologist-defined indices, it provides a more comprehensive picture of scalp health compared to limited-scope systems. Additionally, the cloud-based platform facilitates data storage, analysis, and potentially allows remote monitoring of scalp care. However, limitations exist. The system's accuracy, reported to be between 87.3% and 91.3% for various scalp conditions, depends heavily on training data quality and diversity. While a sizeable dataset of 100,000 images is mentioned, details regarding its composition and potential biases such as: F1-score, recall and precision are lacking. Transparency surrounding the verification process is also needed to build trust in the system's reliability. Expanding the training dataset with a wider range of scalp conditions and ethnicities is crucial. Additionally, exploring integration with telehealth platforms could revolutionize access to scalp care services.

One of the latest studies presented in Ha et al.'s research [41] proposes a DL-based intelligent healthcare platform to diagnose six common scalp hair disorders (dryness, oiliness, erythema, folliculitis, dandruff, and hair loss) with the same dataset as Jeon et al.'s study [39]. Distinguishing itself from prior research, this platform not only classifies the presence or absence of a condition but also predicts severity levels ranging from 0 to 3 for each disorder. The study advances the field by encompassing a broader spectrum of scalp conditions, incorporating predictive severity assessment, and integrating XAI techniques for lesion visualization. Moreover, its user-friendly software facilitates convenient self-monitoring at home. However, the authors acknowledge the potential influence of lighting environments on data quality, particularly affecting the classification of oiliness severity. Overall, this study underscores the promising potential of DL and XAI, notably ViT models and attention rollout, in the analysis of scalp health, although further research is imperative to ensure widespread clinical adoption.

In summarize, the pursuit of effective methodologies for scalp imaging and hair disorder diagnosis has led to the establishment of multiple research initiatives. DL techniques have outperformed traditional ML approaches in terms of accuracy, efficiency, and generalizability, showcasing their potential in advancing the field. Nevertheless, the inherent opacity of decision-making processes in DL poses challenges for clinical applications. The integration of XAI techniques, such as LIME, Grad-CAM, SHAP and attention rollout presents promising avenues to address this issue. However, a critical need for further research exists to comprehensively understand how these DL methods interact with wider range of datasets, ensuring their efficacy and reliability in real-world clinical scenarios.

V. Conclusion

In conclusion, our comprehensive review of studies underscores the transformative impact of DL in revolutionizing scalp imaging and advancing the diagnosis of hair disorders, especially with the help of XAI in understanding complex decision-making process. The demonstrated synergy between XAI and DL in handling complex imaging tasks marks a significant advancement. However, the imperative for ongoing research in this domain is encouraged, with the possibility to improve treatments for this global concern. The combination of XAI and DL holds promise not only for professionals but also for non-professionals, offering potential applications in self-diagnosis. Looking forward, the pursuit of further research, particularly in real-time detection, stands to benefit both professionals and individuals, contributing to improved living conditions for those affected by hair scalp diseases. However, several limitations remain. Many studies rely on small, non-representative datasets, limiting generalizability, and the lack of transparency regarding training data raises concerns about potential biases. Additionally, while XAI techniques like LIME, Grad-CAM, and SHAP provide valuable insights into model decision-making, they add computational complexity that may hinder clinical adoption. Some models demonstrate strong performance under controlled conditions but struggle in real-world settings due to variables like lighting and image quality. Moreover, the integration of these systems with telehealth platforms and their ability to predict severity levels across diverse patient populations still require further refinement. Despite these challenges, the combination of DL and XAI offers significant potential for improving the diagnosis and treatment of scalp and hair disorders, but further research is crucial to ensure their efficacy, transparency, and widespread applicability in clinical practice.

Acknowledgment

This research Supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF- RS-2023-00237287, NRF-2021S1A5A8062526) and local government-university cooperation-based regional innovation projects (2021RIS-003).

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] S. K. Zhou et al., "A Review of Deep Learning in Medical Imaging: Imaging Traits, Technology Trends, Case Studies With Progress Highlights, and Future Promises," Proceedings of the IEEE, vol. 109, no. 5, pp. 820–838, May 2021, doi: 10.1109/JPROC.2021.3054390.

[2] W.-J. Chang, L.-B. Chen, M.-C. Chen, Y.-C. Chiu, and J.-Y. Lin, "ScalpEye: A Deep Learning-Based Scalp Hair Inspection and Diagnosis System for Scalp Health," IEEE Access, vol. 8, pp. 134826–134837, 2020, doi: 10.1109/ACCESS.2020.3010847.

[3] J.-P. Su et al., "An Intelligent Scalp Inspection and Diagnosis System for Caring Hairy Scalp Health," in 2018 IEEE 7th Global Conference on Consumer Electronics (GCCE), Oct. 2018, pp. 507–508. doi: 10.1109/GCCE.2018.8574619.

[4] W.-C. Wang, L.-B. Chen, and W.-J. Chang, "Development and Experimental Evaluation of Machine-Learning Techniques for an Intelligent Hairy Scalp Detection System," Applied Sciences, vol. 8, no. 6, Art. no. 6, Jun. 2018, doi: 10.3390/app8060853.

[5] M. E. Morocho-Cayamcela, H. Lee, and W. Lim, "Machine Learning for 5G/B5G Mobile and Wireless Communications: Potential,

Limitations, and Future Directions," IEEE Access, vol. 7, pp. 137184–137206, 2019, doi: 10.1109/ACCESS.2019.2942390.

[6] K. Papp, J. Berth-Jones, K. Kragballe, G. Wozel, and M. De La Brassinne, "Scalp psoriasis: a review of current topical treatment options," Journal of the European Academy of Dermatology and Venereology, vol. 21, no. 9, pp. 1151–1160, 2007, doi: 10.1111/j.1468-3083.2007.02424.x.

[7] D. Tucker and S. Masood, "Seborrheic Dermatitis," in StatPearls, Treasure Island (FL): StatPearls Publishing, 2024. Accessed: Mar. 28, 2024. [Online]. Available: http://www.ncbi.nlm.nih.gov/books/NBK551707/

[8] S. Kalam, J. Betkerur, P. S. S. Ranugha, and V. Shastry, "Scalp dermatoses: The patterns and impact on quality of life," Journal of Pakistan Association of Dermatologists, vol. 33, no. 3, Art. no. 3, Aug. 2023.

[9] "The Relationship between Self-esteem, Mental Health and Quality of Life in Patients with Skin Diseases. Asian J. Med. Pharm. Res., 3(2): 50-54.," 2013.

[10] H. Lee, I. Son, J. Yoon, and S.-S. Kim, "Lookism hurts: appearance discrimination and self-rated health in South Korea," Int J Equity Health, vol. 16, no. 1, p. 204, Nov. 2017, doi: 10.1186/s12939-017-0678-8.

[11] B. E. Elewski, "Clinical Diagnosis of Common Scalp Disorders," Journal of Investigative Dermatology Symposium Proceedings, vol. 10, no. 3, pp. 190–193, Dec. 2005, doi: 10.1111/j.1087-0024.2005.10103.x.

[12] F. Lacarrubba, G. Micali, and A. Tosti, "Scalp Dermoscopy or Trichoscopy," Feb. 2015, doi: 10.1159/000369402.

[13] A. Barragán-Montero et al., "Artificial intelligence and machine learning for medical imaging: A technology review," Physica Medica, vol. 83, pp. 242–256, Mar. 2021, doi: 10.1016/j.ejmp.2021.04.016.

[14] A. K. Gupta, I. A. Ivanova, and H. J. Renaud, "How good is artificial intelligence (AI) at solving hairy problems? A review of AI applications in hair restoration and hair disorders," Dermatologic Therapy, vol. 34, no. 2, p. e14811, 2021, doi: 10.1111/dth.14811.

[15] B. H. M. van der Velden, H. J. Kuijf, K. G. A. Gilhuijs, and M. A. Viergever, "Explainable artificial intelligence (XAI) in deep learning-based medical image analysis," Medical Image Analysis, vol. 79, p. 102470, Jul. 2022, doi: 10.1016/j.media.2022.102470.

[16] G. Campos-do-Carmo and M. Ramos-e-Silva, "Dermoscopy: basic concepts," International Journal of Dermatology, vol. 47, no. 7, pp. 712–719, 2008, doi: 10.1111/j.1365-4632.2008.03556.x.

[17] S. González and Z. Tannous, "Real-time, in vivo confocal reflectance microscopy of basal cell carcinoma," Journal of the American Academy of Dermatology, vol. 47, no. 6, pp. 869–874, Dec. 2002, doi: 10.1067/mjd.2002.124690.

[18] W.-J. Chang et al., "A Mobile Device-Based Hairy Scalp Diagnosis System Using Deep Learning Techniques," in 2020 IEEE 2nd Global Conference on Life Sciences and Technologies (LifeTech), Mar. 2020, pp. 145–146. doi: 10.1109/LifeTech48969.2020.1570617332.

[19] J.-H. Kim, S. Kwon, J. Fu, and J.-H. Park, "Hair Follicle Classification and Hair Loss Severity Estimation Using Mask R-CNN," Journal of Imaging, vol. 8, no. 10, Art. no. 10, Oct. 2022, doi: 10.3390/jimaging8100283.

[20] S. Kim et al., "Smartphone-based multispectral imaging and machine-learning based analysis for discrimination between seborrheic dermatitis and psoriasis on the scalp," Biomed. Opt. Express, BOE, vol. 10, no. 2, pp. 879–891, Feb. 2019, doi: 10.1364/BOE.10.000879.

[21] Z. Yu, S. Kaizhi, H. Jianwen, Y. Guanyu, and W. Yonggang, "A deep learning-based approach toward differentiating scalp psoriasis and seborrheic dermatitis from dermoscopic images," Frontiers in Medicine, vol. 9, 2022, Accessed: Nov. 18, 2023. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fmed.2022.965423

[22] M. GAO et al., "Deep Learning-based Trichoscopic Image Analysis and Quantitative Model for Predicting Basic and Specific Classification in Male Androgenetic Alopecia," Acta Derm Venereol, vol. 102, p. 564, Jan. 2022, doi: 10.2340/actadv.v101.564.

[23] M. Di Fraia et al., "A Machine Learning Algorithm Applied to Trichoscopy for Androgenic Alopecia Staging and Severity Assessment," Dermatol Pract Concept, vol. 13, no. 3, p. e2023136, Jul. 2023, doi: 10.5826/dpc.1303a136.

[24] G. Urban et al., "Combining Deep Learning With Optical Coherence Tomography Imaging to Determine Scalp Hair and Follicle Counts," Lasers in Surgery and Medicine, vol. 53, no. 1, pp. 171–178, 2021, doi: 10.1002/lsm.23324.

[25] A. M. Malciu, M. Lupu, and V. M. Voiculescu, "Artificial Intelligence-Based Approaches to Reflectance Confocal Microscopy Image Analysis in Dermatology," Journal of Clinical Medicine, vol. 11, no. 2, Art. no. 2, Jan. 2022, doi: 10.3390/jcm11020429.

[26] H.-C. Shih, "An Unsupervised Hair Segmentation and Counting System in Microscopy Images," IEEE Sensors Journal, vol. 15, no. 6, pp. 3565–3572, Jun. 2015, doi: 10.1109/JSEN.2014.2381363.

[27] H.-C. Shih and B.-S. Lin, "Hair segmentation and counting algorithms in microscopy image," in 2015 IEEE International Conference on Consumer Electronics (ICCE), Jan. 2015, pp. 612–613. doi: 10.1109/ICCE.2015.7066549.

[28] H. Benhabiles et al., "Deep Learning based Detection of Hair Loss Levels from Facial Images," in 2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA), Oct. 2019, pp. 1–6. doi: 10.1109/IPTA.2019.8936122.

[29] S. S. Han, M. S. Kim, W. Lim, G. H. Park, I. Park, and S. E. Chang, "Classification of the Clinical Images for Benign and Malignant Cutaneous Tumors Using a Deep Learning Algorithm," J Invest Dermatol, vol. 138, no. 7, pp. 1529–1538, Jul. 2018, doi: 10.1016/j.jid.2018.01.028.

[30] A. Esteva et al., "Dermatologist-level classification of skin cancer with deep neural networks," Nature, vol. 542, no. 7639, Art. no. 7639, Feb. 2017, doi: 10.1038/nature21056.

[31] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," Jan. 06, 2016, arXiv: arXiv:1506.01497. doi: 10.48550/arXiv.1506.01497.

[32] W. Liu et al., "SSD: Single Shot MultiBox Detector," vol. 9905, 2016, pp. 21–37. doi: 10.1007/978-3-319-46448-0_2.

[33] A. Dosovitskiy et al., "An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale," Jun. 03, 2021, arXiv: arXiv:2010.11929. doi: 10.48550/arXiv.2010.11929.

[34] R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh, and D. Batra, "Grad-CAM: Visual Explanations From Deep Networks via Gradient-Based Localization".

[35] M. T. Ribeiro, S. Singh, and C. Guestrin, "'Why Should I Trust You?': Explaining the Predictions of Any Classifier," in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco California USA: ACM, Aug. 2016, pp. 1135–1144. doi: 10.1145/2939672.2939778.

[36] M. D. Zeiler and R. Fergus, "Visualizing and Understanding Convolutional Networks," Nov. 28, 2013, arXiv: arXiv:1311.2901. Accessed: Nov. 19, 2023. [Online]. Available: http://arxiv.org/abs/1311.2901

[37] W. W. Heng and N. A. Abdul-Kadir, "Deep Learning and Explainable Machine Learning on Hair Disease Detection," in 2023 IEEE 5th Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS), Jun. 2023, pp. 150–153. doi: 10.1109/ECBIOS57802.2023.10218472.

[38] W. Y. Chow, W. W. Heng, N. A. Abdul-Kadir, and H. Nadaraj, "Explainable Machine Learning on Classification of Healthy and Unhealthy Hair," in 2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Oct. 2022, pp. 162–167. doi: 10.1109/ICICyTA57421.2022.10037969.

[39] J.-I. Jeong, D.-S. Park, J.-E. Koo, W.-S. Song, D.-J. Pae, and H.-J. Choi, "Artificial intelligence (AI) based system for the diagnosis and classification of scalp health: AI-ScalpGrader," Instrumentation Science & Technology, vol. 51, no. 4, pp. 371–381, Jul. 2023, doi: 10.1080/10739149.2022.2129382.

[40] M. Roy and A. T. Protity, "Hair and Scalp Disease Detection using Machine Learning and Image Processing," COMPUTE, vol. 3, no. 1, pp.

7–13, Jan. 2023, doi: 10.24018/compute.2023.3.1.85.

[41] C. Ha, T. Go, and W. Choi, "Intelligent Healthcare Platform for Diagnosis of Scalp and Hair Disorders," Applied Sciences, vol. 14, no. 5, Art. no. 5, Jan. 2024, doi: 10.3390/app14051734.

[42] K. Chatfield, K. Simonyan, A. Vedaldi, and A. Zisserman, "Return of the Devil in the Details: Delving Deep into Convolutional Nets," Nov. 05, 2014, arXiv: arXiv:1405.3531. doi: 10.48550/arXiv.1405.3531.

[43] M. Svanera, U. R. Muhammad, R. Leonardi, and S. Benini, "Figaro, hair detection and segmentation in the wild," in 2016 IEEE International Conference on Image Processing (ICIP), Sep. 2016, pp. 933–937. doi: 10.1109/ICIP.2016.7532494.

[44] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the Inception Architecture for Computer Vision," arXiv.org. Accessed: Nov. 20, 2023. [Online]. Available: https://arxiv.org/abs/1512.00567v3

[45] F. N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally, and K. Keutzer, "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size," arXiv.org. Accessed: Nov. 20, 2023. [Online]. Available: https://arxiv.org/abs/1602.07360v4

A Theoretical Framework of Extrinsic Feedback Evaluation in Football Training Based on Motion Templates Using Motion Capture

Amir Irfan Mazian[1], Wan Rizhan[2], Normala Rahim[3], Muhammad D. Zakaria[4],
Mohd Sufian Mat Deris[5], Fadzli Syed Abdullah[6], Ahmad Rafi[7]
Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut, Malaysia[1, 2, 3, 4, 5]
Faculty of Ocean Engineering Technology, Universiti Malaysia Terengganu, Kuala Nerus, Malaysia[6]
Faculty of Creative Multimedia, Multimedia University, Cyberjaya, Malaysia[7]

***Abstract*—Motion capture technology (MoCap) has emerged as a pivotal innovation, significantly impacting various sectors, including sports. In football training, MoCap is especially crucial for analyzing player movements with precision. Despite its potential, there remains a notable gap in the utilization of MoCap to create motion templates (MTs) that generate extrinsic feedback, particularly in football. This article proposes a comprehensive theoretical framework for evaluating extrinsic feedback in football training through MTs created using MoCap technology and Reverse-Gesture Description Language (R-GDL). The development of this framework involves several key steps: a literature review, acquaintance meetings, interviews, procedural approvals, experimentation, data conversion, MTs creation, and data evaluation. The framework integrates elements such as football players, MoCap systems, raw and processed data, MTs, evaluation processes, and extrinsic feedback models. The main purpose is to harness the full potential of MoCap technology, enhancing the evaluation and improvement of football training activities. By implementing this framework, we aim to revolutionize how football training is analyzed and optimized, providing coaches and players with invaluable insights and feedback.**

***Keywords*—Motion capture; motion templates; football; extrinsic feedback; reverse-gesture description language**

I. Introduction

In the current era of rapid technology revolution, motion capture technology (MoCap) has emerged as an important innovation, profoundly impacting sectors such as sport [1], entertainment [2], healthcare [3] and martial arts [16]. This technology, which digitally records and analyzes movements for comprehensive examination, is distinguished into two types of techniques: marker-based and marker-less systems [3,4,17]. Marker-based systems, which involve attaching physical markers to an individual, excel in capturing movement with exceptional precision, making them invaluable for detailed analyses and the creation of animations, though they may limit natural movement. Conversely, marker-less systems rely on advanced computer vision algorithms to detect the body's natural features without additional equipment, offering a more unobtrusive and adaptable approach [5]. Despite facing challenges in accurately capturing intricate movements, the relentless pace of technological progress is continually improving the accuracy and reliability of both techniques.

The fascination and widespread appeal of football, transcending continents and cultures, significantly highlights its stature as a global sporting phenomenon. This sport, predicated on the principles of teamwork, strategic understanding, and peak physical conditioning, demands a holistic approach to player development, encompassing technical prowess, tactical knowledge, physical fitness, and mental fortitude [6]. Both marker-based and marker-less, play a pivotal role in football, especially in the analysis of player movements, thereby refining training methodologies. Marker-based systems, exemplified by Vicon [7], offer unparalleled precision in tracking athletes' movements within controlled environments, whereas marker-less systems such as OpenPose [8], excel in capturing motion in more organic settings. These technological advancements facilitate a comprehensive examination of player performance, enabling coaches and sports scientists to optimize training activities and enhance strategic execution, underscoring the symbiotic relationship between cutting-edge technology and the evolution of football training practices.

Moreover, a ground-breaking application of MoCap technology in football training is the use of MTs. These templates are engineered through detailed analysis of elite athletes' movements, captured via the MoCap system. They provide a standard for the ideal execution of specific sporting actions, such as kicking and passing, facilitating the accurate replication of optimal movement patterns. This methodology offers a dual advantage: a quantitative benchmark for evaluating performance and a visual aid for enhancing technical proficiency [9]. By setting side by side an athlete's movements with these predefined templates, coaches are empowered to pinpoint inaccuracies and provide bespoke corrective feedback. This tailored approach optimizes training efficiency by aligning with each athlete's unique biomechanical characteristics, thereby fostering a customized coaching paradigm.

Feedback can be classified into two types: extrinsic and intrinsic [10]. The confluence of extrinsic and intrinsic feedback mechanisms plays a quintessential role in football training. Extrinsic feedback, provided by external sources, offers invaluable insights into performance analytics and delineates areas ripe for improvement [18]. This is in harmonious complement to intrinsic feedback, which athletes derive from their own sensory experiences during the performance of an

action. Together, these feedback modalities are indispensable in skill development, highlighting the critical importance of external inputs for learning and refining techniques. This synergy underscores a holistic approach to mastering skills, essential for the attainment of excellence in any sporting discipline.

However, there is a lack of MoCap technology usage to create MTs in sport that produce extrinsic feedback, especially in football. Therefore, the application of MoCap technology within football and additional sports disciplines marks a significant advancement in training methodologies and performance analytics. The integration of both marker-based and marker-less systems, supplemented by innovative solutions such as MTs, enables coaches and trainers to refine training regimens with unprecedented precision, efficiency, and customization. This technological evolution not only enhances the analysis and application of specific athletic movements but also paves the way for ground-breaking research and development within the field of sports science. Consequently, this promises to yield substantial enhancements in athlete performance and the refinement of training methodologies.

The research proposes a theoretical framework of extrinsic feedback in evaluating football training based MTs using MoCap. The next sections discuss the methods in Section III, the proposed framework in Section IV, the expected outcome in Section V and discussion and conclusion in Section VI.

II. Related Works

In MoCap technology, it has become a significant tool in football for analyzing player movement, medical evaluation and training improvement. In existing studies, the researchers have employed various techniques with different MoCap systems in football. For example, Yin et al. utilized a deep learning-assisted motion capture system (DL-MCS) in football training, which evaluates complexity, performance, latency and efficiency. This approach integrates deep learning to support training effectiveness, particularly by evaluating the accuracy of player movement [19]. Similarly, Della Villa et al. implemented a 2D video analysis scoring system to identify football players with a high knee abduction moment, which is a risk factor for ACL injuries. Their approach, which involved a stereophotogrammetric camera system and force platform, aimed to provide accurate health measurement to enhance injury prevention plan [20].

In marker-less MoCap, Bampouras and Thomas validated a Light Detection and Ranging (LiDAR)-based player tracking system for football-specific tasks, focusing on metrics such as velocity and acceleration. This technique evaluates the precision and responsiveness of marker-less system in capturing football player performance during fast-paced actions. By analyzing key performance indicators in real time, this study demonstrated the potential of marker-less MoCap system to provide relevant feedback, but with some limitation in data accuracy that affect the reliability of real-time extrinsic feedback [21].

Aughey et al. compared computer vision system with three-dimensional marker-based MoCap for tracking football players' movement in a stadium environment. Their evaluation, using root mean square deviation (RMSD) to calculate speed and accuracy, demonstrated how advance MoCap technology can capture dynamic football players' movement in large, open spaces, showing the adaptability of MoCap technology to diverse training activity condition. However, while computer vision systems support movement analysis, they still lack the precision needed for extrinsic feedback [22].

These studies highlight that while MoCap technologies have advanced considerably in capturing detailed player motion, the lack of extrinsic feedback remains a significant limitation. The integration of motion templates in MoCap system could bridge this gap, enabling real-time adjustment in training.

III. Method

To create MTs that enable effective extrinsic feedback in football training, benefiting coaches and experts, a systematic approach involving both formal and informal research methodology is essential. The approach to create a new framework was adapted [11], which has proven effective in generating MTs for folk dances but lacking for the dynamic requirements of football training. Incorporation of additional elements into approach is necessary to tailor it specifically to football's unique requirements. By refining this approach, acquisition of critical insights and development of MTs specifically designed for football training become possible. The refined approach, shown in Fig. 1, includes literature study, acquaintance meeting, interview, procedure and approval, experiment, data conversion, motion template creation, and data evaluation.

Fig. 1. New proposed approach for creating MTs in football training using MoCap.

A. Literature Study

Systematic Literature Review (SLR) is one of the methods in academic research, purposely to consolidate all existing evidence. The multifaceted process encompasses the

formulation of a research question guided by specific keywords, the detailed selection of relevant studies, the evaluation of their quality, and the systematic extraction and analysis of data. The objective of SLR is to furnish an impartial, exhaustive overview of the evidence at hand [12] This method not only strengthens the foundation for evidence-based practices but also highlights gaps in current research. By being attached to established reporting guidelines like PRISMA, these reviews ensure transparency and reproducibility [13].

B. Acquaintance Meeting

The primary objective of the meeting is to collect critical information about football and its training. Hence, engaging with the State Football Club, recognized as one of football expertise, which involves the qualified coaching staff, becomes a vital initial step for accruing foundational information prior to progressing with the research. The anticipated outcomes from these introductory sessions include:

- Documentation of football and coaching, encompassing evaluation forms and training guidelines.
- Detailed accounts of the processes involved in football training and coaching.
- Proposal for conducting formal interviews with qualified coaches.

The insights obtained from these preliminary meetings are instrumental for advancing to the next phases of the research.

C. Interview

Conducting interviews serves as an essential method for obtaining comprehensive insights regarding football coaching directly from seasoned professionals. The structure of these discussions varies, encompassing formal interviews with predefined queries, semi-structured interviews with a mix of fixed and open-ended questions, and informal conversations that proceed naturally. To facilitate these discussions, a carefully curated set of questions will be prepared in advance. The frequency of these interviews is determined by the relevance and adequacy of the information collected in meeting specific goals and expectations. Furthermore, it is vital to communicate the purpose of the study to the coaches. This communication not only aids in clarifying the objectives of the research but also invites valuable contributions from the coaches regarding the selection of football training activities for the study.

D. Procedure and Approval

Further research on football training can be conducted by applying for and following the required legal procedures and obtaining the necessary approvals.

1) Letter of purpose for conducting the research: Obtaining approval and support from the appropriate authorities or organizations is important for conducting the research. This letter contains the purpose, needs and importance of research in football training. In addition to explaining the use of current technology which is MoCap that has potential to help improve football training through research.

2) Letter of invitation to interview session: This letter serves as an invitation to certified coaches for a formal interview session. The goal is to collect information related to football training activities that are suitable to, along with suggestions, input, and feedback from the qualified coaches to enhance the research. Essential details such as the names of the coaches, the specific date, time, and location of the interview will be included in the letter. This strategy ensures clarity and facilitates the effective participation of these professionals in the study.

3) Request for nomination of qualified football player: The purpose is to reach out to coaches, seeking their assistance in nominating skilled football players who exhibit diverse qualities, such as being adept with either their left or right leg. Given the coaches' deep familiarity with , their teamsensuring that the selected players are indeed the best fit. This approach leverages the coaches' expertise, ensuring that the chosen athletes truly reflect the required attributes, without any room for doubt or challenge regarding their suitability.

4) Letter of invitation for conducting the fieldwork: An invitation to certified coaches and selected football players to participate in the experiment. The goal is to record and collect the MoCap data of football players' movement doing football training activities that had been assigned by the coaches. Essential details such as the names of the coaches, the specific date, time, and location of the interview will be included in the letter.

5) Request for verification of motion template: The goal is to look for assistance from experts to confirm the MTs created with captured movement data. It is crucial to verify the data's authenticity. The request emphasizes the importance of having several experts available at a designated date, time, and place. This ensures a comprehensive evaluation and verification process.

E. Experiment

The main goal of the experiment is to gather detailed MoCap data of football players as they engage in specific training activities. These activities have been carefully selected based on recommendations from experienced coaches from the previous interview session, ensuring it is relevant to research. The experiment is set to take place in the natural environment of the players, which is outdoors on a football field. To record these movements, the proposed MoCap device is marker-based such as Perception Neuron 3, known for its accuracy and reliability in capturing even the most subtle movements.

Football players will be guided through a series of training activities planned by the coaches. These activities are designed to simulate common football scenarios and challenges, helping to gather a wide range of motion data. As the players perform, coaches will not only supervise but also evaluate their performance using a rubric score assessment form that is validated by the expert. The raw MoCap data collected will then be processed to create MTs. These templates aim to offer detailed data of the movements, serving as a valuable resource for further analysis.

F. Data Conversion

Understanding the need to convert raw data arises from a compatibility issue between the initial format provided by the Perception Neuron 3 MoCap device and the requirements of the Gesture Description Language (GDL) system. Unlike the GDL system, which was originally designed to work with the Xbox Kinect—a marker-less MoCap system. The Perception Neuron 3 relies on a marker-based approach to capture movements. This fundamental difference in technology means that the raw data produced by Perception Neuron 3 contain 59 sections of skeleton joints as shown in Table I [14] while the GDL system contains 25 sections of skeleton joints (Table II) that are available in SKL format. The data from Perception Neuron 3 are available in formats like FBX, BVH, CSV, and MBX, and cannot be directly used in a GDL system without first undergoing a conversion process to suit the SKL format.

TABLE I. SKELETAL JOINT GENERATED FROM PERCEPTION NEURON 3

Section Name	Logotype	Serial Number	Parent Node
Buttocks	Hips	0	Root Node
Right thigh	RightUpLeg	1	0
Right Calf	RightLeg	2	1
Right foot	Rightfoot	3	2
Left thigh	LeftUpLeg	4	0
Left calf	Leftleg	5	4
Left foot	LeftFoot	6	5
Lower Part of the Spine	Spine	7	0
Middle Spine section	Spine 1	8	7
Upper Spine section	Spine 2	9	8
Lower Neck section	Neck	10	9
Upper Neck section	Neck 1	11	10
Head	Head	12	11
Right Shoulder	RightShoulder	13	8
Right Arm	RightArm	14	13
Right Forearm	RightForeArm	15	14
Right Hand	RightHand	16	15
Right thumb finger	RightHandThumb1	17	16
Right thumb in the middle finger	RighthandThumb2	18	17
Right Thumb tip	RighthandThumb2	19	18
Right index metacarpal	RightInHandIndex	20	16
Right index finger root	RightHandIndex1	21	20
Middle finger of the right index finger	RightHandIndex2	22	21
Right index fingertip	RightHandIndex3	23	22
Right middle metacarpal	RightInHandMiddle	24	16
Right middle finger to the root	RightHandMiddle1	25	24
Right middle finger middle	RightHandMiddle2	26	25
Right middle fingertip	RightHandMiddle3	27	26
Right ring metacarpal	RightInHandRing	28	16
Right ring finger refers to the root	RightHandRing1	29	28
Right ring finger in the middle	RightHandRing2	30	29
Right ring fingertip	RightHandRing3	31	30
Right little finger metacarpal	RightInHandPinky	32	16
Right pinky finger root	RightHandPinky1	33	32
Right pinky finger in the middle	RightHandPinky2	34	33
Right pinky fingertip	RightHandPinky3	35	34
Left shoulder	LeftShoulder	36	8
Left upper arm	LeftArm	37	36
Left forearm	LeftForeArm	38	37
left hand	LeftHand	39	38
Left thumb finger root	LeftHandThumb1	40	39
Left thumb in the middle finger	LeftHandThumb2	41	40
Left thumb tip	LeftHandThumb3	42	41
Left index metacarpal bone	LeftInHandIndex	43	39
Left index finger root	LeftHandIndex1	44	43
Middle finger of the left index finger	LeftHandIndex2	45	44
Tip of the left index finger	LeftHandIndex3	46	45
Left middle metacarpal	LeftInHandMiddle	47	39
The left middle finger refers to the root	LeftHandMiddle1	48	47
The left middle finger is fingered in the middle	LeftHandMiddle2	49	48
Left middle fingertip	LeftHandMiddle3	50	49
Left ring metacarpal	LeftInHandRing	51	39
The left ring finger refers to the root	LeftHandRing1	52	51
Left ring finger in the middle	LeftHandRing2	53	52
Left ring fingertip	LeftHandRing3	54	53
Left little finger metacarpal bone	LeftInHandPinky	55	39
Left little finger finger root	LeftHandPinky1	56	55
Left little finger in the middle	LeftHandPinky2	57	56
Left little fingertip	LeftHandPinky3	58	57

TABLE II. SKELETAL JOINT GENERATED FROM GDL SYSTEM

No	Joint Name
1	Spine Base
2	Spine Mid
3	Neck
4	Head
5	Right Shoulder
6	Right Elbow
7	Right Wrist
8	Right Hand
9	Left Shoulder
10	Left Elbow
11	Left Wrist
12	Left Hand
13	Right Hip
14	Right Knee
15	Right Ankle
16	Right Foot
17	Left Hip
18	Left Knee
19	Left Ankle
20	Left Foot
21	Spine Shoulder
22	Right Thumb
23	Right Tip
24	Left Thumb
25	Left Tip

A series of steps outlined (see Fig. 2) are followed to transform the raw data into a format that the GDL system can understand and process. This conversion process results in the production of data in the SKL format, making it compatible for use with the GDL system. The conversion is not just a technical requirement but a bridge that enables the advanced MoCap dataset from Perception Neuron 3 to be utilized effectively in the GDL system environment, thereby enhancing the utility and applicability of MoCap data in various applications.

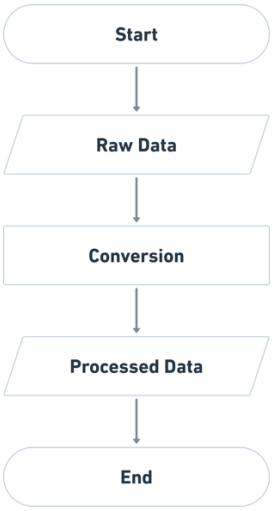


Fig. 2. Data conversion flowchart.

G. Motion Template Creation

R-GDL or Reverse-Gesture Description Language is an extension of the basic concept of GDL, focusing on a machine-learning approach for the recognition of full-body movements. R-GDL's methodology can be considered a form of reverse engineering compared to traditional GDL, as it starts with the outcome (recorded gestures) and works backward to infer the rules that define those gestures. Motion template will be developed by using R-GDL because this method has shown high accuracy in recognizing complex body movements, making it suitable for applications where precise motion detection is required, such as in physical therapy, sports analysis, and advanced human-computer interaction systems [15]. For creating the MTs, features in GDL will be used as shown below:

```
FEATURE angle(ShoulderRight.xyz[0] - ElbowRight.xyz[0],
WristRight.xyz[0] - ElbowRight.xyz[0]) AS RightElbow
 FEATURE angle(ShoulderLeft.xyz[0] - ElbowLeft.xyz[0],
 WristLeft.xyz[0] - ElbowLeft.xyz[0]) AS LeftElbow
 FEATURE angle(ShoulderCenter.xyz[0] - ShoulderRight.xyz[0],
 ElbowRight.xyz[0] - ShoulderRight.xyz[0]) AS RightShoulder
 FEATURE angle(ShoulderCenter.xyz[0] - ShoulderLeft.xyz[0],
 ElbowLeft.xyz[0] - ShoulderLeft.xyz[0]) AS LeftShoulder
 FEATURE angle(HipRight.xyz[0] - KneeRight.xyz[0],
 AnkleRight.xyz[0] - KneeRight.xyz[0]) AS RightKnee
 FEATURE angle(HipLeft.xyz[0] - KneeLeft.xyz[0],
 AnkleLeft.xyz[0] - KneeLeft.xyz[0]) AS LeftKnee
 FEATURE angle(ShoulderRight.xyz[0] - ElbowRight.xyz[0],
 ShoulderLeft.xyz[0] - ElbowLeft.xyz[0]) AS BetweenWrists
 FEATURE angle(KneeLeft.xyz[0] - HipLeft.xyz[0],
 KneeRight.xyz[0] - HipRight.xyz[0]) AS BetweenLeg
```

H. Data Evaluation

GDL are used for the recognition of user actions through the syntactic description of static body poses and movement sequences. It allows for representation of human movements in a way that computer systems can recognize and classify various gestures [15]. By using the GDL system, processed data will be evaluated with a motion template created previously and will produce the output of extrinsic feedback.

IV. PROPOSED FRAMEWORK

In this study, a theoretical framework of extrinsic feedback to evaluate football training has been proposed. Fig. 3 consists of several important models which are the football player, MoCap, raw data, processed data, motion template, evaluation and extrinsic feedback.

Fig. 3 shows the important models in phases of development, testing and evaluation. The development phase consists of football player, MoCap, raw data, processed data and motion template models while the testing phase contains football player, MoCap and raw data models. The evaluation phase consists of comparison and extrinsic feedback models.

A. Football Player

In the development phase of the proposed framework, a certified coach will select skilled and qualified players (Player A). The selection criteria are determined by the coach who also assigns specific football training activities to these players. While in the testing phase, another individual (Player B), who might be new to football or a novice player, participates

alongside Player A in similar training activities. The coach will evaluate their progress using the approved score rubric assessment form.

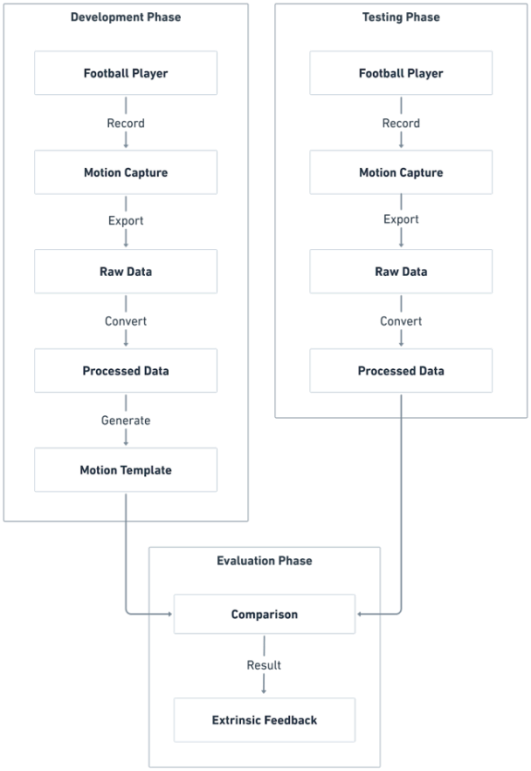


Fig. 3. Proposed framework.

B. Motion Capture

Both development and testing phases, the MoCap device from Perception Neuron with Axis Studio software, will be used on Player A and Player B. Each player will be recorded separately during the same training activities sessions. To ensure the highest quality of data, the actions of each player will be repeated several times per training activities. Specifically for Player A, the data will undergo review by the coach before it can be used as a motion template.

C. Raw Data

The training activities of both players will be digitally captured using the Perception Neuron via Axis Studio, and this data will be accessible in multiple file formats including FBX, BVH, CSV, and MBX that are provided in the software. The FBX and CSV format will be primarily used in the conversion process. This format is preferred because it is widely supported by most of the software, ensuring compatibility and ease of data handling.

D. Processed Data

To produce the processed data from raw data, several procedures in the conversion process (Fig. 2) are needed such as deleting the unused data and rearranging the data. Main purpose of conversion is to have the same attributes of data as the SKL format which is only suitable to use in the GDL system. Both players' data are compulsory to be processed before it can be analyzed.

E. Motion Templates

To create a motion template, the GDL system will be used. This process is exclusively for processed data from player A. As this data has previously received approval from the coach, it will serve as a reference for comparing other data collected from the same training activities by different players or individuals.

F. Comparison

Both motion template data of player A and processed data of player B will be used in the GDL system. To evaluate and get the result of the processed data of player B, the data will be compared to the validated motion template of player A. In the GDL system, it will determine the accuracy and score of the processed data of Player B compared to the motion template of Player A as the result.

The GDL classifier uses rules and features to recognize gestures from MoCap data in the GDL system. It processes MoCap data in several steps. First, it represents a sequence of MoCap data samples taken from ti time to tj, where each sample pta is a vector in R3.d, representing the three-dimensional coordinates (x, y, z) of the body joint.

$$P[ti..tj]=[pti, ...,ptj]$$

This raw data is then transformed into feature space, reducing dimensionality and making it invariant to the camera's position. The transformation is performed by a function *F*.

$$P[ti..tj]F\ ftj$$

The resulting sequence of feature vectors corresponds to the MoCap data samples over time.

$$F[ti..tj]=[fti, ...,ftj]$$

Next, the system evaluates whether specific rules are satisfied at each time step, creating a sequence of rule conclusions rta which can either be true or false.

$$rta \in \{true,false\}r$$

This sequence of rule conclusions over time is represented as

$$R[ti..tj]=[rti, ...,rtj]$$

The transformation function λ considers both the feature vectors and the previous rule conclusions to determine the current rule conclusions.

$$\{F[ti..tj],R[ti..tj-1]\} \rightarrow \lambda\ R[ti..tj]$$

Each time step's data, features, and rule conclusions are stored in a memory stack.

$$sta=\{pta,fta,r'ta\}$$

The entire sequence of MoCap data, feature vectors, and rule conclusions over the given time interval is stored in the GDL memory stack.

$$S[ti..tj]=[sti,...,stj]$$

The classifier uses this stack to apply rules and recognize gestures. When a sequence of rules corresponding to a gesture is satisfied, the gesture is recognized.

G. Extrinsic Feedback

By getting the result of processed data of player B from the GDL system, it can be compared to the previous score rubric assessment form that has the evaluation score from the coach. If the score has high similarity, the expert can verify that the model of motion template of player A can be used to evaluate other players' data because the GDL system produces the same result as the coach evaluation.

V. Expected Outcome

The proposed framework is to improve the way coaches execute and evaluate football training and the player's performance. By integrating MoCap devices, coaches are afforded a clearer picture of player performance. The technology not only assists in detailed analysis but also in decision-making processes and enhances the evaluation of players. Consequently, coaches can refine training methods, ensuring that players are not just practicing harder, but smarter. The immediacy with which feedback is provided to players allows for swift adjustments, fostering an environment of continuous improvement and growth.

Furthermore, MTs are not only an aid in training but a lasting resource that can be accessed, revisited, and utilized repeatedly without degradation or expiration. This aspect guarantees the preservation of data for future use, offering a foundation on which athletes can build and refine their skills over time. Players, therefore, are not just improving in the short term through practice with MoCap devices; they are investing in a resource that supports their long-term development. The reusable nature of these MTs means that both current and future athletes can benefit from a tailored, data-driven approach to skill enhancement, ensuring that the legacy of today's training methods extends far into the future.

VI. Conclusion

A theoretical framework of extrinsic feedback evaluation in football training has been presented in this paper based on MTs. This framework is designed to measure the success of technique execution during football training. To ensure the effectiveness of this study, an initial investigation into the development of MTs in football training, utilizing MoCap, is essential. This includes literature study, acquaintance meeting, procedures and approval, and interview.

In the experiments, the Perception Neuron 3, a marker-based MoCap device, was proposed for utilization due to its accuracy and reliability in capturing data, even for the most subtle movements in sports activities such as football. The data from the device can be used to create MTs, which facilitate the analysis of professional players' data and the preservation of their unique skill movements in digital form. Importantly, this technology is not limited to football but can be explored and applied to other sports activities, enhancing its versatility and value in various athletic disciplines. For futures works, this proposed will be utilized and tested for experimenting the football techniques such as freekick for both left and right footed football players.

Acknowledgment

The author would like to acknowledge the Ministry of Higher Education (MoHE) and Center for Research Excellence and Incubation Management (CREIM), Universiti Sultan Zainal Abidin. This research was supported by the Ministry of Higher Education (MoHE) through Fundamental Research Grant Scheme (Project Code: RR457, Ref. No: FRGS/1/2022/ICT03/UNISZA/02/1). We also want to thank the National Sports Institute of Malaysia and Terengganu Football Club for the shown interest and future collaboration in this study.

References

[1] He, Tianyu, and Qi Luo. 2019. "A Survey of Motion Capture Technology and Its Application in Sports." In *Advances in Intelligent Systems and Computing*, 876:854–59. Springer Verlag. https://doi.org/10.1007/978-3-030-02053-8_129.

[2] Bregler, C. (2007). Motion capture technology for entertainment [In the spotlight]. IEEE Signal Processing Magazine, 24(6), 160–158. https://doi.org/10.1109/msp.2007.906023

[3] Salisu, S., Ruhaiyem, N. I. R., Eisa, T. a. E., Nasser, M., Saeed, F., & Younis, H. A. (2023). Motion Capture Technologies for Ergonomics: A Systematic Literature Review. *Diagnostics*, *13*(15), 2593. https://doi.org/10.3390/diagnostics13152593

[4] Rizhan, Wan Idris, Ahmad Rafi, Azman Bidin, and Azrul Amri Jamal. 2018. "A Theoretical Framework of Extrinsic Feedback Based-Automated Evaluation System for Martial Arts." *International Journal of Engineering & Technology*. Vol. 7.

[5] Halser, Nils, Bodo Rosenhahn, Thorsten Thormahlen, Micheal Wand, Juergen Gall, and Hans-Pieter Siedel. 2009. *Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE Conference on : Dates: 20-25 June 2009.* IEEE.

[6] Carling, Christopher, Jonathan Bloomfield, Lee Nelsen, and Thomas Reilly. 2008. "The Role of Motion Analysis in Elite Soccer Contemporary Performance Measurement Techniques and Work Rate Data." *Sports Med*. Vol. 38.

[7] Perrott, Margaret A., Tania Pizzari, Jill Cook, and Jodie A. McClelland. 2017. "Comparison of Lower Limb and Trunk Kinematics between Markerless and Marker-Based Motion Capture Systems." *Gait and Posture* 52 (February): 57–61. https://doi.org/10.1016/j.gaitpost.2016.10.020.

[8] Nakano, Nobuyasu, Tetsuro Sakura, Kazuhiro Ueda, Leon Omura, Arata Kimura, Yoichi Iino, Senshi Fukashiro, and Shinsuke Yoshioka. 2020. "Evaluation of 3D Markerless Motion Capture Accuracy Using OpenPose With Multiple Video Cameras." *Frontiers in Sports and Active Living* 2 (May). https://doi.org/10.3389/fspor.2020.00050.

[9] Polak, Ewa, Jerzy Kulasa, António VencesBrito, Maria António Castro, and Orlando Fernandes. 2016. "Motion Analysis Systems as Optimization Training Tools in Combat Sports and Martial Arts." *Revista de Artes Marciales Asiáticas* 10 (2): 105. https://doi.org/10.18002/rama.v10i2.1687.

[10] Vliet, Paulette van, and Gabriele Wulf. 2006. "Extrinsic Feedback for Motor Learning after Stroke: What Is the Evidence?" *Disability and Rehabilitation*. https://doi.org/10.1080/09638280500534937.

[11] Mazian, Amir Irfan, Wan Rizhan, Normala Rahim, Azrul Amri Jamal, Ismahafezi Ismail, and Syed Abdullah Fadzli. 2023. "A Theoretical Framework for Creating Folk Dance Motion Templates Using Motion Capture." *International Journal of Advanced Computer Science and Applications* 14 (5): 445–51. https://doi.org/10.14569/IJACSA.2023.0140547.

[12] Paez, Arsenio. 2017. "Grey Literature: An Important Resource in Systematic Reviews." *Journal of Evidence-Based Medicine*, December. https://doi.org/10.1111/jebm.12265.

[13] Moher, David, Alessandro Liberati, Jennifer Tetzlaff, and Douglas G. Altman. 2010. "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement." *International Journal of Surgery* 8 (5): 336–41. https://doi.org/10.1016/j.ijsu.2010.02.007.

[14] Perception Neuron. (n.d.). MocapApi Calc type data in detail. Retrieved from https://support.neuronmocap.com/hc/en-us/articles/12275483246491-MocapApi-Calc-type-data-in-detail

[15] Hachaj, T., & Ogiela, M. (2015). Full body movements recognition - unsupervised learning approach with heuristic R-GDL method. Digital Signal Processing, 46, 239-252. https://doi.org/10.1016/j.dsp.2015.07.004

[16] Idris, W. M. R. W., Rafi, A., Bidin, A., & Jamal, A. A. (2019). Developing new robust motion templates of martial art techniques using R-GDL approach: a case study of SSCM. International Journal of Arts and Technology, 11(1), 36-79.

[17] Hisham, N. F. Z., Jamal, A. A., & Idris, W. M. R. W. Lower Limb Walking Gait Profiling Using Marker-less Motion Capture with GDL and R-GDL methods to Assist Physiotherapy Treatment.

[18] Wan Idris, W.M.R., Rafi, A., Bidin, A. et al. A systematic survey of martial art using motion capture technologies: the importance of extrinsic feedback. Multimed Tools Appl 78, 10113–10140 (2019). https://doi.org/10.1007/s11042-018-6624-y

[19] Yin, Xiaohui, C. Chandru Vignesh, and Thanjai Vadivel. 2022. "Motion Capture and Evaluation System of Football Special Teaching in Colleges and Universities Based on Deep Learning." International Journal of Systems Assurance Engineering and Management 13 (6): 3092–3107. https://doi.org/10.1007/s13198-021-01557-2.

[20] Della Villa, Francesco, Stefano Di Paolo, Dario Santagati, Edoardo Della Croce, N. Lopomo, Alberto Grassi, and Stefano Zaffagnini. 2021. "A 2D Video-Analysis Scoring System of 90° Change of Direction Technique Identifies Football Players with High Knee Abduction Moment." Knee Surgery, Sports Traumatology, Arthroscopy 30 (11): 3616–25. https://doi.org/10.1007/s00167-021-06571-2.

[21] Bampouras, Theodoros M., and Neil M. Thomas. 2022. "Validation of a LiDAR-Based Player Tracking System during Football-Specific Tasks." Sports Engineering 25 (1). https://doi.org/10.1007/s12283-022-00372-7.

[22] Aughey, Robert J., Kevin Ball, Sam Robertson, Grant M. Duthie, Fabio R. Serpiello, Nicolas Evans, Bartholomew Spencer, et al. 2022. "Comparison of a Computer Vision System against Three-Dimensional Motion Capture for Tracking Football Movements in a Stadium Environment." Sports Engineering 25 (1). https://doi.org/10.1007/s12283-021-00365-y.

An Application of Graph Neural Network Model Design for Residential Building Layout Design

Shiyu Wang[1]*, Ningbo Wang[2]
Zhengzhou Urban Construction Vocational College, Zhengzhou 452370, China[1]
State Grid Xinyuan Henan Tianchi Pumped Storage Co., Ltd., Nanyang 473000, China[2]

Abstract—In the current process of residential building layout design, there are problems such as low design efficiency, excessive manual intervention, and difficulty in meeting personalized needs. To address these issues, a residential building layout design method based on graph neural network model is proposed to improve the intelligence level of residential building layout design. Firstly, the residential building floor plan layout design data are transformed into graph data suitable for graph neural network model processing. Then, deep learning techniques are used to analyse and identify the spatial distribution characteristics of the main functional areas in the space. Finally, the trained graph neural network model is applied to the actual residential building floor plan layout design and compared with the traditional method. The experimental results show that compared with the traditional computer-aided design method, the residential building floor plan layout design and optimisation method improves the completeness of the design scheme by about 2.3%, the rationality by about 3.6%, the readability by about 1.9%, and the effectiveness by about 10.3%. The method improves the efficiency and accuracy of residential building floor plan layout design, helps to shorten the design cycle and reduce the design cost, and helps to promote technological progress and sustainable development in the field of architectural design.

Keywords—Residential building layout plan; deep learning; GNN model; space utilization rate; resident comfort level; quantum particle swarm algorithm; Node2vec algorithm

I. Introduction

With the rapid development of social economy and the acceleration of urbanisation, the demand for residential buildings is increasing, and the floor plan layout design, as an important part of residential building design, directly affects the comfort, functionality and aesthetics of the residence [1]. The traditional floor plan layout design of residential buildings mainly relies on the experience and professional knowledge of designers, which is limited by the personal ability and experience accumulation of designers, and the design efficiency and accuracy are relatively low, and it is difficult to ensure the innovation and uniqueness of the design scheme [2]. In recent years, the development of artificial intelligence technology has provided new possibilities for residential building plan layout design [3]. Among them, the graph neural network (GNN) model, as a kind of neural network that can effectively process graphical data, has achieved remarkable results in the fields of computer vision, natural language processing, and recommender systems [4, 5]. However, in the field of residential building layout design, the application of GNN model is still in its infancy. Most existing research focuses on simple spatial relationship modeling, and there are still shortcomings in comprehensively considering various factors such as complex functional requirements, user preferences, and diverse building codes in residential buildings. In addition, how to build an efficient and accurate GNN architecture that can fully adapt to the special requirements of residential building layout design and achieve automatic generation and optimization of design schemes is still an urgent problem to be solved. The research aims to fill these research gaps by exploring the application of graph neural network models in residential building layout design, constructing more comprehensive and practical design models, and improving the quality and efficiency of residential building layout design, bringing new vitality and innovation to the field of residential building design. The study is divided into four parts: the first part is a summary of related studies; the second part is the design of the GNN model for residential building floor plan layout design, which is validated in the third part; and the fourth part is a summary of the whole study. The innovativeness of the study is mainly reflected in the following aspects The study of applying GNN to residential building floor plan layout design provides a new intelligent method for residential building floor plan layout design. Secondly, the study constructed a GNN model applicable to residential building floor plan layout design and optimised it with a large amount of training data, which improved the design efficiency and accuracy; finally, the GNN model was applied to actual design cases, which achieved significant design results.

*Corresponding Author.

II. Related Works

GNN is a neural network that can efficiently process graphical data and automatically learn the structural and relational information in graphical data. Wang et al. proposed a quaternion-based social recommendation knowledge graph neural network, which reduces the parameters during training through the expressibility of quaternion and the weight sharing mechanism of the Hamilton product, and also employs explicit and implicit social relationship integration algorithms to solve the problem of users' social relationship data sparsity problem. Experimental results show that the model can achieve up to 85% recommendation accuracy in study [6]. Huang's group proposes a dynamic spatio-temporal graph neural network model (DSTGNN) to capture the dynamics and dependencies in traffic demand forecasting by constructing a spatial dependency graph. The results show that DSTGNN outperforms existing models in traffic demand prediction on two real datasets [7]. Rusek's group proposes a novel GNN-based network model to understand the complex relationships between topology, routing, and input flows, and to predict key performance indicators. The model was experimentally shown to be accurate up to 88% in predicting

delay distribution, jitter and loss [8]. Lee et al. proposed a new human activity recognition model that combines a pre-trained model and a GNN to effectively overcome the sparsity of radar data. The results showed that the method achieved 96% accuracy in five different human activity classifications [9]. A related study proposes a scalable network slice digital twin based on the GNN model to capture intertwining relationships between slices and monitor end-to-end metrics. Experiments demonstrate that the method accurately reflects network behaviour and predicts latency in various topologies and new environments [10].

Graphic layout design is a design method to achieve an efficient, aesthetically pleasing and comfortable spatial environment by rationally arranging spatial elements. Li et al. proposed an attribute-conditional layout method for solving the problem of design element position and size in graphic layout design while considering element attribute constraints. The method was experimentally demonstrated to be effective in synthesising graphic layouts under different element attribute conditions and supports layout adjustment and original reading order preservation [11]. Murchie's group proposes a graphic design methodology based on the science of communicating vision and provides a high-level overview of terms related to layout, images, fonts, and colours. The method was able to increase graphic design satisfaction by 13% and helped to facilitate research collaboration between scientists and designers [12]. Stephan et al. used a mathematical planning approach to achieve optimal use of urban space by optimising car park layouts. The trade-off between high resolution and computational effort was explored by comparing orthogonal parking mixed integer programs at different resolutions. Experimental results show that the application of the optimised car park design scheme improves the effectiveness by 10% [13]. Boysen's team optimises the layout design of moving walkways through dynamic planning, which effectively improves the total travel time under several relevant extended constraints. The results showed that the method could reduce the total pedestrian travel time by 13% [14]. Wan team members targeted to propose a web page layout aesthetic assessment by automatically predicting the aesthetics of web page layouts based on an improved Adaboost algorithm. Experiments proved the superiority of the model in predicting the aesthetics of web page layouts [15].

In summary, existing research on GNN has achieved significant results in various fields such as social recommendation, transportation demand prediction, network performance indicator prediction, and human activity recognition, demonstrating the powerful ability of GNN to process graphical data structures and relational information. In terms of graphic layout design, although there are various methods such as attribute conditional layout, design based on scientific communication vision, mathematical programming optimization of parking lot layout, dynamic programming of mobile sidewalk layout, and aesthetic evaluation of webpage layout, these studies mostly focus on specific types of layout design or specific optimization objectives. At present, there is a lack of an effective model that deeply applies the powerful graphic data processing capabilities of GNN to residential building layout design, and fails to fully utilize GNN to explore the complex structural and relational information between residential building spatial elements to achieve more comprehensive, intelligent, and universal optimization of residential building layout design. Therefore, the study proposes a GNN model for residential building layout design, aiming to provide intelligent methods for residential building layout design and promote technological progress in the field of architectural design.

III. GNN Model for Residential Building Layout Design

This paper discusses the data acquisition, pre-processing and analysis of residential building floor plan layouts using BIM technology. A layout design method based on GNN and deep learning is proposed to improve space utilisation and occupant comfort. Finally, the quantum particle swarm algorithm is used to optimise the layout design and transform it into a composite model to further enhance the design.

A. Spatial Data Processing of Residential Building Plan Layout

Residential building floor plan layout data acquisition and pre-processing is an important part of the BIM field, which involves the digital modelling of building space and provides basic data for building design, construction and operation [16]. Before carrying out the residential building plan layout, the functional area spatial data need to be collected and processed in order to extract the distribution characteristics of the layout space. The spatial data processing process of residential building plan is shown in Fig. 1.

The data format of spatial layout information mainly includes the location, size, and shape of building floor plans and related functional areas. Specifically, the data will include information such as the coordinates, area, and shape of each functional area. The input of the model is raw spatial data, and the output is processed and analyzed spatial distribution feature information. During the processing, it may be necessary to replace the classification code to adapt to the new data structure and analysis requirements. Finally, the processed data will be verified to ensure its quality [17]. The information entropy of spatial distribution characteristics of the main functional area is shown in Eq. (1).

$$\delta = -\sum_{i=1}^{n}\left(\frac{S_n}{S_0}\right)\ln\left(\frac{S_n}{S_0}\right) \tag{1}$$

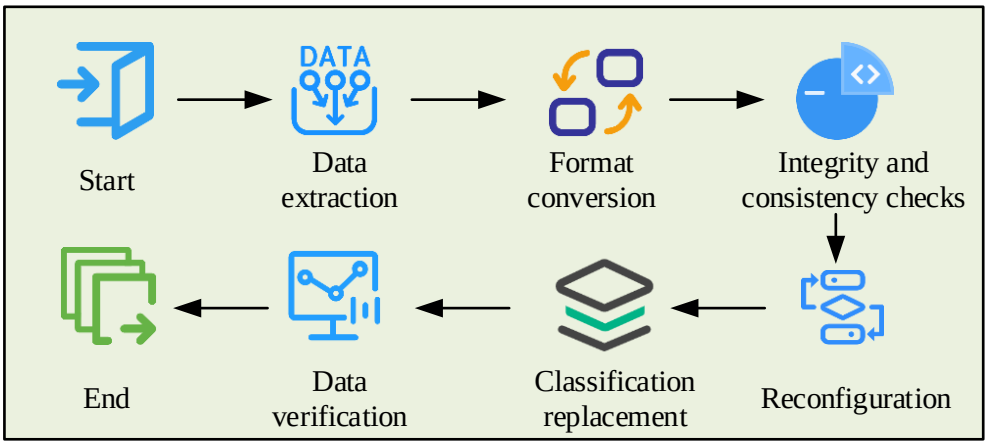


Fig. 1. The data processing process of residential building floor plan space.

In Eq. (2), the measure of spatial functional area land is η and the number of its types is N. The measure of spatial functional area land use can be realised by calculating the equilibrium degree, which takes the value range of [0, 1]. If the equilibrium degree is 0, it means that the use of land in the functional area is unbalanced; if the equilibrium degree is 1, it means that the use of land has reached the ideal equilibrium state. Through this metric, the development of land in the spatial functional area can be better understood and assessed [19]. The morphological characteristics of the main functional zone distribution of the building plan contain shape rate and compactness, and the shape rate of each functional zone is shown in Eq. (3).

$$\lambda = \frac{S_1}{L^2} \tag{3}$$

In Eq. (3), the shape rate of each functional area is λ, the area of the functional area region is S_1, and the length of the region is L. Shape rate is an important indicator to describe the morphological characteristics of the distribution of the main functional area, if the value is small, it means that the area shows obvious belt-like characteristics; if the value is large, it indicates that the distribution of the main functional area in the area is block-like. The compactness of the main functional area is shown in Eq. (4).

$$\mu = \frac{S_1}{S_1^{'}} \tag{4}$$

In Eq. (4), the compactness of each functional area is μ, and the minimum external circle area of functional area is $S_1^{'}$. Subsequently, the study analyses and identifies the spatial distribution characteristics of the main functional zones in the space through the deep neural network technology, and the deep neural network of spatial distribution of the main functional zones in the building plan is shown in Fig. 2.

The spatially relevant feature points of the residential building plan are extracted by deep neural network, and the functional area feature index parameters are calculated as shown in Eq. (5).

$$A = b + \frac{w}{r(s-w)} \tag{5}$$

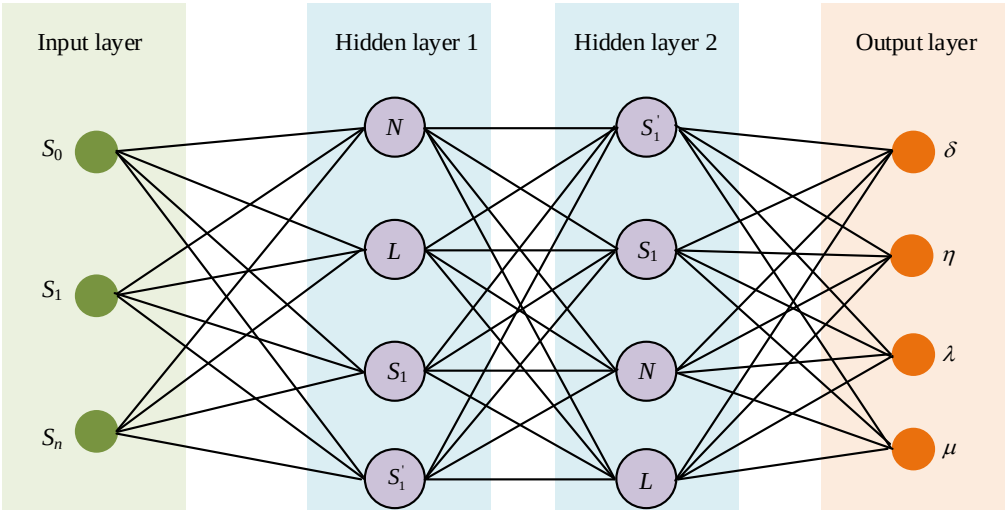


Fig. 2. Deep neural network for spatial distribution of main functional areas in architectural plans.

In Eq. (5), the feature indicator parameter is A, the upper limit value of feature is b, the optimisation coefficient of feature parameter is r, the distribution range is s, and the lower limit value of feature is w. The corresponding feature value index parameters are calculated and the results of the layout feature extraction of the functional area are evaluated. If the result exceeds the preset value range, it indicates that there is an abnormality in the feature extraction and it is necessary to carry out the extraction again. On the contrary, it can be considered that the layout feature extraction results are suitable for layout optimisation design, and the subsequent operations can be continued.

In summary, the study successfully extracted the spatial distribution characteristics of the main functional area by processing and analyzing spatial data using deep neural network technology. Then, using information entropy and spatial functional area land measurement methods, evaluate the development status of land in each functional area. In addition, by calculating the shape ratio and compactness of the main functional area, we have gained a better understanding of the development of the spatial functional area land. The research method not only improves the accuracy of residential building layout design, but also provides effective basis for subsequent layout optimization design.

B. Residential Building Layout Design and Optimisation Methods

Unlike traditional deep learning models, GNN acquires information about graph data by learning the relationships between nodes [20]. The mathematical representation of the graph structure is shown in Eq. (6).

$$G = \langle V, E \rangle \tag{6}$$

In Eq. (6), the graph structure is G, the set of nodes of the graph structure is $V = [v_1, v_2, \ldots, v_i]$, and the set of all edges of the graph structure is $E = [e_{11}, e_{12}, \ldots, e_{ij}]$. The radius subgraph of the nodes is shown in Eq. (7).

$$v_i^{(r)} = (V_i^{(r)}, E_i^{(r)}) \tag{7}$$

In Eq. (7), the subgraph of node v_i within the radius r is $v_i^{(r)}$. The radius subgraph of an edge is shown in Eq. (8).

$$e_{ij}^{(r)} = (V_i^{(r-1)} \bigcup V_j^{(r-1)}, E_i^{(r)} \bigcup E_j^{(r)}) \tag{8}$$

In Eq. (8), the subgraph of edge e_{ij} within radius r is $e_{ij}^{(r)}$. After random initialisation by supervised learning, the node radius subgraphs and edge radius subgraphs are trained by backpropagation. The node embedding representation is updated as shown in Eq. (9).

$$v_i^{(t+1)} = \sigma(v_i^{(t)} + \sum_{j \in N(i)} h_{ij}^{(t)}) \tag{9}$$

In Eq. (9), the node embedding is denoted as $v_i^{(t)}$, the Sigmoid function is σ, and the set of neighbours of the node is $N(i)$. The hidden neighbour vector is $h_{ij}^{(t)}$ and its calculation is shown in Eq. (10).

$$h_{ij}^{(t)} = f\left(W_{neighbor}\left[v_j^{(t)}, e_{ij}^{(t)}\right]^T + b_{neighbor}\right) \tag{10}$$

In Eq. (10), the nonlinear activation function of the neural network is f, the hidden neighbour weight matrix is $W_{neighbor}\left[v_j^{(t)}, e_{ij}^{(t)}\right]^T$, the neighbour offset vector is $b_{neighbor}$, and the edge embedding vector of node $v_i^{(t)}$ and node $v_j^{(t)}$ at time t is $e_{ij}^{(t)}$. The edge embedding vector is updated as shown in Eq. (11).

$$e_{ij}^{(t+1)} = \sigma(e_{ij}^{(t)} + f\left(W_{side}\left(v_i^{(t)}, v_j^{(t)}\right) + b_{side}\right)) \tag{11}$$

In Eq. (11), the edge vector update weight matrix is $W_{side}\left(v_i^{(t)}, v_j^{(t)}\right)$ and the edge embedding vector offset vector is b_{side}. The final output obtained is shown in Eq. (12).

$$y_{build} = \frac{1}{|V|}\sum_{i=1}^{|V|} v_i^{(t)} \tag{12}$$

In Eq. (12), the final output is y_{build} and the number of all nodes is $|V|$. The loss function for residential building prediction is shown in Eq. (13).

$$loss = \sqrt{\frac{1}{m}\sum_{i=1}^{n} W_{reg}(y_i - y_{build})} \tag{13}$$

In Eq. (13), the loss function is $loss$, the regression weight matrix is W_{reg}, the actual score of the samples is y_i, and the number of samples is m. The Node2vec algorithm is an unsupervised machine learning model based on graph embedding, which represents similarity or proximity between nodes by sampling their neighbours in a random wandering manner and mapping the nodes to a high-dimensional space. The Node2vec algorithm borrows from the word2vec algorithm in natural language processing, considering each node in the graph as a word in the text and a sequence of nodes as a sentence in the text. The algorithm mainly solves the problem of how to generate a sequence of nodes starting from an initialised node. The optimisation objective of the Node2vec algorithm is shown in Eq. (14).

$$\max_f \sum_{v \in V} \log \Pr(N_s(u) | f(u)) \tag{14}$$

In Eq. (14), the node mapping function is $f(u)$ and the set of nearest neighbour points of a node is $N_s(u)$. The GNN-based residential building plan layout design model is shown in Fig. 3.

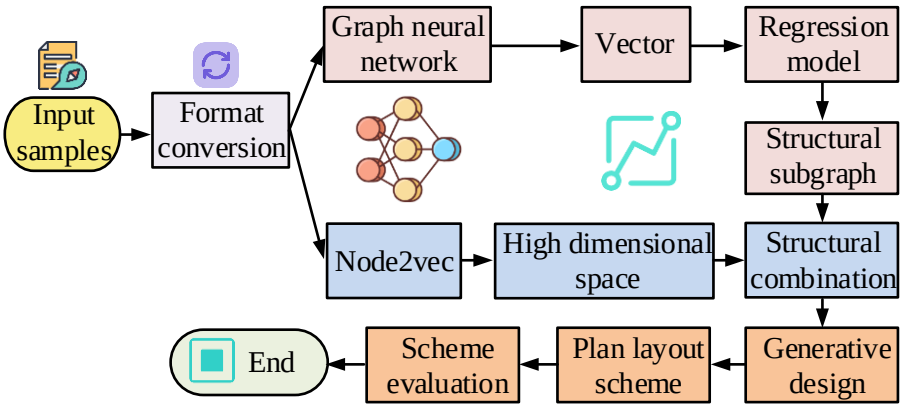


Fig. 3. A residential building layout design model based on GNN.

The residential building floor plan layout design model uses a graph data structure to encode and analyse building floor plans. The graph neural networks involved include Graph Convolutional Neural Networks (GCN) and Graph Attention Networks (GAN). In this model, nodes represent rooms, and node attributes include type, etc.; edges represent connectivity relationships between rooms, such as door connections, open connections, or vertical connections (e.g., stairs, ramps, or lifts). Through supervised learning, the model uses GNN to embed nodes and subgraphs to obtain the corresponding vector representation and the vector representation of the whole graph. Then, the linear regression model assigns weights to the subgraphs to minimise the error between the predicted score and the true score. After training, the subgraphs that have a high impact on the scores are extracted as good design elements. The unsupervised learning part uses the node2vec algorithm to map the sample graph into a high-dimensional space and visualise it to show potential relationships between nodes. This approach provides useful suggestions for subgraph combination, i.e., which nodes should be connected together in the final design. In the structure combination phase, the model identifies the basic modules (subgraphs) and then combines them into a new graph. This process can be achieved by adding new edges and additional nodes. Finally, the validity of the generated design solution is manually evaluated. After obtaining a new diagram that conforms to the design, the model converts the diagram into a residential building plan layout. Overall, the GNN-based residential building floor plan layout design model effectively integrates supervised and unsupervised learning, which helps to generate innovative and design-compliant floor plan layout solutions. The GNN structure used for subgraph construction is shown in Fig. 4.

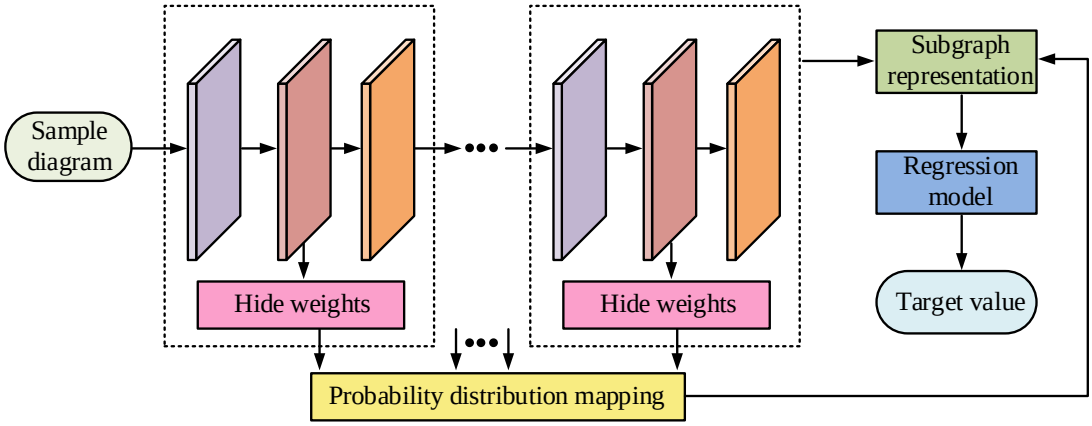


Fig. 4. GNN structure for subgraph construction.

Each layer of the GNN structure used to discover constructed subgraphs consists of neurons that hold real-valued representations of node attributes. In each layer, a convolutional operation processes the node attributes, multiplying the result by the hidden weights and mapping it to a probability distribution via a non-linear function to obtain a potential representation vector. The probability of each layer is related to the objective function score, and subgraph patterns are discovered by accumulating and remembering the neighbourhood contributions of the nodes. The subgraph vector is updated as shown in Eq. (15).

$$x_i^{(t+1)} = x_i^{(t)} + \sum_{j \in N(i)} x_{ij}^{(t)} \quad (15)$$

In Eq. (15), the subplot vector at the time of t is $x_i^{(t)}$ and the subplot vector at the time of $t+1$ after updating is $x_i^{(t+1)}$. The initialisation process of the subplot vector of the residential building plan is shown in Fig. 5.

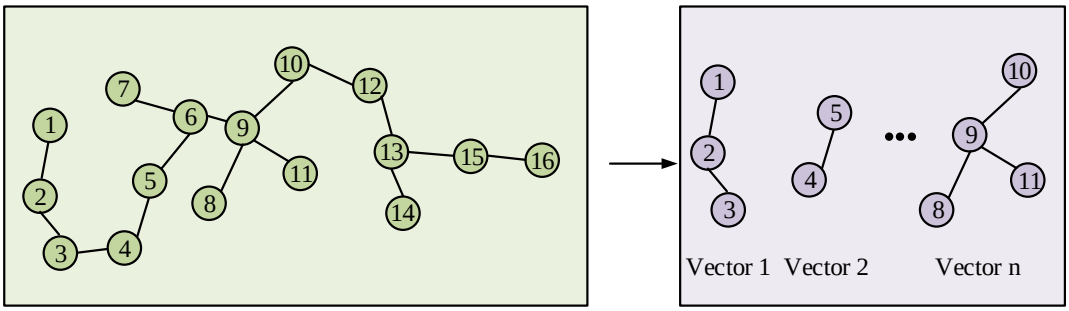


Fig. 5. The initialisation process of subgraph vectors in residential building plans.

The objective of the residential building floor plan layout design optimisation method is to maximise the space utilisation of the residential building while improving the comfort of the occupants, subject to the constraints [21]. The residential building floor plan layout design optimisation method is based on the quantum particle swarm algorithm, which achieves the goal by optimising two factors: the coordination of the layout design and the design cost. The optimisation model transforms the complex layout problem into the form of a composite model, which takes into account a variety of factors such as land type, functional area type, and adjacency. In the solution process, the optimal solution is searched by continuously updating the particle velocity and position, and the preset convergence conditions are satisfied. The final optimal layout design results obtained can be used to guide the actual residential building plan layout design.

IV. Analysis of the Application of Residential Building Layout Design Methods

The content of this chapter focuses on the analysis of data processing, feature extraction and application of design optimisation methods to residential building plan layout images. Firstly, the images in the ScanNet dataset are processed and converted. Then, the frequency and distribution features of different spatial types are analysed. Then, the GNN model performance is evaluated by experimenting different parameters using neural networks and Adam optimiser for training. Finally, the public space layout is optimised by quantum particle swarm algorithm.

A. Analysis of Data Collection and Pre-processing Effects

The experimental environment of the residential building floor plan layout design method includes the following: first, in the software environment, BIM software is used for data acquisition and pre-processing, such as Revit and AutoCAD. This software can help to acquire the relevant information of the building and to organise and process the data. It is also necessary to use deep learning frameworks, such as TensorFlow, PyTorch, etc., for data processing and analysis for model training and prediction. In terms of the hardware environment, we need to use a high-performance computer or server for data processing and model training. Specific configurations include high-speed CPU, high-capacity memory and high-performance graphics card to ensure the efficiency and accuracy of data processing and model training. The programming language uses Python as the main programming language, combined with the corresponding deep learning libraries and APIs of building information modelling software for data processing and model training. The storage device uses high-speed hard discs or solid-state hard discs as the data storage device to improve the data reading and writing speed and model training efficiency. The study selects residential building plan layout images as the raw data for data processing on the ScanNet dataset, and the data conversion processing effect is shown in Fig. 6.

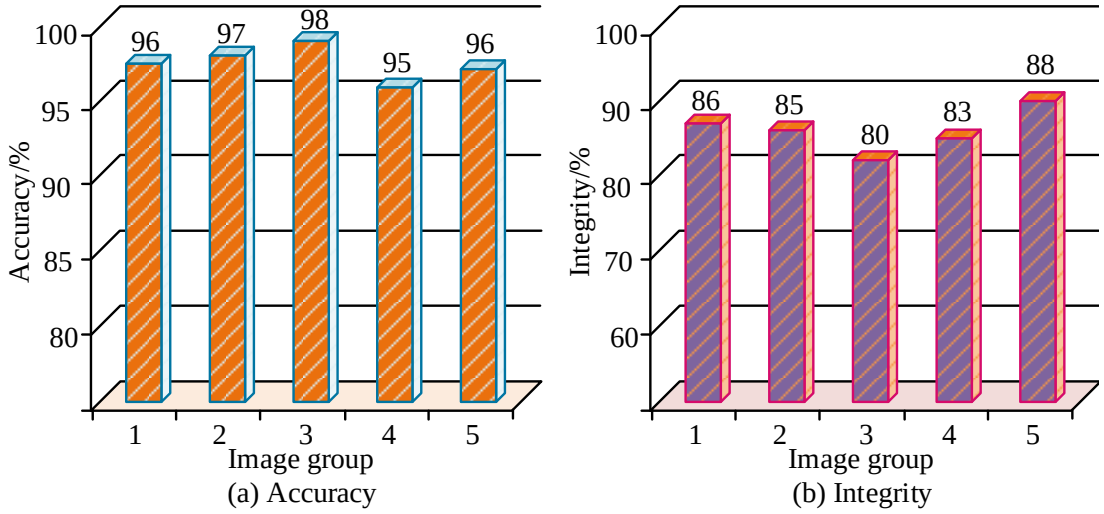


Fig. 6. Data conversion processing effect.

The image grouping in Fig. 6(a) is the random division of the 150 residential building floor plan layout image samples obtained from the ScanNet dataset into five groups of 30 sample images each shows the accuracy of the data conversion, with an average accuracy of up to 96.4%. It indicates that there are very few errors and deviations in the data conversion process, and most of the image samples can maintain a high degree of consistency and accuracy in the conversion process. Fig. 6(b) shows the completeness of data conversion, and the average completeness can reach 84.4%. In the data conversion process, the important information and features of the overall sub-image samples can be retained and reproduced. Comprehensively, the effect of data conversion processing is quite remarkable, with excellent performance in both accuracy and completeness indicators, which lays a solid foundation for further data analysis and processing. The study will contain 24 of the 30 data samples for training and cross-validation, using grid search to adjust the combination of hyperparameters, and the other 6 samples as a test set. The results of feature extraction for residential building plan layout images are shown in Fig. 7.

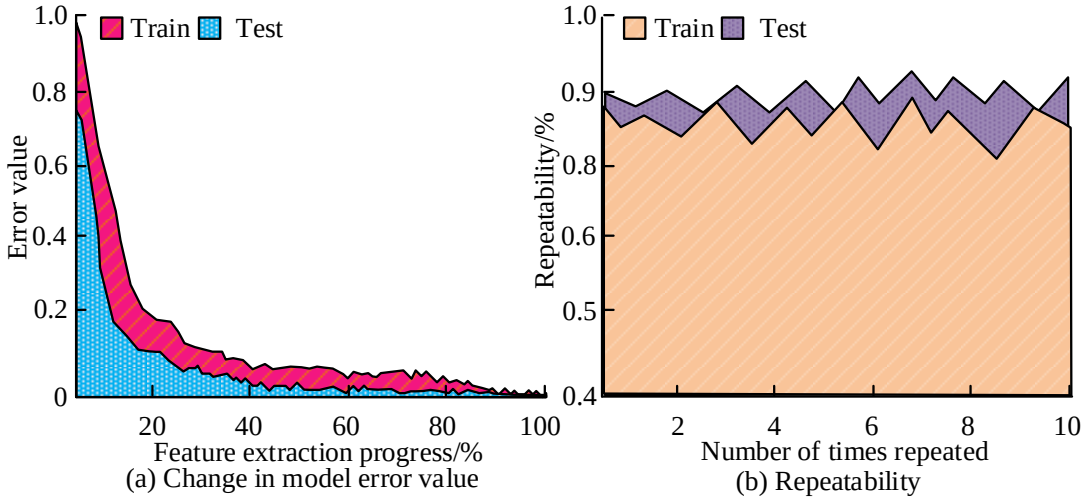


Fig. 7. The effect of feature extraction on residential building layout images.

Fig. 7(a) shows the variation of error values of residential building floor plan layout image feature extraction, and the error values of training and testing tend to be stable in the range of 0-0.01. Fig. 7(b) shows the repeatability test results of residential building floor plan layout image feature extraction, and the repeatability averages of training and testing are 84% and 89%, respectively. The results show that the effect of residential building floor plan layout image feature extraction is more significant, and the accuracy and repeatability are excellent. The results of the sample room type frequency statistics are shown in Fig. 8.

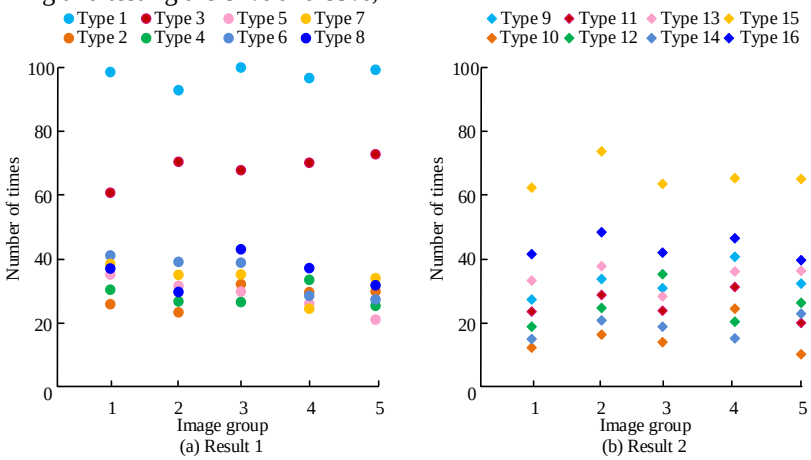


Fig. 8. Sample room type frequency statistics results.

In Fig. 8(a), types 1-8 represent bathroom, bedroom, corridor, kitchen, living room, dining room, parking room and laundry room, respectively. In Fig. 8(b), types 9-16 represent guest rooms, balconies, storage rooms, entrances, studies, master bedrooms, second bedrooms, and bathrooms, respectively. The frequency ranges of different types of spaces are not exactly the same, with bathrooms appearing most frequently, followed by corridors, and to a lesser extent, balconies. With regard to the information entropy of spatial distribution characteristics, the internal spatial distribution of residential buildings presents a high degree of randomness and diversity. In the spatial functional area land metric, functional areas such as bedrooms and living rooms occupy larger areas, while parking rooms and laundry rooms have smaller areas.

Regarding the shape rate of each functional area, kitchen and bathroom show a more regular shape, while bedrooms and living rooms are more irregularly shaped. The main functional areas such as bedrooms and living rooms are more compact, while dining rooms, laundry rooms, etc. are less compact.

B. *Analysis of the Application of Residential Building Layout Design and Optimisation Methods*

When evaluating the application effect of residential building layout design and optimization methods, a comparative evaluation method was used in the experiment to compare the proposed optimization method with computer-aided design (CAD) and poster tools. Nonprofessional and professional users were invited to evaluate the completeness, rationality, readability, and effectiveness of the three design tools. The study uses customised data and parameter settings to train neural networks to solve architectural design problems. Also, the Adam optimiser was used for training and different parameters such as subgraph radius and edge vector dimensions were chosen for the experiments. The effect of different parameters on the GNN model is shown in Fig. 9.

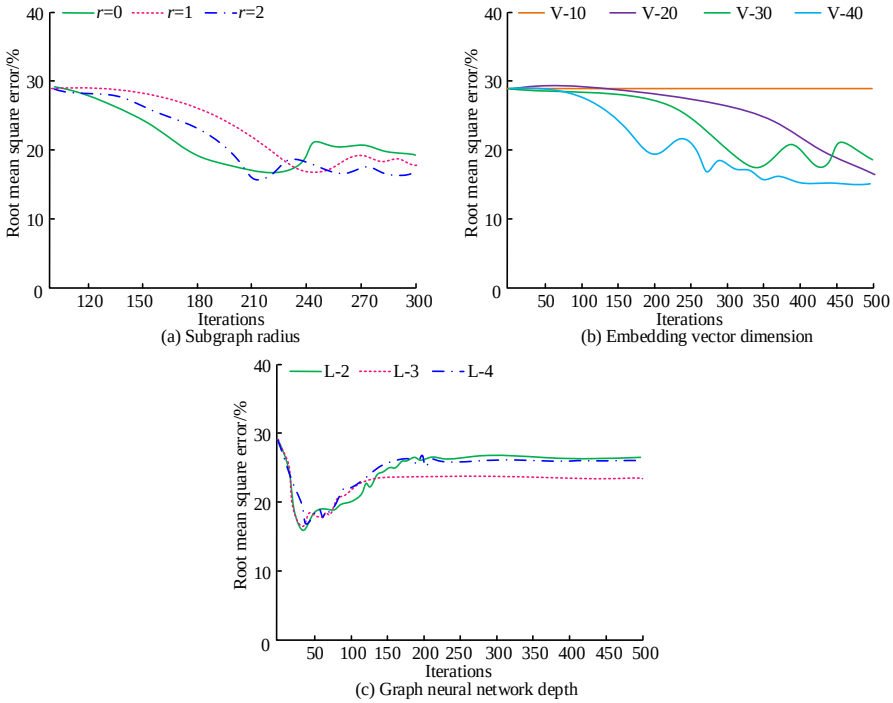


Fig. 9. The impact of different parameters on GNN models.

Fig. 9(a) shows the results of the effect of subgraph radius on the model performance, and it can be seen that the root mean square error of the model can be minimised up to 18.3% when the subgraph radius is 2. Fig. 9(b) shows the results of the effect of vector dimension on the model performance, and it can be seen that the root-mean-square error of the model can be minimised up to 16.9% when the vector dimension is 40. Fig. 9(c) shows the results of the effect of GNN depth on model performance, as can be seen that the model stabilises with a minimum root mean square error of 23.6% at a GNN depth of 3. With the current model setup, a subgraph radius of 2, a vector dimension of 40, and a GNN depth of 3, the smallest root-mean-square error can be obtained, resulting in optimal model performance. The sample room type vector space projection is shown in Fig. 10.

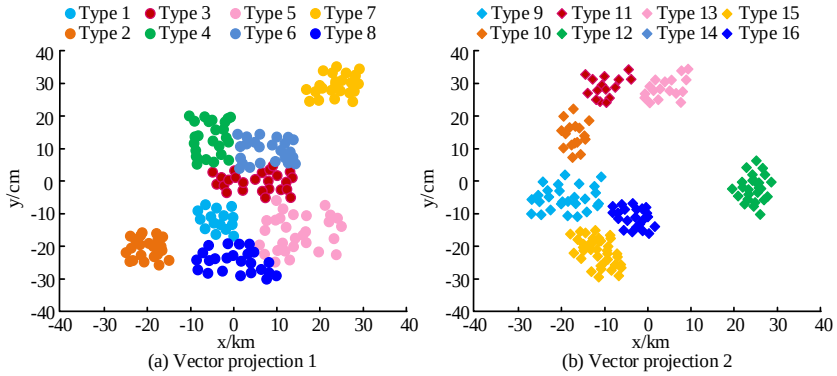


Fig. 10. Sample room type vector space projection.

Fig. 10(a) shows the space vector projections for types 1-8, i.e., bathroom, bedroom, corridor, kitchen, living room, dining room, parking room and laundry room. Fig. 10(b) shows the space vector projections for types 9-16, i.e. guest room, balcony, storage room, entrance, study, master bedroom, second bedroom and bathroom. It can be seen that clusters such as bedrooms and bathrooms are closer to each other, forming a larger category, while kitchens and dining rooms are closer to each other. In addition, clusters such as guest room, bathroom and second bedroom are very close to each other. The optimisation of the residential building floor plan layout design is shown in Fig. 11.

In order to verify the effectiveness of the GNN based residential building layout design and optimization method proposed in the study (marked as Method A), the GCN and GAT models were used as baselines in the experiment, and the intelligent generative method based on genetic algorithm (marked as Method B) and the layout optimization method based on particle swarm optimization (marked as Method C) published in 2023-2024 were compared. The comparison results of different methods are shown in Table I. Table I shows that Method A outperforms the baseline models GCN and GAN in all indicators, and compares Method B with Method C. Compared to the baseline model, the performance of method A has significantly improved, with its root mean square error reduced by nearly half, accuracy increased by about 10%, and F1 value increased by about 6%. Compared with the methods proposed in 2023-2024, Method A leads by about 4% in accuracy and F1 score, demonstrating higher overall performance. This indicates that the GNN based method for residential building layout design and optimization has significant advantages and application potential.

TABLE I. COMPARIING RESULTS OF DIFFERENT METHODS

Method	Root mean square error/%	Accuracy/%	F1 value/%
GCN	20.3%	83.1%	89.3%
GAN	25.1%	80.3%	87.3%
Method A	10.7%	93.2%	95.1%
Method B	13.7%	90.2%	91.3%
Method C	16.1%	89.3%	90.8%

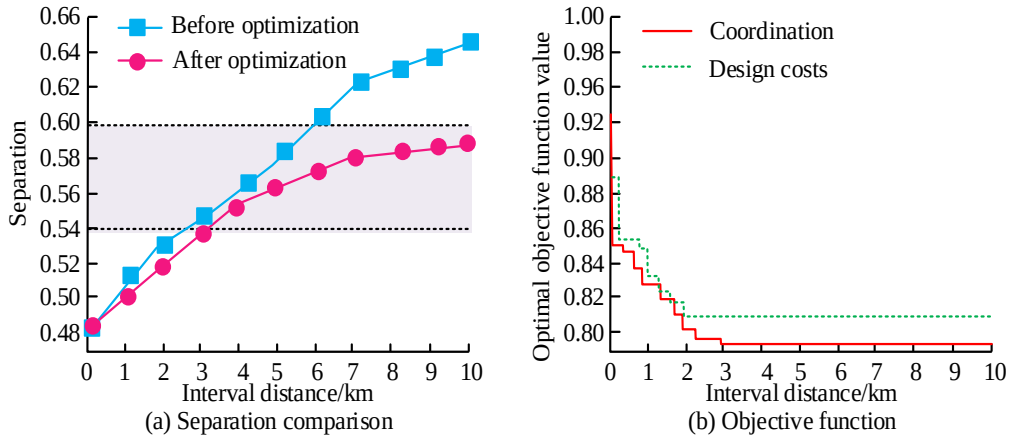


Fig. 11. Optimization of residential building layout design.

Fig. 11(a) shows the results of the comparison of the separation degree of the spatial layout before and after the optimised design. Before the optimal design, the separation degree of each functional area is low, and there are some areas that are not effectively utilised. The separation degree of the functional areas after the optimal design is significantly improved and always within the permitted fluctuation range, which indicates that our proposed design method can effectively optimise the layout of the public space, making the spatial distribution of the functional areas clearer and avoiding the waste of space. Fig. 11(b) shows the results of the objective function solution, which shows a decreasing trend with the increase of the number of iterations. This is because in the quantum particle swarm algorithm, the particles are able to adjust and update all the particle information through quantum mechanics, maintaining the original position and velocity while choosing the appropriate velocity direction based on historical experience. This process of constantly searching and updating position information makes the particles gradually approach the optimal solution, thus optimising the layout of the main functional area of the public space. The evaluation of the application effect of the residential building layout design and optimisation method is shown in Fig. 12.

In Fig. 12, the study compares the proposed method for designing and optimising the floor plan layout of residential buildings with computer-aided design (CAD) and poster tools as a comparison in order to analyse the effectiveness of the application of the proposed method in the study. Fig. 12(a) shows the evaluation results for non-professional users and Fig. 12(b) shows the evaluation results for professional users. Compared with CAD and poster tools, the completeness of the residential building floor plan layout design and optimisation method is improved by about 2.3%, rationality by about 3.6%, readability by about 1.9% and effectiveness by about 10.3%.

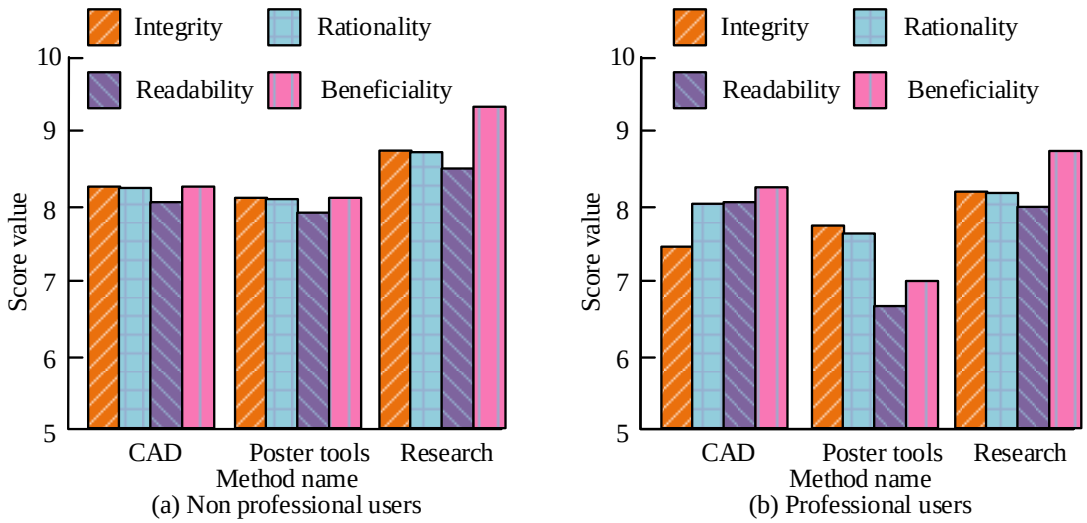


Fig. 12. Evaluation of the application effect of residential building layout design and optimisation methods.

V. Conclusion

In order to improve the space utilisation of residential buildings and the comfort of occupants, the study proposes a GNN-based method for designing and optimising the floor plan layout of residential buildings. The method analyses and identifies the spatial distribution characteristics of the main functional areas in the space through deep learning techniques. The study adopts the quantum particle swarm algorithm to optimise the layout of the public space, and transforms the complex layout problem into the form of a composite model to meet the preset convergence conditions and obtain the optimal layout design results. In the process of data conversion, the average accuracy can reach 96.4% and the average completeness can reach 84.4%, which lays the foundation for further data analysis and processing. The error value of the residential building floor plan layout image feature extraction is within the range of 0-0.01, and the repeatability averages for training and testing are 84% and 89%, respectively. Compared with the most advanced methods, the accuracy and F1 value of the GNN based residential building layout design and optimization method have been improved by about 4%, and its overall performance is better. Compared to CAD and poster tools, the effectiveness of the residential building floor plan layout design and optimisation method was improved by about 10.3%. The results indicate that the GNN-based residential building floor plan layout design and optimisation method has high applicability. This study has made multiple contributions in the field of residential building layout design. Firstly, the innovative application of Graph Neural Networks (GNNs) in residential building layout design provides a new intelligent design approach. Secondly, a GNN model adapted to the layout design of residential buildings was carefully constructed and optimized with a large amount of training data, significantly improving design efficiency and accuracy, effectively addressing the shortcomings of existing research in comprehensively considering multiple factors such as complex functional requirements, user preferences, and building standards of residential buildings. Thirdly, the successful application of the GNN model in practical design cases has improved the completeness, rationality, readability, and efficiency of the design scheme. It has shown outstanding performance in data conversion, image feature extraction, and other aspects. Compared with traditional CAD and poster tools, its efficiency has been significantly improved, effectively promoting technological progress and sustainable development in the field of architectural design. However, the study still has some limitations, such as the limited scope of data collection and the insufficiently fine setting of model parameters. Future research can collect data in a wider range and further optimise the model parameter settings to improve the performance and practicality of the layout design method.

References

[1] Y. Zhou, Y. Jin, Y. Chen, H. Luo, W. Li, and X. He, “Graph-model-based generative layout optimization for heterogeneous SiC multichip power modules with reduced and balanced parasitic inductance,” IEEE Transactions on Power Electronics, Vol. 37, no. 8, PP. 9298-9313, 2022. DOI:10.1109/TPEL.2022.3157873

[2] H. H. Hsu, “How facial symmetry influences the learning effectiveness of computer graphic design in makeup design,” Symmetry, Vol. 14, no. 10, pp. 1982-2000, 2022. https://doi.org/10.3390/sym14101982

[3] J. Skarding, B. Gabrys, and K. Musial, “Foundations and modelling of dynamic networks using dynamic graph neural networks: A survey,” IEEE Access, Vol. 9, no. 1, pp. 79143-79168, 2021. DOI: 10.1109/ACCESS.2021.3082932

[4] H. Feng, G. Cao, H. Xu, and S. S. Ge, “IS-STGCNN: An improved social spatial-temporal graph convolutional neural network for ship trajectory prediction,” Ocean Engineering, Vol.266, no. 3, pp. 112960-112968, 2022. https://doi.org/10.1016/j.oceaneng.2022.112960

[5] T. Rao, J. Li, X. Wang, Y. Sun, and H. Chen, “Facial expression recognition with multiscale graph convolutional networks,” IEEE Multimedia, Vol. 28, no. 2, pp. 11-19, 2021. DOI: 10.1109/MMUL.2021.3065985

[6] C. Wang, L. Li, H. Zhang, and D. Li, “Quaternion-based knowledge graph neural network for social recommendation,” Knowledge-Based Systems, Vol. 257, no. 5, pp. 109940-109952, 2022. https://doi.org/10.1016/j.knosys.2022.109940

[7] F. Huang, P. Yi, J. Wang, M. Li, J. Peng, and X. Xiong, “A dynamical spatial-temporal graph neural network for traffic demand prediction,” Information Sciences. Vol. 594, no. 1, pp. 286-304, 2022. https://doi.org/10.1016/j.ins.2022.02.031

[8] K. Rusek, J. Suárez-Varela, P. Almasa, P. Barlet-Ros, and A. Cabellos-Aparicio, “Routenet: Leveraging graph neural networks for network modelling and optimisation in sdn,” IEEE Journal on Selected Areas in

Communications, Vol. 38, no. 10, pp. 2260-2270, 2020. DOI: 10.1109/JSAC.2020.3000405

[9] G. Lee, and J. Kim, "Improving human activity recognition for sparse radar point clouds: A graph neural network model with pre-trained 3D human-joint coordinates," Applied Sciences, Vol. 12, no. 4, pp. 2168-2183, 2002. https://doi.org/10.3390/app12042168

[10] H. Wang, Y. Wu, G. Min, and W. Miao, "A graph neural network-based digital twin for network slicing management," IEEE Transactions on Industrial Informatics, Vol. 18, no. 2, pp. 1367-1376, 2020. DOI: 10.1109/TII.2020.3047843

[11] J. Li, J. Yang, J. Zhang, C. Liu, C. Wang, and T. Xu, "Attribute-conditioned layout gan for automatic graphic design," IEEE Transactions on Visualisation and Computer Graphics, Vol. 27, no. 10, pp. 4039-4048, 2020. https://doi.org/10.48550/arXiv.2009.05284

[12] K. J. Murchie, and D. Diomede, "Fundamentals of graphic design-essential tools for effective visual science communication," Facets, Vol. 5, no. 1, pp. 409-422, 2020. https://doi.org/10.1139/facets-2018-0049

[13] K. Stephan, F. Weidinger, and N. Boysen, "Layout design of parking lots with mathematical programming," Transportation Science, 2021, Vol. 55, no. 4, pp. 930-945, 2021. https://doi.org/10.1287/trsc.2021.1049

[14] N. Boysen, D. Briskorn, and S. Schwerdfeger, "Walk the line: Optimising the layout design of moving walkways," Transportation Science, Vol. 55, no. 4, pp. 908-929, 2021. https://doi.org/10.1287/trsc.2021.1051

[15] H. Wan, W. Ji, G. Wu, X. Jia, X. Zhan, M. Yuan, and R. Wang, "A novel webpage layout aesthetic evaluation model for quantifying webpage layout design," Information Sciences, Vol. 576, no. 5, pp. 589-608, 2021. https://doi.org/10.1016/j.ins.2021.06.071

[16] M. Najmabadi, and P. Moallem, "Local symmetric directional pattern: A novel descriptor for extracting compact and distinctive features in face recognition," Optik, Vol. 251, no. 1, pp. 168331-168353, 2022. https://doi.org/10.1016/j.ijleo.2021.168331

[17] H. Yan, and C. Song, "Multi-scale deep relational reasoning for facial kinship verification," Pattern Recognition, Vol. 110, no. 2, pp. 107541-107551, 2020. https://doi.org/10.1016/j.patcog.2020.107541

[18] S. C. Wen, and C. H. Yang, "Time series analysis and prediction of nonlinear systems with ensemble learning framework applied to deep learning neural networks," Information Sciences, Vol. 572, no. 1, pp. 167-181, 2021. https://doi.org/10.1016/j.ins.2021.04.094

[19] C. Cheng, C. Li, Y. Han, and Y. Zhu, "A semi-supervised deep learning image caption model based on Pseudo Label and N-gram," International Journal of Approximate Reasoning, Vol. 131, no. 3, pp. 93-107, 2020. https://doi.org/10.1016/j.ijar.2020.12.016

[20] T. Chen, X. Zhang, M. You, G. Zheng, and S. Lambotharan, "A GNN-based supervised learning framework for resource allocation in wireless IoT networks," IEEE Internet of Things Journal, Vol. 9, no. 3, pp. 1712-1724, 2021. https://doi.org/10.1109/JIOT.2021.3091551

[21] J. Purohit, and R. Dave, "Leveraging deep learning techniques to obtain efficacious segmentation results," Archives of Advanced Engineering Science, Vol. 1, no. 1, pp. 11-26, 2023. https://doi.org/10.47852/bonviewAAES32021220

An Intelligent Transport System for Prediction of Urban Traffic Congestion Level

Mohammad Khalid Imam Rahmani[1]*, Shahnawaz Khan[2], Md Ezaz Ahmed[3], Khaurram Jawad[4]*
College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia[1, 3, 4]
School of Information & Communications Technology, Bahrain Polytechnic, Isa Town, Bahrain[2]

***Abstract*—Developing a resilient infrastructure is crucial for nation-building by supporting innovations and promoting sustainable growth. The Kingdom of Saudi Arabia is striving to achieve the Sustainable Development Goals (SDGs) set by the United Nations. Industry, Innovation, and Infrastructure (I3) are some of the strategic objectives of the Kingdom's Vision 2030 par with the United Nations' SDGs. The objective is focused to develop trade and transport networks for international, regional, and local connectivity with an investment of billions of dollars to establish a robust transport network and improve the existing one for enhancing road safety to reduce the costs of deaths and serious injuries. For this, a control center for automatic monitoring could be established for 24x7 monitoring of traffic violators; the key project has been named the National Center for Transportation Safety, apart from launching the "Rental Contracts" facility with the Naql portal. Moreover, the growing urban population is causing more vehicles on the roads leading to more traffic congestion which has become severe during peak hours in the major cities causing several other issues such as environmental pollution, high greenhouse gases (GHGs) including CO_2 emissions, health risks to the citizen and residents, poor air quality, higher risks of road safety, more energy consumption, discomfort to the commuters, and wastage of time and other resources. Therefore, in this research, we propose an intelligent transport system (ITS) for predicting traffic congestion levels and assist commuters in taking alternative routes to avoid congestion. An intelligent model for predicting urban traffic congestion levels using XGBoost, Gated Recurrent Unit (GRU), and Long Short-Term Memory (LSTM) algorithms is developed. The comparative performance analysis of the techniques concerning the performance metrics: Mean Squared Error (MSE), Root Mean Square Error (RMSE), Mean Absolute Error (MAE), Mean Absolute Percentage Error (MAPE), Error cost, Outlier sensitivity, and Model Complexity, demonstrate that the LSTM algorithm excels the other two algorithms.**

Keywords*—Sustainable development goals; traffic congestion; traffic prediction; Gated Recurrent Unit; long short-term memory; intelligent transport system

I. INTRODUCTION

Millions of people visit the Kingdom of Saudi Arabia yearly to perform Hajj and Umrah. During the Hajj period, two Holy cities experience the peak of traffic. Due to the large number of expatriates, the other major cities also usually experience the peak. The Kingdom aims to reduce peak hour congestion levels in the major cities as an important element under the SDGs of Vision 2030. So, the priorities in the Kingdom's Vision 2030 include programs for self-driving vehicles [1]. An intelligent transport system for predicting the congestion level and traffic analysis will assist the self-driving vehicle program initiative.

Apart from the proper road design, the main focus of the Transport Ministry in the Kingdom of Saudi Arabia is on road safety mechanisms, like mounting proper traffic and guide signs, adequate water drainage, and highway fencing to avoid accidents due to animal entry [2]. The concerned committees on existing roads and improving safety policies are trying too hard to prevent fatalities due to accidents. The National Road Safety Center (NRSC) is one of the Kingdom's road safety initiatives to reduce traffic fatalities within the National Transformation Program 2020 [3]. The goal is to establish a center of technical excellence and strategic partner for road safety stakeholders to place the Kingdom among the top 20 countries in road safety by 2030 [3]. Therefore, one of the key initiatives of this research project is to apply Artificial Intelligence (AI) technologies to effectively forecast traffic congestion levels during peak traffic load periods to diversify road traffic efficiently.

So, our proposed system will offer effective management of the congestion level, thereby reducing the cost of accidental deaths, serious injuries, and travel time. Consequently, the quality of social life will improve.

Moreover, higher congestion leads to higher energy consumption and creates related challenges such as environmental pollution, high CO_2 emissions, health risks, etc. An ITS capable of predicting the congestion level will help minimize the traffic congestion levels and related challenges [4].

Novelty and Motivation of the Research Work

1) An intelligent transport model development: The research aims to develop an intelligent transport system model for forecasting traffic congestion levels using an amalgamation of ML and deep learning (DL) techniques.

2) Prediction of the traffic congestion levels: We investigate and exploit various learning techniques capable of effectively predicting the traffic congestion levels for developing an intelligent transport system.

3) Better traffic control and management: Controlling and managing traffic congestion during peak hours and in undesirable circumstances e.g., in an accident or any intentional road blockage is in line with the SDGs.

4) Reduction in transportation time: The project's outcomes can be used in the concerned committee settings to

*Corresponding Author.

reduce the overall transport time for the citizens and the residents.

5) Comparative analysis of multiple techniques: A comparative analysis of the proposed model's results with the existing traffic congestion prediction techniques strengthens its validity and viability.

This document is organized as follows. Section II describes the literature review. Section III discusses the Methodology; Section IV outlines the Proposed Work. Section V covers the Experimental Analysis. Section VI concludes the research.

II. Literature Review

The concept of an intelligent transport system is useful for overcoming the crisis of urban traffic congestion levels raised due to the migration of people to urban areas by efficiently predicting traffic congestion levels in urban areas [5-9]. The goal of such a system is to achieve traffic efficiency by minimizing the commuters' travel time, consumption of energy, and requirement of other resources and maximizing road safety and commuters' comfort level. These applications are deployed as strategic and sustainable development plans in techno-savvy countries to bring the concept of intelligent transport systems into reality.

Faster And Safer Travel Through Routing and Advanced Controls (FAST-TRAC) [9] is one of the earliest projects deployed in Oakland County, Michigan. The system receives and shares data and live video of traffic conditions with the Michigan Department of Transportation. It is one of the first suburban adaptive traffic control systems in the USA; also, the first to use video processing for an adaptive traffic control system in the world, and the first to launch a traffic website about real-time traffic information.

Sydney Coordinated Adaptive Traffic System (SCATS) [10] signal system uses eight phase signals to fit into the changing traffic patterns. This traffic control system optimizes traffic flow and implements intelligent algorithms to process real-time data to predict traffic patterns, reduce congestion and travel time, and enhance travel safety. It has reduced travel time by 28%, stops by 25%, fuel consumption by 12%, and emissions by 15%.

Some similar early systems to mention are Driver Information Radio using Experimental Communication Technologies (DIRECT), ADVANTAGE l-75, Suburban Mobility Authority for Regional Transportation (SMART), Cooperative Intersection Collision Avoidance System (CICAS), and Data Use Analysis and Processing (DUAP), etc.

Recent developments for automated and real-time processing of crowding information are the Google Maps transit service [11], Singapore LTA [12], and the Moovit travel app [13]. These systems are not cost-effective.

The paradigm of road safety has shifted from passive to active safety. Effective traffic congestion detection capability and effective analysis of real-time data are the keys to the efficiency of these systems [14].

The concept of intelligent traffic systems is incomplete without extracting useful and distinctive patterns from the collected data for real-time decision-making. A. Drabicki et al. [7] propose a framework for modeling an RTCI (real-time crowding information) system with an agent-based model with PT (public transport) simulations. This system is not validated as a reliable model and ceases to be an evidence-based analytical tool.

L. Li et al. [8] discuss the critical role of trajectory data focusing on traffic flow by revisiting traffic models at three levels (microscopic/mesoscopic/macroscopic). Their research is based on theoretical aspects of the field without practical implementation.

Authors in study [6] deal with the techniques of improved traffic flow and safety and less congestion including evaluating the performance of intelligent transport systems through a survey among the urban truck drivers. They do not implement a model for intelligent transport systems.

Authors in study [15] discuss sustainable traffic management issues focusing on IoT and intelligent information systems. Their research is based on theoretical aspects of the field without practical implementation.

Authors in study [16] propose a deep autoencoder neural networks model for traffic congestion prediction on the SATCS dataset. During the congestion level prediction in their work, there is a loss of information in representing the congestion levels in the proposed network. There is no clarity on information loss and what is the impact of information loss on prediction performance.

K. Zhang et al. [17] propose a data-driven model to predict traffic congestion flow in urban regions using the Convolutional Neural Network (CNN) LSTM network. The model depends on statistical analyses and employs a black box DL model for congestion prediction which lacks interpretable algorithms for traffic modeling.

Authors in study [18] described an intelligent traffic prediction approach using RFs and SVMs. However, they use simulations to validate the outcomes.

Therefore, in this project, we aim to design an effective intelligent model for traffic congestion prediction using an amalgamation of ML- and DL-based approaches which will improve the weaknesses of the previous work. This work will solve the urban traffic congestion of the Kingdom.

III. Methodology

An ITS consists of multiple components such as traffic management systems, electronic toll collection, vehicle-to-infrastructure communications, traffic flow forecasting, traveler information systems, etc. Traffic flow forecasting is an important component of ITS. Accurate traffic flow forecasting can improve an ITS in multiple ways such as improved traffic conditions by route optimization, improved travel efficiency by mitigating congestion, etc. Vehicle traffic flow is influenced by several factors that exhibit complex spatial-temporal dependencies. These complex spatial-temporal dependencies and non-linear relationships in the traffic data, make the forecasting task more challenging. Hence, different techniques of traffic flow forecasting face many challenges. This paper

analyzes many AI techniques for forecasting effective and efficient traffic flow. Several machine-learning techniques have been utilized in forecasting and other complex real-world applications [19-26]. These techniques include LSTM networks for time series, GRU, Nonlinear Autoregressive with exogenous input (NARX), Random Forest (RF), and XGBoost. Each has been evaluated based on its strengths, weaknesses, and suitability for forecasting the inherent spatial-temporal dependencies within traffic data.

A. Random Forest

RF is a machine learning (ML) technique that can be utilized for classification and regression. However, the most common application of this technique is classification. It belongs to the category of ensemble ML approaches. The ensemble approach can be considered as a group of experts working together to find the solution to a problem. Ensemble techniques rely on multiple models (often base learners) working together to generate the final prediction by combining predictions of all the models. RF ensembles multiple decision trees [27, 28] as illustrated in Fig. 1.

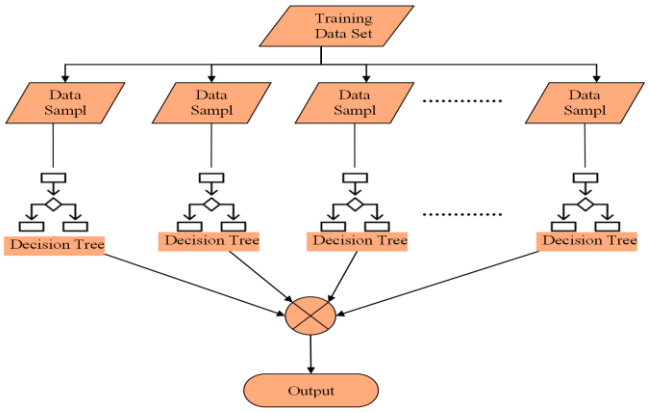


Fig. 1. Random forest.

Therefore, an RF builds an ensemble of multiple decision trees. The predictions of these trees are combined. Each subtree is built on a random subset (with replacement) of training data. This prediction aggregation process is also known as bagging or bootstrap aggregating. At each split in a tree, only a subset of features is considered. This process is known as random feature selection. Due to the randomness, caused by the random feature selection, overfitting is reduced. Each tree gets to vote for the final prediction. In the case of classification, the most likely outcome is the one with the majority of votes, and in the case of regression, the prediction is the averaged predicted value of all the trees [29]. This research predicts the number of vehicles and therefore, the RF regressor model has been utilized for the implementation. The traffic data of the time series has been categorized into four traffic categories for easier interpretation. Therefore, the predicted numbers are converted into high, low, normal, or heavy traffic category. Several research studies have analyzed the effectiveness of RF in forecasting road traffic [29-33]. An analysis by [30] compares the traffic prediction accuracy between the Bayesian network and RF. The study outlines that RF performs better than Bayesian networks in traffic prediction scenarios. Another study [33] analyzes multiple ML models and concludes that RF performs better than the other models.

B. XGBoost

eXtreme Gradient Boosting (XGBoost) is one of the powerful ML techniques for prediction tasks like classification and regression [34]. XGBoost is an ensemble technique. It combines the capabilities of the decision trees and gradient boosting. The decision trees are ensembled sequentially. The prediction errors introduced by the previous tree are corrected by the next tree improving the final prediction. XGBoost incorporates Lasso (L1) and Ridge (L2) regularizations to prevent overfitting. Using regularization also helps in controlling the complexities of the trees. XGBoost allows custom-defined loss functions or uses commonly used loss functions such as MSE and log loss functions. Mean squared is used for regression tasks. As in this research, the model aims to predict the number of vehicles, therefore, the MSE loss function has been used. XGBoost utilizes parallel and distributed computing environments to speed up the training [35]. To improve the speed and optimization, XGBoost uses the computation by pruning the irrelevant branches in the early stage. The pruning process utilizes the sparse learning technique [36]. Several researchers have leveraged the capabilities of XGBoost for traffic predictions [37, 38]. As discussed, it utilizes regularization which helps in preventing overfitting. It can handle complex relationships and non-linearity present in the traffic data points.

C. Neural Network Time Series Nonlinear Autoregressive

Vehicle traffic data can often be subject to high variance and rapid transients. Therefore, time series forecasting models should be able to overcome the non-linearity of these changes. A research study [39] suggests that the following non-linear autoregressive model $\hat{y}(t) = h\big(y(t-1), y(t-2), \dots, y(t-d)\big) + \varepsilon(t)$ can be utilized to model such variance and transient time series data. This model equation has been explained in the next paragraph. The model analyzed past traffic data to predict future traffic volumes for vehicle traffic forecasting. However, as discussed earlier, traffic data is often non-linear, therefore, a non-linear autoregressive neural network has been utilized for traffic volume forecasting. The implemented neural network is a multilayer feedforward network with feedback connections [39, 40]. The general structure of the multilayer nonlinear autoregressive neural network has been illustrated in Fig. 2.

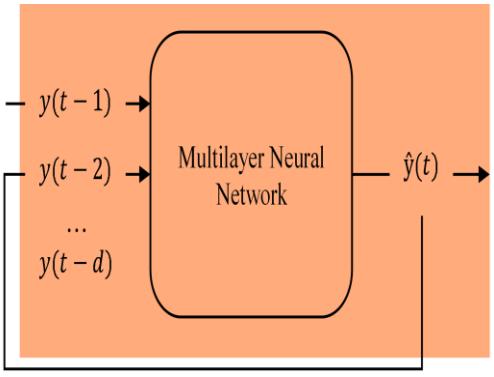


Fig. 2. Structure of the multilayer nonlinear autoregressive neural network.

The mathematical representation of the model can be stated using the following equation:

$$\hat{y}(t) = h\big(y(t-1), y(t-2), \dots, y(t-d)\big) + \varepsilon(t) \quad (1)$$

This equation states that the predicted value can be formulated into a function h of past time-series values. During the training process, weights and bias values are adjusted to approximate the function h. The term $\varepsilon(t)$ represents the error. It is a sequence of random independent variables. The sequence has a mean of zero and a finite variance. The neural network model trains on the past time series data using d feedback delays. The parameter d is the delay and can be tuned by the trial-and-error method for better accuracy. The proposed work has implemented different training algorithms- scaled conjugate gradient, Bayesian regularization (BR), and Levenberg-Marquardt (LM) with the dataset. Due to the features of each algorithm, they may perform differently with the same training data and network architecture. The scaled conjugate gradient algorithm used the gradient calculation method. It made it more memory efficient than the LM and BR training algorithms which utilize Jacobian calculations.

D. Long Short-Term Memory Networks

The LSTM neural network was proposed by Hochreiter and Schmidhuber [41]. These are a category of recurrent neural networks (RNNs) that are types of artificial neural networks. RNNs can identify the patterns in the data sequences or time series.

The vehicle traffic flow data used time series data in this research work. Time series forecasting may lead to sequence dependency issues on the input variable [42]. RNN maintains a memory of the previous inputs through the hidden states to learn from sequential or time-series data. However, RNNs can suffer from the vanishing gradient problem. A vanishing gradient problem where the gradients become very small as they are back-propagated through time. It leads to difficulties in learning long-term dependencies. LSTMs are specifically designed to address this problem. LSTMs utilize memory cells with gates. Gates control the information flow and allow the network to learn long-term temporal patterns. LSTM neural network is composed of multiple cells. The following Fig. 3 illustrates a typical cell of the LSTM neural network at the time t.

The cells of the LSTM network are very similar to those of the RNN neural network and utilize the previous timestep as shown in Fig. 1.

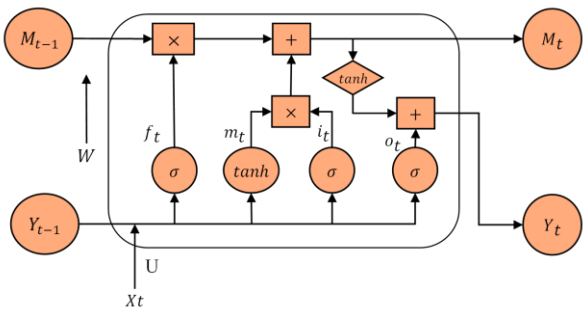


Fig. 3. LSTM neural network cell at the time t.

In LSTM, each cell is composed of an input gate (i_t), an output gate (o_t), a forget gate (f_t) and memory (m_t). The additional component in the LSTM neural network is the memory unit. These cells are the elementary units for the layers of the neural network. The memory of the LSTM neural network comes from the cells of the hidden units. The cell memorizes the values of the unit for an arbitrary period. The forget gate and input gate apply the sigmoid activation function (represented as σ) and the activation function for memory is $tanh$. M_{t-1} represents the memory from the previous cell and M_t represents the memory of the current cell. Similarly, the Y_{t-1} is the output from the previous cell and Y_t represents the output of the current cell. The symbol '×' illustrates the elementwise multiplication and the symbol '+' represents the elementwise addition. X_t is the t^{th} timestep input to the cell. U and W are the weight vectors. The output of these gates is the vectors computed by applying the weights and corresponding activation functions on the input for every timestep. Each cell generates a memory and an output. The memory can either be utilized or forgotten by the next cell depending on the values from the activation function of the forget gate as depicted in Fig. 1.

E. Gated Recurrent Units

The GRUs were introduced by [43], one of the powerful architectures based on RNN. Similar to LSTM, they use a gating mechanism to manage information flow. However, they have simpler architectures with fewer parameters than LSTM, making them faster to train than LSTM [43]. The vanishing gradient issue is where the information from old data sequences does not propagate properly through the network. The GRUs mitigate this issue by capturing long-term dependencies. Research studies [44, 45] have implemented GRUs for traffic prediction with promising results. We discuss the functions of each component of GRUs in the below paragraph.

A GRU unit consists of two main gating mechanisms known as update gate (z_t) and reset gate (r_t). The output hidden state (h_{to}) at time t is determined by the candidate's hidden state (h_t), update gate (z_t) and reset gate (r_t). The update gate is represented mathematically as:

$$z_t = \sigma\,(W_z[h_{t-1},\ x_t] + b_z) \quad (2)$$

The values close to 0 disregard the past state and values close to 1 indicate the higher influence of the past states. The update gate controls the information flow from the previous hidden state (h_{t-1}). The reset gate (r_t) controls the influence of the past states. That is, how much or to what extent, the processing of the current state (x_t) of the network relies on the past hidden states. The reset gate is represented mathematically as:

$$r_t = \sigma\,(W_r[h_{t-1},\ x_t] + b_r) \quad (3)$$

The values close to 1 indicate that the network can utilize the past state and the values close to zero indicate that the network should focus on the current input. The information flow is managed using the activation functions such as sigmoid (σ) or hyperbolic tangent ($tanh$). The candidate's hidden state is calculated using the current input and the selective

information from the previous hidden state. It is represented mathematically as:

$$h_t = tanh\,(W_h[r_t * h_{t-1},\ x_t] + b_h) \quad (4)$$

The output hidden state (h_{to}) is computed by using the previous hidden state, candidate hidden state, and update gate as:

$$h_{to} = (1 - z_t) * h_{t-1} + z_t * h_t \quad (5)$$

In the above equations, W and b are parameter metrics and vectors.

GRUs offer compelling performance with simple architecture which is computationally lighter to train than LSTM.

The predictive ability of the combined method was evaluated by four indices, namely, the MAE, the MSE, the RMSE, and the MAPE:

$$MAE = \frac{1}{n}\sum_{t=1}^{n}|y_t - \hat{y}_t|$$

$$MSE = \frac{1}{n}\sum_{t=1}^{n}(y_t - \hat{y}_t)^2$$

$$RMSE = \sqrt{\frac{1}{n}\sum_{t=1}^{n}(y_t - \hat{y}_t)^2}$$

$$MAPE = \frac{1}{n}\sum_{t=1}^{n}\frac{y_t - \hat{y}_t}{y_t} \times 100\% \quad (6)$$

IV. Proposed Work

Fig. 4 represents the proposed system's general architecture. This project will investigate and exploit several prediction techniques using three algorithms, XGBoost, GRUs, and LSTMs. These methods will be compared based on the performance of prediction accuracy. After evaluating the implemented techniques, the model that performs the best among these alternatives will be selected for forecasting the congestion level and presented as a model for deployment.

A. Dataset Description and Analysis

Actual urban traffic scenarios are complex. Traffic is dynamic over the days of the week and hours of the day. Therefore, proper data analysis depends on the actual traffic scenario. During the weekdays there are very high volumes of traffic usually called rush hours often from 6 am to 8 am and from 4 pm to 6 pm when most people are either going to or coming from work. This period heavily impacts traffic congestion levels. Fridays show unique deviation from anticipated as typical weekday traffic patterns; despite being considered part of weekdays. Congestion is not experienced during normal working hours but there is still increased road usage though not as much as on other days of the week perhaps due to leisure activities and social gatherings. Monday is the only day commuters commute consistently, most likely because it is the first day after taking a weekend off. Therefore, temporal factors should be considered when designing effective management systems since they offer better insights into the potential intensity of bottlenecks at specific times if nothing is done to mitigate them.

The dataset used in the research work is publicly available at Kaggle [46]. Table I summarizes the features of the dataset. The detailed dataset description is available in Table II.

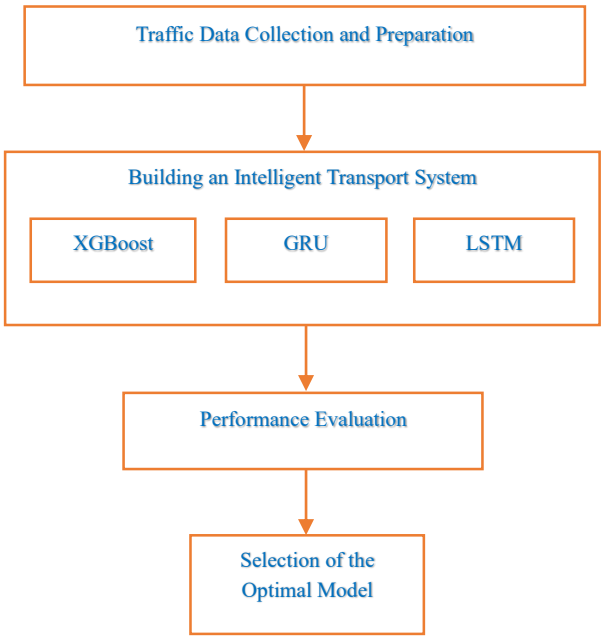


Fig. 4. The proposed ITS architecture.

TABLE I. Dataset Summary

Total Records	5952
No. of Attributes	9
Attributes	Time, Date, Day of the week, CarCount, BikeCount, BusCount, TruckCount, Total, Traffic Situation

TABLE II. Summary of Temporal Traffic Dataset

Day	Period	Traffic Volume	Key Observations
Weekdays	06:00 - 08:00	High	Morning rush hour due to work commutes
	16:00 - 18:00	High	Evening rush hour due to work commutes
Friday	06:00 - 08:00	Lower	Reduced morning congestion compared to other weekdays
	16:00 - 18:00	Moderate	Evening traffic due to social and recreational activities
Weekends	Various	Variable	Much lesser uniformed traffic patterns contrast to weekdays

The quantiles and distributions of the four vehicle types are illustrated in Fig. 5 with box plots and histograms respectively.

The research considers four categories of traffic situations namely low, normal, high, and heavy to analyze the traffic congestion situations. The number of average total transportation for each category of traffic situations has been depicted in Fig. 6.

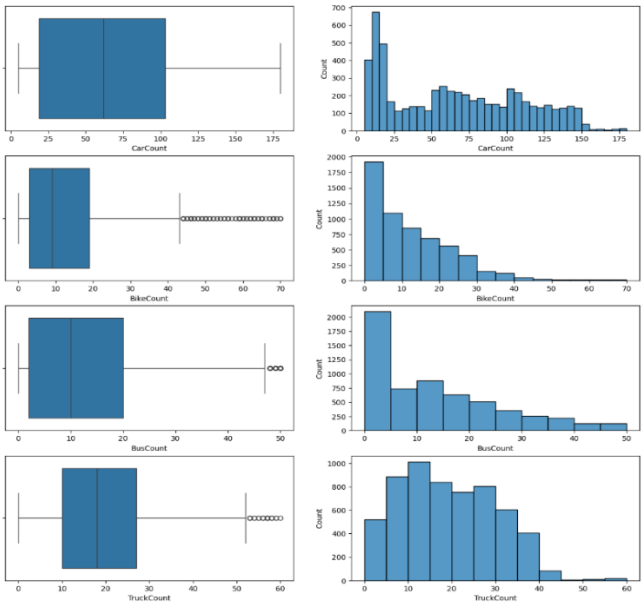


Fig. 5. The box plots and distributions (histograms) of the four vehicle types.

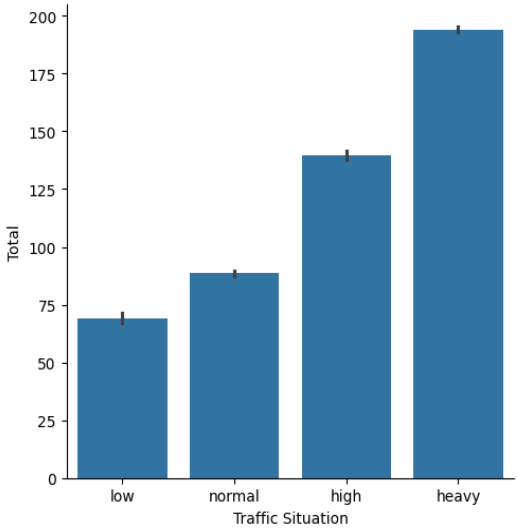


Fig. 6. The number of average total transportation for each category of traffic situations.

A pie chart of total vehicles by traffic situation has been shown in Fig. 7.

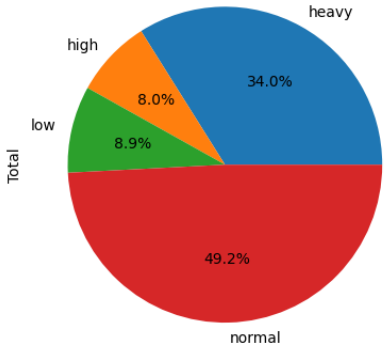


Fig. 7. Total vehicles by traffic situations.

B. Proposed Models

Temporal traffic pattern insights are useful for urban planners and decision-makers to reduce congestion and plan for infrastructural growth and transport system development toward building resilient cities that can withstand natural calamities and shocks such as heavy rains, floods, and earthquakes. Three algorithms are used for predicting future transportation states: XGBoost, GRUs, and LSTMs. The performance metrics used to evaluate the XGBoost model with 100 estimators included MSE, RMSE, MAE, MAPE, Error cost, Outlier sensitivity, Model complexity, etc. We compare the forecast against actual data to visualize our models' performance.

The GRU model, which consisted of a single GRU layer followed by two dense layers, underwent extensive training and evaluation. Performance measures were calculated, and predictions were compared to the real data. However, a type error occurred during the visualization step because the test set and predictions had different formats. This issue was resolved by transforming the forecasts into a NumPy array.

The training, assessment, and presentation procedures for the LSTM model—which consists of one LSTM layer followed by two dense layers—should be mentioned, among other things. It's also important to note that Fig. 8 displays the graphical representation of error distribution for each model, providing insight into the distribution and concentration sections where such errors are in the prediction cluster.

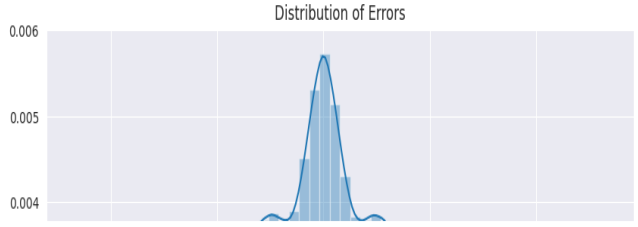


Fig. 8. Error distribution for each model.

V. Analysis of the Experiments

An experimental setup will be established, and its comprehensive experimental analysis will be performed in this section.

We discuss traffic forecast techniques using three models: XGBoost, GRU, and LSTM. To enable the chosen models to use the dataset, we first do considerable pre-processing on it. These procedures include encoding categorical information like the day of the week and traffic conditions and standardizing time to a 24-hour format. The data set is split into train-test sets for model training and evaluation, following the pre-processing. Our investigation begins with the RF model, well known for its ability to handle complex information. It offers insights into its predicted performance through an extensive evaluation process. Specifically, its ensemble learning approach exhibits competitive performance metrics, indicating strong performance in tasks such as traffic prediction where multiple factors influence the final result. The metrics employed by the models are summarized in Table III to give individual and comparative performance evaluations.

TABLE III. COMPARATIVE EVALUATION OF METRICS FOR MODEL PERFORMANCE

Metrics	Performance Values		
	XGBoost	***GRU***	***LSTM***
Mean Squared Error (MSE)	15.6	12.8	10.5
Root Mean Squared Error (RMSE)	3.95	3.58	3.24
Mean Absolute Error (MAE)	2.75	2.45	2.15
Mean Absolute Percentage Error (MAPE)	5.3%	4.7%	3.9%
Error Cost	Moderate	Moderate	Low
Outlier Sensitivity	Low	Moderate	Low
Model Complexity	High	Medium	High

The metrics employed by the XGBoos model are demonstrated in Fig. 9. The MSE for the XGBoos model between the actual and projected values is 15.6. RMSE provides a comprehensible metric of error magnitude and a small deviation from true values because it is the square root of MSE. This relatively low MSE suggests that the model's predictions are reliable. With an MAE of 2.75, the model demonstrates modest prediction errors, indicating its forecasting reliability. These figures are supported by a MAPE of 5.3%, which displays MAPE about actual values, presenting that on average the system's predictions should not deviate significantly (within a range of ±%) from reality. Such an accomplishment reflects an important degree of precision needed in real-world traffic forecasting applications, where it may not always be possible to obtain detailed or reliable historical data on past events to use as the foundation for future projections. In urban traffic management, moderate mistake costs imply manageable effects on flow control strategies intended to reduce congestion within cities; therefore, they can be effortlessly handled using suitable actions taken at strategic points along important paths serving various parts of the city. Mild mistake costs show operational/financial impacts related to incorrect predictions. The RF model's insensitivity to outliers is a crucial feature that makes it perfect for handling traffic data with irregular abnormalities like accidents or abrupt volume increases. This resistance against anomalous values guarantees smooth functioning and accurate predictions are made throughout, even in the face of random data points. Furthermore, the building of numerous decision trees combined is the cause of the high inherent complexity in the RF design. This complexity increases forecasting accuracy and makes it possible to represent intricate relationships within databases, such as those including multiple communicating variables, whose collective impact can either facilitate or obstruct flow depending on what is occurring at any given time. Yet, managing large amounts of input/output data can be challenging and require a higher level of interpretability, requiring more processing power than would typically be necessary under less demanding limitations. These examples show how effective an RF model can be in traffic prediction: Comparatively low MSE and RMSE readings, which indicate accuracy, corroborate its precision; MAE and MAPE exhibit reliability. Moderate error costs show applicability for usage in real-world scenarios where certain errors are expected but don't necessarily result in significant financial losses by striking a balance between accurate forecasts and controllable economic ramifications. When dealing with abnormal data points, XGboost is a good option because of its low sensitivity to outlying observations. This is especially true if the data points are frequently found along major highways with numerous entrances and exits close to one another over short distances, heavy traffic during peak hours, and sharp changes over time due to various factors like accidents, road works, etc.

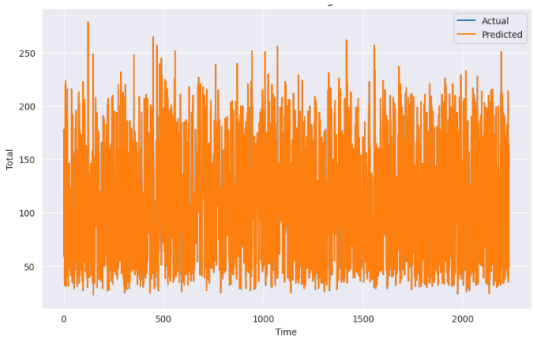


Fig. 9. XGBoost actual vs. predicted values.

The Recurrent Neural Network (RNN) architectures begin with the GRU model. The GRU model is trained and assessed by leveraging its ability to capture sequential dependencies in data. Despite promising results, with significant improvements over traditional ML methods, it does not achieve optimal performance metrics compared to the XGBoost model. Fig. 10 depicts the performance characteristics of the GRU model and provides valuable comparisons with the XGBoost model previously evaluated and shown in Fig. 9. The mean squared variance between the expected and actual values compared to XGBOOST is less than the MSE of 12.8, which indicates that the GRU model can capture temporal correlations in traffic data. The model's RMSE of 3.58, which places it higher in overall predictive performance than the XGBOOST model, further demonstrates its capacity to foresee with a smaller margin of inaccuracy. The MAE of the GRU model is 2.45, a lower value that highlights the model's accuracy in predicting traffic patterns. Furthermore, with a MAPE of 4.7% indicating that it is within 4.7% of the real values, the GRU model performs somewhat better than the XGBOOST model. Despite these promising metrics, the GRU model has moderate error costs, similar to the XGBOOST model, it represents that even though it makes generally accurate predictions, prediction errors can still have adverse operational and economic consequences that must be managed in real-world applications. While handling irregular data points better than many traditional ML models, the GRU model is not as robust as the XGBOOST model due to its moderate sensitivity to outliers. The model's performance in scenarios where anomalies occur frequently, such as traffic accidents or sudden volume increases, may be affected by this moderate sensitivity. In terms of model complexity, the GRU is classified as medium. Due to its gating mechanisms and sequential nature, it is more complex by nature than typical ML models, but not as complex as the ensemble-based XGBOOST model. The medium complexity is a suitable option for capturing temporal trends without unduly straining computational resources as it balances computational needs and predictive capabilities.

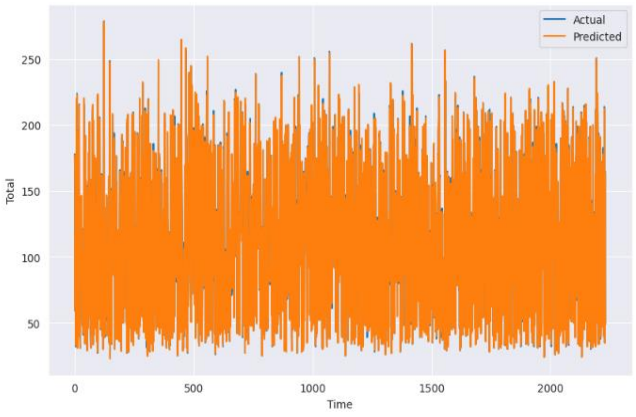


Fig. 10. GRU actual vs. predicted values.

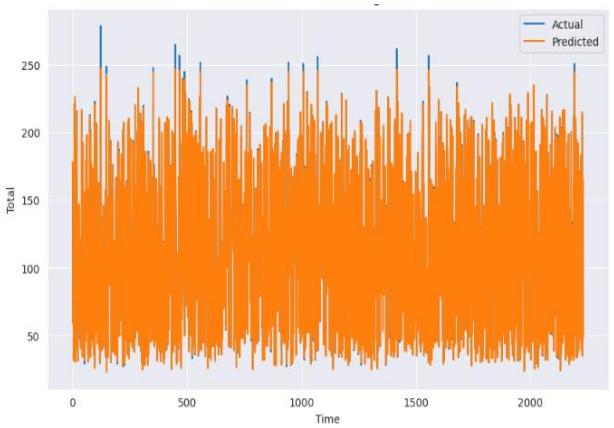


Fig. 11. LSTM actual vs. predicted values.

Next, we introduce the LSTM model known as the best for long-term dependency recognition in sequence data. In this light, traffic prediction tasks are conducted to see how well it can perform. However, there should be some more tests against an XGBOOST model, so we know what works better. Known for its depth and memory cells with specialized functions, the LSTM model has proved effective in traffic prediction. The training phase had several other models whose performance metrics were not as good as those of this one because during evaluation it achieved the lowest test loss among all considered models. This demonstrates that the only algorithm capable of making such complex predictions about traffic patterns would have been the LSTM model, which processes inputs over time and steps into outputs across variable sequence lengths until convergence on some fixed point. What more could you ask for from an LSTM model? Furthermore, the results obtained from examining the plots depicted in Fig. 11 indicate the potential success or failure of a certain predictive capability with other similar ones, such as the two displayed here, where they differ. The difference between the two models' accuracy in predicting all points examined so far throughout our research into each model's strengths and weaknesses is ΔY (Actual – Predicted), which is always within ΔX rather than zero. This indicates that both models perform equally poorly in predicting weak areas closer to either endpoint, possibly in part as none recognize features outside a certain range of values. As an illustration of the lack of consistency between anticipated forecasts made based solely on this type of proof, we can see that, between various points along the x-axis, the most faraway ones are more closely related than the two most adjacent indicated values themselves farther apart, but never precisely identical distance away from each other. This still fails to account for the least squares fits noticed.

The experimental investigation showed that many traffic forecast models ranging from deep DL techniques like GRU and LSTM to conventional ones, like XGBoost, are effective. Each model in traffic congestion prediction has demonstrated pros and cons. However, the LSTM model outperformed the others, achieving the highest accurate rate in traffic trend prediction. These results are critical in transportation planning and management because they offer practical guidance to enhance system efficiency and traffic flow optimization.

VI. Conclusion and Future Work

Our research considers many traffic scenarios to predict traffic congestion levels using an amalgamation of ML- and DL-based algorithms. The research outcomes show that both traditional ML and DL algorithms are effective. Three models, namely XGBOOST, LSTM, and GRU have been implemented on the dataset and are found powerful. The LSTM model is better than others due to its ability to capture long-term relationships between traffic data points and various patterns embedded in them. The concerned committees will utilize the research outcomes for transportation planning and management settings to optimize the flow of vehicles through different traffic routes to maximize the transportation system's efficiency. Citizens will save much of their precious time knowing the congestion level in advance; helping them plan their travel better. Business and industrial sectors can better plan the logistics and manage transport-related requirements. A high congestion level is the root of several environmental bad factors. Proper management of the congestion will improve the environment and will reduce pollution. A high level of congestion can waste commuters' time putting adverse effects on several other economic factors and accounts for high energy consumption. An ITS will assist in mitigating these factors and hence will enhance economic benefits.

The proposed model can be implemented as a mobile application in future work that can collect live data and aid the commuters in suggesting, in advance, the best route to travel based on the traffic congestion level.

While the proposed system considers various traffic scenarios occurring on specific periods of the day of the week, it does not consider other factors like weather and road conditions. We will focus on improving DL models to a hybrid of LSTM with techniques to exploit their strengths in future studies to improve the prediction effectiveness of the traffic congestion levels in ITS.

Moreover, to further increase the effectiveness of the ITS, accessing the real-time traffic data streams through comprehensive integration of vehicles' speed, location, and weather conditions to the ITS can be plenty of achievements like better accuracy in forecasting, scalability, and interoperability.

CONFLICT OF IINTEREST

The authors confirm that there is no conflict of interest to declare for this publication.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at Saudi Electronic University for funding this research (9425).

REFERENCES

[1] Budget Statement 2022, Government Budget 2022, Available online: https://www.mof.gov.sa/en/budget/2022/Pages/default.aspx, accessed on October 23, 2023.

[2] https://www.vision2030.gov.sa/v2030/a-sustainable-saudi-vision/ accessed on October 20, 2023.

[3] https://nrsc.gov.sa/5951-2/ accessed on May 20, 2024.

[4] VNR Report97, (2018), First Voluntary national review, online: https://saudiarabia.un.org/sites/default/files/2020-02/VNR_Report972018_FINAL.pdf, accessed on August 21, 2023.

[5] C. Chen, B. Liu, S. Wan, P. Qiao, and Q. Pei, "An edge traffic flow detection scheme based on deep learning in an intelligent transportation system," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 3, pp. 1840–1852, 2021.

[6] N. Drop and D. Garli´nska, "Evaluation of intelligent transport systems used in urban agglomerations and intercity roads by professional truck drivers," Sustainability, vol. 13, no. 5, p. 2935, 2021.

[7] A. Drabicki, R. Kucharski, O. Cats, and A. Szarata, "Modelling the effects of real-time crowding information in urban public transport systems," Transportmetrica A: Transport Science, vol. 17, no. 4, pp. 675–713, 2021.

[8] L. Li, R. Jiang, Z. He, X. M. Chen, and X. Zhou, "Trajectory data-based traffic flow studies: A revisit," Transportation Research Part C: Emerging Technologies, vol. 114, pp. 225–240, 2020.

[9] Danielle Deneau P.E., "FAST-TRAC and Other Innovations at the Road Commission for Oakland County," Online: http://ctt.mtu.edu/sites/default/files/resources/cew2018/06_deneau_fasttrac.pdf, accessed on August 22, 2023.

[10] "SCATS is an intelligent, adaptive traffic control system installed in over 55,000 intersections across 187 cities and 28 countries worldwide," Online: https://www.scats.nsw.gov.au/, accessed on December 22, 2023.

[11] Google, L. L. C. 2021. "Google Maps – Transit & Food [Mobile Application Software]." Online: https://apps.apple.com/us/app/google-maps-transit-food/id585027354, accessed on December 31, 2023.

[12] Singapore Land Transport Data Mall 2021. Online: https://datamall.lta.gov.sg/content/datamall/en/datamall-new-domain.html, accessed on December 30, 2023.

[13] Moovit Inc. 2021. Online: https://moovitapp.com, accessed on August 31, 2023.

[14] E. D. Andrea and F. Marcelloni, "Detection of traffic congestion and incidents from GPS trace analysis," Expert Systems with Applications, vol. 73, pp. 43-56, 2017. doi: https://doi.org/10.1016/j.eswa.2016.12.018

[15] A. A. Musa, S. I. Malami, F. Alanazi, W. Ounaies, M. Alshammari, and S. I. Haruna, "Sustainable traffic management for smart cities using internet-of-things-oriented intelligent transportation systems (ITS): challenges and recommendations," Sustainability, vol. 2023, no. 15, p. 9859, 2023. doi: https://doi.org/10.3390/su15139859

[16] S. Zhang, Y. Yao, J. Hu, Y. Zhao, S. Li, and J. Hu, "Deep autoencoder neural networks for short-term traffic congestion prediction of transportation networks," Sensors, vol. 2019, no. 19, p. 2229, 2019. doi: 10.3390/s19102229

[17] K. Zhang, Z. Chu, J. Xing, H. Zhang, and Q. Cheng, "Urban traffic flow congestion prediction based on a data-driven model," Mathematics, vol. 2023, no. 11, p. 4075, 2023. doi: https://doi.org/10.3390/math11194075

[18] P. Kar, and S. Feng, "Intelligent traffic prediction by combining weather and road traffic condition information: a deep learning-based approach," International Journal of Intelligent Transportation Systems Research, vo. 2023, no. 3, 2023.

[19] Bashir, T., Usman, I., Khan, S., & Rehman, J. U. (2017). Intelligent reorganized discrete cosine transform for reduced reference image quality assessment. Turkish Journal of Electrical Engineering and Computer Sciences, 25(4), 2660-2673.

[20] Khan, S., Alourani, A., Mishra, B., Ali, A., & Kamal, M. (2022). Developing a credit card fraud detection model using machine learning approaches. International Journal of Advanced Computer Science and Applications, 13(3).

[21] Nadeem, Z., Khan, Z., Mir, U., Mir, U. I., Khan, S., Nadeem, H., & Sultan, J. (2022). Pakistani traffic-sign recognition using transfer learning. Multimedia Tools and Applications, 81(6), 8429-8449.

[22] Khan, S., Thirunavukkarasu, K., Hammad, R., Bali, V., & Qader, M. R. (2021). Convolutional neural network based SARS-CoV-2 patients detection model using CT images. International Journal of Intelligent Engineering Informatics, 9(2), pp. 211-228, 2021.

[23] Shende, P., Bhosale, P., Khan, S., & Patil, P. (2016). Bus tracking and transportation safety using internet of things. International Research Journal of Engineering and Technology (IRJET), 3(02).

[24] Md Ezaz Ahmed, Mohammad Arif, Mohammad Khalid Imam Rahmani, Md Tabrez Nafis and Javed Ali, "Smart Parking: An Efficient System for Parking and Payment," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 15, no. 6, 2024. doi: http://dx.doi.org/10.14569/IJACSA.2024.01506130

[25] Tiwari, S. K., Al-Dmour, A., Kumaraswamidhas, L. A., Kushwaha, P., Khan, S., & Kamal, M. (2022, June). Noise and vibration exposure on the physiological parameters of bus drivers using machine learning algorithm. In 2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS) (pp. 164-169). IEEE.

[26] Qader, M. R., Khan, S., Kamal, M., Usman, M., & Haseeb, M. (2021). Forecasting carbon emissions due to electricity power generation in Bahrain. Environmental Science and Pollution Research, 1-12.

[27] V. Priyadarshni, S.K. Sharma, M. K. I. Rahmani, B. Kaushik, and R. Almajalid, "Machine Learning Techniques Using Deep Instinctive Encoder-Based Feature Extraction for Optimized Breast Cancer Detection," Computers, Materials & Continua, vol. 78, no. 2, pp. 2441-2468, 2024. doi: https://doi.org/10.32604/cmc.2024.044963

[28] L. Cheng, X. Chen, J. D. D. Vos, X. Lai, F. Witlox, "Applying a random forest method approach to model travel mode choice behavior, Travel Behaviour and Society," vol. 14, pp. 1-10, 2019. doi: https://doi.org/10.1016/j.tbs.2018.09.002.

[29] J. Evans, B. Waterson, and A. Hamilton, "Forecasting road traffic conditions using a context-based random forest algorithm," Transportation Planning and Technology, 2019. doi: https://www.tandfonline.com/doi/abs/10.1080/03081060.2019.1622250

[30] J. Roos, G. Gavin, S. Bonnevay, "A dynamic Bayesian network approach to forecast short-term urban rail passenger flows with incomplete data," Transportation Research Procedia, vol. 26, pp. 53-61, 2017. doi: https://doi.org/10.1016/j.trpro.2017.07.008.

[31] Z. Nadeem, Z. Khan, U. Mir, U. I. Mir, S. Khan, H. Nadeem, and J. Sultan, "Pakistani traffic-sign recognition using transfer learning," Multimedia Tools and Applications, vol. 81, no. 6, pp. 8429–8449, 2022. doi: https://doi.org/10.1007/s11042-022-12177-8

[32] M. Yan, and Y. Shen, "Traffic accident severity prediction based on random forest," Sustainability, vol. 14, no. 3, 2022. doi: https://doi.org/10.3390/su14031729

[33] N. Zafar, and I. U. Haq, "Traffic congestion prediction based on estimated time of arrival," PLOS ONE, vol. 15, no. 12, e0238200, 2020. doi: https://doi.org/10.1371/journal.pone.0238200

[34] T. Chen, and C. Guestrin, "XGBoost: a scalable tree boosting system," Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 785–794, 2016. doi: https://doi.org/10.1145/2939672.2939785

[35] X. Gao, S. Fan, X. Li, Z. Guo, H. Zhang, Y. Peng, and X. Diao, "An improved XGBoost based on weighted column subsampling for object classification," 2017 4th International Conference on Systems and Informatics (ICSAI), pp. 1557–1562, 2017. doi: https://doi.org/10.1109/ICSAI.2017.8248532

[36] Z. He, D. Lin, T Lau, M. Wu, "Gradient Boosting Machine: A Survey," ArXiv. https://arxiv.org/abs/1908.06951, 2019.

[37] X. Dong, T. Lei, S. Jin, S., and Z. Hou, “Short-term traffic flow prediction based on XGBoost,” 2018 IEEE 7th Data Driven Control and Learning Systems Conference (DDCLS), pp. 854–859, 2018. doi: https://doi.org/10.1109/DDCLS.2018.8516114

[38] Y. Yang, K. Wang, Z. Yuan, and D. Liu, “Predicting freeway traffic crash severity using XGBoost-Bayesian network model with consideration of features interaction,” Journal of Advanced Transportation, vol. 2022, e4257865, 2022. doi: https://doi.org/10.1155/2022/4257865.

[39] S. Kiranyaz, T. Ince, O. Abdeljaber, O. Avci and M. Gabbouj, "1-D Convolutional Neural Networks for Signal Processing Applications," ICASSP 2019 - IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 2019, pp. 8360-8364, doi: 10.1109/ICASSP.2019.8682194.

[40] S. Ryu, J. No, H. Kim, “Deep Neural Network Based Demand Side Short Term Load Forecasting,” Energies, vol. 10, no. 3, pp. 1-20, 2017. doi: https://doi.org/10.3390/en10010003.

[41] B. Lindemann, T. Müller, H. Vietz, N. Jazdi, M. Weyrich, “A survey on long short-term memory networks for time series prediction,” Procedia CIRP, vol. 99, pp. 650-655, 2021, doi: https://doi.org/10.1016/j.procir.2021.03.088.

[42] M. R. Qader, S. Khan, M. Kamal, M. Usman, and M. Haseeb, “Forecasting carbon emissions due to electricity power generation in Bahrain,” Environmental Science and Pollution Research, vol. 29, no. 12, pp. 17346–17357, 2022. doi: https://doi.org/10.1007/s11356-021-16960-2

[43] K. Cho, B. V. Merrienboer, C. Gulcehre, D. Bahdanau, F. Bougares, H. Schwenk, and Y. Bengio, “Learning phrase representations using RNN encoder-decoder for statistical machine translation,” (arXiv:1406.1078). arXiv, 2014. doi: https://doi.org/10.48550/arXiv.1406.1078

[44] S. M. Abdullah, M. Periyasamy, N. A. Kamaludeen, S. K. Towfek, R. Marappan, S. K. Raju, H. A. Alharbi, and D. S. Khafaga, “Optimizing traffic flow in smart cities: soft GRU-based recurrent neural networks for enhanced congestion prediction using deep learning,” Sustainability, vol. 15, no. 7, 2023. doi: https://doi.org/10.3390/su15075949

[45] R. Fu, Z. Zhang, and L. Li, “Using LSTM and GRU neural network methods for traffic flow prediction,” 2016 31st Youth Academic Annual Conference of Chinese Association of Automation (YAC), pp. 324–328, 2016. doi: https://doi.org/10.1109/YAC.2016.7804912

[46] Traffic Prediction Dataset. Online: https://www.kaggle.com/datasets/hasibullahaman/traffic-prediction-dataset accessed on 20th August 2024.

SAM-PIE: SAM-Enabled Photovoltaic-Module Image Enhancement for Fault Inspection and Analysis Using ResNet50 and CNNs

SAM-Enabled Photovoltaic-Module Image Enhancement (SAM-PIE)

Rotimi-Williams Bello*, Pius A. Owolawi, Etienne A. van Wyk, Chunling Du
Department of Computer Systems Engineering-Faculty of Information and Communication Technology,
Tshwane University of Technology, South Africa

***Abstract*—Different models have been developed for segmentation tasks, each with its uniqueness. Recently, the Segment Anything Model (SAM) was added to the pool of these models with expectations of addressing their weaknesses. SAM, although trained on a huge dataset for segmentation of anything, particularly images of natural source, produces suboptimal results when applied to segmentation of photovoltaic module image due to difference in semantic between photovoltaic module and natural images. In spite of the current suboptimal performance of SAM in segmentation of photovoltaic module images, it demonstrates detection and identification of thermal anomalies in photovoltaic module images that majorly contribute to power production loss. The implication of this is that, the task, the model, and the data corresponding to SAM are applicable to photovoltaic module image diagnosis. In this paper, we propose SAM-enabled photovoltaic-module image enhancement (SAM PIE) for fault inspection and analysis using ResNet50 and CNNs. SAM-PIE combines the strength of SAM for enhancement of the fault inspection and analysis procedure, for optimal performance of the proposed method. Experiments were performed on three thermal anomaly image datasets of photovoltaic modules to validate the performance of SAM-PIE for the classification tasks. The results obtained validates the potential capability of SAM-PIE to perform photovoltaic module image classification. The dataset is publicly and freely available for scientific community use at https://doi.org/10.17632/5ssmfpgrpc.1**

***Keywords*—Anomaly; convolution neural networks; crack; hotspot; photovoltaic; Residual Network-50; shading**

I. INTRODUCTION

Recently, there was an emergence of a state-of-the-art foundational model called the Segment Anything Model (SAM) [1] in the field of Computer Vision (CV) for image segmentation tasks. The main components that make the leap possible for the SAM are: (a) Prompts for new segmentation task, (b) SAM's model, and (c) SA-1B dataset. The prompt-able segmentation task was proposed in order to return a valid segmentation mask provided any prompt for segmentation is given. The main task of the prompt is simply to specify the image's object to segment, e.g., spatial or text information can be a prompt for object identification. For an output mask to be valid, there is a requirement that the output under any circumstances (for example, when there is an ambiguity in what object a prompt specifies in an image) should generate sensible mask at the least for one of the objects in the image.

The innovative design of the SAM model satisfies all the constraints imposed on the model architecture due to prompt-able task of segmentation and reality in real-world applications. In particular, prompts flexibility support masks computation in amortized real-time and ambiguity-aware [1-2]. Based on the abovementioned qualities attributed to SAM and its demonstration as a good model trained on a wide-ranging scalable data for flexibility, studies reveal the tendency of it facing challenges in tasks involving domain-specific segmentation solution [3], as noticed in some photovoltaic (PV) module image segmentation scenarios [4-6]. The rise of PV power has given a new dimension to renewable energy as evident in the global renewable energy, and this trend continues in gaining more acceptance as alternative to power generation [7-12].

The PV explosion requires an in-depth knowledge of its widespread, challenges, and prospect for concern individuals [13-15]; and this knowledge is essential for its proper monitoring, management, and maintenance across borders [16-20]. The inspection, detection, identification, and analysis of faults in PV installations have greatly been enhanced by the progress made in CV [21-24]. However, the majority of research on PV installations concentrate on using conventional CV techniques for inspection and analysis of the anomalies in solar cells of PV modules, which performs below expectations [25-27]. Moreover, high-resolution images are extremely required to obtain accurate inspection and analysis of PV modules [28], and the conventional techniques pose challenges regarding this.

Many researchers have attributed the inaccuracy obtained in their segmentation tasks to incapability of SAM when applied to PV image segmentation tasks, confirming the discrepancies in the tasks, model, and datasets. Although SAM shows segmentation efficiency in object-specific tasks, it still has limitations when dealing with fine structures, small disconnected components, weak boundaries and modalities [29-30]. Complex modalities, fine modular structures, small disconnected cell components, and absence of sharp boundaries are the challenges confronting SAM in PV image segmentation [28]. Additionally, the segment anything-1

The authors received funding from the Tshwane University of Technology, South Africa.

billion (SA-1B) of natural images on which SAM was pre-trained couple with the approach to determine boundaries based on discrepancy in intensity [28] is not applicable to PV images due to analysis of solar cells of the PV modules.

Moreover, while SAM can carry out many tasks, it does not have the prompts capability for panoptic and semantic segmentation implementation. Lately, SAM has experienced so much improvement due to many studies commitment to enhancing it due to its disappointing results to suit domain-specific tasks as noticed in PV image analysis. Several of these studies has dedicated their strength to fine-tuning the SAM model to enhance its performance and reliability for PV image analysis. Yang et al. [13] in their quest to meet the demand for the extraction of large-scale PV panel, proposed a novel weakly-supervised method that was based on the SAM model. Knowing the importance of broad data volumes and the knowledge that the extraction process requires the concept of latent PV locations for reduction in scope of the amount processed subsequently, they applied the method to the segmentation of latent PV locations for smooth passage from classification to segmentation. They achieved segmentation results that could stand the test of time.

Although SAM being initialized with a self-supervised technique [28], its efficiencies depend on large-scale supervised training. Rafaeli et al. [2] addressed this issue by proposing segmentation that is prompt-based at varied light conditions and resolutions using SAM 2. Their study revealed the efficiency of SAM 2 over SAM, particularly when prompted by points under lighting conditions that are sub-optimal. SAM's strength is challenged in segmentation of PV images, being a model trained on massive natural images. Although SAM may be prompt-able to efficiently segment PV images, it can still differentiate conspicuous solar cells of PV modules according to changes in image pixels. PV images are images of solar panels with a lot of revealing information only under high thermal image and pixel resolutions [31-32].

Therefore, thermal captured and enhanced images give visual quality to PV images for valuable information on anomalies detection, and analysis beyond what can be obtained from original image. Based on this, the aim of applying the techniques of PV image enhancement (PIE) in this study is to attain efficient and excellent inspection and analysis of PV faults from the available original PV imagery [33]. Therefore, we propose a new SAM-based PIE method (SAM-PIE) with the sole aim of enhancing the inspection and analysis of PV image segmentation models, and giving different perspective to the potential value of SAM in PV image analysis.

Under moderate prompts, the stability scores and masks generated by SAM are essential resource for PV image segmentation and analysis. An important factor that distinguished SAM-PIE from the traditional IE methods is the low-level in which the traditional IE methods frequently work, which is below the high-level requirement for reconstructing and recovering an original image [5], which is what SAM-PIE aims to achieve. This feat by SAM-PIE was attained by increasing semantic structures from SAM. Our proposed image enhancement method, SAM-PIE is easy to adapt to SAM, ensuring its applicability in solving anomalies in solar cells of PV modules by PV experts. In this paper, two classification models, ResNet50 [34] and Convolutional Neural Networks (CNNs), popular for their applications in PV image segmentation tasks were selected for the evaluation of SAM-PIE. One thousand PV module datasets [35], a Mendeley data comprising Hotspots (350 thermal generated images), Cracks (350 thermal generated images) and Shadings (300 thermal generated images) were used in performing the image segmentation experiments.

Research reveals that prior maps generated from effect of adding together the original and SAM's generated images can be employed for network inputs enhancement and thus improving the efficiency and performance of downstream models developed for segmenting PV images. This revelation motivated us to embark upon proposing SAM-PIE by applying the SAM's generated stability scores and masks. The regions of thermal anomalies in the original image can be spotted by the enhanced images, thereby providing the attention maps for the classification models for an enhanced classification of PV images. The techniques in the proposed SAM-PIE enable its effectiveness in inspection and analysis of thermal anomalies in solar cells of PV modules. The work carried out in this paper is a step towards automated inspection and analysis of thermal anomalies in solar cells of PV modules. The unique contributions of the proposed SAM-PIE method are as follows:

- Images of PV modules were originally collected, processed into datasets and publicly and freely available for scientific community use at https://doi.org/10.17632/5ssmfpgrpc.1
- Using drone (DJI Mavic 3 Thermal) for data collection addresses limitations in prior works that focused on collecting static images of PV modules. Moreover, this approach solves data limitations that could negatively influence the performance and accuracy of the proposed SAM-PIE.
- Integration of a novel PIE model into an existing SAM model to generate enhanced images for accurate classification of the thermal anomalies in solar cells of PV modules.

The rest of the paper's contents is as follows: Section II presents the related work. Section III presents the materials and methods. Section IV presents the experiments. Section V presents the results and discussions. Section VI concludes the study.

II. Related Work

Kirillov et al. [1] proposed a model called SAM model for the segmentation of any objects in an image. The model displayed great efficiency in fundamental instance segmentation task. Rafaeli et al. [2] applied SAM model 2 for a prompt-based segmentation at multiple resolutions and lighting conditions. Wang et al. [3] proposed an image enhancement based on SAM model that facilitates diagnosis of medical images. Lüddecke and Ecker [4] proposed in their work, a method based on text and image prompts for segmenting images. Mazurowski et al. [5] in their work, proposed an experimental study for analyzing medical images using SAM

model. Wang et al. [6] proposed a SAM model for scaling-up segmentation dataset of remote sensing. Feldman and Margolis [7] presented a report that contained update on industrial production and consumption of solar energy. Huang et al. [8], by considering dust impact, proposed a method for diagnosing PV faults based on a designed hybrid artificial bee colony algorithm and semi-supervised extreme learning machine. Cubukcu and Akanalci [9] proposed an inspection and determination methods in real-time of PV power systems faults by thermal imaging. Tsanakas et al. [10] proposed an advanced installation inspection method of PV by aerial triangulation and terrestrial georeferencing of thermal/visual imagery. Herraiz et al. [11] proposed thermal images analysis through structure based on CNNs for PV plant condition monitoring. Cheng et al. [12] employed self-adaptive chaos particle swarm optimization algorithm for the extraction of solar cell model parameters. Yang et al. [13] proposed a perfectly consistent and coherent transition from classification to segmentation using a novel SAM-based weakly-supervised method with a case study in latent PV locations segmentation. Pei and Hao [14] used voltage and current observation and evaluation method in their proposed PV systems to detect a fault. Georgijevic et al. [15] employed arc current entropy for detecting series arc fault in PV systems. Zhao et al. [16] presented a fault analysis method and protection challenges for solar PV arrays based on line-line fault analysis. Hariharan et al [17] proposed a method for detecting in PV systems, partial shading and other faults in PV array. Pillai and Rajasekar [18] proposed a sensorless line-line and line-ground technique based on MPPT for detecting faults for PV systems. Kurukuru et al. [19] proposed a novel approach for PV systems designed for fault classification. Chine et al. [20] proposed a novel method for diagnosing fault for PV systems based on artificial neural networks (ANNs). Hussain et al. [21] proposed a method integrating two bi-directional input parameters driven by ANN for detecting PV fault. Vieira et al. [22] proposed a method for detecting faults in PV systems by comparing multilayer perceptron and probabilistic neural network. Yuan et al. [23] conducted a survey on ANN for solar PV systems fault diagnosis. Hichri et al. [24] applied genetic-algorithm-based neural network to grid-connected PV systems for fault detection and diagnosis. Zhu et al. [25] proposed an approach based on unsupervised sample clustering and probabilistic neural network model for diagnosing fault for PV arrays. Eskandari et al. [26] proposed an autonomous fault diagnosis method based on weighted ensemble learning for PV systems using genetic algorithm. Wang et al. [27] proposed a support vector machine method for diagnosing PV array fault. Ravi et al. [28] proposed a Sam 2, a SAM model for segmenting anything in images and videos. Bommasani et al. [29] presented a work on the advantages and disadvantages of foundation models. Badr et al. [30] proposed a machine learning classifiers for identifying PV array fault. Lu et al. [31] proposed a CNN and electrical time series graph for diagnosing PV array fault. Liu et al. [32] proposed an approach based on stacked auto-encoder and clustering with IV curves for diagnosing PV array fault. Mellit [33] proposed a method based on thermographic images and deep CNNs as embedded solution for detecting and diagnosing PV module fault. He et al. [34] proposed a deep residual learning method for recognizing images. Bello et al. [35] proposed a PVMD dataset for automated detection and analysis of fault in large PV systems using PV module fault detection.

III. Materials and Methods

A. Data Collection and Description

The main hardware materials employed in this study comprise the hardware components for collecting and processing the data used in performing the experiment in this study. The materials are: (1) DJI Mavic 3 Thermal which is a state-of-the-art drone specifically designed for thermal imaging and inspection tasks, (2) Solar panels, (3) PV modules which include two panels of Jinko JKM200M-72 modules, each producing 200 W, (4) Inverter, (5) Storage battery, (6) DC Load, and (7) Solar charge controller. Table I shows the PVMD Dataset with the number of images in each anomaly category.

Popular PV image classification models, ResNet50 and CNNs were employed in carrying out the experiments of this study with one thousand PV module datasets [35], a Mendeley data comprising Hotspots (350 thermal generated images), Cracks (350 thermal generated images) and Shadings (300 thermal generated images). Afterward, we partitioned the dataset into training dataset (80%) and testing dataset (20%) to ease model evaluation. The images were pre-processed to standard size dimensions, and normalization techniques were applied for dataset consistency.

Additionally, the RGB images which were originally of different dimensions due to unfriendly and unstable environmental conditions were trimmed to size 512x512x3 (3 keeps the color information) and augmented using augmentation techniques such as geometric transformation, color-based transformations, illumination transformation, noise injection, etc., for dataset robustness.

Fig. 1 shows the framework of PV image classification with SAM-enabled PV-module image enhancement (SAM-PIE). The Fig. 1 shows the step-by-step process comparing the PV image classification output with SAM-PIE and without SAM-PIE.

TABLE I. PVMD Dataset with the Number of Images in Each Anomaly Category [35]

Thermal Anomaly of PV Module	Number of images
Hotspots	350
Cracks	350
Shadings	300
Total	**1000**

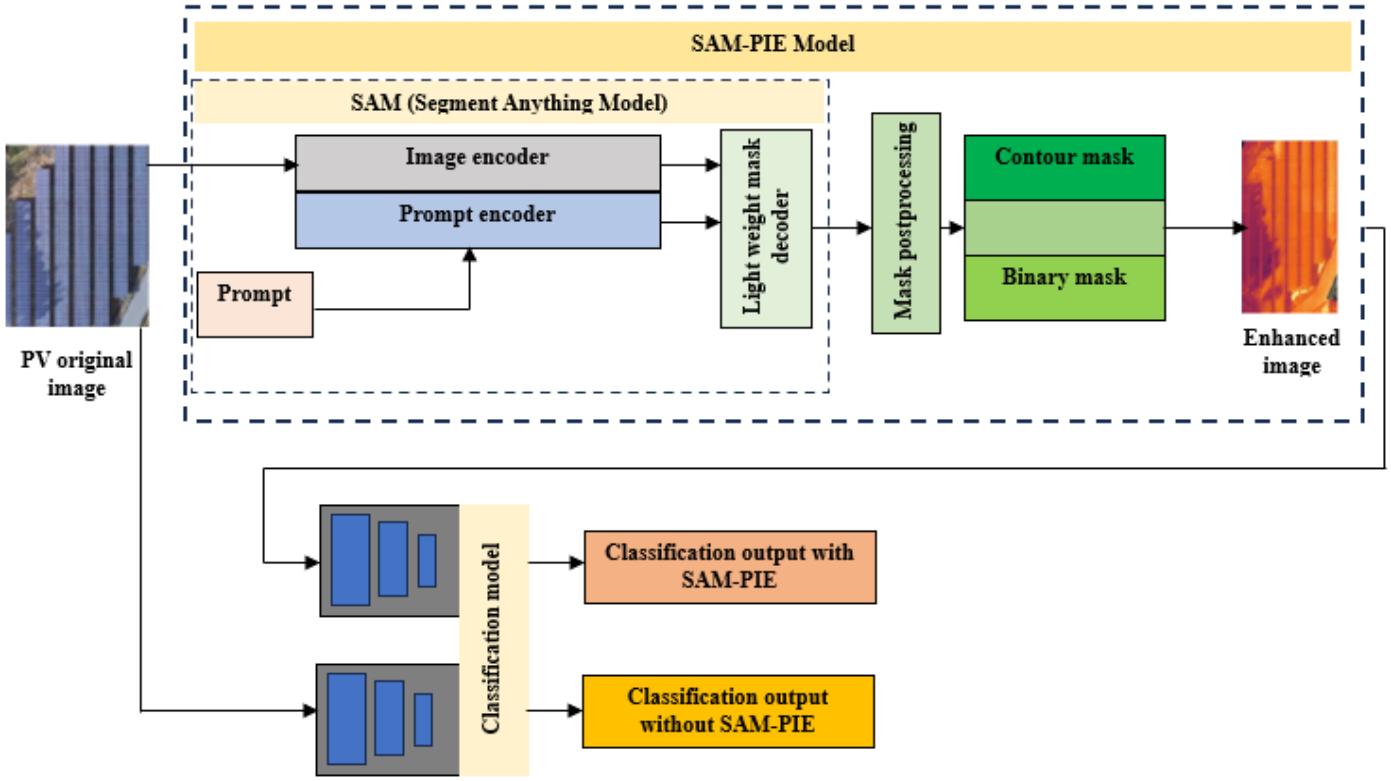


Fig. 1. The proposed framework of PV image classification with SAM-enabled PV-module image enhancement (SAM-PIE).

B. Image Processing Methods

The foundation of this study lies in the utilization of image processing techniques to detect and analyze faults in large PV systems. High-resolution images of PV panels are captured using drones equipped with advanced imaging sensors. These images undergo a series of preprocessing steps, including noise reduction, contrast enhancement, and normalization, to prepare the data for further analysis. The primary method for fault detection is based on the identification of anomalies such as cracks, hotspots, and shadings effects within the images. CV classification models, including ResNet50 and CNNs are employed to highlight these anomalies. Specifically, SAM-PIE method is used to improve the visibility of potential faults.

PV image segmentation method of SAM-PIE is applied to isolate areas of interest, facilitating targeted analysis. Once the segmentation is complete, each segment is analyzed using pattern recognition and classification algorithms to determine the presence and type of fault. The system is designed to operate unsupervised, utilizing machine learning models trained on a diverse dataset of labeled fault types. This approach allows for the automatic classification of detected faults without the need for manual intervention, significantly reducing the time and effort required for maintenance. Fig. 2 shows the hardware components used in developing the system.

C. Video Processing Methods

In addition to image processing, video processing is implemented to provide a comprehensive overview of the PV system's health. Drones equipped with video cameras capture continuous footage of the solar panels, which is then processed frame-by-frame to detect dynamic changes and faults that may not be visible in still images. The video processing workflow begins with the extraction of key frames from the video feed, focusing on frames that show significant changes or potential faults. These key frames are processed using similar techniques used in image processing. However, video processing also allows for the analysis of temporal changes, such as the progression of hotspots or the spread of shadings over time. To enhance the fault detection process, motion detection and tracking algorithms are used to follow up anomalies across multiple frames. This enables the system to monitor the development of faults and assess their impact on the overall performance of the PV system.

The combination of image and video processing ensures a more robust and reliable fault detection mechanism, capable of adapting to varying environmental conditions and operational challenges. As illustrated in Fig. 2, the deployment of a DJI Mavic 3 drone, equipped with a thermal camera, captures the detailed images and videos of a solar PV array. The drone flies over the solar installation, systematically collecting visual data that reveals the thermal characteristics of the PV panels. This data is then transferred to a computer where a specialized application (proposed in this paper) processes the images and videos. The processing involves analyzing the thermal data to detect anomalies such as hotspots, cracks, and shadings issues, which are indicative of faults in the solar panels. This method provides a comprehensive and efficient approach to monitoring and maintaining large PV systems. The drone is equipped with a thermal camera to record the condition of the solar panels.

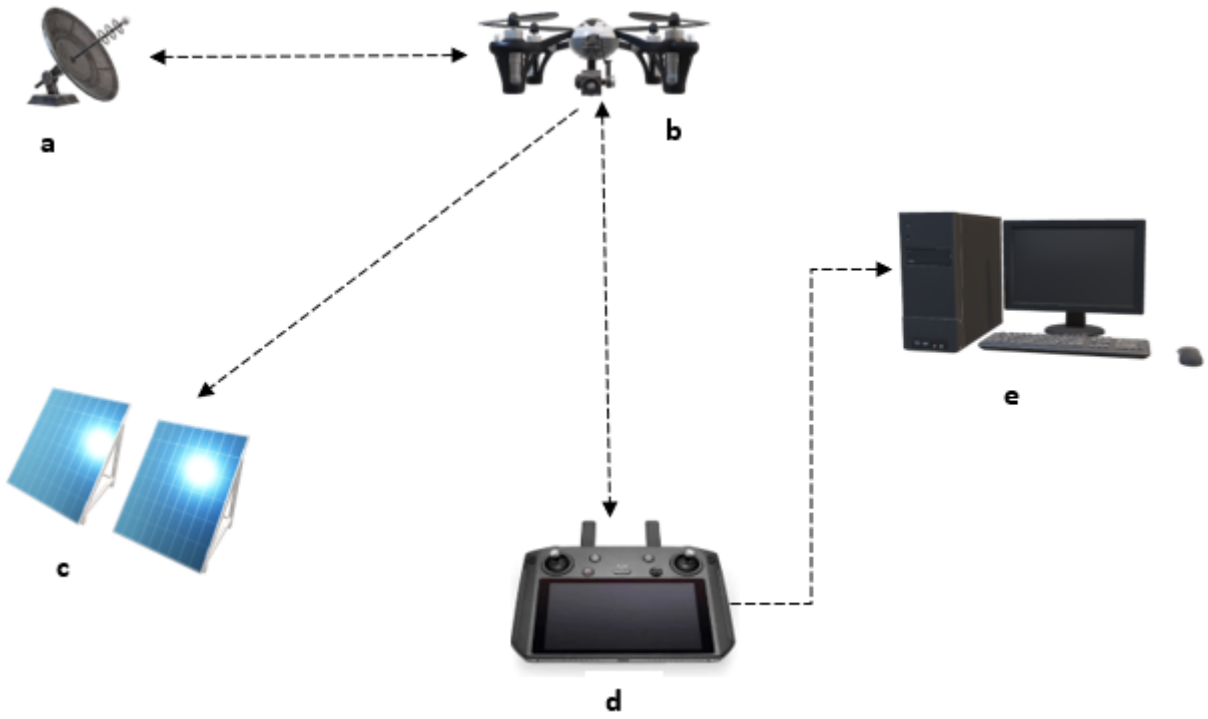


Fig. 2. System description showing the hardware components for (a) Satellite, (b) DJI Mavic 3 Thermal drone, (c) PV, (d) Remote control, (e) Computer system.

The drone captures thermal images and videos of the PV array, collecting comprehensive data on the surface temperature and potential anomalies across the solar panels. After capturing the necessary data, the drone transmits the thermal images and videos to a computer for further processing and analysis. The transferred data undergoes preprocessing, which includes steps like noise reduction and normalization to enhance the quality and clarity of the images and videos, making them suitable for analysis. Machine vision algorithms (proposed in this paper) are applied to the preprocessed data to detect any anomalies, such as hotspots, cracks, or shadings that might indicate faults in the PV panels.

D. Image Enhancement and Classification Models

Applying the pre-trained SAM enables the segmentation masks generation for PV images, and the segmentation masks (including stability scores) can be generated by SAM for the whole regions in a PV image with no antecedent prompts; binary mask and contour mask are also generated, this is followed by a procedure performed to generate enhanced images as evident in Fig. 1 and Fig. 3. Two types of segmentation tasks are involved when segmenting PV images; the foreground (that contains region of object) and the background. Given the following set as the original training dataset $\{(p_1, q_1), (p_2, q_2), (p_3, q_3), \ldots, (p_n, q_n)\}$, where the classification label of the PV image p_i is denoted as $p_i \in \mathbb{R}^{w \times h \times 3}$, $q_1 \in \{0, 1\}$. By the application of SAM-PIE method to each image of PV in the training set, the following set is generated as a new enhanced training dataset: $\{(p_1^{PIE}, q_1), (p_2^{PIE}, q_2), (p_3^{PIE}, q_3), \ldots, (p_n^{PIE}, q_n)\}$, where $p_i^{PIE} \in \mathbb{R}^{w \times h \times 3}$ is the enhanced image p_i of PV. ResNet50 and CNNs (denoted as M) were applied in order to learn from training sets that were not enhanced by SAM-PIE; optimization of the parameters of M is as follows:

$$\sum_{i=1}^{n} loss(M(p_i), q_i) \quad (1)$$

In essence, to minimize the target based on M parameters is the new learning objective:

$$\sum_{i=1}^{n} \alpha loss(M(p_i), q_i) + \theta loss(M(p_i^{PIE}), q_i) \quad (2)$$

Where α and θ put under check the training loss value for original and enhanced images; Eq. (2) would be simplified to Eq. (1) when α=1 and θ=0. However, in this paper, both α and θ take the same number 1, in order to assign equal weight to both original and enhan ced images. Cross-entropy loss was employed for the construction of loss function (expressed in Eq. (1) and Eq. (2)). Eq. (3) is used for testing the model as follows:

$$q = f\left(M(p)\right) \quad (3)$$

where f the sigmoid output activation function.

IV. EXPERIMENTS

A. Implementation Details and Evaluation Metrics

The main software materials employed to process the images and the videos are: (1) Python 3.x on a Windows 11 Home, along with libraries such as Flask, OpenCV, NumPy, Matplotlib, Google Colab and GPU for training the model, (2) CV classification models, including ResNet50 and CNNs. The initial learning rate of 0.01 was set for ResNet50, with batch size fixed at 70; the initial learning rate of 0.001 was set for CNNs, with batch size fixed at 40. The classification experiment was conducted on all the original datasets and the performance compared with the performance of the classification experiment conducted on SAM-PIE enhanced datasets.

In this paper, the performance of the proposed method was evaluated using the evaluation metrics in terms of Precision, Average Precision (AP), and Recall. Precision is denoted by Eq. (4), Recall is denoted by Eq. (5), AP is denoted by Eq. (6), IOU, which stands for Intersection Over Union is denoted by Eq. (7). The analysis stage involves evaluating the detected faults, determining their types, and pinpointing their exact locations on the solar panels. The results of the analysis would be compiled into a comprehensive report. This report not only includes the identified faults and their locations but also suggests potential maintenance actions to address the detected issues.

$$P = \frac{True\ positive}{True\ positive + False\ positive} \quad (4)$$

$$R = \frac{True\ positive}{True\ positive + False\ negative} \quad (5)$$

$$AP = \sum_{n=1}^{N} [R(n) - R(n-1)].maxP(n) \quad (6)$$

Where, N is the number for PR points calculate

$$IOU = \frac{A \cap B}{A\ U\ B} \times 100 \quad (7)$$

Where, f is the sigmoid output activation function.

V. Results and Discussions

A. Results

This study achieved the image enhancement solution for PV thermal Hotspots, PV thermal Shadings, and PV thermal Cracks datasets with the aid of SAM-PIE; this is shown in Fig. 3, which depicts the original images and the enhanced images by SAM-PIE (the processed contour and binary masks resulted in enhanced images).

The performance of the classification experiment conducted on all the original datasets was compared with the performance of the classification experiment conducted on SAM-PIE enhanced datasets. Table II shows the results of the classification task on three datasets, namely Hotspots, Cracks, and Shadings.

The results obtained in this study support SAM performance as a fundamental model that has produced significant achievements in natural image segmentation tasks, even with more better results if well guided for prompt-able segmentation. SAM's performance in segmentation tasks involving PV images is below par with the best due to the dissimilarity between images of solar cells of PV modules and natural images. The performance of SAM's application in PV image segmentation tasks remains a topic of public interest. Fig. 4 shows the graphical results of ResNet50 and CNNs classification models on original Hotspot thermal anomaly dataset and SAM-PIE enhanced Hotspot thermal anomaly dataset. The metrics measure the classification accuracy of the ResNet50 and CNNs classification models on original Hotspot thermal anomaly dataset and SAM-PIE enhanced Hotspot thermal anomaly dataset.

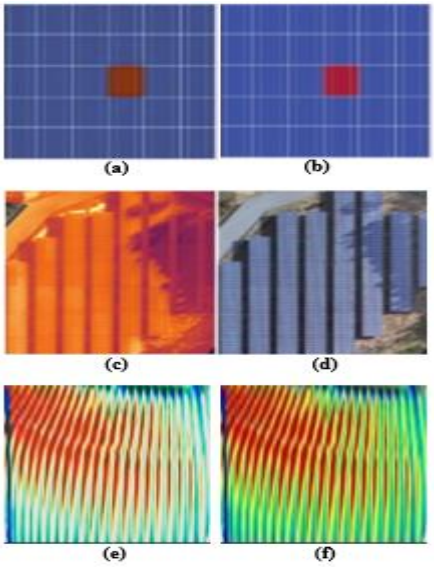


Fig. 3. Image segmentation showing (a) raw image of thermal Hotspot, (b) SAM-PIE enhanced image of thermal Hotspot, (c) raw image of thermal Shading, (d) SAM-PIE enhanced image of thermal Shading, (e) raw image of thermal Crack, (f) SAM-PIE enhanced image of thermal Crack.

TABLE II. The Results of ResNet50 and CNNs Classification Models on Original Three Thermal Anomaly Datasets (Hotspots, Cracks, and Shadings) and SAM-PIE Enhanced Three Thermal Anomaly Datasets (Hotspots, Cracks, and Shadings)

Dataset	Model	AUC	Accuracy	Precision	Recall	F1 score
Hotspot	CNNs	0.906	0.778	0.756	0.900	0.828
	ResNet50	0.958	0.889	0.789	0.915	0.852
	CNNs with SAM-PIE	0.964	0.878	0.766	0.910	0.838
	ResNet50 with SAM-PIE	0.966	0.891	0.847	0.955	0.901
Crack	CNNs	0.899	0.776	0.750	0.888	0.826
	ResNet50	0.950	0.879	0.788	0.910	0.848
	CNNs with SAM-PIE	0.962	0.878	0.764	0.905	0.834
	ResNet50 with SAM-PIE	0.964	0.895	0.795	0.945	0.870
Shading	CNNs	0.850	0.766	0.735	0.824	0.826
	ResNet50	0.940	0.877	0.768	0.915	0.848
	CNNs with SAM-PIE	0.955	0.855	0.765	0.895	0.830
	ResNet50 with SAM-PIE	0.955	0.890	0.785	0.935	0.860

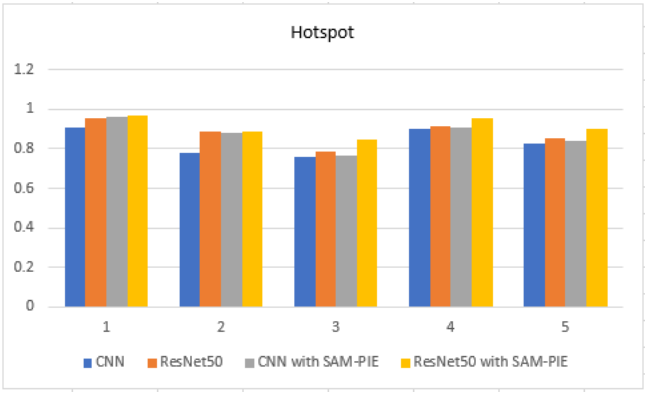


Fig. 4. Graphical results of ResNet50 and CNNs classification models on original Hotspot thermal anomaly dataset and SAM-PIE enhanced Hotspot thermal anomaly dataset.

The solar cells of PV modules are not among the natural images covered in SAM datasets, making it difficult for SAM to be applied to the PV image segmentation task, however, the experimental evidence shows that the performance of SAM, although may not be excellent on solar cells image segmentation, it could perform excellently well on region of thermal anomaly (region of interest) in an image by adjusting the confidence level of the region segmented. In PV fault diagnosis, whether during installation, repair or maintenance, the anomalies occurrence in solar cells of the PV modules are often traced to changes in their morphologies and other components due to environmental factors, making it worthy to apply SAM for the extraction of those regions of interest in this paper. Fig. 5 shows the graphical results of ResNet50 and CNNs classification models on original Crack thermal anomaly dataset and SAM-PIE enhanced Crack thermal anomaly dataset. The metrics measure the classification accuracy of the ResNet50 and CNNs classification models on original Crack thermal anomaly dataset and SAM-PIE enhanced Crack thermal anomaly dataset.

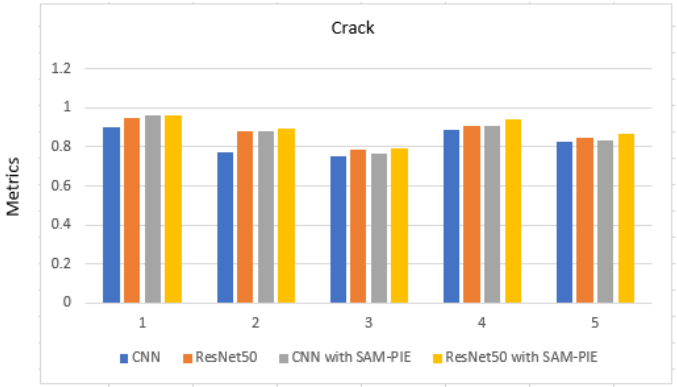


Fig. 5. Graphical results of ResNet50 and CNNs classification models on original Crack thermal anomaly dataset and SAM-PIE enhanced Crack thermal anomaly dataset.

According to Table II, the classification results obtained by ResNet50 and CNNs classification models with SAM-PIE enhanced images in AUC, Accuracy, Precision, Recall, and F1 score were higher than the results obtained by ResNet50 and CNNs classification models without SAM-PIE enhanced images. Moreover, according to Fig. 3, SAM-PIE performed excellently well on image enhancement of raw images of thermal Hotspot, thermal Shading, and thermal Crack as presented in Fig. 3 (a) to Fig. 3 (f).

These results were influenced by the characteristics of individual thermal anomalies. Although SAM-PIE produced promising results, it faced some performance challenges and compromise in enhancing some regions of interest on the image due to unrevealed external information in the image. Fig. 6 shows the graphical results of ResNet50 and CNNs classification models on original Shading thermal anomaly dataset and SAM-PIE enhanced Shading thermal anomaly dataset. The metrics measure the classification accuracy of the ResNet50 and CNNs classification models on original Shading thermal anomaly dataset and SAM-PIE enhanced Shading thermal anomaly dataset.

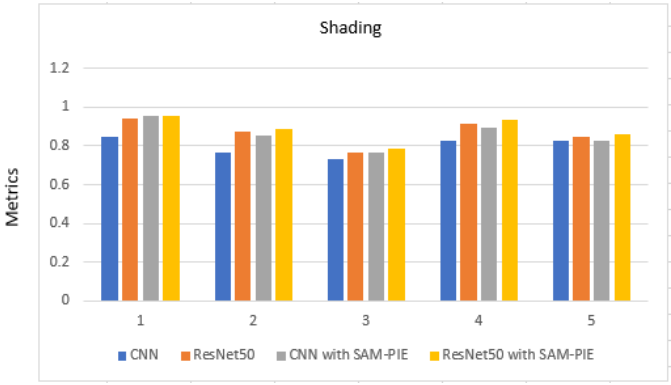


Fig. 6. Graphical results of ResNet50 and CNNs classification models on original Hotspot Graphical results of ResNet50 and CNNs classification models on original Shading thermal anomaly dataset and SAM-PIE enhanced Shading thermal anomaly dataset.

B. Discussions

Table II shows the results of ResNet50 and CNNs classification models on original three thermal anomaly datasets (hotspots, cracks, and shadings) and SAM-PIE enhanced three thermal anomaly datasets (hotspots, cracks, and shadings). These results were compared with similar previous work. The findings from the result obtained in Huang et al. [8] validate the effectiveness of SAM-PIE proposed in this study for diagnosing PV faults. The thermal imaging applied in Cubukcu and Akanalci [9] produced results that also validate the results generated by the drone used in this study to inspect and determine PV power systems faults in real-time. The advanced installation inspection method employed in Tsanakas et al. [10] for PV systems produced results that are on a par with the results produced in Herraiz et al. [11], who applied thermal images analysis through structure based on CNNs for PV plant condition monitoring. However, the performance of the thermal images applied in [10] and [11] was less accurate than the performance obtained in this study for anomaly classification of hotspots, cracks and shadings. The application of the proposed SAM-PIE in this study performed better than the method applied in Cheng et al. [12] for the extraction of solar cell model parameters. The novel SAM-based weakly-supervised method applied in Yang et al. [13], though showed promising results, however, their approach in transiting from classification to segmentation of latent PV locations

segmentation did not extensively cover the thermal anomalies studied in this work. Moreover, the SAM model on which their experiment was based does not have the prompts capability for panoptic and semantic segmentation implementation. The voltage and current observation and evaluation method used in Pei and Hao [14] to detect a fault in PV systems had limitations in its application to hotspots, cracks, and shadings thermal anomalies detection. The results obtained in Georgijevic et al. [15] were on a par with the results obtained in Zhao et al. [16] for detecting fault in PV systems. Their results were in contrast to the results obtained in this study and this is due to the difference in method employed and problem addressed. The problem addressed and the results obtained in Hariharan et al [17] were similar to the problem and results obtained in this study except for the methods. In this study, we addressed and detected full shadings in PV systems, however, partial shading was addressed in [17]. The sensorless line-line and line-ground technique based on MPPT used in Pillai and Rajasekar [18] could not give accurate account of the three anomalies addressed in this study, which are the main challenges faced by PV systems. The method applied in this study are similar to the method employed in Chine et al. [20], Hussain et al. [21], Vieira et al. [22], and Yuan et al. [23] with promising results obtained. The method, CNN and electrical time series graph, used in Lu et al. [31] for diagnosing PV array fault was partially similar to the method used in this study except for the electrical time series graph. However, the classification results of the diagnosed PV array fault were not as accurate as the results obtained in this study. An important factor that distinguished SAM-PIE from the traditional IE methods is the low-level in which the traditional IE methods frequently work, which is below the high-level requirement for reconstructing and recovering an original image [5], which is what SAM-PIE achieved in this study.

VI. Conclusion

SAM-enabled photovoltaic-module image enhancement (SAM-PIE) for fault inspection and analysis using ResNet50 and CNNs has been proposed in this paper. The results from the classification experiments were obtained from three different publicly available thermal anomaly datasets of PV modules, which also validate SAM-PIE efficiency and performance in image enhancement for PV image classification tasks by classification models.

However, SAM-PIE faces some performance challenges and compromise in enhancing some regions of interest on the image due to unrevealed external information in the image. To improve on SAM-PIE limitations for PV image classification, it is part of our future work to employ more practicable tactics such as integrating SAM-PIE into more different PV image classification models or related tasks, for instance.

References

[1] A. Kirillov, E. Mintun, N. Ravi, H. Mao, C. Rolland, L. Gustafson, ... and R. Girshick, "Segment anything," In Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 4015-4026, 2023.

[2] O. Rafaeli, T. Svoray, and A. Nahlieli, "Prompt-Based segmentation at multiple resolutions and lighting conditions using segment anything model 2," arXiv preprint arXiv:2408.06970, 2024.

[3] C. Wang, H. Chen, X. Zhou, M. Wang, and Q. Zhang, "SAM-IE: SAM-based image enhancement for facilitating medical image diagnosis with segmentation foundation model," Expert Systems with Applications, pp. vol. 249, pp. 123795, 2024.

[4] T. Lüddecke, and A. Ecker, "Image segmentation using text and image prompts," In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 7086-7096, 2022.

[5] M. A. Mazurowski, H. Dong, H. Gu, J. Yang, N. Konz, and Y. Zhang, "Segment anything model for medical image analysis: an experimental study," Medical Image Analysis, vol. 89, pp. 102918, 2023.

[6] D. Wang, J. Zhang, B. Du, M. Xu, L. Liu, D. Tao, and L. Zhang, "Samrs: Scaling-up remote sensing segmentation dataset with segment anything model," Advances in Neural Information Processing Systems, vol. 36, 2024.

[7] D. J. Feldman, and R. M. Margolis, "Q4 2018/Q1 2019 Solar industry update [Slides] (No. NREL/PR-6A20-73992)," National Renewable Energy Laboratory (NREL), Golden, CO (United States), 2019.

[8] J. M. Huang, R. J. Wai, and G. J. Yang, "Design of hybrid artificial bee colony algorithm and semi-supervised extreme learning machine for PV fault diagnoses by considering dust impact," IEEE Transactions on Power Electronics, vol. 35, No. 7, pp. 7086-7099, 2019.

[9] M. E. T. E. Cubukcu, and A. Akanalci, "Real-time inspection and determination methods of faults on photovoltaic power systems by thermal imaging in Turkey," Renewable Energy, vol. 147, pp. 1231-1238, 2020.

[10] J. A. Tsanakas, L. D. Ha, and F. Al Shakarchi, "Advanced inspection of photovoltaic installations by aerial triangulation and terrestrial georeferencing of thermal/visual imagery," Renewable Energy, vol. 102, pp. 224-233, 2017.

[11] A. H. Herraiz, A. P. Marugán, and F. P. G. Márquez, "Photovoltaic plant condition monitoring using thermal images analysis by convolutional neural network-based structure," Renewable Energy, vol. 153, pp. 334-348, 2020.

[12] Z. Cheng, M. N. Dong, T. K. Yang, and L. J. Han, "Extraction of solar cell model parameters based on self-adaptive chaos particle swarm optimization algorithm," Transactions of China Electrotechnical Society, vol. 29, No. 9, pp. 245-252, 2014.

[13] R. Yang, G. He, R. Yin, G. Wang, Z. Zhang, T. Long, ... and J. Wang, "A novel weakly-supervised method based on the segment anything model for seamless transition from classification to segmentation: A case study in segmenting latent photovoltaic locations," International Journal of Applied Earth Observation and Geoinformation, vol. 130, pp. 103929, 2024.

[14] T. Pei, and X. Hao, "A fault detection method for photovoltaic systems based on voltage and current observation and evaluation," Energies, vol. 12, No. 9, pp. 1712, 2019.

[15] N. L. Georgijevic, M. V. Jankovic, S. Srdic, and Z. Radakovic, "The detection of series arc fault in photovoltaic systems based on the arc current entropy," IEEE Transactions on Power Electronics, vol. 31, No. 8, pp. 5917-5930, 2015.

[16] Y. Zhao, J. F. De Palma, J. Mosesian, R. Lyons, and B. Lehman, "Line–line fault analysis and protection challenges in solar photovoltaic arrays," IEEE transactions on Industrial Electronics, vol. 60, No. 9, pp. 3784-3795, 2012.

[17] R. Hariharan, M. Chakkarapani, G. S. Ilango, and C. Nagamani, "A method to detect photovoltaic array faults and partial shading in PV systems," IEEE Journal of Photovoltaics, vol. 6, No. 5, pp. 1278-1285, 2016.

[18] D. S. Pillai, and N. Rajasekar, "An MPPT-based sensorless line–line and line–ground fault detection technique for PV systems," IEEE Transactions on Power Electronics, vol. 34, No. 9, pp. 8646-8659, 2018.

[19] V. S. B. Kurukuru, F. Blaabjerg, M. A. Khan, and A. Haque, "A novel fault classification approach for photovoltaic systems," Energies, vol. 13 No. 2, pp. 308, 2020.

[20] W. Chine, A. Mellit, V. Lughi, A. Malek, G. Sulligoi, and A. M. Pavan, "A novel fault diagnosis technique for photovoltaic systems based on artificial neural networks," Renewable Energy, vol. 90, pp. 501-512, 2016.

[21] M. Hussain, M. Dhimish, S. Titarenko, and P. Mather, "Artificial neural network based photovoltaic fault detection algorithm integrating two bi-

directional input parameters," Renewable Energy, vol. 155, pp. 1272-1292, 2020.

[22] R. G. Vieira, M. Dhimish, F. M. U. de Araújo, and M. I. da Silva Guerra, "Comparing multilayer perceptron and probabilistic neural network for PV systems fault detection," Expert Systems with Applications, vol. 201, pp. 117248, 2022.

[23] Z. Yuan, G. Xiong, and X. Fu, "Artificial neural network for fault diagnosis of solar photovoltaic systems: a survey," Energies, vol. 15, No. 22, pp. 8693, 2022.

[24] A. Hichri, M. Hajji, M. Mansouri, K. Abodayeh, K. Bouzrara, H. Nounou, and M. Nounou, "Genetic-algorithm-based neural network for fault detection and diagnosis: Application to grid-connected photovoltaic systems," Sustainability, vol. 14 No. 17, pp. 10518, 2022.

[25] H. Zhu, L. Lu, J. Yao, S. Dai, and Y. Hu, "Fault diagnosis approach for photovoltaic arrays based on unsupervised sample clustering and probabilistic neural network model," Solar Energy, vol. 176, pp. 395-405, 2018.

[26] A. Eskandari, M. Aghaei, J. Milimonfared, and A. Nedaei, "A weighted ensemble learning-based autonomous fault diagnosis method for photovoltaic systems using genetic algorithm," International Journal of Electrical Power & Energy Systems, vol. 144, pp. 108591, 2023.

[27] J. Wang, D. Gao, S. Zhu, S. Wang, and H. Liu, "Fault diagnosis method of photovoltaic array based on support vector machine," Energy sources, part a: recovery, utilization, and environmental effects, vol. 45 No. 2, pp. 5380-5395, 2023.

[28] N. Ravi, V. Gabeur, Y. T. Hu, R. Hu, C. Ryali, T. Ma, ... and C. Feichtenhofer, "Sam 2: Segment anything in images and videos," arXiv preprint arXiv:2408.00714, 2024.

[29] R. Bommasani, D. A. Hudson, E. Adeli, R. Altman, S. Arora, S. von Arx, ... and P. Liang, "On the opportunities and risks of foundation models," arXiv preprint arXiv:2108.07258, 2021.

[30] M. M. Badr, M. S. Hamad, A. S. Abdel-Khalik, R. A. Hamdy, S. Ahmed, and E. Hamdan, "Fault identification of photovoltaic array based on machine learning classifiers," IEEE Access, vol. 9, pp. 159113-159132, 2021.

[31] X. Lu, P. Lin, S. Cheng, Y. Lin, Z. Chen, L. Wu, and Q. Zheng, "Fault diagnosis for photovoltaic array based on convolutional neural network and electrical time series graph," Energy Conversion and Management, vol. 196, pp. 950-965, 2019.

[32] Y. Liu, K. Ding, J. Zhang, Y. Li, Z. Yang, W. Zheng, and X. Chen, "Fault diagnosis approach for photovoltaic array based on the stacked auto-encoder and clustering with IV curves," Energy Conversion and Management, vol. 245, pp. 114603, 2021.

[33] A. Mellit, "An embedded solution for fault detection and diagnosis of photovoltaic modules using thermographic images and deep convolutional neural networks," Engineering Applications of Artificial Intelligence, vol. 116, pp. 105459, 2022.

[34] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 770-778, 2016.

[35] R. W. Bello, P. A. Owolawi, E. A. Van Wyk, and C. Du, "Photovoltaic module dataset for automated fault detection and analysis in large photovoltaic systems using photovoltaic module fault detection," Mendeley Data, V1, https://doi.org/10.17632/5ssmfpgrpc.1, 2024.

Understanding Mental Health Content on Social Media and It's Effect Towards Suicidal Ideation

Mohaiminul Islam Bhuiyan, Nur Shazwani Kamarudin*, Nur Hafieza Ismail
Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, Pahang, Malaysia

***Abstract*—The study "Understanding Mental Health Content on Social Media and Its Effect Towards Suicidal Ideation" aims to detail the recognition of suicidal intent through social media, with a focus on the improvement and part of the machine learning (ML), deep learning (DL), and natural language processing (NLP). This review underscores the critical need for effective strategies to identify and support individuals with suicidal ideation, exploiting technological innovations in ML and DL to further suicide prevention efforts. The study details the application of these technologies in analyzing vast amounts of unstructured social media data to detect linguistic patterns, keywords, phrases, tones, and contextual cues associated with suicidal thoughts. It explores various ML and DL models like SVMs, CNNs, LSTM, neural networks, and their effectiveness in interpreting complex data patterns and emotional nuances within text data. The review discusses the potential of these technologies to serve as a life-saving tool by identifying at-risk individuals through their digital traces. Furthermore, it evaluates the real-world effectiveness, limitations, and ethical considerations of employing these technologies for suicide prevention, stressing the importance of responsible development and usage. The study aims to fill critical knowledge gaps by analyzing recent studies, methodologies, tools, and techniques in this field. It highlights the importance of synthesizing current literature to inform practical tools and suicide prevention efforts, guiding innovation in reliable, ethical systems for early intervention. This research synthesis evaluates the intersection of technology and mental health, advocating for the ethical and responsible application of ML, DL, and NLP to offer life-saving potential worldwide while addressing challenges like generalizability, biases, privacy, and the need for further research to ensure these technologies do not exacerbate existing inequities and harms.**

***Keywords*—Suicidal ideation detection; social media analysis; mental health; text analysis; machine learning**

I. Introduction

As digital technologies permeate and reshape society, social media has emerged as a massive window into the psychological landscape of users. Individual expressions within these platforms can serve as a mirror, presenting critical insights into the mental well-being of the global population. Although revealing various pathologies, a stark reality is reflected that demands urgent attention - suicidal ideation. This affliction continues to take an unconscionable toll, with the World Health Organization (WHO) reporting nearly 800,000 people dying by suicide annually [1]. Shockingly, it is the second leading cause of death for those aged 15-29 years [2]. Many suicides relate to mental health issues like depression, substance abuse, and psychosis. But the causes are complex. Those struggling deserve support [1]. These alarming statistics underscore the human loss and suffering that suicidal behaviors induce worldwide. Clearly, there is a pressing need to earnestly seek more effective strategies for identifying those with suicidal ideation to provide life-saving prediction, prevention and intervention.

Fortunately, advancements in Machine Learning (ML) and Deep Learning (DL) are illuminating a promising path forward, offering technological innovations that could drastically further suicide prevention efforts [3], [4]. The potential of machine learning for suicide prevention is significant, but practical application faces hurdles regarding transparency, ethics, and data quality for which further research is needed [5]. At the core is the ongoing amassment of vast digital traces as we communicate, browse, share, and express ourselves through online conduct. Analyses of resulting "big data" repositories using sophisticated analytical techniques promise to usher impactful progress in decoding and responding to human behaviors and states of mind [6]. Specifically, by applying ML and DL tools to mine social media communications, the recognition of linguistic patterns and semantic complexities associated with suicidal ideation can be realized to an unprecedented degree [7], [8]. Essential human expressions conveyed through unstructured text data can now be computationally elucidated to discern what once remained invisible. This paper aims to comprehensively review the detection of suicidal ideation on social media, focusing on the roles and advancements of machine learning (ML), deep learning (DL), and natural language processing (NLP).

Machine learning, deep learning, and natural language processing are being applied to detect signs of suicidal ideation in social media posts. These technologies can analyze large volumes of unstructured text data to identify linguistic patterns, keywords, phrases, tones, and contextual cues associated with suicidal thoughts. While traditional ML techniques like SVMs and Random Forests can learn predictive rules, they are limited in understanding nuanced semantics and emotions. However, deep learning methods like CNNs and LSTM neural networks, which model complex data patterns, show promise for interpreting broader concepts and context to represent the intricacies of human experience [9], [10], [11]. Though still imperfect, deep learning's ability to comprehend subtext and vulnerability in language offers hope for identifying cries for help and risk factors in a more meaningful way. Advanced NLP and deep learning may enable breakthroughs in computationally decoding the complexities of human expression to uncover suicidal warning signs in text.

*Corresponding Author.

Thus, while challenges and ethical quandaries persist, powerful capacities now exist to extract and analyze massive stores of social expressions for life-saving insights. If properly nurtured under responsible development and usage guidelines, AI and learning systems could gain competencies to serve the public good [12]. Though much progress is still sorely needed, thoughtfully designed mechanisms harnessing big data may move within reach to provide rich awareness of mental states, risk and distress... potentially before tragic outcomes occur [5]. With compassion and diligent effort, the possibility of channeling AI's emerging potential shouldn't be readily dismissed. Perhaps computational tools aimed toward understanding hearts and minds could reveal key markers that humans often miss in order to guide care and resources to those facing darkest moments. Lives awaits saving by transforming big data into wisdom and decisive action [13].

This comprehensive review aims to address critical knowledge gaps by thoroughly analyzing existing research on detecting suicidal ideation through social media using machine learning (ML) and deep learning (DL). It will scrutinize the specific methodologies, tools, and techniques utilized in recent studies, assessing their real-world effectiveness, limitations, and ethical considerations. The review traces the evolution of ML and DL in this application, highlighting advancements that show promise while surfacing areas needing additional exploration and development. Questions around generalizability, biases, and privacy represent just some emerging issues that require elucidation if these technologies are to progress responsibly.

Ultimately, the significance of synthesizing current literature lies not merely in its academic contribution, but also in its potential to meaningfully inform practical tools and suicide prevention efforts. By consolidating empirical insights around the capabilities and development needs of ML and DL for suicide risk detection, this review seeks to guide beneficial innovation of reliable, ethical systems. Such systems could enable early intervention, connecting vulnerable individuals with support and resources.

This research synthesis aims to navigate the intersections of technology and mental health by evaluating recent studies, distilling knowledge, and charting an informed path forward. Applied ethically and responsibly, these emerging analytical methods may offer life-saving potential across populations worldwide. But vigilance around limitations and directing further research is required to ensure applications counter, not exacerbate, existing inequities and harms. This review confronts these multifaceted issues to support deliberate, compassionate translation of scientific discoveries into societal solutions. The primary contributions of this paper are:

- Survey key computational techniques for social media-based screening of suicidal ideation.
- Evaluate the effectiveness of combining sentiment analysis with machine learning on benchmark suicide risk assessment tasks.
- Examine strengths and limitations of social media data sources like Twitter, Reddit, Facebook and various mental health forums.
- Discuss ethical implications including privacy, stigma, and duty of care when analysing social media content.
- Synthesize critical directions and opportunities for impactful research at the intersection of NLP, machine learning, mental health, and suicide prevention.

Advanced analytical methods offer capabilities to decode warnings, risks and signs of suicidal ideation expressed through digital traces. This review article will present a comprehensive analysis of the current state of the art and research trajectory in this critical domain. It will scrutinize in depth the methodologies, tools and techniques being applied to social media data. Key dimensions evaluated will encompass demonstrable performance, advantages, limitations and ethical considerations of using machine learning and AI to detect patterns of mental health distress. The overarching aim is to consolidate current knowledge regarding the promises and perils of computationally surveilling the social landscape with techniques that peer deeply into the collective psyche through the lens of big data... potentially illuminating who requires help and enabling intervention with greater acuity. What is at stake warrants continued exploration to thoughtfully harness such technology for the greatest good.

The remainder of this paper is structured as follows: Section II reviews related work on the detection of suicidal ideation from social media. Section III discusses the evolution of methodologies and details current techniques, including data handling and model applications. Finally, Section IV summarizes insights and outlines future research directions.

II. Previous Works

The detection and analysis of suicidal ideation through social media have gained increasing attention in the field of mental health research. This section provides an overview of the existing literature, outlining the evolution of methodologies and the various approaches used in the detection of suicidal ideation.

In embarking on an analysis of recent studies focused on the detection of suicidal ideation through social media using machine learning (ML), deep learning (DL) and Natural Language Processing (NLP) techniques, we delve into a domain of computational psychiatry that has shown both promising advancements and encountered significant challenges. This analysis will synthesize key findings from various research efforts, evaluating their methodologies, effectiveness, and broader implications within the public health context.

Table I represents a comparison table featuring key details from some of the previous studies on suicidal ideation detection via social media.

The growing prevalence of mental health issues, particularly suicidal ideation, and its manifestation on social media platforms, presents an urgent need for innovative monitoring and intervention strategies. Studies such as those conducted by Samer Muthana et al. [30], Arunima Roy et al. [31], and Swati Jain et al. [32], have explored the utilization of platforms like Twitter, employing techniques ranging from sentiment analysis to complex neural network architectures.

These studies highlight the potential of ML and DL in deciphering the nuanced language of distress and suicidal thoughts expressed in social media posts.

TABLE I. COMPARISON OF STUDIES ON SUICIDAL IDEATION DETECTION

Study Reference	Year	Platform	ML/DL Techniques Used	Dataset Size	Key Features Analyzed	Results (e.g., Accuracy, Precision, Recall)	Limitations
Jorge Parraga-Alva et al. [14]	2019	Various	Unsupervised learning	102 texts	Suicide message categorization	Avg rate: 79% - 87%	-small corpus -lack of multiple categories
Pratyaksh Jain et al. [15]	2022	Reddit	Naïve Bayes, SVM, Logistic Regression	60,000 data points	Depression, Suicidal behavior	Acc: 74.35% - 77.29%, F1: ~0.77	-still room for improve the predictive model
Syed Tanzeel Rabani et al. [16]	2020	Twitter	Random Forest	4,266 tweets	Suicidal ideation	Acc: 98.5%, Precision: 98.7%, Rec: 98.2%	-no direct communication or intervention
Seunghyong Ryu et al. [17]	2019	KNHANES	Random forest	5,773 subjects	Suicide ideation	AUC: 0.947, Acc: 88.9%	-One ML algorithm -SMOTE used to overcome class imbalance problem
Ning Wang et al. [18]	2021	Social media	KNN, SVM, C-Attention network	CLPsych 2021 dataset	Suicide attempts prediction	Best F1 score: 0.737 (6 months prior)	- Traditional ML methods better in some metrics
Samh J. Fodeh et al. [19]	2019	Twitter	LSA, LDA, NMF and Decision Tree and K-means Clustering	12,066 Tweets	Suicide risk factors	Precision: 0.844, Sensitivity: 0.912	-Biased Data Selection -Missing Twitter Metadata -Ignored Ground Truth
Shi Ru Lim et al. [20]	2023	Twitter	SVM, Decision Tree, Naïve bayes	16,158 Tweets	Mental health disorders prediction	Acc: SVM: 99.80% (training), 98.43% (testing)	-Larger dataset needed
Tianlin Zhag et al. [21]	2021	Online	Transformer RNN	659 samples	Suicide notes identification	94.9% recall, 94.9% F1 score, 95% precision	-Explore linguistic -psychological features
Ayaan Haque et al. [22]	2021	Reddit, IMDB large movie dataset	SDCNL, BERT, Sentence-BERT, GUSE	1,895 posts, 50,000 reviews	Depression vs suicidal ideation classification	Strong performance in classification	-Evaluate on other datasets
Yaakov Ophir et al. [23]	2020	Facebook	ANN models (STM, MTM)	83,292 posts of 1002 users	Detect suicide risk	AUC: .697 to .746 (MTM)	-practical detection tools for suicide risk
Tadesse et al. [7]	2019	Reddit	LSTM-CNN, word embedding	Posts from Suicide Watch forum	Suicidal ideation detection	Acc: 93.8% (LSTM-CNN)	-data deficiency -annotation bias
Prasadith Buddhitha et al. [24]	2019	WASSA-2017, CLPsych-2015	Deep Neural Network	-	Depression, PTSD detection	AUC: >90% (multi-channel CNN)	-insufficient unstructured data -lack of intervention
Diniz et al. [25]	2022	Twitter	ML, DL, BerTimbau Large	3788 instances	Suicidal ideation from text	Acc: 0.955, F1: 0.954	-inability to detect typos
Aldhyani et al. [26]	2022	Reddit	CNN-BiLSTM, XGBoost	232074 samples	Textual and LIWC based features from post	Acc: 95% (Textual) Acc: 84.5% (LIWC)	-variations in performance
Renjith et al. [27]	2022	Reddit	LSTM-Attention-CNN	55,680 posts	Suicidal ideation in text	Acc: 90.3%, F1 Score: 92.6%	-
Kholifah et al. [28]	2020	Twitter	LSTM Deep Learning model	-	Level of depression	Acc: 70.89%, Precision: 50.24%, Recall: 70.89%	-accuracy of the classification results can be improved
Cao et al. [29]	2022	Microblog, Reddit	Deep neural networks integrated with knowledge graph	7,329 subjects	Personal factors related to suicidal ideation	Acc: >93%	-Data lacking, noisy abundance

However, this promising avenue is not without its complexities. The critical evaluation of these studies reveals a common challenge – the balance between the technical efficacy of detection algorithms and the ethical implications of privacy and data usage. For instance, while studies like those by Pratyaksh Jain et al. [15] on Reddit and Syed Tanzeel Rabani et al. [16] on Twitter demonstrate high accuracies in detecting suicidal ideation, they also raise questions about the representativeness of their datasets and the ethical management of sensitive personal information.

Moreover, the generalizability of these models across different demographics and social media platforms remains a significant concern. Studies often use datasets that may not adequately represent the broader population, leading to potential biases in prediction models. This limitation is evident in the work of researchers like Jorge Parraga-Alva et al. [14]and Hannah Yao et al. [33], who have tried to categorize and understand the complexity of suicide-related messages across various platforms. Seunghyong Ryu et al. [17] and Tatiana Falcone et al.'s [34] studies offer unique insights into suicide ideation detection in specific contexts. Ryu et al. [17] used data from the Korea National Health & Nutrition Examination Survey to develop predictive models for identifying individuals at risk of suicide, demonstrating the use of machine learning in a clinical or community setting. Falcone et al.'s [34] research on open-source digital conversations among people with epilepsy provides an interesting perspective on how machine learning can uncover specific concerns and struggles related to suicidality in distinct patient groups.

Jianhong Luo et al. [35] and Ning Wang et al. [18] both utilized Twitter data for their research but with different focuses. Luo et al. [35] examined temporal patterns of potential suicidal ideations, using topic modeling to identify latent suicide topics, while Wang et al. [18] developed models for predicting suicide attempts based on social media posts. These studies reveal the complexity and multifaceted nature of suicidal behavior as expressed on social media, and the potential of machine learning in capturing these nuances. John Torous et al. [5] and Gen-Min Lin et al. [36] addressed the integration of technology in suicide prevention and prediction. Torous et al. discussed the potential of tools like text messaging, smartphone apps, and machine learning algorithms in suicide prevention, while Lin et al. focused on predicting suicide ideation in military personnel using various machine learning techniques. These studies illustrate the diverse applications of machine learning and technology in different contexts and populations for suicide prediction and prevention.

Xingyun Liu et al. [37], ML Tlachac et al. [38], and E. Rajesh Kumar et al. [39] explored novel approaches in suicide ideation detection. Liu et al. assessed the feasibility of a proactive suicide prevention approach on social media, while Tlachac et al. investigated the use of smartphone-based communication for passive screening of suicidal ideation. Kumar et al. focused on Twitter data to establish an early warning system for suicidal thoughts detection. These studies highlight innovative applications of machine learning in real-time and proactive detection of suicide risk.

Atika Mbarek et al. [40] and Samh J. Fodeh et al. [19] emphasized the detection of suicidal profiles and factors contributing to suicide risk on Twitter. Mbarek et al. developed a machine learning-based approach for detecting suicidal profiles, while Fodeh et al. used machine learning algorithms to identify factors related to suicide risk. These studies underscore the potential of machine learning in profiling and understanding the underlying factors of suicide risk on social media platforms. Shi Ru Lim et al. [20] and Ibrahim et al.'s [41] studies focused on the prediction of mental health disorders using machine learning techniques. Lim et al. applied various algorithms like SVM and Naive Bayes to predict mental health issues based on Twitter data, while Ibrahim et al. detected PTSD symptoms through Twitter postings. Both studies demonstrate the broader application of machine learning in mental health beyond suicide prevention.

Kamarudin et al.'s [42], [43] two studies expanded the scope of machine learning in understanding mental health challenges through social media data. Their first study employed machine learning and natural language processing to dissect data from virtual communities, while their second study focused on linguistic analysis of online mental health communities. These studies highlight the rich potential of social media data in increasing mental health awareness and informing policy decisions. Kamarudin et al. [44] conducted another study exploring the role of Reddit in providing support to individuals dealing with rape and sexual abuse. Using natural language processing, they analyzed the diversity of topics in responses, including emotional support, relationships, therapy, and legal advice. The findings highlighted the comprehensive nature of support on Reddit, differing from traditional physical-world responses. The study suggests future research involving detailed surveys to understand the perspectives of both support seekers and providers.

Farsheed Haque et al. [45] and Shini Renjith et al. [27] both employed advanced machine learning models for detecting suicidal ideation in social media posts. Haque et al. used Transformer models for text classification, while Renjith et al. developed an ensemble deep learning technique for fast and accurate detection of suicidal ideation. These studies showcase the advancements in machine learning algorithms for suicide ideation detection.

Tianlin Zhang et al. [21], Ayaan Haque et al. [22], and Yaakov Ophir et al. [23] further contributed to the field by developing specialized models and algorithms for suicide and depression classification. Zhang et al. developed a transformer-based deep learning model for identifying suicide notes online, Haque et al. proposed an unsupervised label correction method for classifying depression and suicidal ideation, and Ophir et al. also focused on distinguishing between depression and suicidal ideation using advanced word embedding models. These studies represent the cutting-edge of machine learning applications in mental health.

Michael Mesfin Tadesse et al. [7] and Ramit Sawhney et al. [8] utilized deep learning techniques for detecting suicide ideation in social media. Tadesse et al. developed an LSTM-CNN model for early detection of suicide ideation, while Sawhney et al. compared various deep learning architectures

for suicidal ideation detection. These studies reflect the ongoing evolution and refinement of machine learning techniques in the context of suicide prevention. Prasadith Buddhitha et al. [24] proposed a unique multi-task learning approach with a multi-channel CNN for detecting depression and PTSD. Their approach of incorporating emotional patterns identified by clinical practitioners demonstrates an innovative integration of clinical insights with machine learning.

These studies collectively represent a significant advancement in the use of machine learning and natural language processing techniques to detect, predict, and understand suicide ideation and mental health issues through social media platforms. The diversity in methods, from supervised and unsupervised learning to deep learning and ensemble techniques, highlights the versatility and potential of these technologies in addressing the critical issue of mental health. Moreover, the focus on different populations, languages, and social media platforms underscores the need for tailored approaches that consider the unique aspects of each context and population group. As machine learning continues to evolve, it holds immense promise for enhancing our understanding and prevention of mental health issues, particularly in the realm of suicide prevention. The analysis of these studies also underscores the importance of interdisciplinary collaboration in this field. The integration of insights from psychology, computer science, and ethical considerations is crucial for the development of reliable, effective, and ethically sound detection systems.

This critical analysis aims to provide a comprehensive overview of the current state of research in detecting suicidal ideation through social media. It will highlight the innovations and strengths of recent studies while also addressing the significant challenges and limitations that need to be overcome to harness the full potential of ML and DL in this critical area of public health.

III. Early Styles and Evolution

Initial research in the field of suicidal ideation detection was primarily focused on traditional psychological assessments and face-to-face interactions. However, the emergence of social media as a pervasive communication medium opened new avenue for mental health research. Early studies in this domain utilized basic text analysis techniques, relying on keyword searches and simple statistical methods to identify posts indicative of suicidal thoughts. These methods, though pioneering, were limited in their ability to understand the complexities of human language and context.

A. Advancement in Machine Learning (ML)

The introduction of machine learning algorithms marked a significant advancement in this field. Machine learning, particularly supervised learning techniques, began to be used to identify patterns and features in social media posts that were indicative of suicidal ideation. These approaches involved training models on annotated datasets where posts were labeled as showing signs of suicidal ideation or not. Commonly used machine learning algorithms in this context included Support Vector Machines (SVM), Decision Trees, and Naive Bayes classifiers.

One of the key challenges in applying machine learning was the need for large, annotated datasets. The creation of such datasets involved manually labeling social media posts, a process that was both time-consuming and subject to human error and bias. Despite these challenges, machine learning algorithms proved to be significantly more effective than earlier methods, as they could capture a wider range of linguistic and semantic features.

B. The Role of Natural Language Processing (NLP)

Natural language processing (NLP) emerged as a critical tool in enhancing the effectiveness of machine learning models. NLP techniques allowed for more sophisticated analysis of text data, enabling the extraction of features such as sentiment, thematic elements, and linguistic structures. The use of NLP in conjunction with machine learning algorithms led to more nuanced and accurate detection of suicidal ideation. Techniques such as tokenization, stemming, and lemmatization were employed to preprocess the data, making it more amenable for machine learning models. Sentiment analysis, a subset of NLP, was particularly useful in identifying the emotional tone of posts, which is a crucial aspect in detecting suicidal ideation.

C. The New Frontier of Deep Learning (DL)

The advent of deep learning brought about a paradigm shift in the detection of suicidal ideation on social media. Deep learning models, particularly neural networks, were capable of modeling complex patterns in large datasets. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), including their variants like Long Short-Term Memory (LSTM) networks, started being used extensively. These models excelled at understanding the contextual nuances and varied expressions of language, making them particularly effective for this task.

Deep learning models were trained on vast amounts of unstructured social media data, learning to identify subtle patterns and linguistic cues associated with suicidal ideation. These models outperformed traditional machine learning algorithms in many aspects, particularly in their ability to understand the context and semantic meaning of text. The application of deep learning, however, required substantial computational resources and large, well-annotated datasets.

D. Integration of ML, DL and NLP

The integration of machine learning, deep learning, and NLP represents the current state-of-the-art in suicidal ideation detection on social media. This integrated approach leverages the strengths of each of these technologies, offering a more robust and accurate detection mechanism. Machine learning algorithms provide the basis for pattern recognition, deep learning models add an understanding of contextual and semantic nuances, and NLP techniques enable the effective processing and analysis of textual data.

A comprehensive comparison table focusing on suicidal ideation using NLP, Machine Learning, and Deep Learning including various models, their features, performance metrics, and other relevant details is given in Table II:

TABLE II. COMPREHENSIVE COMPARISON TABLE OF NLP, ML, DL MODELS FOR SUICIDAL IDEATION DETECTION

Feature/Model	Traditional ML Models	Deep Learning Models	NLP Techniques
Model Examples	- SVM (Support Vector Machine) - Decision Trees - Random Forest	- CNN (Convolutional Neural Network) - RNN (Recurrent Neural Network) - LSTM (Long Short-Term Memory)	- Sentiment Analysis - Topic Modeling - Word Embeddings
Data Requirements	- Structured data - Limited data size	- Large datasets - Unstructured data	- Large text corpora - Contextual data
Processing Time	- Generally faster - Less computational resources	- Longer due to complexity - High computational resources	- Varies based on technique and data size
Accuracy	- Moderate (depending on the dataset)	- High (especially with large and complex datasets)	- Depends on the complexity of the language and context
Interpretability	- High (easier to understand model decisions)	- Low (often referred to as "black box" models)	- Moderate (varies with techniques)
Suitability for Short Text (e.g., Tweets)	- Less effective due to limited context	- More effective with context preservation techniques	- Effective with appropriate preprocessing
Common Challenges	- Overfitting on small datasets - Limited in capturing complex patterns	- Requires large training datasets - Overfitting risks	- Handling of sarcasm, idioms, and contextual meanings
Preprocessing Needs	- Feature selection - Data cleaning	- Data normalization - Sequence padding (for RNN, LSTM)	- Tokenization - Stop word removal - Lemmatization/Stemming
Application in Suicidal Ideation Detection	- Effective in structured, labeled data - Quick initial assessments	- High accuracy in pattern recognition - Effective in large-scale social media data analysis	- Essential for understanding linguistic nuances - Contextual sentiment analysis

E. Challenges and Ethical Considerations

Despite the advancements in technology, there are significant challenges in this field. The ethical considerations of privacy and consent are paramount. The use of social media data for mental health research raises questions about the privacy of individuals and the potential for misuse of sensitive information. Ensuring that research in this area is conducted with strict ethical guidelines is crucial.

Another challenge is the accuracy and generalizability of these models. Suicidal ideation is a complex and deeply personal phenomenon, and its expression can vary greatly among individuals. Models trained on specific datasets may not generalize well to broader populations. Additionally, the risk of false positives and false negatives in detection is a concern, as it can have serious implications for the individuals involved.

The literature in the field of suicidal ideation detection on social media using machine learning, deep learning, and NLP indicates a rapidly evolving landscape. From basic text analysis to sophisticated deep learning models, the methodologies have advanced significantly. The integration of these technologies offers promising avenues for early detection and intervention in mental health crises. However, the challenges of data privacy, ethical considerations, and the need for accurate, generalizable models remain areas that require ongoing research and attention.

F. Commonly Followed Methods

This section outlines the methodologies and techniques employed in the detection of suicidal ideation on social media, focusing on dataset collection, preprocessing, feature extraction, and the application of machine learning, deep learning, and NLP models.

Following taxonomy represents various approaches and tools used in the studies. Each method or technique is nested within its broader category, illustrating the hierarchical relationship between them:

1) Dataset collection: One of the initial steps in studying suicidal ideation using social media data is the collection of relevant datasets. This process involves selecting social media platforms (such as Twitter, Facebook, Reddit, etc.) and extracting posts that potentially indicate suicidal thoughts or behaviors. The selection criteria for these posts often involve keyword searches, using terms commonly associated with suicidal ideation.

The complexity of dataset collection is amplified by ethical considerations, such as the privacy and consent of social media users. Researchers must navigate these challenges while ensuring that the data is representative and unbiased. Additionally, the dynamic nature of social media, where content is continually created and modified, poses a challenge in creating stable and reliable datasets.

2) Preprocessing: Once the datasets are collected, the next crucial step is preprocessing. This stage involves cleaning and preparing the data for analysis, which is pivotal in NLP and machine learning applications.

3) Some Common Techniques for Suicidal Ideation Detection

a) Lexicon based emotion analysis

i) NRC Affect Intensity Lexicon: The NRC Affect Intensity Lexicon is a lexicon that provides real-valued scores of affect intensity for a large set of English words. It's an extension of the NRC Emotion Lexicon and was developed by Saif M. Mohammad, a senior research officer at the National Research Council Canada [46]. The lexicon aims to quantify the intensity of the affect (emotion) evoked by a word. Each word in the lexicon is associated with an affect intensity score for each of eight basic emotions: anger, fear, anticipation, trust, surprise, sadness, joy, and disgust. The score ranges from 0 (no association with the emotion) to 1 (strong association).

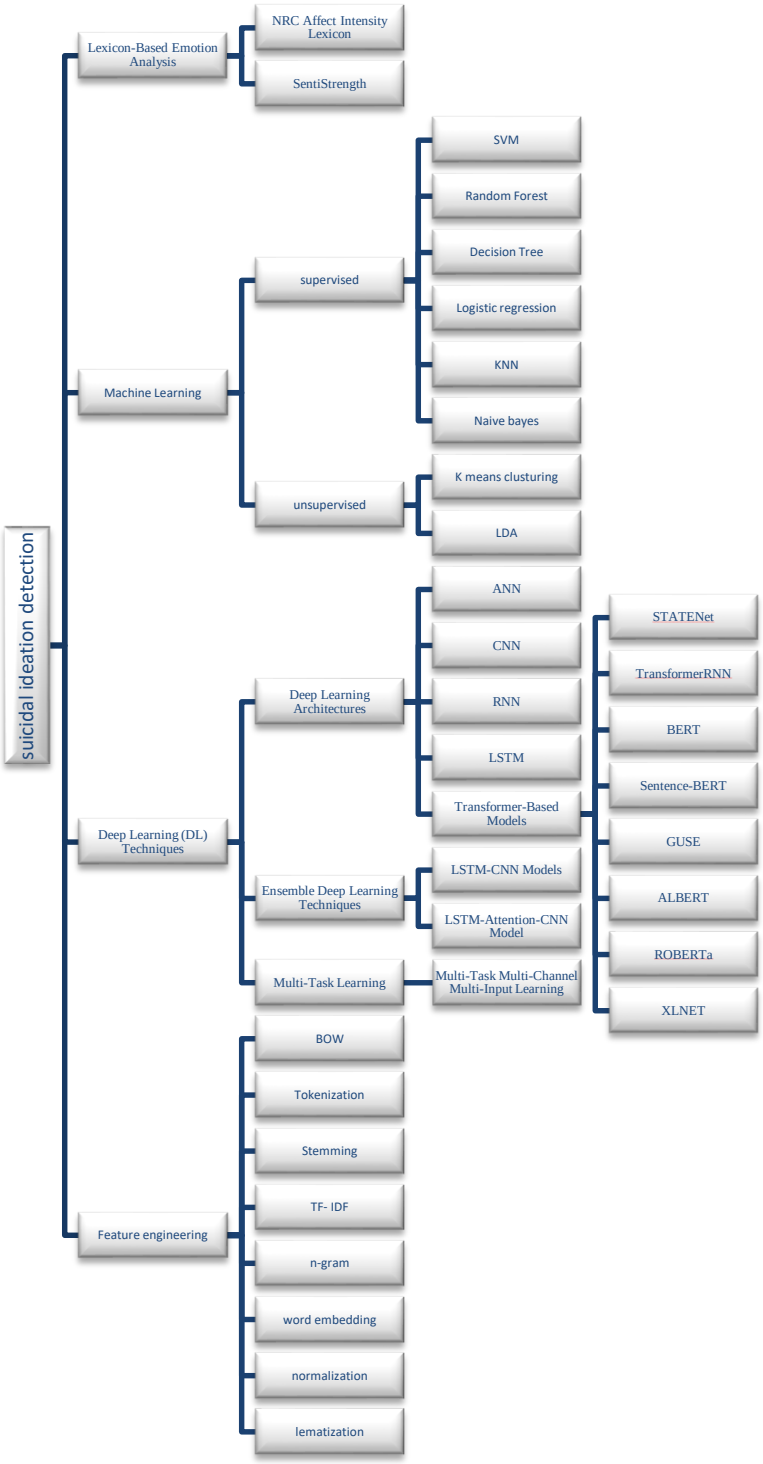


Fig. 1. Hierarchical taxonomy of methodologies for detecting suicidal ideation on social media.

It's widely used in sentiment analysis, social media monitoring, customer feedback analysis, and other areas of natural language processing (NLP) where understanding emotional content is important [47].

ii) SentiStrength: SentiStrength is a sentiment analysis tool designed to decipher the sentiment strength of texts, particularly short informal text found on social media platforms. It is based on a lexicon approach, which means it relies on a dictionary of sentiment-related words, each tagged with sentiment strength scores [48]. SentiStrength can be fine-tuned for specific domains (e.g., software engineering) [49] by adjusting its dictionary to include jargon and terminologies unique to those fields. It can also be adapted to different contexts and languages, recognizing that sentiment expression

varies greatly across cultural and linguistic landscapes. It is used to gauge public sentiment on various topics by analysing social media posts on platforms like Twitter and YouTube. Governments and organizations use it to understand public opinion on policies, products, or events. SentiStrength struggles with posts that contain images [50], as its lexical approach does not account for visual sentiment indicators. Like many sentiment analysis tools, SentiStrength may not accurately interpret sarcasm and irony, which are prevalent in social media text. The rapid evolution of online language can outpace the tool's dictionary updates, potentially leading to inaccurate sentiment scores.

SentiStrength stands out for its ability to decipher sentiment in informal, web-based text, making it a valuable tool for researchers and organizations looking to tap into public sentiment.

The heart of suicidal ideation detection lies in the application of machine learning and deep learning models. These models are trained on preprocessed and feature-extracted data to classify social media posts as indicative of suicidal ideation or not.

b) Supervised machine learning models

i) Support Vector Machines (SVM): Support Vector Machine (SVM) is a robust and versatile supervised machine learning algorithm widely used for classification and regression tasks [51], but primarily known for its applications in classification. The core idea behind SVM is to find the optimal hyperplane that maximizes the margin between different classes in the feature space. For a linear SVM (the simplest form) [52], the decision boundary is a hyperplane, and the goal is to find the hyperplane that leaves the maximum margin from the nearest points of all classes, which are known as support vectors. Mathematically, this can be represented by the equation of the hyperplane:

$$w.x - b = 0 \quad (1)$$

where w is the weight vector perpendicular to the hyperplane, x represents the input features, and b is the bias term. In more complex scenarios, where classes are not linearly separable, SVM uses kernel functions to transform the input space into a higher-dimensional space [53] where a hyperplane can effectively segregate the classes. This is known as the Kernel trick, allowing SVM to perform non-linear classification.

SVM's strength lies in its versatility and efficiency, particularly in high-dimensional spaces. It's relatively memory efficient as it uses a subset of training points in the decision function (the support vectors), making it both powerful and efficient. The optimization of SVM involves finding the right balance between increasing the margin size and minimizing classification error, controlled by a regularization parameter. Support Vector Machine (SVM) is adept at detecting suicidal ideation from social media data, largely due to its proficiency in managing high-dimensional spaces [53]. By employing techniques like TF-IDF for feature extraction, SVM transforms complex and nuanced social media text into a structured format. It then identifies an optimal hyperplane to differentiate between posts that indicate suicidal ideation and those that don't, maximizing the margin between these categories using key data points, known as support vectors. This approach is particularly effective due to the subtle linguistic cues and contextual nuances present in social media content, though its success is contingent on precise data preprocessing and feature selection to capture the complexities of emotional expressions online.

ii) Decision tree: A Decision Tree is a widely used non-parametric supervised learning algorithm used for classification and regression tasks [54]. It models decisions and their possible consequences as a tree-like structure, where each internal node represents a "test" on an attribute, each branch represents the outcome of the test, and each leaf node represents a class label (decision taken after computing all attributes). The paths from root to leaf represent classification rules. In building the decision tree, algorithms like ID3, C4.5, or CART [54]are used to determine how to split the data and construct the tree. These algorithms typically employ measures such as Gini impurity or entropy to choose which feature to split at each step. The Gini impurity for a set is given by:

$$Gini\ Impurity = 1 - \sum_{i=1}^{n} {p_i}^2 \quad (2)$$

Where p_i is the probability of an object being classified to a particular class. Alternatively, entropy, a measure of disorder or impurity, is given by:

$$Entropy = -\sum_{i=1}^{n} p_i \log_2(p_i) \quad (3)$$

In the context of detecting suicidal ideation from social media text data, a Decision Tree algorithm works by learning from the features extracted from the text (such as specific keywords, phrases, sentiment scores, or linguistic patterns) and creating a model that can classify new texts based on these learned patterns [38]. Each node in the tree represents a feature, and the branches represent the decision rules leading to the final classification in the leaf nodes. This approach is particularly suitable for such tasks due to its interpretability; the tree structure allows for easy understanding and tracing of the decision path and reasoning [19]. This transparency is crucial in sensitive applications like mental health monitoring, where understanding the rationale behind a classification (such as why a particular post is flagged as indicative of suicidal ideation) is as important as the classification itself.

iii) Random forest: Random Forest is a machine learning technique for classification, regression, and other tasks that operates by constructing a multitude of decision trees at training time and outputting the mode of the classes or mean prediction of the individual trees [55]. It builds upon the concept of bagging, an approach that improves the stability and accuracy of machine learning algorithms by combining multiple models to 'vote' on the final output [56]. Each tree in a Random Forest makes a class prediction, and the class with the most votes becomes the model's overall prediction. The algorithm injects randomness into the model building process, which not only helps in reducing the variance of the model but also prevents overfitting. This is done by randomly selecting

subsets of the training data set (with replacement) and subsets of the features used for splitting nodes. The decision tree equation typically involves measures like Gini impurity or entropy [57] to find the best split at each node:

$$Gini\ Impurity = 1 - \sum(p_i)^2 \quad (4)$$

$$Entropy = -\sum p_i \log_2(p_i) \quad (5)$$

Where p_i is the proportion of samples that belong to a certain class in a given node.

In the context of suicidal ideation detection from social media text data, Random Forest can be highly effective [7]. It starts with preprocessing and transforming textual data into a numerical format, typically using vectorization methods such as TF-IDF or word embeddings. Each decision tree in the Random Forest then learns from a random subset of these features, creating a diverse set of perspectives for interpreting the data. When new data is inputted, each tree makes a prediction based on its learned patterns, and the final output is decided by a majority vote across all trees. This methodology is particularly suitable for analyzing social media content, as it accommodates the high variability and noise often found in this type of data. The ensemble nature of Random Forest also helps in capturing a wide array of linguistic and contextual indicators associated with suicidal ideation, making it a robust tool for mental health monitoring in digital platforms [16], [17].

iv) Logistic regression: Logistic Regression is a statistical method used for binary classification problems, which models the probability of a binary response based on one or more predictor variables [58]. It operates under the principle that the log odds of the probability of an event occurring versus it not occurring is linearly related to the independent variables [59]. This relationship is expressed through the logistic function:

$$\log\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n \quad (6)$$

Here, p is the probability of the dependent event occurring, β_0 is the intercept, β_1 , β_2 , ..., β_n) are the regression coefficients, and X_1, X_2, ..., X_n are the independent variables. The output is then transformed using the logistic function (or sigmoid function), ensuring that the output always lies between 0 and 1, making it interpretable as a probability:

$$p = \frac{1}{1+e^{-(\beta_0+\beta_1 X_1+\beta_2 X_2+\cdots+\beta_n X_n)}} \quad (7)$$

In utilizing Logistic Regression for identifying suicidal ideation within social media text, a nuanced approach is adopted to process and analyze the content [32]. Initially, the textual data undergoes preprocessing to extract meaningful attributes, which might include the frequency of emotive words, the structure of sentences, or the usage of certain language patterns associated with mental health indicators. Logistic Regression then applies its algorithm to these extracted features, determining the likelihood of a post reflecting suicidal thoughts. The output, given as a probability, offers a graded scale of risk assessment rather than a binary classification, providing a more refined analysis. This method stands out for its straightforward interpretability, essential for mental health monitoring, where understanding the reasoning behind a prediction is crucial. However, the model's effectiveness hinges on the relevance and quality of the features selected, necessitating careful curation to avoid biases or misinterpretations [15], [32]. Such an approach allows Logistic Regression to be a potent tool in the sensitive area of mental health surveillance on digital platforms.

v) KNN: K-Nearest Neighbors (KNN) is a simple, yet versatile supervised learning algorithm used for both classification and regression tasks, but it's most utilized for classification [60]. KNN operates on the principle that similar things exist in proximity; in other words, it assumes that similar data points are near to each other. The algorithm doesn't explicitly learn a model; instead, it classifies a new data point based on the majority vote of its 'K' nearest neighbors. The number of neighbors, K, is a critical user-defined parameter, and the distance between data points is calculated using metrics like Euclidean distance, Manhattan distance, or Hamming distance [61]. The Euclidean distance between two points in a plane is given by [62]:

$$d(p,q) = \sqrt{(q_1-p_1)^2 + (q_2-p_2)^2 + \cdots + (q_n-p_n)^2} \quad (8)$$

In suicidal ideation detection from social media text using K-Nearest Neighbors (KNN), the algorithm classifies new posts based on linguistic and emotional similarities with existing posts [18]. After transforming text data into numerical features, KNN identifies the 'K' closest posts in this feature space, determining the new post's category based on the prevalence of categories (indicative of suicidal ideation or not) among these nearest neighbors. This method effectively captures subtle patterns in personal expression [41], with the choice of 'K' and the nature of features used being crucial for accuracy. The model's reliance on direct comparisons with known cases makes it uniquely suited for discerning nuanced expressions of mental states in social media, provided the training data is diverse and representative.

vi) Naïve bayes classifiers: Naïve Bayes is a probabilistic machine learning model based on applying Bayes' Theorem with the assumption of independence among predictors [63]. It's particularly popular for text classification tasks due to its simplicity and effectiveness, even with high-dimensional data. The fundamental equation is Bayes' Theorem [64]:

$$P(A/B) = \frac{P(B/A)P(A)}{P(B)} \quad (9)$$

In this context, A and B represent different events, where $P(A/B)$ is the probability of A given B , $P(B/A)$ is the probability of B given A, $P(A)$ and $P(B)$ are the probabilities of observing A and B independently of each other.

For suicidal ideation detection in social media texts, Naive Bayes works by first transforming text data into a feature vector (often using techniques like bag-of-words or TF-IDF). Each word or phrase in the text contributes independently to the probability that the message reflects suicidal ideation. The model then uses these probabilities, derived from the training data, to predict whether new texts suggest suicidal thoughts [15], [20]. This method's efficiency in handling large volumes of text and its ability to quickly classify new data make it

suitable for real-time monitoring of social media platforms. However, the assumption of independence among words can sometimes oversimplify the linguistic complexities of human communication, particularly in the nuanced context of mental health discussions. Despite this, Naive Bayes remains a popular choice due to its ease of implementation and its proficiency in processing and classifying large datasets efficiently.

c) Unsupervised machine learning models

i) K-Means Clustering: K-Means Clustering is an unsupervised learning algorithm that partitions a dataset into k clusters by minimizing the intra-cluster variance [65]. It does so by iteratively assigning data points to the nearest cluster centroid and updating the centroid to the mean of the points in the cluster. The algorithm's objective is to minimize the sum of squared distances between points and their respective cluster centroids, expressed as:

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^{(j)} - c_j \right\|^2 \quad (10)$$

Here, $\left\| x_i^{(j)} - c_j \right\|^2$ is the Euclidean distance between a data point $x_i^{(j)}$ and the cluster centroid c_j, n is the number of data points in cluster j, and k is the number of clusters.

For suicidal ideation detection in social media text, K-Means can group posts into clusters based on textual similarities, using features like TF-IDF vectors. These clusters can then be analyzed to identify common themes or expressions indicative of suicidal thoughts [19]. This clustering approach helps in organizing large, unlabeled datasets into meaningful categories, facilitating the identification of mental health concerns. However, the effectiveness of K-Means in this context heavily relies on the choice of k and the initial centroid selection, alongside robust preprocessing of the text data.

ii) Latent Dirichlet Allocation (LDA): Latent Dirichlet Allocation (LDA) is a popular unsupervised learning algorithm in natural language processing, primarily used for topic modeling [66]. It assumes that documents are mixtures of topics and that topics are mixtures of words. This generative model allows it to discover hidden thematic structures in large collections of text documents. LDA represents each document as a distribution over topics and each topic as a distribution over words.

For detecting suicidal ideation in social media texts, LDA helps identify topics that may signify mental distress. It processes text data to extract latent topics, potentially flagging those aligned with suicidal thoughts. This method is valuable for exploratory analysis, identifying linguistic patterns related to mental health [19], [43]. However, the effectiveness of LDA depends on accurate text preprocessing and parameter tuning, requiring careful interpretation in the sensitive context of mental health monitoring.

d) Deep learning models

i) Artificial Neural Networks (ANN): Artificial Neural Networks (ANNs) are computational models inspired by the human brain's structure and function, particularly effective in pattern recognition and predictive modeling [67]. An ANN consists of layers of interconnected nodes or neurons, each node in one layer connected to several others in the next layer. The basic operation in a neuron involves weighted input summation and a non-linear activation function [68]. Mathematically, the output y of a neuron can be described by the equation,

$$y = f(\sum_{i=1}^{n} w_i x_i + b) \quad (11)$$

where x_i are the inputs, w_i are the weights, b is the bias, and f is the activation function, like a sigmoid or ReLU function. The network learns to model complex relationships by adjusting these weights and biases based on the input data.

For suicidal ideation detection from social media text, ANNs can be employed to analyze and classify text data [23]. The process involves preprocessing the text (like tokenization, stemming, and vectorization) to transform it into a format suitable for the ANN. The network then processes this data through its layers, learning to identify patterns and linguistic cues that are indicative of suicidal ideation. This might include specific keywords, phrases, or the overall sentiment of the text. The final layer of the network, typically a SoftMax layer, classifies the text based on the learned patterns, indicating whether it likely contains suicidal ideation. The performance of ANNs in this application largely depends on the network's depth and complexity, the quality of the training data, and the model's capacity to capture subtle nuances in the language that may suggest suicidal thoughts or tendencies.

ii) Convolutional Neural Networks (CNN): CNN, or Convolutional Neural Networks, are a class of deep neural networks commonly used in image processing [69] but also effective in text classification [70], particularly for feature extraction [71]. CNNs are particularly effective due to their ability to learn spatial hierarchies of features through the use of convolutional layers. A basic CNN structure includes an input layer, convolutional layers, pooling layers, fully connected layers, and an output layer [72]. The convolutional layers apply a convolution operation to the input, passing the result to the next layer. This can be represented by the equation:

$$Output = Activation(Weights.Input + Bias) \quad (12)$$

where Activation is a non-linear function like ReLU. Pooling layers reduce the spatial size of the convolved features to decrease the computational power required. Finally, fully connected layers combine these features to classify the input into various categories.

For suicidal ideation detection from social media text, CNNs can be utilized to analyze and classify textual data [27]. The process begins with the collection and preprocessing of social media texts, which involves cleaning, normalization, and tokenization to convert text into a form that can be fed into a CNN. CNN then learns to identify patterns and features in the text indicative of suicidal ideation, such as specific keywords, phrases, or linguistic patterns. This involves multiple layers of convolution and pooling to extract and condense the relevant features from the text data. The fully connected layers at the end of the CNN then interpret these features to classify the text,

often outputting a probability score indicating the likelihood of suicidal ideation present in the text. The effectiveness of this approach relies on the quality and diversity of the training data, as well as the complexity and depth of the CNN model used.

iii) Recurrent Neural Networks (RNN): Recurrent Neural Networks (RNNs) are a type of neural network particularly suited for processing sequential data, such as time series or text [73]. Unlike traditional neural networks, RNNs have a unique feature: they maintain a form of memory by using their output as input for the subsequent step. This is achieved through loops within the network [74]. In mathematical terms, the hidden state h_t at time t in a simple RNN is calculated as

$$h_t = activation(W_{hh}h_{t-1} + W_{xh}x_t + b_h) \quad (13)$$

where W_{hh} and W_{xh} are weight matrices, x_t is the input at time t, h_{t-1} is the previous hidden state, and b_h is the bias. The output y_t is then a function of the current hidden state: $y_t = activation(W_{hy}h_t + b_y$ with W_{hy} being the output layer weights and b_y the output bias.

For suicidal ideation detection in social media text, RNNs are particularly effective due to their ability to process and learn from the sequential nature of language. The process starts with preprocessing the text data, including tokenization and possibly embedding the words into a vector space [8]. The RNN then processes this sequential data, with each word (or token) being input sequentially. The RNN's hidden state updates with each word, effectively allowing the network to remember and utilize the context from previous words. This context understanding is crucial for identifying patterns or linguistic cues indicative of suicidal ideation, such as expressions of despair, hopelessness, or direct mentions of self-harm. The final output layer of the RNN can classify the text based on the learned patterns, potentially indicating whether the text suggests suicidal ideation. The performance of RNNs in this application hinges on the depth of the network, the quality of the training data, and the network's ability to capture and utilize long-term dependencies in the text.

iv) Long Short-Term Memory (LSTM) and Bidirectional LSTM (BiLSTM): Long Short-Term Memory (LSTM) networks are an advanced type of Recurrent Neural Network (RNN) designed to better capture long-range dependencies and address the vanishing gradient problem common in standard RNNs [75]. The key to LSTM's effectiveness is its unique cell structure comprising three gates: the input gate i_t, the forget gate f_t, and the output gate o_t. These gates collectively decide what information to retain or discard as the network processes data sequentially. The LSTM cell updates are governed by the following equations:

$$f_t = \sigma\big(W_f.[h_{t-1}, x_t] + b_f\big), (\text{Forget Gate} \quad (14)$$

$$i_t = \sigma(W_i.[h_{t-1}, x_t] + b_i), (\text{Input Gate}) \quad (15)$$

$$\widetilde{C_t} = \tanh(W_c.[h_{t-1}, x_t] + b_c), (Cell\ State\ Candidate) \quad (16)$$

$$C_t = f_t * C_{t-1} + i_t * \widetilde{C_t}, (Cell\ State\ Update) \quad (17)$$

$$o_t = \sigma(W_o.[h_{t-1}, x_t] + b_o), (Output\ Gate) \quad (18)$$

$$h_t = o_t * \tanh(C_t), (Hidden\ State) \quad (19)$$

A Bidirectional LSTM (BiLSTM) extends the standard LSTM by introducing a second layer that processes data in the reverse order [76]. While a regular LSTM processes data from past to future (left to right in a sequence), a BiLSTM also processes data from future to past (right to left), effectively capturing information from both directions. This dual processing makes BiLSTMs particularly effective in applications where the context of the entire sequence is crucial for understanding each part of it.

In the context of suicidal ideation detection from social media text, LSTMs excel due to their ability to capture and remember pertinent information across long text sequences [8], [28], which is crucial in understanding the context and nuances of language. By processing sequential data, LSTMs can identify patterns or phrases indicative of suicidal thoughts, such as expressions of hopelessness or mentions of self-harm. In suicidal ideation detection, a BiLSTM would analyze the text from both directions [45], offering a more comprehensive understanding of the context and sentiment expressed, thus potentially improving the accuracy of detecting signs of suicidal ideation.

v) Transformer models: Transformer-based models have revolutionized natural language processing by offering a more efficient and effective means of handling sequential data compared to traditional RNNs or LSTMs. The core concept of Transformers is the self-attention mechanism, which computes the output of a layer by attending to all positions within the same layer [77]. The basic equation for self-attention can be written as:

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (20)$$

where Q, K, and V are queries, keys, and values matrices, respectively, and d_k is the dimensionality of the keys. This mechanism allows the model to weigh the importance of different parts of the input sequence differently, making it highly effective for tasks involving contextual understanding.

Different transformer-based models have emerged, each with unique characteristics [78]:

- STATENet integrates spatial-temporal attention networks for enhanced sequence modeling.
- TransformerRNN combines the transformer architecture with RNNs to capitalize on both methods' strengths.
- BERT (Bidirectional Encoder Representations from Transformers) and its variant Sentence-BERT offer deep bidirectional context understanding by pre-training on large text corpora.
- GUSE (Google Universal Sentence Encoder) is optimized for sentence-level embeddings.
- ALBERT (A Lite BERT) is a more efficient version of BERT with shared parameters across layers.
- RoBERTa (Robustly optimized BERT approach) enhances BERT through robust training methods.

- XLNet combines the best of BERT and autoregressive methods for improved language modeling.

In the context of suicidal ideation detection from social media text, these transformer-based models excel due to their ability to understand and interpret the nuances and context of natural language [22]. By analyzing the text data from social media, these models can capture the subtleties of language that indicate suicidal thoughts or tendencies, such as specific phrases, sentiment, and contextual clues. The self-attention mechanism allows the models to focus on relevant parts of the text, potentially identifying warning signs hidden in normal conversation. This can include detecting direct expressions of suicidal thoughts or more subtle indicators like expressions of hopelessness or isolation. The effectiveness of these models in such applications depends significantly on the quality of the training data and the specific architectural choices made in the model design.

e) Feature engineering

- Bag of Words (BoW): This model treats text as an unordered collection of words, focusing on the frequency of each word but ignoring the order and context [79]. In suicidal ideation detection, BoW can help identify frequently used words in posts that are indicative of distress or suicidal thoughts, such as "helpless" or "worthless."
- Tokenization: This process involves breaking down text into smaller units, typically words or phrases [80]. For suicidal ideation detection, tokenization is the first step in analyzing social media posts, as it helps in isolating individual words or phrases for further examination.
- Stemming: Stemming reduces words to their root form, often by chopping off prefixes or suffixes. For instance, "running" becomes "run" [81]. In suicidal ideation detection, stemming can help in consolidating different forms of a word to a single root, making it easier to analyze and categorize texts.
- TF-IDF (Term Frequency-Inverse Document Frequency): This is a statistical measure used to evaluate the importance of a word in a document, which is part of a corpus. It increases with the number of times a word appears in the document but is offset by the frequency of the word in the corpus [82]. In suicidal ideation detection, TF-IDF can help in identifying unique terms in individual posts that are unusual in general but common in texts expressing suicidal thoughts.
- N-gram: N-grams are continuous sequences of 'n' items from a given sample of text or speech [83], [84]. For suicidal ideation detection, analyzing bigrams (2-grams) or trigrams (3-grams) can reveal specific phrases that are more indicative of suicidal ideation, such as "end my life".
- Word Embedding: This technique involves mapping words or phrases to vectors of real numbers [85], capturing the context and semantic relationships between words. In suicidal ideation detection, word embeddings can provide a deeper understanding of the context and nuances in social media posts, which simple frequency counts cannot.
- Normalization: This process involves transforming text into a more uniform format, such as converting all characters to lowercase, removing punctuation, or converting numbers to words [86]. In detecting suicidal ideation, normalization ensures that the analysis isn't skewed by superficial variations in the text.
- Lemmatization: Similar to stemming, lemmatization also reduces words to their base or dictionary form, but it does so use linguistic knowledge about the word's proper form or lemma [87]. For instance, "better" is lemmatized to "good". In the context of suicidal ideation detection, lemmatization helps in accurately grouping together different forms of a word, leading to more effective analysis.

Each of these techniques contributes to transforming raw text into a structured, analyzable form, aiding in the identification of language patterns associated with suicidal thoughts and behavior.

4) Evaluation matrices: After developing the models, evaluating their performance is crucial. Common evaluation metrics include [88]:

- Accuracy: The ratio of correctly predicted instances to the total instances in the dataset.
- Precision and Recall: Precision measures the proportion of true positive identifications among the positive identifications made by the model, while recall measures the proportion of true positive identifications among the actual positives.
- F1 Score: The harmonic mean of precision and recall, providing a balance between the two metrics.
- AUC-ROC Curve: A performance measurement for classification problems at various thresholds settings.

5) Challenges to address: Despite the advancements in methodologies, there are inherent challenges. One major challenge is the balance between model complexity and interpretability. While deep learning models offer advanced capabilities, they often act as 'black boxes', making it difficult to interpret their decision-making processes.

Moreover, the issue of data imbalance, where instances of suicidal ideation are significantly less than non-suicidal posts, can skew model training and affect the reliability of predictions.

Another challenge is the generalizability of these models. Models trained on specific datasets or demographics might not perform effectively when applied to different datasets or populations. This issue underscores the importance of creating diverse and representative training datasets.

The detection of suicidal ideation on social media using machine learning, deep learning, and NLP involves a complex interplay of various methodologies. From dataset collection

and preprocessing to the application of advanced algorithms and evaluation, each step plays a crucial role in the effectiveness of the detection process. While significant progress has been made, ongoing research is needed to address the challenges of model interpretability, data imbalance, and generalizability.

IV. CONCLUSION

Social media has become a valuable data source for detecting mental health conditions, such as suicidal ideation. This review synthesizes current research utilizing machine learning, deep learning, and NLP techniques to identify warning signs in social media posts. The study highlights the advancement of AI in suicide prevention, showcasing models that leverage deep neural networks and transfer learning to decipher complex linguistic patterns indicative of suicidal thoughts. Key findings demonstrate precision rates of 82-97% and recall rates of 71-94% using models such as SVMs, Random Forests, and neural networks. Despite promising results, model robustness must be improved for real-world application.

Challenges include limited, non-representative datasets that hinder generalizability and may introduce demographic biases. Most models were developed using English data from American users, lacking validation across cultures, languages, and demographics. Achieving a balance between accuracy, complexity, and interpretability remains difficult, with simpler models underperforming and complex models being opaque. Future work should focus on testing across age groups and integrating additional risk indicators, alongside addressing privacy concerns and ensuring ethical data use.

Differentiating genuine suicidal intent from rhetorical expressions is an ongoing challenge, as individuals communicate distress uniquely, influenced by personal and cultural factors. Addressing these nuances requires further qualitative research and interdisciplinary collaboration for better contextual understanding. Early identification through improved technology can facilitate timely intervention, but real-world implementation must consider privacy rights and avoid stigmatization. Clear, ethically aligned protocols are essential for the responsible handling of flagged data.

In conclusion, while significant strides have been made in using machine learning for large-scale screening of suicidal ideation, future research should expand datasets, enhance generalizability, and refine contextual interpretation. Ensuring ethical standards and practical protocols will be vital for maximizing the public health benefits of these technological advances.

ACKNOWLEDGMENT

This research was fully funded by the UMPSA Research Grant Scheme under grant RDU230353 and PGRS2303109.

REFERENCES

[1] S. Bachmann, “Epidemiology of suicide and the psychiatric perspective,” Jul. 06, 2018, MDPI AG. doi: 10.3390/ijerph15071425.

[2] S. C. Curtin and M. Heron, “Death Rates Due to Suicide and Homicide Among Persons Aged 10-24: United States, 2000-2017 Key findings Data from the National Vital Statistics System.” [Online]. Available: https://www.cdc.gov/nchs/products/index.htm.

[3] J. Torous et al., “Smartphones, Sensors, and Machine Learning to Advance Real-Time Prediction and Interventions for Suicide Prevention: a Review of Current Progress and Next Steps,” Jul. 01, 2018, Current Medicine Group LLC 1. doi: 10.1007/s11920-018-0914-y.

[4] K. P. Linthicum, K. M. Schafer, and J. D. Ribeiro, “Machine learning in suicide science: Applications and ethics,” Behavioral Sciences & the Law, vol. 37, no. 3, pp. 214–222, May 2019, doi: 10.1002/bsl.2392.

[5] J. Torous and R. Walker, “Leveraging Digital Health and Machine Learning Toward Reducing Suicide - From Panacea to Practical Tool,” Oct. 01, 2019, American Medical Association. doi: 10.1001/jamapsychiatry.2019.1231.

[6] A. Paxton and T. L. Griffiths, “Finding the traces of behavioral and cognitive processes in big data and naturally occurring datasets,” Behav Res Methods, vol. 49, no. 5, pp. 1630–1638, Oct. 2017, doi: 10.3758/s13428-017-0874-x.

[7] M. M. Tadesse, H. Lin, B. Xu, and L. Yang, “Detection of suicide ideation in social media forums using deep learning,” Algorithms, vol. 13, no. 1, Jan. 2020, doi: 10.3390/a13010007.

[8] R. and M. P. and M. P. and S. R. and S. R. Sawhney, “Exploring and learning suicidal ideation connotations on social media with deep learning,” in Proceedings of the 9th workshop on computational approaches to subjectivity, sentiment and social media analysis, Oct. 2018, pp. 167–175.

[9] Q. Huang, R. Chen, X. Zheng, and Z. Dong, “Deep sentiment representation based on CNN and LSTM,” in Proceedings - 2017 International Conference on Green Informatics, ICGI 2017, Institute of Electrical and Electronics Engineers Inc., Nov. 2017, pp. 30–33. doi: 10.1109/ICGI.2017.45.

[10] T. Guo, T. Lin, and N. Antulov-Fantulin, “Exploring Interpretable LSTM Neural Networks over Multi-Variable Data,” May 2019, [Online]. Available: http://arxiv.org/abs/1905.12034

[11] I. Priyadarshini and C. Cotton, “A novel LSTM–CNN–grid search-based deep neural network for sentiment analysis,” Journal of Supercomputing, vol. 77, no. 12, pp. 13911–13932, Dec. 2021, doi: 10.1007/s11227-021-03838-w.

[12] A. Sigfrids, M. Nieminen, J. Leikas, and P. Pikkuaho, “How Should Public Administrations Foster the Ethical Development and Use of Artificial Intelligence? A Review of Proposals for Developing Governance of AI,” Frontiers in Human Dynamics, vol. 4, May 2022, doi: 10.3389/fhumd.2022.858108.

[13] P. Scott, K. Emerson, and T. Henderson-Reay, “Data saves lives,” BMJ, p. n1694, Jul. 2021, doi: 10.1136/bmj.n1694.

[14] J. Parraga-Alava, R. A. Caicedo, J. M. Gomez, and M. Inostroza-Ponta, “An Unsupervised Learning Approach for Automatically to Categorize Potential Suicide Messages in Social Media,” in Proceedings - International Conference of the Chilean Computer Science Society, SCCC, IEEE Computer Society, Nov. 2019. doi: 10.1109/SCCC49216.2019.8966443.

[15] P. Jain, K. R. Srinivas, and A. Vichare, “Depression and Suicide Analysis Using Machine Learning and NLP,” in Journal of Physics: Conference Series, IOP Publishing Ltd, Jan. 2022. doi: 10.1088/1742-6596/2161/1/012034.

[16] S. T. Rabani, Q. R. Khan, and A. M. Ud Din Khanday, “Detection of suicidal ideation on Twitter using machine learning & ensemble approaches,” Baghdad Science Journal, vol. 17, no. 4, pp. 1328–1339, Dec. 2020, doi: 10.21123/bsj.2020.17.4.1328.

[17] S. Ryu, H. Lee, D. K. Lee, S. W. Kim, and C. E. Kim, “Detection of suicide attempters among suicide ideators using machine learning,” Psychiatry Investig, vol. 16, no. 8, pp. 588–593, Aug. 2019, doi: 10.30773/pi.2019.06.19.

[18] N. Wang et al., “Learning Models for Suicide Prediction from Social Media Posts,” Apr. 2021, [Online]. Available: http://arxiv.org/abs/2105.03315

[19] S. Fodeh et al., “Using machine learning algorithms to detect suicide risk factors on twitter,” in IEEE International Conference on Data Mining Workshops, ICDMW, IEEE Computer Society, Nov. 2019, pp. 941–948. doi: 10.1109/ICDMW.2019.00137.

[20] S. R. Lim, N. S. Kamarudin, N. H. Ismail, N. A. Hisham Ismail, and N. A. Mohamad Kamal, "Predicting Mental Health Disorder on Twitter Using Machine Learning Techniques," in 8th International Conference on Software Engineering and Computer Systems, ICSECS 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 23–27. doi: 10.1109/ICSECS58457.2023.10256420.

[21] T. Zhang, A. M. Schoene, and S. Ananiadou, "Automatic identification of suicide notes with a transformer-based deep learning model," Internet Interv, vol. 25, Sep. 2021, doi: 10.1016/j.invent.2021.100422.

[22] A. Haque, V. Reddi, and T. Giallanza, "Deep Learning for Suicide and Depression Identification with Unsupervised Label Correction," Feb. 2021, [Online]. Available: http://arxiv.org/abs/2102.09427

[23] Y. Ophir, R. Tikochinski, C. S. C. Asterhan, I. Sisso, and R. Reichart, "Deep neural networks detect suicide risk from textual facebook posts," Sci Rep, vol. 10, no. 1, Dec. 2020, doi: 10.1038/s41598-020-73917-0.

[24] P. Buddhitha and D. Inkpen, "Multi-Task, Multi-Channel, Multi-Input Learning for Mental Illness Detection using Social Media Text," pp. 54–64, 2019, doi: 10.18653/v1/D19-62.

[25] E. J. S. Diniz et al., "Boamente: A Natural Language Processing-Based Digital Phenotyping Tool for Smart Monitoring of Suicidal Ideation," Healthcare (Switzerland), vol. 10, no. 4, Apr. 2022, doi: 10.3390/healthcare10040698.

[26] T. H. H. Aldhyani, S. N. Alsubari, A. S. Alshebami, H. Alkahtani, and Z. A. T. Ahmed, "Detecting and Analyzing Suicidal Ideation on Social Media Using Deep Learning and Machine Learning Models," Int J Environ Res Public Health, vol. 19, no. 19, Oct. 2022, doi: 10.3390/ijerph191912635.

[27] S. Renjith, A. Abraham, S. B. Jyothi, L. Chandran, and J. Thomson, "An ensemble deep learning technique for detecting suicidal ideation from posts in social media platforms," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, pp. 9564–9575, Nov. 2022, doi: 10.1016/j.jksuci.2021.11.010.

[28] B. Kholifah, I. Syarif, and T. Badriyah, "Mental Disorder Detection via Social Media Mining using Deep Learning," Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, pp. 309–316, Nov. 2020, doi: 10.22219/kinetik.v5i4.1120.

[29] L. Cao, H. Zhang, and L. Feng, "Building and Using Personal Knowledge Graph to Improve Suicidal Ideation Detection on Social Media," IEEE Trans Multimedia, vol. 24, pp. 87–102, 2022, doi: 10.1109/TMM.2020.3046867.

[30] S. M. Sarsam, H. Al-Samarraie, A. I. Alzahrani, W. Alnumay, and A. P. Smith, "A lexicon-based approach to detecting suicide-related messages on Twitter," Biomed Signal Process Control, vol. 65, Mar. 2021, doi: 10.1016/j.bspc.2020.102355.

[31] A. Roy, K. Nikolitch, R. McGinn, S. Jinah, W. Klement, and Z. A. Kaminsky, "A machine learning approach predicts future risk to suicidal ideation from social media data," NPJ Digit Med, vol. 3, no. 1, Dec. 2020, doi: 10.1038/s41746-020-0287-6.

[32] S. and N. S. P. and D. R. K. and B. U. and M. N. and K. V. Jain, "A machine learning based depression analysis and suicidal ideation detection system using questionnaires and twitter," in 2019 IEEE students conference on engineering and systems (SCES), IEEE, May 2019, pp. 1–6.

[33] H. Yao, S. Rashidian, X. Dong, H. Duanmu, R. N. Rosenthal, and F. Wang, "Detection of suicidality among opioid users on reddit: Machine learning-based approach," J Med Internet Res, vol. 22, no. 11, Nov. 2020, doi: 10.2196/15293.

[34] T. Falcone et al., "Digital conversations about suicide among teenagers and adults with epilepsy: A big-data, machine learning analysis," Epilepsia, vol. 61, no. 5, pp. 951–958, May 2020, doi: 10.1111/epi.16507.

[35] J. Luo, J. Du, C. Tao, H. Xu, and Y. Zhang, "Exploring temporal suicidal behavior patterns on social media: Insight from Twitter analytics," Health Informatics J, vol. 26, no. 2, pp. 738–752, Jun. 2020, doi: 10.1177/1460458219832043.

[36] G. M. Lin, M. Nagamine, S. N. Yang, Y. M. Tai, C. Lin, and H. Sato, "Machine Learning Based Suicide Ideation Prediction for Military Personnel," IEEE J Biomed Health Inform, vol. 24, no. 7, pp. 1907–1916, Jul. 2020, doi: 10.1109/JBHI.2020.2988393.

[37] X. Liu et al., "Proactive suicide prevention online (PSPO): Machine identification and crisis management for Chinese social media users with suicidal thoughts and behaviors," J Med Internet Res, vol. 21, no. 5, May 2019, doi: 10.2196/11705.

[38] M. L. Tlachac, K. Dixon-Gordon, and E. Rundensteiner, "Screening for suicidal ideation with text messages," in BHI 2021 - 2021 IEEE EMBS International Conference on Biomedical and Health Informatics, Proceedings, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/BHI50953.2021.9508486.

[39] E. Rajesh Kumar, K. V. S. N. Rama Rao, S. R. Nayak, and R. Chandra, "Suicidal ideation prediction in twitter data using machine learning techniques," Journal of Interdisciplinary Mathematics, vol. 23, no. 1, pp. 117–125, Jan. 2020, doi: 10.1080/09720502.2020.1721674.

[40] A. Mbarek, S. Jamoussi, A. Charfi, and A. Ben Hamadou, "Suicidal Profiles Detection in Twitter," Scitepress, Feb. 2022, pp. 289–296. doi: 10.5220/0008167600002366.

[41] M. A. Ibrahim, N. H. Ismail, N. S. Kamarudin, N. S. Mohd Nafis, and A. F. A. Nasir, "Identifying PTSD Symptoms Using Machine Learning Techniques on Social Media," in 8th International Conference on Software Engineering and Computer Systems, ICSECS 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 392–395. doi: 10.1109/ICSECS58457.2023.10256290.

[42] N. S. Kamarudin, G. Beigi, L. Manikonda, and H. Liu, "Social Media for Mental Health: Data, Methods, and Findings," 2020, pp. 195–220. doi: 10.1007/978-3-030-41251-7_8.

[43] N. S. Kamarudin, G. Beigi, and H. Liu, "A Study on Mental Health Discussion through Reddit," in Proceedings - 2021 International Conference on Software Engineering and Computer Systems and 4th International Conference on Computational Science and Information Management, ICSECS-ICOCSIM 2021, Institute of Electrical and Electronics Engineers Inc., Aug. 2021, pp. 637–643. doi: 10.1109/ICSECS52883.2021.00122.

[44] N. S. and R. V. and B. G. and M. L. and L. H. Kamarudin, "A study of reddit-user's response to rape," in 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), IEEE, Aug. 2018, pp. 591–592.

[45] F. Haque, R. U. Nur, S. Al Jahan, Z. Mahmud, and F. M. Shah, "A Transformer Based Approach to Detect Suicidal Ideation Using Pre-Trained Language Models," in ICCIT 2020 - 23rd International Conference on Computer and Information Technology, Proceedings, Institute of Electrical and Electronics Engineers Inc., Dec. 2020. doi: 10.1109/ICCIT51783.2020.9392692.

[46] S. M. Mohammad, "Word Affect Intensities," Apr. 2017, [Online]. Available: http://arxiv.org/abs/1704.08798

[47] S. M. Mohammad and F. Bravo-Marquez, "Emotion Intensities in Tweets," Aug. 2017, [Online]. Available: http://arxiv.org/abs/1708.03696

[48] M. Thelwall, "The Heart and Soul of the Web? Sentiment Strength Detection in the Social Web with SentiStrength," 2017, pp. 119–134. doi: 10.1007/978-3-319-43639-5_7.

[49] M. R. Islam and M. F. Zibran, "SentiStrength-SE: Exploiting domain specificity for improved sentiment analysis in software engineering text," Journal of Systems and Software, vol. 145, pp. 125–146, Nov. 2018, doi: 10.1016/j.jss.2018.08.030.

[50] C. Reithmeier, K. Buschbaum, and D. Kanwischer, "Spatialities, Social Media and Sentiment Analysis: Exploring the Potential of the Detection Tool SentiStrength," GI_Forum, vol. 1, pp. 85–96, 2018, doi: 10.1553/giscience2018_02_s85.

[51] J. Cervantes, F. Garcia-Lamont, L. Rodríguez-Mazahua, and A. Lopez, "A comprehensive survey on support vector machine classification: Applications, challenges and trends," Neurocomputing, vol. 408, pp. 189–215, Sep. 2020, doi: 10.1016/j.neucom.2019.10.118.

[52] V. K. Chauhan, K. Dahiya, and A. Sharma, "Problem formulations and solvers in linear SVM: a review," Artif Intell Rev, vol. 52, no. 2, pp. 803–855, Aug. 2019, doi: 10.1007/s10462-018-9614-6.

[53] D. Boswell, "Introduction to Support Vector Machines," 2002. [Online]. Available: https://api.semanticscholar.org/CorpusID:18986102

[54] Y. Song and Y. Lu, "Decision tree methods: applications for classification and prediction," Shanghai Arch Psychiatry, vol. 27, pp. 130–135, 2015, [Online]. Available: https://api.semanticscholar.org/CorpusID:18242585

[55] A. B. Shaik and S. Srinivasan, "A Brief Survey on Random Forest Ensembles in Classification Model," 2019, pp. 253–260. doi: 10.1007/978-981-13-2354-6_27.

[56] S. Huang, W. Gu, and S. Chen, "Optimization of Classification Rules and Voting Strategies for Random Forest," in 2021 IEEE 7th International Conference on Cloud Computing and Intelligent Systems (CCIS), IEEE, Nov. 2021, pp. 381–387. doi: 10.1109/CCIS53392.2021.9754599.

[57] N. S. Sheth and A. R. Deshpande, "A Review of Splitting Criteria for Decision Tree Induction," Fuzzy Systems, vol. 7, pp. 1–4, 2015, [Online]. Available: https://api.semanticscholar.org/CorpusID:125714163

[58] V. Bewick, L. Cheek, and J. Ball, "Statistics review 14: Logistic regression," Crit Care, vol. 9, no. 1, p. 112, 2005, doi: 10.1186/cc3045.

[59] E. C. Norton and B. E. Dowd, "Log Odds and the Interpretation of Logit Models," Health Serv Res, vol. 53, no. 2, pp. 859–878, Apr. 2018, doi: 10.1111/1475-6773.12712.

[60] K. Taunk, S. De, S. Verma, and A. Swetapadma, "A Brief Review of Nearest Neighbor Algorithm for Learning and Classification," in 2019 International Conference on Intelligent Computing and Control Systems (ICCS), IEEE, May 2019, pp. 1255–1260. doi: 10.1109/ICCS45141.2019.9065747.

[61] K. Chomboon, P. Chujai, P. Teerarassammee, K. Kerdprasop, and N. Kerdprasop, "An Empirical Study of Distance Metrics for k-Nearest Neighbor Algorithm," in The Proceedings of the 2nd International Conference on Industrial Application Engineering 2015, The Institute of Industrial Applications Engineers, 2015, pp. 280–285. doi: 10.12792/iciae2015.051.

[62] J. Draisma, E. Horobeţ, G. Ottaviani, B. Sturmfels, and R. Thomas, "The euclidean distance degree," in Proceedings of the 2014 Symposium on Symbolic-Numeric Computation, New York, NY, USA: ACM, Jul. 2014, pp. 9–16. doi: 10.1145/2631948.2631951.

[63] D. D. Lewis, "Naive (Bayes) at forty: The independence assumption in information retrieval," 1998, pp. 4–15. doi: 10.1007/BFb0026666.

[64] Y. Zhang, "The Application of Bayesian Theorem," Highlights in Science, Engineering and Technology, vol. 49, pp. 520–526, May 2023, doi: 10.54097/hset.v49i.8605.

[65] V. R. Patel and R. G. Mehta, "Modified k-Means Clustering Algorithm," 2011, pp. 307–312. doi: 10.1007/978-3-642-25734-6_46.

[66] D. Andrzejewski and X. Zhu, "Latent Dirichlet Allocation with topic-in-set knowledge," in Proceedings of the NAACL HLT 2009 Workshop on Semi-Supervised Learning for Natural Language Processing - SemiSupLearn '09, Morristown, NJ, USA: Association for Computational Linguistics, 2009, pp. 43–48. doi: 10.3115/1621829.1621835.

[67] S. Agatonovic-Kustrin and R. Beresford, "Basic concepts of artificial neural network (ANN) modeling and its application in pharmaceutical research," J Pharm Biomed Anal, vol. 22, no. 5, pp. 717–727, Jun. 2000, doi: 10.1016/S0731-7085(99)00272-1.

[68] C. Grosan and A. Abraham, "Artificial Neural Networks," 2011, pp. 281–323. doi: 10.1007/978-3-642-21004-4_12.

[69] A. Bilal, A. Jourabloo, M. Ye, X. Liu, and L. Ren, "Do Convolutional Neural Networks Learn Class Hierarchy?," IEEE Trans Vis Comput Graph, vol. 24, no. 1, pp. 152–162, Jan. 2018, doi: 10.1109/TVCG.2017.2744683.

[70] R. Johnson and T. Zhang, "Effective Use of Word Order for Text Categorization with Convolutional Neural Networks," in Proceedings of the 2015 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Stroudsburg, PA, USA: Association for Computational Linguistics, 2015, pp. 103–112. doi: 10.3115/v1/N15-1011.

[71] A. Madasu and V. Anvesh Rao, "Sequential Learning of Convolutional Features for Effective Text Classification," in Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), Stroudsburg, PA, USA: Association for Computational Linguistics, 2019, pp. 5657–5666. doi: 10.18653/v1/D19-1567.

[72] S. Albawi, T. A. Mohammed, and S. Al-Zawi, "Understanding of a convolutional neural network," in 2017 International Conference on Engineering and Technology (ICET), IEEE, Aug. 2017, pp. 1–6. doi: 10.1109/ICEngTechnol.2017.8308186.

[73] Z. C. Lipton, "A Critical Review of Recurrent Neural Networks for Sequence Learning," ArXiv, vol. abs/1506.00019, 2015, [Online]. Available: https://api.semanticscholar.org/CorpusID:5837849

[74] Y. Ming et al., "Understanding Hidden Memories of Recurrent Neural Networks," in 2017 IEEE Conference on Visual Analytics Science and Technology (VAST), IEEE, Oct. 2017, pp. 13–24. doi: 10.1109/VAST.2017.8585721.

[75] H. Sak, A. W. Senior, and F. Beaufays, "Long Short-Term Memory Based Recurrent Neural Network Architectures for Large Vocabulary Speech Recognition," ArXiv, vol. abs/1402.1128, 2014, [Online]. Available: https://api.semanticscholar.org/CorpusID:16904319

[76] S. Siami-Namini, N. Tavakoli, and A. S. Namin, "The Performance of LSTM and BiLSTM in Forecasting Time Series," in 2019 IEEE International Conference on Big Data (Big Data), IEEE, Dec. 2019, pp. 3285–3292. doi: 10.1109/BigData47090.2019.9005997.

[77] H. Luo, S. Zhang, M. Lei, and L. Xie, "Simplified Self-Attention for Transformer-Based end-to-end Speech Recognition," in 2021 IEEE Spoken Language Technology Workshop (SLT), IEEE, Jan. 2021, pp. 75–81. doi: 10.1109/SLT48900.2021.9383581.

[78] A. Gillioz, J. Casas, E. Mugellini, and O. A. Khaled, "Overview of the Transformer-based Models for NLP Tasks," Sep. 2020, pp. 179–183. doi: 10.15439/2020F20.

[79] W. Rui, K. Xing, and Y. Jia, "BOWL: Bag of Word Clusters Text Representation Using Word Embeddings," 2016, pp. 3–14. doi: 10.1007/978-3-319-47650-6_1.

[80] A. Mikheev, "Text Segmentation," in The Oxford Handbook of Computational Linguistics 2nd edition, R. Mitkov, Ed., Oxford University Press, 2018. doi: 10.1093/oxfordhb/9780199573691.013.34.

[81] A. G. Jivani, "A Comparative Study of Stemming Algorithms," 2011. [Online]. Available: https://api.semanticscholar.org/CorpusID:204091414

[82] S. Qaiser and R. Ali, "Text Mining: Use of TF-IDF to Examine the Relevance of Words to Documents," Int J Comput Appl, vol. 181, no. 1, pp. 25–29, Jul. 2018, doi: 10.5120/ijca2018917395.

[83] C. Y. Suen, "n-Gram Statistics for Natural Language Understanding and Text Processing," IEEE Trans Pattern Anal Mach Intell, vol. PAMI-1, no. 2, pp. 164–172, Apr. 1979, doi: 10.1109/TPAMI.1979.4766902.

[84] L. Egghe, "The Distribution of N-Grams," Scientometrics, vol. 47, no. 2, pp. 237–252, 2000, doi: 10.1023/A:1005634925734.

[85] O. Papakyriakopoulos, S. Hegelich, J. C. M. Serrano, and F. Marco, "Bias in word embeddings," in Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, New York, NY, USA: ACM, Jan. 2020, pp. 446–457. doi: 10.1145/3351095.3372843.

[86] T. Abu-Ain, S. N. H. S. Abdullah, A. Abu, H. Script, K. Bin Omar, and B. Bataineh, "Text Normalization," 2014. [Online]. Available: https://api.semanticscholar.org/CorpusID:207920819

[87] I. Akhmetov, A. Pak, I. Ualiyeva, and A. Gelbukh, "Highly Language-Independent Word Lemmatization Using a Machine-Learning Classifier," Computación y Sistemas, vol. 24, no. 3, Sep. 2020, doi: 10.13053/cys-24-3-3775.

[88] Jude Chukwura Obi, "A comparative study of several classification metrics and their performances on data," World Journal of Advanced Engineering Technology and Sciences, vol. 8, no. 1, pp. 308–314, Feb. 2023, doi: 10.30574/wjaets.2023.8.1.0054.

Classification of Liver Disease Using Conventional Tree-Based Machine Learning Approaches with Feature Prioritization Using a Heuristic Algorithm

Proloy Kumar Mondal[1], Haewon Byeon[2]*
Department of Electronics and Communication Engineering, Khulna University, Khulna, Bangladesh[1]
Department of Digital Anti-aging Healthcare (BK21), Inje University, Gimhae 50834, South Korea[2]

***Abstract*—Liver disease ranks as one of the leading causes of mortality globally, often going undetected until advanced stages. This study aims to enhance early detection of liver disease by employing machine learning models that utilize key health indicators. Utilizing the Indian Liver Patient Dataset (ILPD) from the UCI repository, we developed a predictive model using the CatBoost algorithm, achieving an initial accuracy of 74%. To improve this, feature selection was performed using the Whale Optimization Algorithm (WOA) and Harris Hawk Optimization (HHO), which increased accuracy to 82% and 85% respectively. The methodology involved preprocessing to correct data imbalances and outlier removal through univariate and bivariate analyses. These optimizations highlight the critical features enhancing the model's predictive capability. The results indicate that integrating metaheuristic algorithms in feature selection significantly improves the accuracy of liver disease prediction models. Future research could explore the integration of additional datasets and machine learning models to further refine predictive capabilities and understand the underlying pathophysiology of liver diseases.**

***Keywords*—Liver disease; classification; prediction; CatBoost algorithm; machine learning; optimization algorithm**

I. Introduction

The liver is an important part of the body that conducts functions such as gall generation, chemical detoxification, and a supply of critical proteins for blood [1]. A huge increase in different liver illnesses has been observed the world in recent years. About two million people are diagnosed with liver disease each year, with one million dying from cirrhosis complications and one million from viral hepatitis and hepatocellular carcinoma. Because cause-specific death data is scarce in many places where liver disease is common, notably in Africa, accurate figures are not always accessible. Furthermore, nearly one-third of the world's countries lack reliable mortality statistics. Even in industrialized nations, it is impossible to distinguish the burden of liver disease according to the cause and stage of the disease [2]. Cirrhosis is the 11th leading cause of death worldwide, while liver cancer is the 16th, an estimated 1.16 million and 788,000 people die each year. They are responsible for 3.5 percent of all deaths worldwide [3]. Liver-related deaths accounted for 3% of all deaths worldwide in 2000. They are ranked 13th (cirrhosis) and 20th (liver cancer). However, the effects can be even greater if acute hepatitis and alcohol use are considered major factors. According to these Fig. 1, the liver disease dies over two million people worldwide each year. Due to worldwide population pressure, India accounts for one-fifth (18.3%) of all cirrhosis fatalities while China's contribution is 11 In Central Asia and the Russian Federation, mortality is increasing. In the UK, mortality is increasing, but in France and Italy, it is decreasing. Males are affected by cirrhosis at a higher rate than females all over the world [2]. Refer to Fig. 1. Liver disease and cancer are among the leading causes of death worldwide.

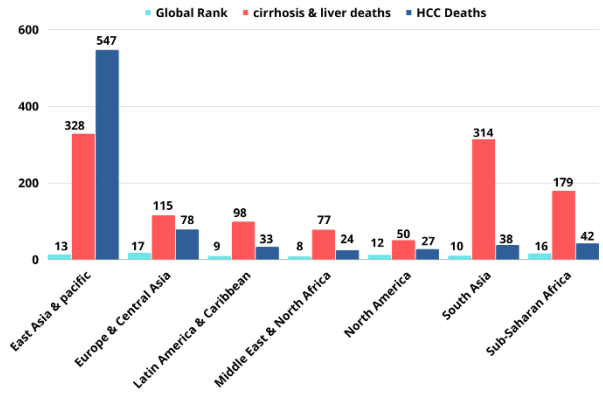


Fig. 1. Global mortality from liver illness and liver cancer.

First, the number of patients with liver disease is increasing every year, however the number of specialist doctors is not increasing. As a result, it has become impossible to diagnose the disease or serve the patient well. It takes a lot of doctors to monitor patients with liver problems which can be very challenging. If we can collect human data in every hospital and every clinic then this process will be much easier for everyone and easy to manage. However, by analyzing the data of these people, we can easily detect the symptoms of the disease if ML is applied. As a result, the number of doctors will be less and the process will be much more comfortable. Artificial Intelligence (AI) includes ML, which allows the system to learn without information. Human inputs and outputs are employed in the training process and prediction accuracy of supervised algorithms, which are used in a variety of classification applications [4]. Fig. 2 shows the five causes of liver failure.

* Corresponding Author

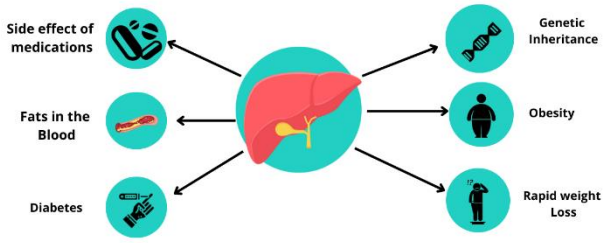


Fig. 2. Five cause of liver failure.

ML is making a significant contribution to healthcare and is expanding day by day. One of the most important problems in healthcare is the growing number of liver patients. The incidence of fatty liver in liver disease is early stage and cirrhosis is the final stage of chronic liver disease which later leads to liver cancer. Many data mining techniques and medical data mining techniques help to present and predict liver disease first and foremost. As a result, the use of this technique greatly reduces the doctor's work.

This paper is organized as follows: Section II provides an overview of related work and highlights the main differences between our work and other existing studies. Section III presents the research methodology, experimental details, configuration and system flowchart. The test results and analysis are discussed in detail in Section IV. Finally, the paper is concluded in Section V.

II. Related Work

Disease prediction has become possible by uncovering hidden features in medical datasets using machine learning algorithms. Different types of datasets, such as blood panels with liver function tests, histologically stained slide images, and the presence of specific molecular markers in blood or tissue samples, have been used to train classifier algorithms to predict liver disease, which provided good accuracy. Machine learning methods described in previous studies have been evaluated for accuracy using a combination of confusion matrix, area under the receiver operating characteristic curve, and k-fold cross-validation. In study [2], the authors studied the prognosis of liver disease and used genetic algorithm combined with XGBoost to predict liver disease and analyzed from the test that the algorithm helped to predict the disease efficiently.

In recent studies, various machine learning algorithms have been applied to improve the diagnosis and prediction of liver-related diseases. In study [3], four machine learning algorithms were tested on ILDP datasets with the Pearson Correlation Coefficient (PCC-FS) optimization technique, resulting in the AdaBoost algorithm achieving a maximum accuracy of 92.19%. Similarly, the study in [4] explored the use of Support Vector Machine (SVM) and Logistic Regression (LR) for diagnosing liver disease, achieving an accuracy of 96%. Additionally, the study in [5] implemented a Random Forest (RF) algorithm to predict liver disease with notable accuracy. Furthermore, the research in [6] focused on the prediction of hepatocellular carcinoma (HCC) using the RF algorithm, achieving an accuracy of 80.86%. These studies collectively highlight the potential of machine learning techniques in enhancing the accuracy of liver disease diagnosis and prediction.

In study [1], the authors in this paper help to identify the patient's liver disease from the data and contribute to the field of medical science so that treatment can be started and the disease can be cured before it becomes severe. To do this they first used the classifier model decision tree (DT) algorithm and achieved the highest accuracy. Then they use seven more classifier algorithms: RF, LR, SVM, K-nearest neighbors (KNN), linear discriminant analysis, AdaBoost, and gradient boosting. Then they used the least absolute shrinkage and selection operator (LASSO) feature selection technique to achieve better accuracy.

Furthermore, recent research has delved into various machine learning techniques to enhance the diagnosis and prediction of liver-related diseases. In study [7], a diagnostic system for chronic liver infections was developed using six classifiers: Logistic Regression (LR), Random Forest (RF), Decision Tree (DT), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Naive Bayes (NB), with LR achieving the highest accuracy at 75%. Similarly, the study in [8] utilized LR, SVM, and KNN for liver disease prediction, identifying LR as the most effective. Dhamodharan et al. [9] focused on predicting cirrhosis, liver cancer, and hepatitis, employing Naive Bayes and the FT Tree algorithm, with Naive Bayes providing the highest accuracy. Rosalina et al. [10] used SVM and the Wrapper method for hepatitis prognosis, effectively removing noise features before classification and achieving optimal results by combining these methods. Soliman et al. [11] introduced a hybrid classification system for HCV detection, utilizing Least Squares Support Vector Machine (LS-SVM) and Modified Particle Swarm Optimization (PSO). With Principal Component Analysis (PCA) for feature extraction and a modified PSO for parameter optimization, their method outperformed other systems in accuracy using HCV benchmark data from the UCI repository. Lastly, in study [12], NB and SVM algorithms were applied for liver disease prediction, with SVM achieving the highest accuracy. Collectively, these studies highlight the significant role of machine learning in enhancing the precision and effectiveness of diagnostics for liver diseases.

III. Methodology

This suggested model uses data from machine learning Indian Liver Patient Dataset (ILPD) that has been taken from the UCI Repository to predict the disease in multiple patients with liver disease. To begin, pre-processed data is used to create "clean" data. The feature extraction approach selects the relevant data from all of the dataset's attributes in order to improve accuracy by using only relevant data. After then, the algorithms and data used to classify the objects were examined. CatBoost classifier Algorithm is used to classify the data throughout the analysis process. Performance is evaluated based on the classification findings. We then employed optimization methods, such as the whale Optimization algorithm, in order to improve our results even further. Algorithms are compared on accuracy, sensitivity, precision and f1-scores in order to determine the best performing algorithm for the system's performance. Fig. 3 depicts the system's overall working procedure.

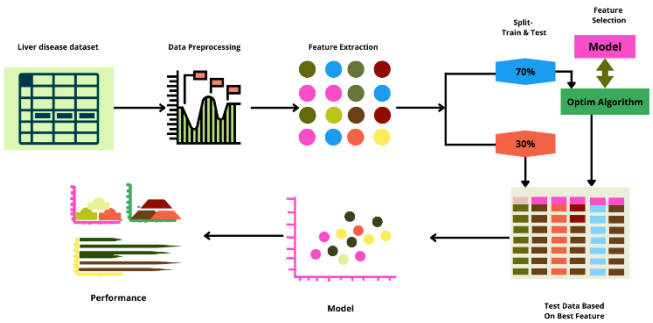


Fig. 3. Working procedure.

1) Dataset description: This dataset was collected from the northeastern Andhra Pradesh of India. In addition, this dataset is publicly available in the UCL machine learning repository [13]. There are 583 patients in the ILPD dataset which 441 are males and 142 are females. Anyone over the age of 89 is reported as having an age of 90. There is also a selector field to determine whether the patient having liver disease or not. Non-LD patients (0) total 167, whereas LD patients (1) total 416. Attribute properties of the dataset include multivariate, integer, and real values. Table I represented the dataset contains a total of 11 specific parameters, out of which we selected 10 parameters for our analysis and 1 was used as the target class. These data are used to train and test the models, and the models' performance is assessed based on their own output. In addition, we have divided the dataset into two parts: 70% for training and 30% for testing. Thus, we have 408 samples in our training set and 175 samples in our validation set. In Fig. 4 the dataset's distribution is displayed.

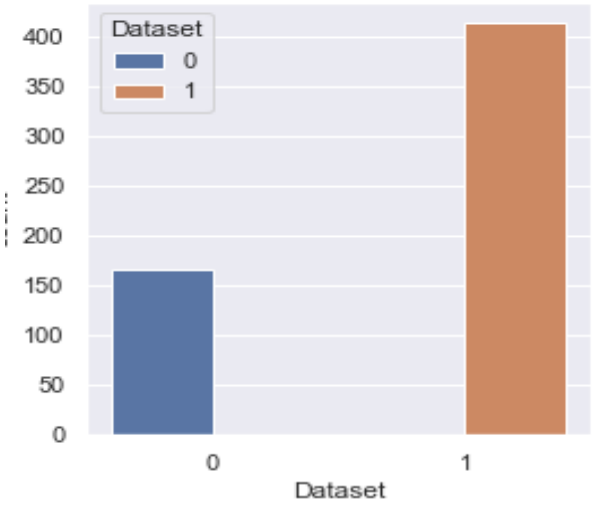


Fig. 4. Dataset description.

TABLE I. DESCRIPTION OF VARIABLES

Features No	Dataset Information	
	Features Name	***Description***
1	Age	Age of the patient
2	Gender	Gender of the patient
3	TB	Total Bilirubin
4	DB	Direct Bilirubin
5	Alkphos	Alkaline Phosphotase
6	Sgpt	Alamine Aminotransferase
7	Sgot	Asparatate Aminotransferase
8	TP	Total Proteins
9	ALB	Albumin
10	AG Ratio	Albumin and Globulin Ratio

2) Data Preprocessing: As stated in the preceding paragraph, the dataset referred to has flaws and scattered data. Pre-processing has been done so that we can get the most out of this dataset. We manually corrected any incorrect data by going through the dataset and looking for any anomalies. When there are no values to fill in, the median of a feature is used. However, Information is extracted from sources and collected in the form of data or discrete analytical data. Each attribute acts as a variable and each instance has specific attributes. Liver disease is predicted using a dataset, which is created through data collection and pre-processing methods. The dataset helps us diagnose the disease based on its various parameters. 10 features are considered to get accurate results in the dataset of the proposed work. Classification is a process of data mining consisting of problem identification. Best performance-based prediction is provided by observing liver disease characteristics in patients and using machine learning algorithms.

3) Classification and Performance Metrics: Dorogush et al. [14] developed CatBoost in 2018 based on improvements to XGBoost. Yandex released CatBoost, an open-source machine learning algorithm, in 2017, which is still relatively new [15]. The model is built using a training dataset, which consists of a set of objects with known features and labels. The training dataset is also referred to as the "data set". The validation dataset is only used to evaluate the effectiveness of training and contains similarly organized data, but is not used for training. The basis of CatBoost is gradient-boosted decision trees, where a series of decision trees is generated sequentially during training. Each subsequent tree is built with less damage than the previous tree. The initialization parameter determines how many trees will grow. To prevent overfitting, overfitting detectors are used which stop tree growth when activated. We used CatBoost algorithm to classify liver diseases.

4) Features selection: Feature selection is an important process in machine learning, where the most important features (variables or predictors) are selected from the dataset, which play a role in predicting the target variable. This is helpful in reducing dataset dimensions, improving model performance,

and reducing the likelihood of overfitting. In this study, we used two metaheuristic optimization algorithms such as, WOA and HHO. It is well-known swarm-based metaheuristic method for feature selection.

5) Whale optimization algorithm (WOA): WOA is a metaheuristic optimization algorithm that was proposed by Mirjalili and Lewis [16]. The bubble-net hunting method utilized by humpback whales is modelled after and imitated by the algorithm. The entire process can be broken down into three stages: the first stage involves encircling the prey, the second stage involves bubble-net foraging (the exploitation phase), and the third stage involves searching for prey (exploration phase). To better understand these three stages of the WOA strategy we present in Fig. 5. An initial solution candidate is chosen at the beginning of the algorithm, and their fitness is determined with the help of a function. During each cycle of the iterative process, the solution set is either updated through the shrinking encircling mechanism or the spiral updating mechanism (exploitation phase), with the choice of the mechanism being determined by a probability p. In addition, the shrinking encircling mechanism can either update the new solution set so that it is closer to the global best solution or it can use a random search agent. This is determined by a coefficient called A. The equation for the coefficient is presented in the following example:

$$\boldsymbol{A = 2a.r - a} \quad (1)$$

where, a is a random vector in the range [0, 1] and r is a vector that decreases linearly from 2 to 0 over the course of the generation. Because the update that leads to a random agent conducts a worldwide search, the subsequent phase is known as the exploration phase. In Algorithm 1, the pseudo-code for feature selection using WOA is presented.

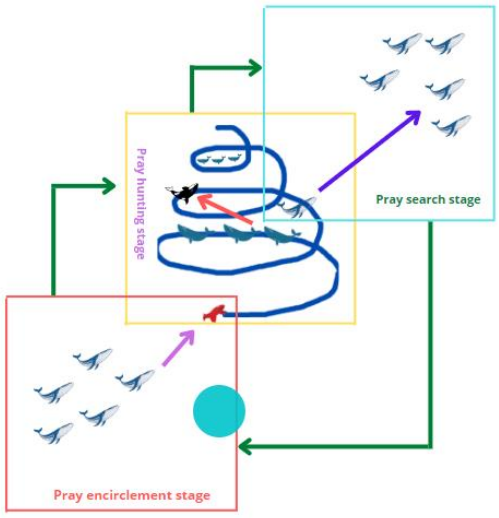


Fig. 5. Whale Optimisation Algorithm.

Algorithm 1: Feature Selection Using WOA

Create the first group of n whales xi (1,2,3……., n)
Set the iteration counter $t_{counter}$ = 0
figure out how fit each whale is.
figure out which whale is the fittest, i.e., Y_{best}
for each whale **do**
  Decode whale position
  Find out the fitness value (F1 score) using
  Feature set using CatBoost classifier
end
while ($t_{counter}$< Max_Iter number **do**)
for each whale **do**
a new parameter has been updated
if (p< 0.5) **then**
if (|A|< 1) **then**
update the current position of the whale
if (|A > 1) then
else
if (|A| ≥ 1) **then**
select the random position X_{rand}
using the mechanism, adjust the whale's
end
end
else
if (p≥0.5) **then**
update the whale's position towards the global
end
end
end
for each while **do**
Decode feature set from whale position
Calculate the fitness value using CatBoost classifier
end
update X* if a set of the best solutions exists
t = t + 1
end
Save the best feature set

6) Harris hawk optimization algorithm (HHO): Haidari and his colleagues (2019) [17] proposed the use of a new metaheuristic algorithm known as the Harris Hawk Optimization (HHO). HHO imitates the notions of Harris hawks in order to investigate the diverse prey, surprise pounces, and attack techniques used by Harris hawks in the natural world. In HHO, the candidate solutions are symbolized by hawks, and the best solution, which is also referred to as the nearly optimum solution, is referred to as prey. The Harris hawks make use of their keen vision to locate their prey and

then execute a surprise attack in order to successfully capture the target they have located [18].

In most cases, HHO is modeled into two distinct phases: the exploitation phase, and the exploration phase. The HHO algorithm may be used for either exploration or exploitation, and after it has been used for either purpose, the exploration behavior can be altered dependent on the amount of energy that the prey is able to escape with. It is possible to mathematically determine the escape energy of prey using the Eq. (2) to (3):

$$E = 2E_0(t - \frac{t}{T}) \quad (2)$$

$$E_0 = 2r - 1 \quad (3)$$

where t represents the current iteration, T represents the maximum number of iterations, E0 represents the initial energy that is created at random in the range [1,1], and r represents a random value that falls in the range [0, 1]. In Algorithm 2, the pseudo-code for feature selection using HHO is presented.

Algorithm 02: Feature Selection Using HHO algorithm

Inputs: N is the population size, while T is the maximum

Outputs: Rabbit's position and fitness value initialize

While (stopping conditions is not met) **do**

for (each hawk (X_i)) **do**

Update the initial energy E0 and jump strength j

If (|E|≥) **then**

Update the location vector

If (|E|<1) **then**

if (r≥0.5 and |E|≥0.5) **then**

Update the location vector

else if (r≥ 0.5 and |E|<0.5) **then**

Update the location vector

else if (r <0.5 and |E|≥0.5) **then**

Update the location vector

else if (r <0.5 and |E|<0.5) **then**

Update the location vector

Return X_{rabbit}

Our feature subset was optimized using the WOA and HHO to minimize the number of features while also increasing prediction accuracy. The feature subsets are selected from the WOA and HHO solution sets. The solution set's value indicates whether or not to choose a feature. The CatBoost algorithm was then used to classify liver disease based on the feature subsets. F1 score true and the predicted class is used as the value of an agent's fitness. The advantage of F1 score is that it helps to provide harmonic mean, accuracy and recall. Because of this, it is harsher on values at the extremes. Overall, an agent's fitness value is referred to as the F1 score (feature subset). The WOA and HHO take the best fitness value as a baseline and update the position in accordance with the methodology used by each. This iteration is repeated until a predetermined end point is achieved.

IV. Results and Analysis

The results of classifier algorithm are detailed in Section A on the experimental evaluation of our proposed CatBoost model. In addition, the relevance of the feature selection with two metaheuristic algorithms mentioned in Section B.

A. Performance Analysis

In the previous section, we discussed the various contents of the dataset. We used a technique and method to classify the class samples in this dataset. In this section, we will present the research findings. Following the described procedure, we set up a classification model where the CatBoost model was used for training the model and the rest of the samples were used for testing. We have split our dataset in the ratio of 70:30. In this paper we have proposed classification algorithms like CatBoost algorithm. However, after finishing data preprocessing steps without applying feature selection techniques, algorithms are used for classification. Our model provided and accuracy of 74%. Besides accuracy, various evaluation criteria such as precision, recall, and f1-score values are compared in Table II.

TABLE II. Classification Report of our Model

Class	Precision	Recall	F1-Score
Non-LD	0.50	0.37	0.42
LD	0.80	0.87	0.84

In Fig. 6 shows a confusion matrix, which is used as a powerful tool for evaluating the performance of classification models in machine learning. This matrix clearly shows how the model classified the data into actual and predicted categories. It divides the results into four different categories, providing important insights into the model's strengths and weaknesses: true positives, true negatives, false positives, and false negatives. In this confusion matrix, the result of a binary classification task, where there are two possible outcomes - "0" and "1". The actual value, or true label, is displayed along the vertical axis and the model predicted value along the horizontal axis. The number in each cell shows how many examples fall into that particular category. In this model, it correctly predicted class "1" in 76 instances (true positives) and correctly assigned class "0" in 11 instances (true negatives). However, the model incorrectly classified class "0" as "1" (false positive) in 19 instances and class "1" as "0" (false negative) in 11 instances. These errors show where the model is having trouble, especially distinguishing between two classes. The confusion matrix gives a clear picture of the prediction performance of the model, which helps us better understand the accuracy, precision, and other evaluation metrics of the model.

Fig. 7 shows a receiver operating characteristic (ROC) curve, which is commonly used to evaluate the performance of binary classification models. This curve depicts the relationship between the true positive rate (TPR) and the false positive rate (FPR) at different threshold settings, giving an understanding of how well the model is able to distinguish between the two classes. The dashed diagonal line represents the performance of a random classifier and serves as a baseline with an AUC of 0.5. The orange curve shows the actual performance of the model, which lies above the diagonal, indicating that the model is giving

better results than the random guess. An AUC value of 0.82 suggests that the model is able to distinguish between positive and negative classes and has an 82% chance of correctly identifying a positive instance.

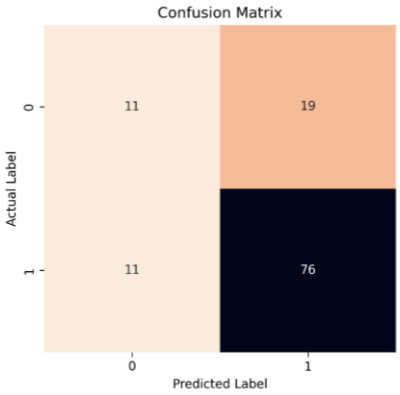


Fig. 6. Confusion matrix.

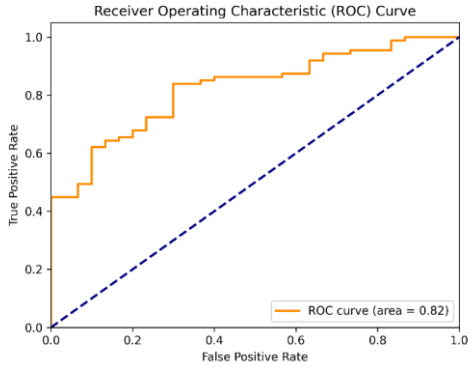


Fig. 7. ROC curves of various classes.

B. Feature Selection Outcome

We applied the FS algorithm to increase the accuracy of the CatBoost classifier and reduce the dimensionality of the features. The FS process was carried out using two metaheuristic algorithms named WOA and HHO. A fitness function is constructed based on the performance evaluation of the CatBoost classifier. Other performance metrics, such as F1 score, precision and recall, are also taken into account. We checked the 'p_r' parameter of WOA and HHO between 0.21, indicating the learning rate potential. A value of 0.25 was identified as optimal for 'p_r', while values were 50 for 'pop_size' and 'epoch' parameters. Various 'p_r' values are shown in Table III, which highlights the set of features returned from the WOA and HHO processes.

TABLE III. BEST FEATURE SOLUTION

Optimization Algorithm	Feature Name	Optimization Algorithm	Feature Name
HHO	Total Bilirubin	WOA	Age
	Direct Bilirubin		Total_Bilirubin
	Alamine Aminotransferase		Alamine Aminotransferase

Table III outlines the best features obtained from two optimization algorithms, HHO and WOA, which have been used to identify the most important features for liver disease detection. Selected parameters for HHO include Total Bilirubin, which is important in evaluating liver function because high bilirubin levels usually indicate liver problems. It also selects Direct Bilirubin and Alanine Aminotransferase, where it is an enzyme that increases in the blood when liver cells are damaged. On the other hand, the WOA algorithm identified Age, Total Bilirubin, and Alanine Aminotransferase as important characteristics that are influential in liver disease. Both algorithms selected Total Bilirubin and Alanine Aminotransferase, indicating their high importance in the diagnosis of liver disease, and proved to be important features for accurate detection.

In Fig. 8, the confusion matrix of the HHO algorithm shows that the model correctly classified 82 cases as true negative (TN) and 96 cases as true positive (TP). However, it misclassified 17 cases as false positive (FP) and 3 cases as false negative (FN). The HHO model achieved 85% accuracy, indicating strong performance in liver disease detection. A particularly low number of false negatives makes the model useful in medical diagnosis, as it indicates that very few cases of true disease are missed.

In Fig. 9, the confusion matrix of the WOA shows that the model correctly classified 13 cases as True Negative (TN) and 84 cases as True Positive (TP). At the same time it misclassified 17 cases as false positive (FP) and 3 cases as false negative (FN). The WOA model achieved 82% accuracy. Although the number of false negatives is low, the model lags slightly behind HHO in detecting true negatives, showing slight weakness in detecting cases without disease.

On the other hand, the previously used CatBoost algorithm achieved only 74% accuracy, which is significantly lower than HHO and WOA. This proves these two optimization algorithms more effective in liver disease detection. Overall, the HHO model shows the best performance in liver disease detection, as it is able to maintain a good balance between high accuracy and true positive and true negative detection.

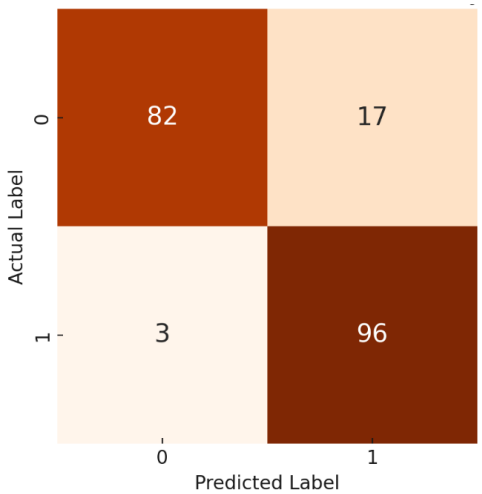


Fig. 8. Confusion matrix for HHO.

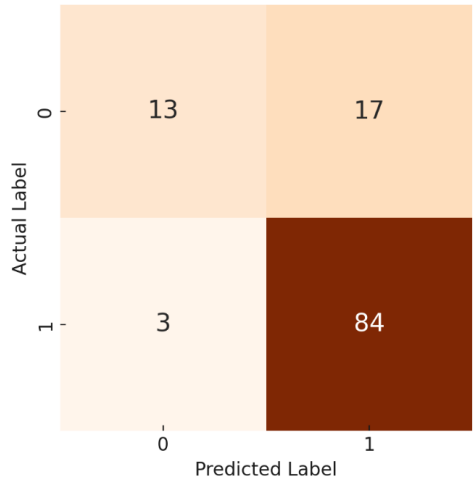


Fig. 9. Confusion matrix for WOA.

V. Conclusion

This study successfully identified key features for liver disease detection using two optimization algorithms: Harris Hawk Optimization (HHO) and Whale Optimization Algorithm (WOA). Both algorithms highlighted Total Bilirubin and Alanine Aminotransferase as critical indicators for diagnosing liver disease. Additionally, Direct Bilirubin and Age were also recognized as significant factors in assessing liver function. Our findings align with existing research while offering new insights that can enhance diagnostic accuracy using clinical data. These results underscore the efficacy and potential of machine learning models combined with optimization algorithms in advancing liver disease diagnosis. This work contributes to the growing evidence that such computational approaches can significantly improve early detection and intervention strategies in healthcare. Future research could explore integrating additional datasets and machine learning techniques to further refine these predictive models and expand their applicability across diverse populations.

Fund

This research Supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF- RS-2023-00237287, NRF-2021S1A5A8062526) and local government-university cooperation-based regional innovation projects (2021RIS-003).

References

[1] S. Afrin et al., "Supervised machine learning based liver disease prediction approach with LASSO feature selection," Bull. Electr. Eng. Inform., vol. 10, no. 6, pp. 3369–3376, 2021.

[2] M. A. Kuzhippallil, C. Joseph, and A. Kannan, "Comparative analysis of machine learning techniques for indian liver disease patients," in 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2020, pp. 778–782.

[3] M. F. Rabbi, S. M. Hasan, A. I. Champa, M. AsifZaman, and M. K. Hasan, "Prediction of liver disorders using machine learning algorithms: a comparative study," in 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT), IEEE, 2020, pp. 111–116.

[4] C. Geetha and A. R. Arunachalam, "Evaluation based Approaches for Liver Disease Prediction using Machine Learning Algorithms," in 2021 International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2021, pp. 1–4.

[5] S. Ambesange, A. Vijayalaxmi, R. Uppin, S. Patil, and V. Patil, "Optimizing Liver disease prediction with Random Forest by various Data balancing Techniques," in 2020 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), IEEE, 2020, pp. 98–102.

[6] S. Rajesh, N. A. Choudhury, and S. Moulik, "Hepatocellular carcinoma (HCC) liver cancer prediction using machine learning algorithms," in 2020 IEEE 17th India Council International Conference (INDICON), IEEE, 2020, pp. 1–5.

[7] A. S. Rahman, F. J. M. Shamrat, Z. Tasnim, J. Roy, and S. A. Hossain, "A comparative study on liver disease prediction using supervised machine learning algorithms," Int. J. Sci. Technol. Res., vol. 8, no. 11, pp. 419–422, 2019.

[8] A. S. Singh, M. Irfan, and A. Chowdhury, "Prediction of liver disease using classification algorithms," in 2018 4th international conference on computing communication and automation (ICCCA), IEEE, 2018, pp. 1–3.

[9] S. Dhamodharan, "Liver disease prediction using bayesian classification," 2016.

[10] A. H. Roslina and A. Noraziah, "Prediction of hepatitis prognosis using support vector machines and wrapper method," in 2010 Seventh International Conference on Fuzzy Systems and Knowledge Discovery, IEEE, 2010, pp. 2209–2211.

[11] O. S. Soliman and E. A. Elhamd, "Classification of hepatitis C virus using modified particle swarm optimization and least squares support vector machine," Int. J. Sci. Eng. Res., vol. 5, no. 3, p. 122, 2014.

[12] S. Vijayarani and S. Dhayanand, "Liver disease prediction using SVM and Naïve Bayes algorithms," Int. J. Sci. Eng. Technol. Res. IJSETR, vol. 4, no. 4, pp. 816–820, 2015.

[13] "Indian Liver Patient Records." Accessed: Jun. 23, 2022. [Online]. Available: https://www.kaggle.com/uciml/indian-liver-patient-records

[14] A. V. Dorogush, V. Ershov, and A. Gulin, "CatBoost: gradient boosting with categorical features support," Oct. 24, 2018, arXiv: arXiv:1810.11363. doi: 10.48550/arXiv.1810.11363.

[15] S. Thiesen, "CatBoost regression in 6 minutes," Medium. Accessed: Jun. 27, 2022. [Online]. Available: https://towardsdatascience.com/catboost-regression-in-6-minutes-3487f3e5b329

[16] S. Mirjalili and A. Lewis, "The whale optimization algorithm," Adv. Eng. Softw., vol. 95, pp. 51–67, 2016.

[17] A. A. Heidari, S. Mirjalili, H. Faris, I. Aljarah, M. Mafarja, and H. Chen, "Harris hawks optimization: Algorithm and applications," Future Gener. Comput. Syst., vol. 97, pp. 849–872, 2019.

[18] J. Too, A. R. Abdullah, and N. Mohd Saad, "A new quadratic binary harris hawk optimization for feature selection," Electronics, vol. 8, no. 10, p. 1130, 2019.

Optimizing Deep Learning for Diabetic Retinopathy Diagnosis

Krit Sriporn[1], Cheng-Fa Tsai[2]*, Li-Jia Rong[3], Paohsi Wang[4], Tso-Yen Tsai[5], Chih-Wen Chen[6]
Department of Digital Technology, Suratthani Rajabhat University, Surat Thani, Thailand[1]
Department of Management Information Systems, National Pingtung University of Science and Technology, Pingtung, Taiwan[2, 3]
Department of Food and Beverage Management, Cheng Shiu University, Kaohsiung, Taiwan[4]
Chunri Township Public Health Center-Public Health Bureau, Pingtung County Government, Pingtung, Taiwan[5]
Department of Emergency Medicine, Pingtung Christian Hospital, Pingtung, Taiwan[6]

***Abstract*—The detection of diabetic retinopathy traditionally requires the expertise of medical professionals, making manual detection both time- and labor-intensive. To address these challenges, numerous studies in recent years have proposed automatic detection methods for diabetic retinopathy. This research focuses on applying deep learning and image processing techniques to overcome the issue of performance degradation in classification models caused by imbalanced diabetic retinopathy datasets. It presents an efficient deep learning model aimed at assisting clinicians and medical teams in diagnosing diabetic retinopathy more effectively. In this study, image processing techniques, including image enhancement, brightness correction, and contrast adjustment, are employed as preprocessing steps for fundus images of diabetic retinopathy. A fusion technique combining color space conversion, contrast limited adaptive histogram equalization, multi-scale retinex with color restoration, and Gamma correction is applied to highlight retinal pathological features. Deep learning models such as ResNet50-V2, DenseNet121, Inception-V3, Xception, MobileNet-V2, and InceptionResNet-V2 were trained on the preprocessed datasets. For the APTOS-2019 dataset, DenseNet121 achieved the highest accuracy at 99% for detecting diabetic retinopathy. On the Messidor-2 dataset, InceptionResNet-V2 demonstrated the best performance, with an accuracy of 96%. The overall aim of this research is to develop a computer-aided diagnosis system for classifying diabetic retinopathy.**

Keywords*—Diabetic retinopathy; deep learning; image processing technologies; imbalanced image dataset; computer aided diagnosis

I. Introduction

Diabetes is a chronic disease and a major public health issue that significantly affects quality of life due to its rising incidence. According to the International Diabetes Federation's Diabetes Atlas, 537 million people worldwide have diabetes, and this number is expected to increase to 629 million by 2045. Most cases occur in low-to-middle-income countries, with more than half undiagnosed. The World Health Organization predicts that diabetes will become the seventh leading cause of death globally.

A common and often unnoticed complication of diabetes is diabetic retinopathy, which progresses slowly but can severely impact patients' quality of life, affecting their families, the economy, and society. The condition necessitates comprehensive care and regular screening. Diabetic retinopathy involves changes to the retina caused by diabetes, as elevated blood sugar levels lead to nerve and blood vessel damage. This results in complications such as retinal swelling, detachment, bleeding, and vision loss [1].

Many countries face shortages in medical resources and ophthalmologists, particularly in rural or remote areas, where patients may not receive timely diagnosis and treatment due to the uneven distribution of healthcare resources. Traditional manual diagnosis by specialists also presents challenges, as it can be time-consuming and early-stage symptoms are often subtle, increasing the risk of misdiagnosis even by a single expert. As a result, monitoring and treating diabetic retinopathy demands considerable time and human resources, while training professional ophthalmologists entails significant costs.

Given these challenges, recent years have seen numerous studies [2–4] proposing automated detection methods to assist medical teams and ophthalmologists in diagnosing diabetic retinopathy more efficiently. Automated diagnostic systems also help address the issue of low screening efficiency in areas with limited medical resources.

Research on automating diabetic retinopathy detection has focused on areas such as medical image enhancement, machine learning, and deep learning-based image recognition. Scholars have reviewed these studies, discussing the advantages and disadvantages of various methods and the factors that may influence recognition results.

The quality of fundus images for diabetic retinopathy is often inconsistent, making image preprocessing a crucial step in many studies. Different research efforts employ appropriate preprocessing techniques based on their specific objectives [5].

This study aims to develop a computer-aided diagnosis system for detecting diabetic retinopathy by addressing the imbalance in data characteristics within the diabetic retinopathy dataset and using categorical focal loss as the loss function instead of categorical cross-entropy loss. The research utilizes the Asia Pacific Tele-Ophthalmology Society-2019 Blindness Detection (APTOS-2019) and Messidor-2 datasets, containing 3,662 and 1,744 images respectively, to train and compare the performance of various convolutional neural network models in diabetic retinopathy classification against other studies. Six convolutional neural network (CNN) models ResNet50-V2, DenseNet121, Inception-V3, Xception, MobileNet-V2, and

InceptionResNet-V2 were used to determine the most suitable model for training with these datasets.

The remaining content research is organized as follows: materials and methodology are presented in Section II. implementation details are shown in Section III. Section IV presents the experimental results, while Section V presents the discussion, and finally, Section VI concluded the paper.

II. Materials and Methodology

This study divides the experimental procedures into four sections: image collection, image preprocessing, deep learning model training, and system performance evaluation. The following subsections detail the processes and methods involved in each step.

The first step is to confirm the dataset accessible under the experimental conditions. Due to concerns regarding medical privacy, diabetic retinopathy datasets often require annotation and grading by ophthalmic experts. To address these issues, a practical approach is to use existing publicly available datasets for experimentation. Public datasets offer several advantages: many previous studies have utilized them to evaluate their systems. By using the same publicly available datasets, researchers can assess the novelty of their approach and compare it with prior work. This also enhances the comparability and credibility of the current study.

The APTOS-2019 and Messidor-2 datasets are foundational resources in artificial intelligence research for the detection and classification of diabetic retinopathy. These datasets contain extensive collections of eye images, each annotated with a specific severity level of diabetic retinopathy, making them instrumental for training and evaluating computer vision models aimed at accurate disease diagnosis.

This research applies a variety of image processing techniques and deep learning models to train a classifier on the diabetic retinopathy dataset, as described in [5]. The classifier is responsible for categorizing images into five distinct stages of diabetic retinopathy: No Diabetic Retinopathy (NDR), Mild Diabetic Retinopathy (MiDR), Moderate Diabetic Retinopathy (MoDR), Severe Diabetic Retinopathy (SDR), and Proliferative Diabetic Retinopathy (PDR). Visual representations of these five stages are provided in Fig. 1.

In addition, the diabetic retinopathy datasets face issues with class imbalance. This imbalance can negatively affect system performance, as certain classes in the dataset may be overrepresented or underrepresented. As a result, the model tends to predict the more frequent classes more easily, while the less frequent classes are harder to predict and are more likely to be misclassified as one of the dominant classes.

In the second step, various image processing techniques were employed, including RGB color space conversion, commission internationale de l'eclairage (CIELAB), contrast-limited adaptive histogram equalization (CLAHE), multi-scale retinex with color restoration (MSRCR), and Gamma correction. These techniques enhance image features to improve the neural network's ability to learn features effectively. Following this, the dataset was split into training, validation, and testing sets, with 80% allocated to training and 20% for testing, as shown in Table I.

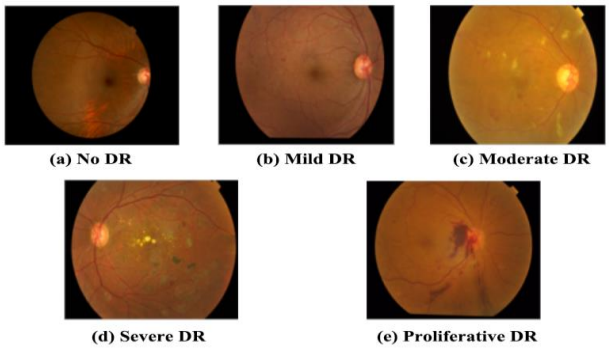


Fig. 1. Classification of the five levels of diabetic retinopathy.

TABLE I. Distribution of Image Quantities Across Disease Categories

Dataset Name	categories					Total
	NDR	MiDR	MoDR	SDR	PDR	
APTOS-2019	1,805	370	999	193	295	3,662
Messidor-2	1,020	264	347	77	36	1,744

After splitting the dataset, the training set undergoes data augmentation techniques, including horizontal flipping, vertical flipping, and pixel value scaling. Before being fed into the convolutional neural network (CNN) models for training, each image is resized to the optimal dimensions required by the model.

Fig. 2 presents a schematic representation of the hybrid image enhancement method used in this investigation, based on findings from previous studies [6–11]. Our proposed technique integrates the CLAHE algorithm with enhancements to the CIELAB color space. Empirical results show that this combined approach produces better results compared to using the hue, saturation, and value (HSV) color space or other color space transformations. In this framework, CLAHE is applied exclusively to the luminance (L) channel of the CIELAB color space. The process of splitting the V channel refers to isolating the Value component from the HSV color space, which allows for further processing or enhancement tasks such as sharpening or brightening.

In medical imaging, particularly in retinal imaging, researchers often convert images to the CIELAB color space to separate luminance (L channel) from color information (a and b channels). Subsequently, CLAHE is applied to enhance the luminance component in CIELAB, preserving the original color information. This approach effectively enhances image details without compromising color fidelity. The synergistic combination of CIELAB and CLAHE provides a robust solution for improving image clarity and quality, particularly when processing high-detail images.

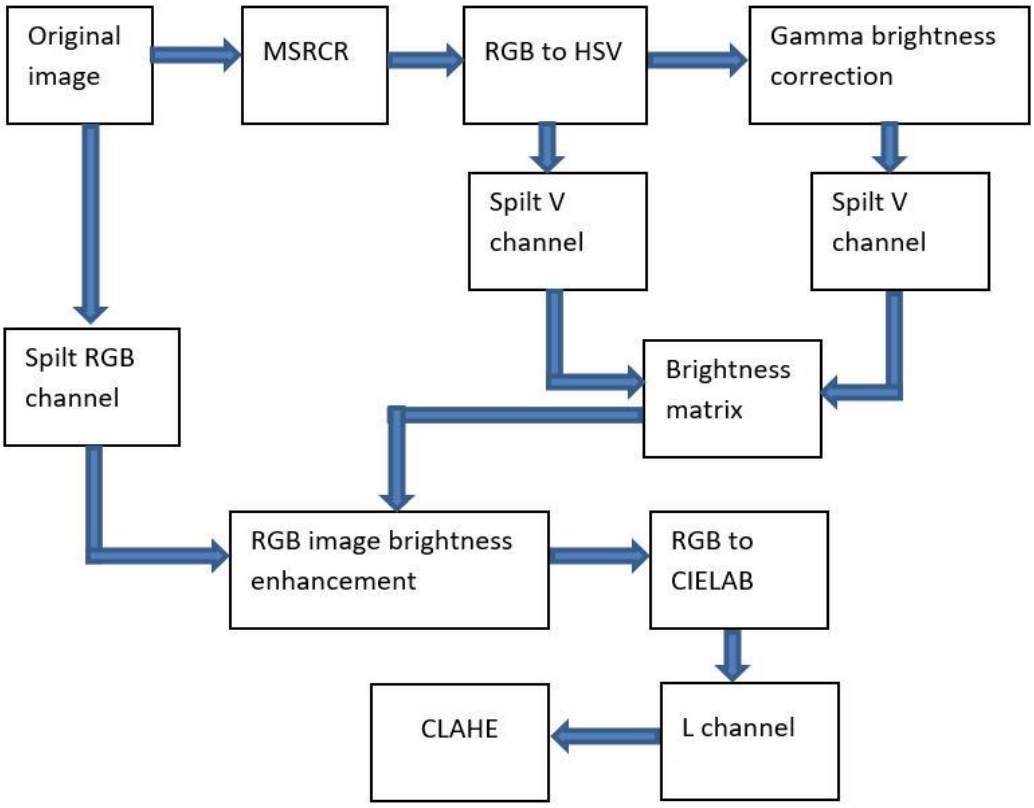


Fig. 2. The schematic of hybrid image enhancement method.

Fig. 3 presents a schematic of alternative image enhancement methods, which are standard preprocessing techniques used in diabetic retinopathy severity grading. The multi-scale retinex with color restoration (MSRCR) transformation is a pivotal aspect of the hybrid image enhancement strategy adopted in this research. MSRCR has been extensively applied in medical image segmentation and classification, including retinal vessel segmentation and arterial-venous classification, as evidenced by studies [12–15].

Data augmentation is a technique that enhances the amount of data by synthesizing new images from an original dataset. This method not only increases the dataset's size but also offers additional advantages, such as more efficient use of computer memory during model training and a regularization effect that helps mitigate overfitting. Common techniques for data augmentation include horizontal and vertical flipping, resizing, cropping, shifting, and scaling pixel values. While these transformations create variations of the original image that may look different to the model, they still allow humans to recognize them as the same image. This principle of generating multiple images from a single original image is the foundation of data augmentation [16].

In the third step, this study employs deep learning models, including ResNet50-V2 and InceptionResNet-V2, which were trained on diabetic retinopathy image datasets processed in the second step. Various CNN models were combined with image enhancement methods to identify the optimal combination and compare the advantages of each. The architecture of the models used in this study is illustrated in Fig. 4. All pretrained deep learning models mentioned serve as base models in this research, utilizing pretrained weights from the ImageNet image database. A custom dense neural network is connected beneath the base model, with each final layer of the CNNs configured to use a SoftMax activation function for five-class classification.

To ensure that model training achieves the expected classification performance, continuous testing and parameter tuning are conducted. Ultimately, other public datasets are used to validate the system's performance and the model's reliability. The evaluation metrics used in this study are described below, sourced from studies related to diabetic retinopathy severity classification [5, 17, 18]. Table II presents the definitions of True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN).

TABLE II. MEANINGS OF TP, TN, FP, FN

Indicator Names:	Descriptions:
True Positive (TP)	True Positive (TP): Predicted positive and predicted correctly.
True Negative (TN)	True Negative (TN): Predicted negative and predicted correctly.
False Positive (FP)	False Positive (FP): Predicted positive but predicted incorrectly.
False Negative (FN)	False Negative (FN): Predicted negative but predicted incorrectly.

Accuracy is used to calculate the proportion of correctly predicted samples by the model among the total number of samples in a classification task. It is calculated as shown in Eq. (1).

$$\text{Accuracy} = （TP+TN）/\text{Total} \quad (1)$$

Precision is the proportion of correctly identified samples of a particular class among all samples predicted to belong to that class by the model. It is calculated as shown in Eq. (2).

$$\text{Precision} = TP/（TP+FP） \quad (2)$$

Sensitivity, also known as the True Positive Rate or Recall, refers to the proportion of true positive samples that are correctly predicted by the model among all actual positive samples. It is calculated as shown in Eq. (3).

$$\text{Sensitivity} = TP/（TP+FN） \quad (3)$$

Specificity, also known as the True Negative Rate, refers to the proportion of true negative samples that are correctly predicted by the model among all actual negative samples. It is calculated as shown in Eq. (4).

$$\text{Specificity} = TN/（FP+TN） \quad (4)$$

Additionally, the diabetic retinopathy datasets exhibit issues with class imbalance. This problem can adversely affect system performance, as certain classes in the dataset may be overrepresented while others are underrepresented. As a result, the more frequent classes are easier to predict, whereas the less frequent classes are harder to predict and more likely to be misclassified by the model as one of the more frequent classes.

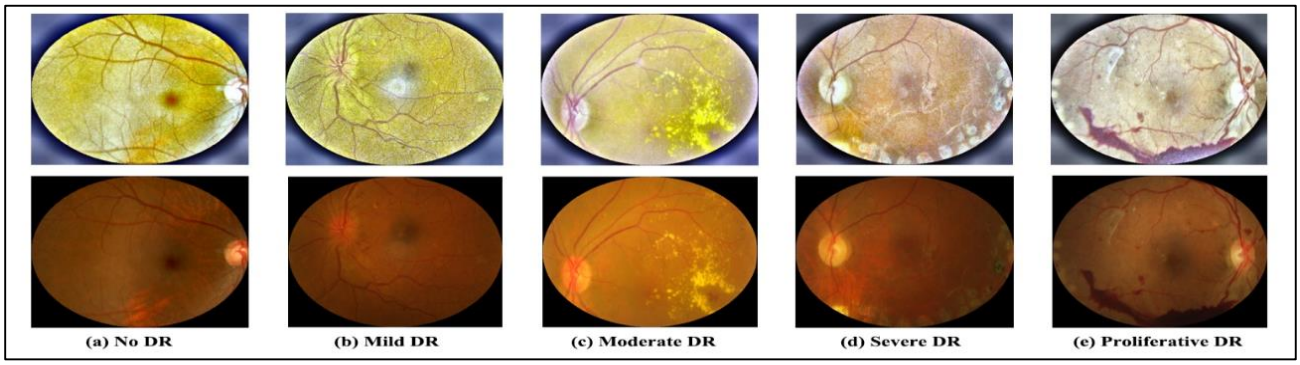


Fig. 3. The results of image enhancement methods.

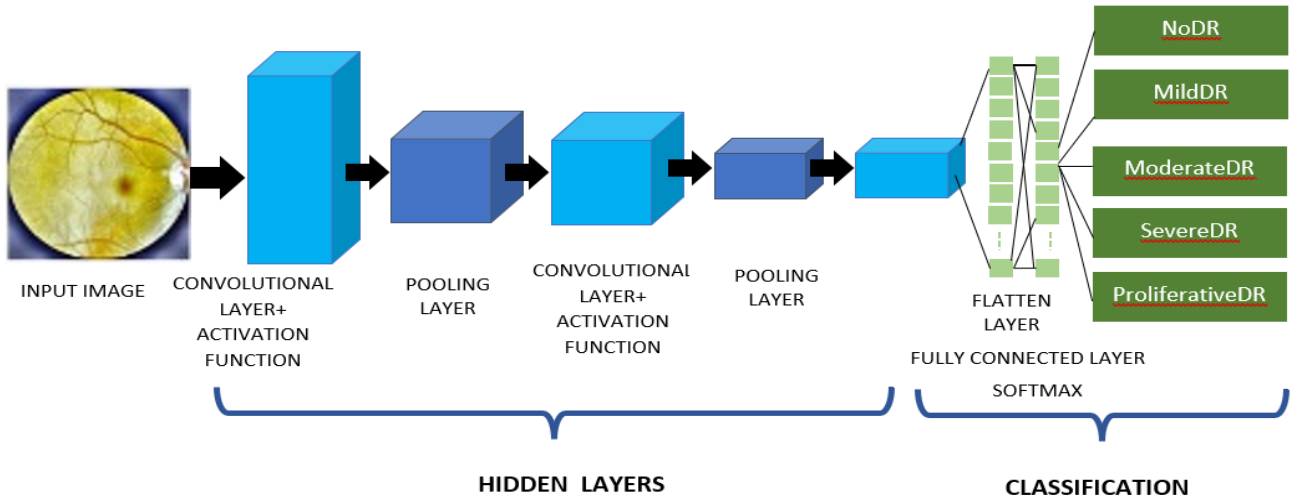


Fig. 4. Deep learning model.

III. Implementation Details

A. Experimental Environment

The configuration of the experimental environment in this paper is shown in Table III. The computer hardware used includes an Intel® Core™ i9-9900K CPU 3.60GHz as the central processing unit, an NVIDIA GeForce RTX 2080 Ti 11GB as the graphics processing unit, and 64GB of memory. In terms of software configuration, the operating system is Windows 10 Pro 64-bit. The platform used for programming is Jupyter Notebook 6.4.6, and the programming language used is Python 3.7.11. The deep learning frameworks utilized are TensorFlow-GPU 2.8.0 and Keras 2.8.0.

B. Model Parameter Settings

Each model was trained for a maximum of 100 epochs, with a callback function set to monitor the validation loss for early stopping, saving the model with the best training performance. In addition to early stopping, this study employed ModelCheckpoint to track and save the model weights with the highest validation specificity.

The batch size for all training processes was set to 8. Nadam [16], an adaptive learning rate optimizer, was employed to enhance training stability by adjusting the learning rate based on its variance. The class weight parameters were adjusted according to the proportion of classes from class 0 to class 4 to

balance the training weights for each class. Classes with more examples were assigned lower weights, while classes with fewer examples were assigned higher weights. Instead of using the traditional categorical cross-entropy loss, this study employed categorical focal loss as the loss function.

TABLE III. HARDWARE AND SOFTWARE ENVIRONMENT OF THE EXPERIMENT

experimental environment configuration	specifications
operating system	Windows 10 Professional 64-bit
processor	Intel (R) Core (TM) i9-9900K CPU 3.60GHz
graphic processor	NVIDIA GeForce RTX 2080 Ti 11G
memory	64GB
software development platform	Jupyter Notebook 6.4.6
programming language	Python 3.7.11
deep learning framework	Tensorflow-gpu 2.8.0、Keras 2.8.0

ResNet50-V2 is an improved version of ResNet50 [19], which outperforms both ResNet101 and ResNet50 in terms of system performance on the large-scale ImageNet database. The primary enhancement in ResNet50-V2 involves modifying the propagation formula within the basic building blocks of the Residual Network (ResNet). The architectural differences between the basic units of ResNet50-V1 and ResNet50-V2 are shown in Fig. 5 (with ResNet50-V1 on the left and ResNet50-V2 on the right). In ResNet50-V2, the batch normalization layer and ReLU activation function are moved before the weight layers, resulting in a pre-activation structure. The advantage of this structure is that it accelerates model convergence without changing the model's depth, and placing the batch normalization layer before the ReLU activation function and weight layers enhances the model's regularization effect.

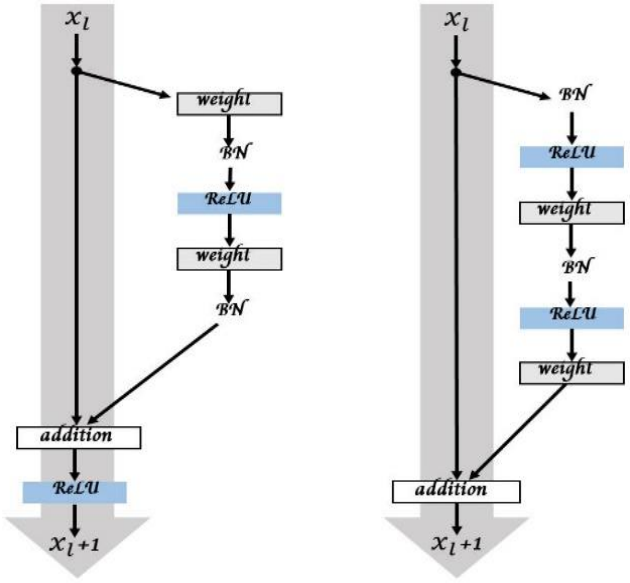


Fig. 5. Architectural differences between basic residual units of ResNet50-V1 and ResNet50-V2.

DenseNet (Densely Connected Convolutional Network) offers several advantages over ResNet, such as reducing network complexity, lowering the number of model parameters, mitigating the gradient vanishing problem, and enhancing feature propagation [20]. Due to its densely connected architecture, DenseNet efficiently improves feature utilization, reduces gradient vanishing, and aids model convergence. Reusing features means there is no need to learn new feature maps, leading to a reduction in the number of model parameters. Fig. 6 illustrates the architecture of a dense block in DenseNet.

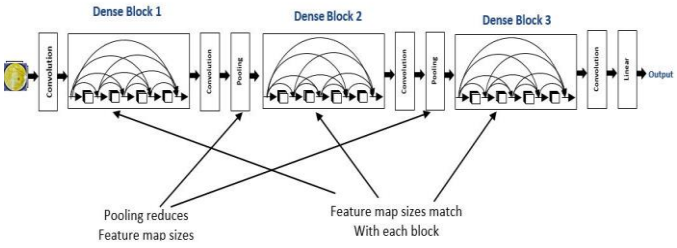


Fig. 6. Schematic diagram of dense block.

Inception-V3 was released in December 2015. The principle of Inception involves connecting convolutional layers of different sizes in parallel. The output from these convolutional layers is then used as input for the next inception block utilizing convolutional layers of varying sizes allows for the creation of better feature maps by extracting diverse feature information. Inception avoids bottleneck issues, which, although reducing the model's parameters, can result in the loss of important features and require slow dimensionality reduction to prevent excessive data loss [21]. Fig. 7 shows a schematic diagram of the inception block, including convolutional layers of different sizes.

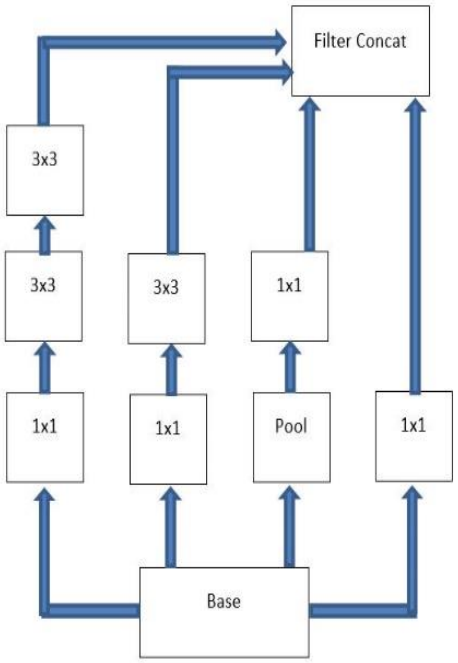


Fig. 7. Schematic diagram of inception block.

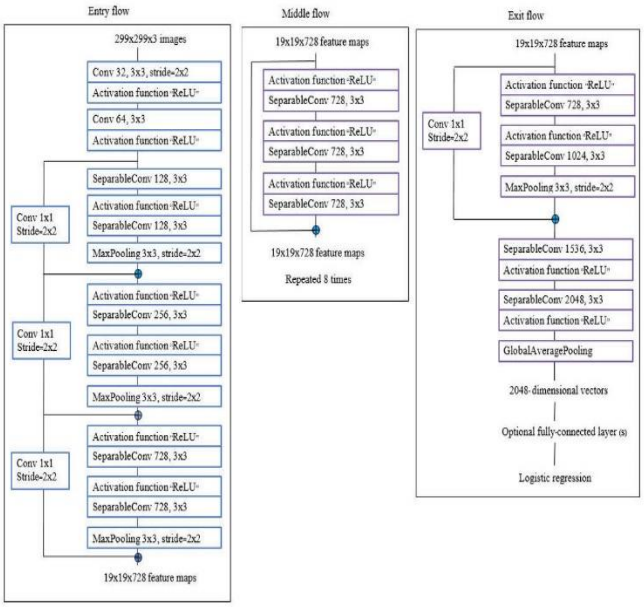


Fig. 8. Xception network architecture diagram.

Xception, short for extreme inception, is a network based on Inception-V3 [22]. It employs a depthwise separable Convolution architecture to replace the inception module structure in the original Inception-V3. depthwise separable convolution maintains the number of parameters of the original Inception-V3 network while reducing model complexity, increasing network width, and improving model accuracy, as illustrated in Fig. 8.

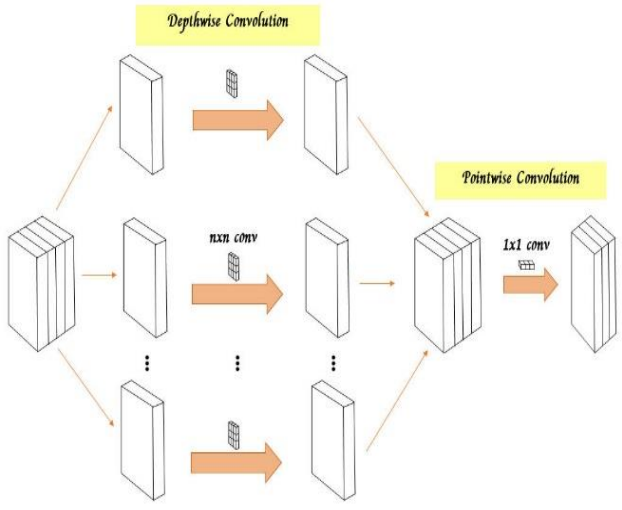


Fig. 9. Convolution operation flowchart of depthwise convolution.

MobileNet is a lightweight CNN model proposed by Google, designed to balance model size and computational speed for use in devices or mobile platforms [23]. MobileNet utilizes a depthwise separable convolution structure, which significantly reduces computational resources while maintaining good accuracy. Although both MobileNet and Xception use depthwise separable convolution, their goals differ: MobileNet focuses on model compression and computational speed, while Xception aims to enhance system performance with a parameter count similar to Inception-V3. The depthwise separable convolution consists of two parts: depthwise convolution and pointwise convolution. Depthwise convolution applies a k×k convolutional layer separately to each input channel, followed by pointwise convolution, which multiplies the output from the previous step using a 1×1 convolutional layer. The combined results provide a feature map, as illustrated in Fig. 9.

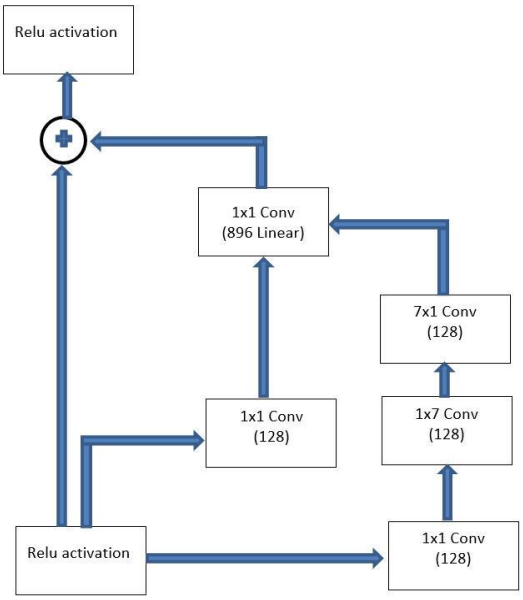


Fig. 10. Architecture diagram of inception block combined with residual connection.

InceptionResNet is a model developed by combining Inception-V3 and ResNet architectures [24]. The developers integrated residual connections into the inception architecture. Experimental results demonstrate that Inception networks with residual connections perform better in terms of system efficiency compared to inception networks without them. Additionally, residual connections significantly accelerate the training speed of the inception network. Fig. 10 illustrates the architectural diagram of an inception block integrated with a residual connection.

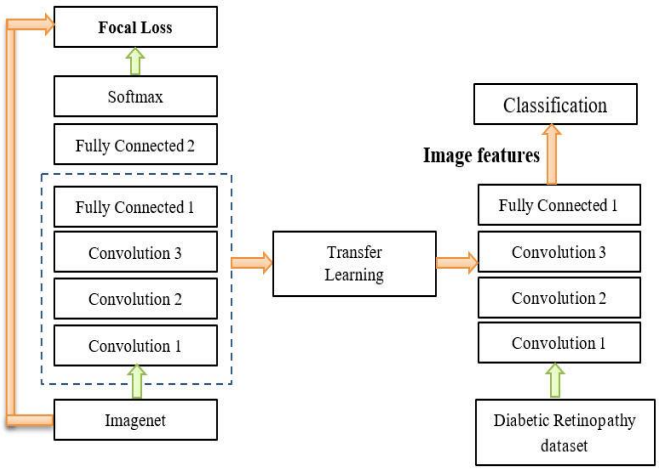


Fig. 11. Transfer learning technique.

Transfer learning involves training a neural network model on a related task and then adapting it to a new, similar problem. This technique leverages the model's pre-trained weights, often learned from large datasets like ImageNet. Transfer learning offers flexibility, enabling the use of pre-trained models as feature extractors or components of entirely new models. It has also been successfully applied in cancer subtype discovery, as illustrated in Fig. 11 [25].

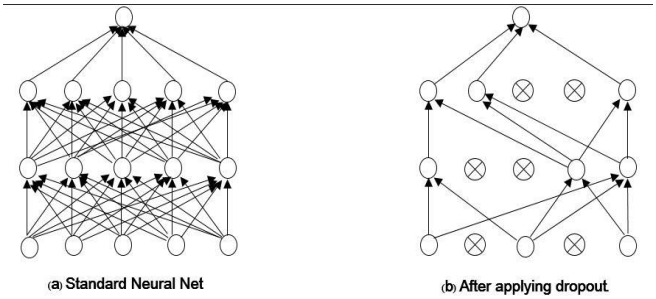


Fig. 12. Dropout technique.

To address overfitting, dropout is employed as a simple regularization technique that randomly deactivates neurons during training. In the context of CNNs, this means that some neurons are temporarily ignored, preventing them from sending signals to other neurons. A dropout rate of 0.5 in fully connected layers indicates that 50% of the neurons are deactivated. Dropout effectively mitigates overfitting by disrupting co-adaptations among neurons, thereby enhancing the model's ability to generalize and reducing its tendency to overfit the training data [25].

C. Categorical Focal Loss

The term α in the focal loss formula serves as a balancing factor that addresses class imbalance. It is calculated as shown in Eq. (5).

$$FL(p_t) = -\alpha(1-p_t)^{\gamma}.log(p_t) \quad (5)$$

Focal loss focuses on difficult examples by adjusting the loss based on the probability of correct classification (p_t). Hard examples, which have low p_t values, exert minimal influence on the modulating factor $(1-p_t)\ \gamma$, while easy examples with high pt values have a diminishing effect [26].

D. Optimizer

Nadam [23] is an optimization algorithm that utilizes past information to efficiently update model weights. It combines the strengths of both Adam and Nesterov momentum, addressing the decaying learning rate issue of Adagrad. This combination leads to faster convergence and reduced parameter instability, enabling more effective model training. Nadam is calculated as shown in Eq. (6).

$$\theta_{t+1} = \theta_t - \frac{\eta}{\sqrt{V_t} + \varepsilon}\left(\beta_1 m_t + \frac{(1-\beta_1)g_t}{1-\beta_1^t}\right) \quad (6)$$

Nadam utilizes a learning rate of 0.002 (η) with an objective function (θ_t) defined by $\varepsilon = 1e^{-08}$ and $\beta_1 = 0.9$. These settings, inspired by [27], leverage v_t, g_t and m_t to enhance the optimizer's efficiency at each time step t.

IV. Experimental Results

Tables IV and V present the system evaluation results of the image enhancement fusion techniques and six deep learning model combinations on the APTOS-2019 and Messidor-2 datasets, respectively.

TABLE IV. System Evaluation Results of Image Enhancement Fusion Techniques and Six Deep Learning Model Combinations used in this Study on the APTOS-2019 Dataset

Models	Accuracy%	Precision%	Sensitivity %	Specificity %
ResNet50-V2	92.4	86.1	99.1	99.5
DenseNet121	93.0	86.7	99.8	99.7
Inception-V3	89.7	85.6	99.7	99.0
Xception	91.9	87.0	99.5	99.6
MobileNet-V2	91.2	83.0	99.7	99.5
Inception ResNet-V2	91.8	82.5	99.1	99.5

DenseNet121 achieved the highest performance on the APTOS-2019 dataset with an accuracy of 93.0%, precision of 86.7%, sensitivity of 99.8%, and specificity of 99.7%. Xception and ResNet50-V2 exhibited slightly lower accuracy compared to DenseNet121. Xception achieved an accuracy of 91.9%, precision of 87.0%, sensitivity of 99.5%, and specificity of 99.6%, while ResNet50-V2 had an accuracy of 92.4%, precision of 86.1%, sensitivity of 99.1%, and specificity of 99.5%. The remaining three models, InceptionV3, MobileNet-V2, and InceptionResNet-V2, showed the following performance: InceptionResNet-V2 achieved an accuracy of 91.8%, precision of 82.5%, sensitivity of 99.1%, and specificity of 99.5%; MobileNet-V2 achieved an accuracy of 91.2%, precision of 83.0%, sensitivity of 99.7%, and specificity of 99.5%; and Inception-V3 achieved an accuracy of 89.7%, precision of 85.6%, sensitivity of 99.7%, and specificity of 99.0%. Overall, the sensitivity and specificity of all six deep learning classification models were greater than 99.0%. In conclusion, the image preprocessing methods used in this study consistently demonstrated good performance across all models with minimal variation, as illustrated in Table IV.

TABLE V. System Evaluation Results of Image Enhancement Fusion Techniques and Six Deep Learning Model Combinations used in this Study on the Messidor-2 Dataset

Models	Accuracy %	Precision %	Sensitivity %	Specificity %
ResNet50-V2	84.0	80.0	99.1	90.6
DenseNet121	85.9	72.9	99.7	94.7
Inception-V3	81.4	57.2	98.9	87.3
Xception	86.9	79.5	99.1	96.2
MobileNet-V2	84.0	64.1	96.9	91.6
Inception ResNet-V2	87.9	75.7	99.4	97.0

InceptionResNet-V2 demonstrated the best performance on the Messidor-2 dataset, achieving an accuracy of 87.9%, precision of 75.7%, sensitivity of 99.4%, and specificity of 97.0%. The second and third best performing models were Xception and DenseNet121, respectively, with slightly lower accuracies. Xception had an accuracy of 86.9%, precision of 79.5%, sensitivity of 99.1%, and specificity of 96.2%. DenseNet121 achieved an accuracy of 85.9%, precision of 72.9%, sensitivity of 99.7%, and specificity of 94.7%. The remaining three models, ranked fourth to sixth, were ResNet50-V2, MobileNet-V2, and Inception-V3, respectively. ResNet50-V2 had an accuracy of 84.0%, precision of 80.0%, sensitivity of 99.1%, and specificity of 90.6%. MobileNet-V2 achieved an accuracy of 84.0%, precision of 64.1%, sensitivity of 96.9%, and specificity of 91.6%. Inception-V3 had the lowest performance with an accuracy of 81.4%, precision of 57.2%, sensitivity of 98.9%, and specificity of 87.3%. Overall, the sensitivity and specificity of all six deep learning classification models were greater than 97.0%. In conclusion, the image preprocessing methods used in this study consistently demonstrated good performance across all models with minimal variation, as illustrated in Table V.

TABLE VI. COMPARISON WITH OTHER STUDIES USING THE APTOS-2019 DATASET

Researches	Accuracy%	Precision %	Sensitivity %	Specificity %
[28]	86.5	85.7	86.1	85.9
[29]	92.0	85.0	99.0	99.0
[30] VGG19	88.1	90.3	79.3	94.0
[30] DenseNet121	89.5	83.8	92.1	87.7
[31]	84.2	-	98.5	98.8
[32]	83.4	69.7	67.7	67.0
This research methodology	**93.2**	**86.8**	**99.5**	**99.6**

Research in [28] utilized the APTOS-2019 Dataset to develop a diabetic retinopathy classification model. The model achieved an accuracy of 86.5%, precision of 85.7%, sensitivity of 86.1%, and specificity of 85.9%. Research [29] reported an accuracy of 92.0%, precision of 85.0%, sensitivity of 99.0%, and specificity of 99.0%. Research in [30] evaluated both VGG19 and DenseNet121 models, with VGG19 achieving an accuracy of 88.1%, precision of 90.3%, sensitivity of 79.3%, and specificity of 94.0, while DenseNet121 attained an accuracy of 89.5%, precision of 83.8%, sensitivity of 92.1%, and specificity of 87.7%, while research [31] showed an accuracy of 84.2%, sensitivity of 98.5%, and specificity of 98.8%. Research [32] reported an accuracy of 83.4%, precision of 69.7%, sensitivity of 67.7%, and specificity of 67.0. The proposed model demonstrated superior performance, achieving an accuracy of 93.2%, precision of 86.8%, sensitivity of 99.5%, and specificity of 99.6%. Overall, the model developed in this experiment demonstrated superior performance in classifying diabetic retinopathy compared to previous studies, as shown in Table VI.

Research in [30] utilized the Messidor-2 dataset to construct a diabetic retinopathy classification model using InceptionResNet-V2 and Inception-V3. The models' performance metrics were as follows: InceptionResNet-V2 achieved an accuracy of 69.2%, precision of 60.2%, sensitivity of 54.9%, and specificity of 75.9%. Inception-V3 obtained an accuracy of 72.8%, precision of 54.3%, sensitivity of 50.2%, and specificity of 80.6%. In contrast, research [33] reported a sensitivity of 81.0% and specificity of 86.1%, while research [29] showed an accuracy of 80.0%, precision of 85.0%, sensitivity of 89.0%, and specificity of 90.0%. Research [34] reported an accuracy of 89.6%, sensitivity of 91.4%, and specificity of 93.2. Comparing these results to the current experiment, which achieved an accuracy of 87.3%, precision of 75.2%, sensitivity of 99.6%, and specificity of 97.8%, it is evident that the current model exhibits high performance compared to other research and closely resembles the results of research [34]. The model in this experiment demonstrated a strong ability to detect positive cases due to its higher sensitivity compared to other studies, as shown in Table VII.

TABLE VII. COMPARISON WITH OTHER STUDIES USING THE MESSIDOR-2 DATASET

Researches	Accuracy%	Precision %	Sensitivity %	Specificity %
[29]	80.0	85.0	89.0	90.0
[30] Inception ResNet-V2	69.2	60.2	54.9	75.9
[30] Inception-V3	72.8	54.3	50.2	80.6
[33]	-	-	81.0	86.1
[34]	89,6	-	91.4	93.2
This research methodology	**87.3**	**75.2**	**99.6**	**97.8**

V. DISCUSSION

In this research, the diabetic retinopathy dataset consists of retinal images with varying resolutions and aspect ratios. The dataset has been adjusted to accommodate different CNN architectures. Additionally, background information or images unrelated to retinal diseases may impact classification accuracy, consistent with findings in prior research [5] [35]. Automated detection of diabetic retinopathy often involves preprocessing original images, including cropping, resizing, and adjusting resolution, to mitigate these issues and improve model training efficiency.

The imbalanced nature of the diabetic retinopathy dataset used to train the classification model resulted in suboptimal performance. To address this issue, categorical focal loss was employed to balance class weights instead of the standard categorical cross-entropy loss, aligning with findings from studies [36–38]. This approach demonstrated improved evaluation metrics. The dataset often suffers from class imbalance, where certain classes are overrepresented or underrepresented. This imbalance can bias the model toward predicting the majority class, making it challenging to accurately classify minority classes.

To enhance feature extraction, this research employed various image preprocessing techniques, including MSRCR, Gamma correction, CIELAB color space conversion, and CLAHE. MSRCR, based on retinex theory, simulates human visual perception by adjusting image brightness and color across multiple scales. Gamma correction controls brightness by

manipulating the gamma value, while CIELAB conversion transforms RGB images into a perceptually uniform color space. CLAHE enhances local contrast by adjusting histograms within image blocks. These techniques provide deeper insights and additional perspectives, contributing to a more comprehensive understanding of the underlying problem. Current research highlights the potential of deep learning techniques for feature extraction in medical image and signal processing.

Feature extraction relates to dimensionality reduction and is a crucial preprocessing step in deep learning, potentially leading to new discoveries. In this study, six models were used to extract features, along with an optimizer, which continuously adjusts model parameters (weights and biases) to improve accuracy. The main goal is to minimize the loss function, enhancing the model's predictive ability. The Nadam optimizer was employed, improving the measurement of the difference between predicted and actual results. The development of these techniques enhances classifier performance and aids in better decision-making for diagnosis. Evaluating large mixed input data requires significant memory and computational power. In this research, transfer learning and dropout techniques were applied to optimize model performance. Feature extraction ultimately helps save processing power and disk space while improving classification, thus enhancing the efficiency of diagnostic support systems. Therefore, developing effective algorithms for feature extraction is essential in building diagnostic support systems. A common method to eliminate irrelevant or redundant data is dimensionality reduction, with feature extraction being a popular approach.

Transfer learning was utilized by fine-tuning the weights of models trained on the APTOS-2019 dataset to adapt them to the Messidor-2 dataset. Although the results were slightly inferior, the best-performing model combination on the Messidor-2 dataset was InceptionResNet-V2, with a sensitivity of 99.4% and specificity of 97.0%. Sensitivity and specificity scores remained stable between 97% and 99%, demonstrating effective differentiation between diabetic retinopathy and normal retina. Compared to other research methods, these results were excellent, showcasing the effectiveness of transfer learning in this study.

VI. Conclusion

In recent years, the application of artificial intelligence-based diabetic retinopathy screening technologies has surged in the medical field. Automated screening methods effectively address the limitations of traditional manual diagnosis, enabling ophthalmologists to make quicker and more accurate assessments. Additionally, these technologies have played a crucial role in overcoming the challenges of inefficient screening in rural areas with limited medical resources, significantly enhancing the chances of early detection and treatment of diabetic retinopathy.

In this experiment, various image processing techniques were combined, including MSRCR, Gamma correction, CIELAB, CLAHE, and image enhancement. These techniques were integrated with six deep learning models and optimization techniques such as Nadam, transfer learning, and dropout. The models were trained and evaluated on the APTOS-2019 and Messidor-2 datasets, consisting of 3,662 and 1,744 images, respectively. These datasets exhibit class imbalance, with five severity levels: NDR, MiDR, MoDR, SDR, and PDR. The experimental results demonstrated that DenseNet121 achieved the highest performance on the APTOS-2019 dataset, with a sensitivity of 99.8% and specificity of 99.7%, outperforming previous studies.

Tables VI and VII present a comparison of the evaluation results between the best model from this research and other studies utilizing the same datasets (APTOS-2019 and Messidor-2). The data in these tables are directly cited from the best results of each study. For the APTOS-2019 dataset, the proposed method demonstrated comparable performance in terms of sensitivity and specificity, achieving values close to 100%. The model excelled across all metrics. In the case of the Messidor-2 dataset, although accuracy was not as optimal, sensitivity and specificity were more stable compared to other studies.

This study employed a fusion technique for image enhancement to improve the feature extraction efficiency of six deep learning models (ResNet50-V2, DenseNet121, Inception-V3, Xception, MobileNetV2, InceptionResNet-V2). The models were trained to classify healthy retinas and four different severities of diabetic retinopathy. Class-weighting techniques, including parameter setting and categorical focal loss, were utilized to enhance the model's accuracy in distinguishing various categories of retinal images, even when certain categories were underrepresented in the dataset.

To address the class imbalance problem and improve feature extraction performance, these models were trained to classify normal retinas and diabetic retinopathy across four different severity levels. categorical focal loss was adopted as the loss function to enhance classification accuracy for different types of retinal images, particularly those with smaller sample sizes. This loss function is specifically designed to address class imbalance issues in classification tasks, especially when the minority class has fewer samples than the majority class. By assigning more weight to samples from the minority class, categorical focal loss enables the model to better classify these underrepresented classes, which is a common challenge in real-world classification problems. This approach significantly contributes to the model's performance on datasets characterized by diabetic retinopathy. However, these methods can impact the model's ability to effectively classify classes with fewer samples. The greater the imbalance in sample proportions between classes, the more pronounced this effect becomes, particularly in improving classification performance for classes with minimal representation. The evaluation scores from this study's best results are compared with those from other research studies.

Acknowledgment

The authors would like to express their sincere gratitude to the anonymous reviewers for their useful comments and suggestions for improving the quality of this paper, and we thank National Pingtung University of Science and Technology Council of the Republic of China, Taiwan for financially supporting this research under Contract No. 111-2410-H-020-007.

REFERENCES

[1] J. Chantra, and S. Pratoom, “Factors Related to Diabetic Retinopathy in Type – 2 diabetes in Damnoensaduak Hospital, Ratchaburi Province, Thailand” J. Res. Improv. Qual. Life, vol. 3, pp. 25–36, 2023.

[2] V. Bellemo, G. Lim, T. H. Rim, G. S. W. Tan, C. Y. Cheung, S. Sadda, M. G. He, A. Tufail, M. L. Lee, W. Hsu, and D. S. W. Ting, "Artificial intelligence screening for diabetic retinopathy: the real-world emerging application," Curr. Diab. Rep., vol. 19, pp. 1-12, 2019.

[3] V. Bellemo, Z. W. Lim, G. Lim, D. Q. Nguyen, Y. Xie, M. Y. T. Yip, H. Hamzah, J. Ho, X. Q. Lee, W. Hsu, M. L. Lee, L. Musonda, M. Chandran, G. Chipalo-Mutati, M. Muma, G. S. W. Tan, S. Sivaprasad, G. Menon, T. Y. Wong, and D. S. W. Ting, "Artificial intelligence using deep learning to screen for referable and vision-threatening diabetic retinopathy in Africa: a clinical validation study," Lancet Digit. Health, vol. 1, no. 1, pp. e35-e44, 2019.

[4] A. Grzybowski, P. Brona, G. Lim, P. Ruamviboonsuk, G. S. Tan, M. Abramoff, and D. S. Ting, "Artificial intelligence for diabetic retinopathy screening: a review," Eye, vol. 34, no. 3, pp. 451-460, 2020.

[5] N. Tsiknakis, D. Theodoropoulos, G. Manikis, E. Ktistakis, O. Boutsora, A. Berto, F. Scarpa, A. Scarpa, D. I. Fotiadis, and K. Marias, "Deep learning for diabetic retinopathy detection and classification based on fundus images: A review," Comput. Biol. Med., vol. 135, pp. 104599, 2021.

[6] M. Zhou, K. Jin, S. Wang, J. Ye, and D. Qian, "Color Retinal Image Enhancement Based on Luminosity and Contrast Adjustment," IEEE Trans. Biomed. Eng., vol. 65, no. 3, pp. 521-527, 2018.

[7] Y. Chang, C. Jung, P. Ke, H. Song, and J. Hwang, "Automatic Contrast-Limited Adaptive Histogram Equalization With Dual Gamma correction," IEEE Access, vol. 6, pp. 11782-11792, 2018.

[8] S. Sonali, S. Sahu, A. K. Singh, S. P. Ghrera, and M. Elhoseny, "An approach for de-noising and contrast enhancement of retinal fundus image using CLAHE," Opt Laser Technol., vol. 110, pp. 87-98, 2019.

[9] M. R.Islam, L. F. Abdulrazak, M. Nahiduzzaman, M. O. F. Goni, M. S. Anower, M. Ahsan, J. Haider, and M. Kowalski, "Applying supervised contrastive learning for the detection of diabetic retinopathy and its severity levels from fundus images," Comput. Biol. Med., vol. 146, pp. 105602, 2022.

[10] [10] G. Cao, L. Huang, H. Tian, X. Huang, Y. Wang, and R. Zhi, "Contrast enhancement of brightness-distorted images by improved adaptive Gamma correction," Comput. Electr. Eng., vol. 66, pp. 569-582, 2018.

[11] M. Veluchamy and B. Subramani, "Image contrast and color enhancement using adaptive Gamma correction and histogram equalization," Optik, vol. 183, pp. 329-337, 2019.

[12] M. R. K. Mookiah, S. Hogg, T. J. MacGillivray, V. Prathiba, R. Pradeepa, V. Mohan, R. M. Anjana, A. S. Doney, C. N. A. Palmer, and E. Trucco, "A review of machine learning methods for retinal blood vessel segmentation and artery/vein classification," Med. Image Anal., vol. 68, pp. 101905, 2021.

[13] Y. E. Almalki, N. A. Jandan, T. A. Soomro, A. Ali, P. Kumar, M. Irfan, M. U. Keerio, S. Rahman, A. Alqahtani, S. M. Alqhtani, M. A. Hakami, W. A. Aldhabaan, and A. S. Khairallah, "Enhancement of Medical Images through an Iterative McCann Retinex Algorithm: A Case of Detecting Brain Tumor and Retinal Vessel Segmentation," Appl. Sci., vol. 12, no. 16, pp. 8243, 2022.

[14] Y. Jiang, Z. Ma, C. Wu, Z. Zhang, and W. Yan, "RSAP-Net: joint optic disc and cup segmentation with a residual spatial attention path module and MSRCR-PT pre-processing algorithm," BMC Bioinform., vol. 23, no. 1, pp. 1-21, 2022.

[15] Q. Mirsharif, F. Tajeripour, and H. Pourreza, "Automated characterization of blood vessels as arteries and veins in retinal images," Comput. Med. Imaging Graph., vol. 37, no. 8, pp. 607-617, 2013.

[16] K. Sriporn, C. F. Tsai, C. E. Tsai, and P. Wang, “Analyzing lung disease using highly effective deep learning techniques,” Healthcare, vol. 8, pp.1-21, 2020.

[17] D. Nagpal, S. N. Panda, M. Malarvel, P. A. Pattanaik, and M. Zubair Khan, "A review of diabetic retinopathy: Datasets, approaches, evaluation metrics and future trends," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 9, pp. 7138-7152, 2022.

[18] N. Salamat, M. M. S. Missen, and A. Rashid, "Diabetic retinopathy techniques in retinal images: A review," Artif. Intell. Med., vol. 97, pp. 168-188, 2019.

[19] K. He, X. Zhang, S. Ren, and J. Sun, “Identity Mappings in Deep Residual Networks,” arXiv, pp.1-15, 2016.

[20] G. Huang, Z. Liu, L. Maaten, and K. Q. Weinberger, “Densely Connected Convolutional Networks,” arXiv, pp.1-9, 2018.

[21] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," arXiv, pp.1-10, 2015.

[22] F. Chollet, “Xception: Deep Learning with Depthwise Separable Convolutions,” arXiv, pp.1-8, 2017.

[23] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, "Mobilenets: Efficient convolutional neural networks for mobile vision applications," arXiv, pp.1-9, 2017.

[24] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. A. Alemi, "Inception-v4, inception-resnet and the impact of residual connections on learning," arXiv, pp.1-12, 2016.

[25] K. Sriporn, C. F. Tsai, C. E. Tsai, and P. Wang, “Analyzing malaria disease using effective deep learning approach,” Diagnostics, vol. 10, pp. 1-22, 2020.

[26] T.-Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollár, "Focal loss for dense object detection," arXiv, pp.1-10, 2018.

[27] S. Ruder, “An overview of gradient descent optimization algorithms,” arXiv, pp.1-14, 2017.

[28] M. Tian, H. Wang, Y. Sun, S. Wu, Q. Tang, and M. Zhang, "Fine-grained attention & knowledge-based collaborative network for diabetic retinopathy grading," Heliyon, vol. 9, no. 7, pp. e17217, 2023.

[29] M. Fatima, M. Imran, A. Ullah, M. Arif, and R. Noor, "A unified technique for entropy enhancement based diabetic retinopathy detection using hybrid neural network," Comput. Biol. Med., vol. 145, pp. 105424, 2022.

[30] S. El-Ateif and A. Idri, "Single-modality and joint fusion deep learning for diabetic retinopathy diagnosis," Sci. Afr., vol. 17, pp. e01280, 2022.

[31] A. Sugeno, Y. Ishikawa, T. Ohshima, and R. Muramatsu, "Simple methods for the lesion detection and severity grading of diabetic retinopathy by image processing and transfer learning," Comput. Biol. Med., vol. 137, pp. 104795, 2021.

[32] G. Yue, Y. Li, T. Zhou, X. Zhou, Y. Liu, and T. Wang, "Attention-Driven Cascaded Network for Diabetic Retinopathy Grading from Fundus Images," Biomed. Signal Process. Control., vol. 80, pp. 104370, 2023.

[33] G. Saxena, D. K. Verma, A. Paraye, A. Rajan, and A. Rawat, "Improved and robust deep learning agent for preliminary detection of diabetic retinopathy using public datasets," Intell.-Based Med., vol. 3-4, pp. 100022, 2020.

[34] P. Modi and Y. Kumar, "Smart detection and diagnosis of diabetic retinopathy using bat based feature selection algorithm and deep forest technique," Comput. Ind. Eng., vol. 182, pp. 109364, 2023.

[35] W. L. Alyoubi, W. M. Shalash, and M. F. Abulkhair, "Diabetic retinopathy detection through deep learning techniques: A review," Inform. Med. Unlocked, vol. 20, pp. 100377, 2020.

[36] M. Saini and S. Susan, "Deep transfer with minority data augmentation for imbalanced breast cancer dataset," Appl. Soft Comput., vol. 97, pp. 106759, 2020.

[37] M. Saini and S. Susan, "Diabetic retinopathy screening using deep learning for multi-class imbalanced datasets," Comput. Biol. Med., vol. 149, pp. 105989, 2022.

[38] H. Li, X. Dong, W. Shen, F. Ge, and H. Li, "Resampling-based cost loss attention network for explainable imbalanced diabetic retinopathy grading," Comput. Biol. Med., vol. 149, pp. 105970, 2022.

Assessing the Usability of M-Health Applications: A Comparison of Usability Testing, Heuristics Evaluation and Cognitive Walkthrough Methods

Obead Alhadreti
Dept. of Computers-Engineering and Computing College, Umm Al-Qura University, Al-Qunfudah, Saudi Arabia

***Abstract*—Mobile health applications have increasingly become an important channel for providing services in the health sector. However, poor usability can be a major barrier for the rapid adoption of mobile services. The purpose of this study is to compare the relative performance of three usability evaluation methods, namely, usability testing, heuristics evaluation, and the cognitive walkthrough methods in determining the usability level of mobile health applications. The study also explores the relationship between the metrics of usability testing and the current level of mobile health applications in Saudi Arabia. An experimental approach has been used in this study, which gathered qualitative and quantitative data. The methods were used to assess two mobile health interfaces and were compared on the number, severity, and types of usability problems identified. Correlation tests were also carried out to examine areas of overlap between usability testing metrics. The heuristic evaluation found significantly greater numbers of usability problems than the other techniques. The usability testing method, however, detects problems of greater severity. There is also a significant correlation between the number of usability issues found and how long it takes to perform tasks in usability tests. Moreover, the level of usability of the Saudi applications tested is below expectation and in need of further improvement. Based on the study results, both usability testing and heuristic evaluation should be employed during the design process of mobile health applications for maximum effectiveness. Additionally, it is recommended that SUS questionnaires should not be the sole method of determining the usability level of mobile health applications.**

Keywords*—Mobile health applications; usability; usability testing; heuristics evaluation; cognitive walkthrough

I. Introduction

Digitalization has come to play a prominent role in delivering health services to individuals and communities. It not only improves patient safety and satisfaction but is instrumental in keeping large-scale health statistics up to date. Hospitals and other healthcare service providers are offering more digitalized services, which has fundamentally altered healthcare systems. Among these services are mobile health (m-health) applications, which are becoming a major avenue of healthcare provision, given that approximately six billion people (around 75% of the world's population) have regular access to mobile phones [1]. As a result, m-health is now a rapidly expanding field of research.

The term, m-health refers in general to the use of mobile devices in the provision of healthcare services [2]. The Global Observatory for e-health defines m-health as "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices" [3]. M-health applications also include processes of data collection [4], service delivery [5], communication between doctors and patients [6] and support for monitoring and adherence in real time [7]. The market for m-health applications is expected to grow in coming years at a significant rate: from USD 99 billion globally in 2021 to USD 332.7 billion by 2025 [8]. The scope for the adoption of m-health applications is further increased by their diversification into such health sectors as nutrition, sports, productivity and behavioral therapy [9].

A crucial requirement for m-health applications is usability. An information system that people cannot use easily represents a threat to the safety of patients, as well as being inefficient and a contributor to staff burn-out and dissatisfaction. An easy-to-use system, on the other hand, is more efficient, enhances emergency care safety and is a real benefit to staff [10]. Usability is generally considered as "the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [11]. It is clear from this definition that usability (real and perceived) can differ between contexts, target audiences and products, which is especially true in the m-health sector due to its unique characteristics which are as follows. First, unlike general commercial applications, which can use personalized messages to seduce customers into feeling comfortable with the system, it is difficult to establish user satisfaction with m-health applications, which have to give both positive and negative messages about users' health-related behavior. For example, appropriate advice (such as switching off the television and going for a walk instead) may not be what users wish to hear, which has the potential to affect their satisfaction with the system. Second, m-health communication needs to be tailored to individual users' knowledge levels and awareness regarding health, which can vary significantly from one user to the next [10]. Third, these factors are exacerbated when someone has a chronic illness, as this can increase anxiety and stress, which makes the assimilation of information and self-management skills more difficult [11].

The assessment of mobile applications' usability is challenging due to the small screens on which they are viewed and the resolution of their displays, limited input options, restricted processing speeds and power, and connectivity issues [12]. Several methods exist for assessing the usability of mobile applications. The most frequently employed usability evaluation

methods (UEMs) are usability testing (UT), heuristic evaluation (HE), and the cognitive walkthrough (CW) [13]. The UT method is a user-based method that is widely used to measure how easily end–users can use an interface. However, recruiting test participants and performing tests can be an expensive process. HE is a usability inspection method that involves having an expert examines an interface against a set of principles. These principles provide a template to help identify issues a user will likely encounter. One of the limitations of HE is that it tends to detect many low-severity problems. CW is also a reviewer-based method, but the emphasis is on tasks. The idea is to identify users' goals, and how they achieve them in the interface, then experts detect issues users would encounter as they learn to use the system [13]. So far, there has not been any research which compares UT, HE, and CW methods in terms of their performance in measuring m-health application usability. This study, therefore, aims to examine the effectiveness of these UEMs in the context of m-health applications used in Saudi Arabia.

The Saudi healthcare sector is undergoing a digital transformation, including an increasing dependency on m-health applications for expanding access to healthcare, health education, communicating with patients, monitoring their conditions and ensuring conformity to treatments. Various m-health applications have been promoted by the Ministry of Health in Saudi Arabia, such as Sehhaty1. These applications have several purposes, such as booking appointments, remote consultations and delivery of medicines, and they became particularly important in the course of the Covid-19 pandemic, when there was a significant increase in Saudis using m-health applications [14], although this was down to necessity, not their actual interest in using the technology. Indeed, research has shown that it was factors such as stress, fear and depression which led to the rapid adoption of m-health applications, not such reasons as usefulness, ease of use, enjoyability or self-interest [15]. It is therefore crucial to establish whether or not users of m-health applications are satisfied and whether they are continuing to make use of them after the pandemic.

The current study's findings contribute significantly to the research literature on the usability evaluation of m-health apps. This will help usability practitioners to make more informed decisions about which of the examined methods to use and in which context. The findings will also be of value to the governmental and non-government organizations providing healthcare in Saudi Arabia. The rest of this paper is structured as follows. Section II reviews related work. Later sections present the study's methodology, data analysis and its results. The final section sets out the conclusions drawn from the study.

II. Related Work

A number of studies have compared the effectiveness of the UT, HE, and CW evaluation methods across different systems. A study by Tan et al., [16] compared UT and HE and found that HE identified a larger number of problems and more severe issues than UT. However, the study discovered that UT found problems missed by HE. Another study conducted by Hasan et al., [17] indicated that HE identified 72% of problems, UT extracted only 10% and 18% of the problems were found by both techniques. A study by Doubleday et al. [18] revealed that 40% of issues detected were unique to HE, whereas 39% were extracted by the UT method. Jeffries et al, [19] stated that the HE method found approximately three times more issues than UT; but UT found more important problems.

Thankam et al. [20] contrasted the performance of HE with UT to find out which usability issues were revealed by both methods. The comparison was conducted on four dental computer-based patient record interfaces. 50% of the issues were identified by each method. The study recommended that HE can be a useful tool to assess design early in the development process. In a paper by Khajouei et al. [21], the HE and CW evaluation methods were assessed based on the number and severity of the problems extracted and the ISO and Nielsen usability attributes. The number of issues related to the "satisfaction" attribute detected by HE was significantly higher than those identified using CW. However, CW identified a greater number of problems concerning the "learnability" attribute. In addition, Maguire and Isherwood examined the results of UT and HE, and it was found that HE detected approximately five times more problems than UT, thus it could be seen as more effective.

Few studies have explored the user-friendliness level of Saudi m-health applications. AlanziI [8] found that Saudi users were reasonably satisfied. Furthermore, Arafa et al. [22] studied barriers to the use of Saudi m-health applications, along with their personalization and usability, and found that usability scores were low, whereas Shilbayeh and Ismail found an average usability score of 76.8% for the CATA mobile application overall, suggesting general satisfaction [23]. However, most of the research which has been carried out have the significant limitation of having used only subjective data (e.g. from questionnaires), which was not validated against such objective data as expert inspections or task performance in the context of usability testing. It is, therefore, important that this study sheds a light on the usability levels of the m-health applications in use in Saudi Arabia.

The study's research questions are therefore as follows.

- Is there a difference between the performance of UT, HE, and CW methods in evaluating m-health applications?
- Is there a correlation between UT metrics?
- What is the current usability level of m-health applications in the Kingdom of Saudi Arabia?

III. Methodology

A. Study Approach and Variables

This study adopted an experimental approach, using both quantitative and qualitative data collection techniques [24]. The type of evaluation method (UT, HE or CW) formed the independent variable for the study and there were three dependent variables measured: number of usability issues

[1]https://apps.apple.com/sa/app/%D8%B5%D8%AD%D8%AA%D9%8A-sehhaty/id1459266578

detected, problem severity and problem type. Data on participants' task performance and their satisfaction with the usability of the test system was also gathered in the UT sessions to explore how these outcome variables are related to other metrics.

B. Test Objects and Tasks

From a careful assessment of m-health applications used in Saudi Arabia, two were selected as test subjects. It was decided to assess two m-apps instead of one to gain more reliable results pertaining to the UEMs' effectiveness. The two applications were chosen because they had a broad user base, which simplified the participant recruitment process, whilst also making the sample more likely to be representative of actual users. The two applications also had many similarities, which facilitated the formulation of tasks which resembled each other in terms of focus and difficulty. One test subject, App A, was developed by the ministry of health; the other, App B, comes from the private sector. They both have similar features, allowing the booking of GP appointments, the viewing of laboratory reports and health condition monitoring. The names of the applications are anonymized for confidentiality.

An independent usability expert, with extensive health system knowledge, performed a preliminary examination of both applications (and was not involved in later stages of the study). This examination was mainly to ensure that the two test subjects were of sufficient complexity and had sufficient scope for user interaction and the emergence of problems, although the expert did not make any predictions concerning potential problems, nor did she report any.

An analysis of the context of use was then carried out for each application to identify the characteristics of a representative user and select appropriate tasks [25]. Next, each application was examined to reveal typical use cases in order to set the tasks. 15 tasks were then formulated for each application, covering varying degrees of difficulty, as a long list from which the actual tasks set in this study were subsequently selected by the aforementioned independent expert. Equivalence of difficulty between the tasks set for each application was ensured by matching tasks according to the level and depth of their solution within each app. Five tasks were set for each application and their design was done carefully to avoid any bias related to task-related cues or language. These were then piloted by three representative users prior to the main test sessions. Two task examples are given below.

You wish to book an appointment with your general practitioner. What would you do? (App A)

You wish to seek a remote consultation from your doctor. What would you do? (App B)

C. Participants

For the UT evaluation, statistical validity was ensured by recruiting 20 participants [26]. For the HE and CW evaluations, which are done by experts, between three and five evaluators are generally considered sufficient [27], thus four usability experts were recruited for each of the HE and CW tests. 28 participants were therefore included in this study in total. They were recruited by means of convenience and snowball sampling [24].

All of the participants were native Arabic speakers and, for the UT evaluation, averaged 22 years of age (ranging from 18 to 26). All of them had more than five year's daily use of mobile applications and almost 95% had used an m-health application previously, but not the ones under evaluation.

For the HE and CW evaluations, the two evaluator groups were matched with respect to general HCI knowledge and their expertise in relation to user interface design and usability of m-health applications specifically. Of the evaluators, two in each UEM test (four in total) had a PhD related to HCI. The other four had an HCL-related MSc. They all had extensive experience of conducting evaluations by HE and CW, and all had at least seven years' experience of usability evaluation. All of the participants affirmed their informed consent in writing before the study commenced and none were offered, nor received any incentive for their involvement.

D. Experimental Procedure

Due to the risk of a participant being influenced in a second test by their experience in the first [24], a two-week break was inserted between the evaluation sessions. In addition, half of each participant group used App A in the first session and App B in the second, with the other half doing the reverse. The same type of mobile phone was used by all participants (iPhone 15), chosen because of it being the most common type in Saudi Arabia [28].

1) UT evaluation: The setting for the usability testing of both applications in this study was a laboratory. The participants were asked to make themselves familiar with the phone used and then to perform an initial pilot task. After that they were asked to read a sheet of task instructions before setting out to complete the five tasks, which were presented in a different order to each participant to control for any effect on results of task order [26].

The performance measures for the UT condition were 1) the rate of completion of each task, 2) the time each task took to complete and 3) navigational behaviour (such as how many clicks were made and which screens were browsed). After completing all five tasks, the participants were invited to watch a muted recording of their performance and give a retrospective commentary. Participants then completed a System Usability Scale (SUS) [18], which is designed to assess user satisfaction with application usability. Subsequently, all of the test data were reviewed to extract evidence of usability issues.

2) HE evaluation: This study followed the HE procedure as recommended in the work of Nielsen and Molich [29]. 1) a list of ten heuristic principles was distributed to the evaluators as a guideline by which each evaluator then evaluated the user interface, independently. The evaluators all presented a list of the problems they had identified with the system's usability, each with a description, including its frequency, persistence and likely impact on the user, and illustrative screenshots. They were, however, instructed not to share their thought with one another during the session, as one evaluator might miss several problems and each evaluators may identify a broad spectrum of unique problems [24]. The results tend to be more

comprehensive, therefore, when the findings of several evaluators are combined. However, once the independent evaluations were over, the evaluators were asked to collaborate on producing one list of usability issues. That done, each evaluator estimated the severity of every problem detected and classified it by type. They all met finally to determine average severity of the problems identified and the type classifications [29].

3) CW evaluation: In the CW condition, the applications were assessed following Blackmon et al.'s methodology [30]. The evaluators used the five tasks from the UT evaluation and answered the following questions as they did so.

- Will users attempt to achieve the correct result?
- Will users see that a necessary action is available to them?
- Will users connect the desired result with the action necessary to achieve it?
- Are users given confirmation that they have made progress towards the desired result once a necessary action has been carried out?

The overall user goals and the requisite subgoals for each task were determined and the necessary actions were identified in the way illustrated by Blackmon et al. [30]. The evaluators then examined each task systematically, noting 1) the goals users are expected to seek, 2) their subgoals and 3) actions, 4) the responses from the application and 5) potential problems with user interaction. Each evaluator produced a list of problems independently and recorded information about the issue in the same way as for the HE evaluation. Following the completion of each task, the list of usability issues identified was reviewed by the evaluator, adding or correcting items if necessary. The five task-specific lists from each evaluator were gathered and compared communally and a consolidated list of issues was established. As with the HE evaluation, the evaluators determined the types and severity of problems independently, before meeting to agree the average severity of each problem and classify all those listed [30].

E. Analysis of Usability Problems

Usability problems found in the UT evaluation were extracted in a structured manner, as employed in [31] to mitigate biases (i.e. evaluator effect) and enhance data validity and reliability. An inter-coder check on reliability was also conducted, by an independent evaluator, on the UT usability problem analysis. This evaluator coded the usability problems experienced by the first participant in the experiment and discussed them with the researcher, before performing an independent analysis on two videos of the testing, selected at random. The agreement between the problems identified by the test subject and those revealed in the videos was a respectable 78% [32].

Problem severity in all evaluation conditions was classified according to the following scale [24]:

1) A catastrophic problem, which prevents users reaching their goal and has to be remedied.

2) A major problem, which leads to user frustration and difficulty in continuing, which should be remedied.

3) A minor problem, which leads to user frustration and difficulty in continuing, which could be remedied.

4) A cosmetic problem, which leads to minor issues for users and which can be remedied easily.

The problems were also classified in four types, navigation, layout, content and functionality (as in Table I), derived from prior research [31].

TABLE I. PROBLEM TYPE CODING SCHEME

	Type	Problem Definition
1	**Navigation**	Users have difficulty moving between pages or finding the right links for specific functions or information.
2	**Layout**	Users have difficulties in respect of the interface, such as display and visibility problems, inconsistent design and awkward design of structures and forms.
3	**Content**	Users either find unnecessary information or expect information which is not there, or they do not understand the information due to its terminology or style.
4	**Functionality**	Users have difficulties because some functions are missing or otherwise problematic.

IV. RESULTS

A. App A

1) Usability problems identified: A total of *66* problems were identified with App A in the test sessions, 56 with the HE method, 46 with CW and 44 with UT. HE therefore identified a wider range of problems than either UT or CW, significantly more so according to a Kruskal Wallis H test ($p < 0.0001$). The HE evaluators each found an average of 25 problems, while the CW evaluators found an average of 18 problems. In the UT evaluation, 11 individual issues arose in each session. However, HE found 14 unique issues which were not found by the CW and UT approaches. UT identified six issues not found in the other evaluations and CW found four. All of the methods were able to detect 38 of the total problems. This is illustrated in Fig. 1.

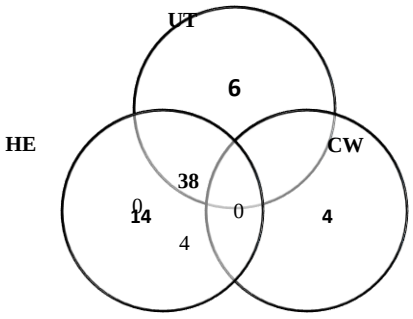


Fig. 1. Venn diagram of the numbers of problems identified by the three evaluation methods (App A).

2) Problem severity: 26 (59%) of the final problems identified in the UT evaluation were of high impact, i.e. either

major or catastrophic). The remaining 41% had low impact, i.e. either minor or cosmetic. However, HE and CW both found 20 (36% and 43% respectively) problems of high impact. In fact, all the problems which were only found by UT method were of high impact, whereas those only found by HE and CW were of low impact (Table II).

3) Problem types: The 66 final problems found on App A were classified as 22 navigational, 19 layout issues, 16 content-related and 9 functional. HE found more layout and content problems, as well as identifying more problems of those types uniquely (Table III).

TABLE II. ISSUE SEVERITY

	UT		HE		CW	
	Unique	**Common**	**Unique**	**Common**	**Unique**	**Common**
Cosmetic	0	4	5	8	2	8
Minor	0	14	9	14	2	14
Major	4	19	0	19	0	19
Catastrophic	2	1	0	1	0	1
Total	6	38	14	42	4	42

TABLE III. PROBLEM TYPES

	UT		HE		CW	
	Unique	**Common**	**Unique**	**Common**	**Unique**	**Common**
Navigation	4	13	3	13	2	13
Layout	1	9	6	11	1	11
Content	1	7	5	9	1	9
Functionality	0	9	0	9	0	9
Total	6	38	14	42	4	42

4) User task performance and satisfaction: Table IV presents the descriptive statistics for task performance and user satisfaction in the UT evaluation. The rate of successful completion indicates that participants encountered difficulties in executing the tasks, as only half were completed, on average. It is clear that the fourth and fifth tasks were found most difficult, being completed only 10% and 8% of the time respectively. The first and second tasks were easier, being completed by 82.1% and 77.4% respectively. This explains why the UT evaluation found more catastrophic usability problems. However, the UT participants evaluated the application's usability highly, giving it an average score of 85, which exceeds the global average SUS score of 68 by a large margin.

TABLE IV. USER TASK PERFORMANCE AND SATISFACTION STATISTICS

	UT	
	Mean	**SD**
Tasks completed	2.50	1.00
Time to complete tasks (m)	33.04	7.35
Number of clicks	170.00	26.63
Number of screens browsed	15.15	4.34
SUS	85.35	10.10

B. App B

1) Usability problems identified: A total of 57 problems were found across the three evaluations for App B. 44 were found by HE, 36 by CW and 32 by UT. Once again, HE found significantly more issues than the other two techniques, which was confirmed by a Kruskal Wallis H test ($p < 0.0001$). The HE evaluators each found 21 problems on average, while those using CW found 16 and each UT session detected nine. The UT and CW methods both failed to spot 15 problems detected by HE, but found five and six, respectively, not found in the other tests. 24 problems were identified by all three evaluation methods (see Fig. 2).

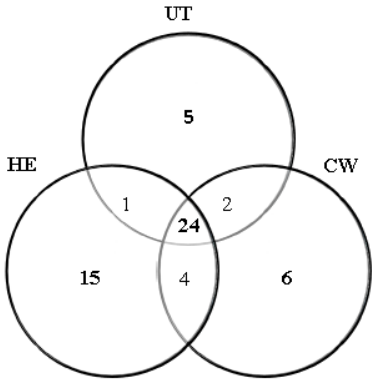


Fig. 2. Venn diagram of the numbers of problems identified by the three evaluation methods (App B).

2) Problem severity: 20 problems identified by the UT method (62%) were of high impact, while 14 (31%) and 15 (41%) of those identified by HE and CW, respectively, were of high impact. The UT method therefore performed better at identifying more severe problems and all of the problems found uniquely by UT were of high impact, whereas all of those found uniquely by HE were of low impact, as shown in Table V.

TABLE V. PROBLEM SEVERITY

	UT		HE		CW	
	Unique	**Common**	**Unique**	**Common**	**Unique**	**Common**
Cosmetic	0	3	3	3	3	2
Minor	0	9	12	12	3	13
Major	4	14	0	13	0	14
Catastrophic	1	1	0	1	0	1
Total	5	27	15	29	6	30

TABLE VI. PROBLEM TYPES

	UT		HE		CW	
	Unique	**Overlap Problems**	**Unique**	**Overlap Problems**	**Unique**	**Overlap Problems**
Navigation	2	8	3	10	0	10
Layout	3	4	6	6	3	5
Content	0	2	5	2	3	2
Functionality	0	13	1	11	0	13
Total	5	27	15	29	6	30

3) Problem types: App B's 57 final problems were classified as 15 navigational, 18 layout-related, 10 content-related and 14 functional (see Table VI). As with App A, HE found more layout and content problems, as well as identifying more problems of all types uniquely.

4) User task performance and satisfaction: Table VII presents the descriptive statistics for task performance and user satisfaction in the UT evaluation. The rate of successful completion indicates that participants encountered difficulties in executing the tasks, as only 3.2 were completed, on average. As with App A, the fourth and fifth tasks were most difficult, having completion rates of 14% and 11% respectively, while the first and second tasks were easier. Participants rated the application with a SUS of 77, which is also above the global average SUS score.

C. Correlation Analysis

Spearman's correlation coefficient was used across the two application case studies to examine any correlations that exist between the measures employed in the study [33]. As can be seen from Table VIII, one correlation that is statistically significant was found, between the time spent by participants on tasks and the number of problems found.

TABLE VII. USER TASK PERFORMANCE AND SATISFACTION STATISTICS

	UT	
	Mean	**SD**
Tasks completed	3.20	1.10
Time to complete tasks (m)	35.16	11.10
Number of clicks	173.30	28.45
Number of screens browsed	17.35	3.88
SUS	77.65	11.74

D. The Applications' Usability Levels

As described above, the usability evaluations revealed 123 problems with the two applications under test. This is a significant number of issues, which corresponds to a low level of usability. 46 of these problems (nearly 38%) were severe issues, having a significant impact on task performance. The majority of problems were navigational and related to the layout of the interface (both 30%), which indicates that users are likely to find it difficult to navigate within the applications. This finding is also supported by the rates of successful task completion. The results therefore clearly show that there needs to an improvement of both of these applications' usability.

TABLE VIII. CORRELATIONS BETWEEN MEASURES IN THE UT METHOD

	Tasks completed	**Time to complete tasks**	**No. of clicks**	**No. of screens browsed**	**SUS**	**No. of problems**
Tasks completed	1	-0.02	0.21	0.1	0.01	0.12
Time to complete tasks	-0.02	1	-0.18	-0.17	-0.25	0.39*
No. of clicks	0.21	-0.18	1	0.08	0	-0.02
No. of screens browsed	0.1	-0.17	0.08	1	0.1	-0.16
SUS	0.01	-0.25	0	0.1	1	0.05
No. of problems	0.12	0.39*	-0.02	-0.16	0.05	1

* The significance level is 0.05

V. DISCUSSION

No prior research has compared the UEMs considered in this study in relation to m-health applications in Saudi Arabia, so it is no possible to draw any comparisons with comparable studies.

A. Is there a Difference between the Performance of UT, HE, and CW Methods in Evaluating M-Health Applications?

In general, the findings of this study are common to both m-health applications studied. HE found the most problems overall and detected more problems than either UT or CW techniques, but UT was able to detect more severe problems. Similar findings emerged from studies of other systems [19,21,34], where HE was found to detect more minor issues than did UT. This is also in line with Farzandipour et al. [35], who found that HE was better at detecting usability issues than the CW technique.

HE's identification of greater numbers of problems can be attributed to the fact that the HE evaluator were able to explore the applications, whereas the CW and UT participants were given specific tasks to do, so that there was a limit to the kind and number of usability problems that they would encounter. It is therefore recommended that the design of m-health applications should utilise both HE and UT methods in order to derive the maximum benefits.

B. Is there a Correlation between UT Metrics?

A strong correlation was found between the time taken to complete tasks and the number of usability problems encountered on these two m-health applications. This result indicates that time taken is a better indicator of the presence of usability problems than other measures.

It was also evident that the SUS does not serve well as a usability metric for m-health applications on its own. This is because it does not predict the presence of usability problems as well as task completion time. Usability practitioners should therefore at least report task completion times in addition to SUS in usability reports. This is in agreement with the findings of recent research into SUS. For instance, Broekhuis et al. [36] also found SUS to be inadequate by itself for e-health system usability evaluations.

SUS's poor predictive power may be due to a number of factors. 1) it is subjective, which means that usability is but one factor influencing the perception of the assessor, along with, for instance, usefulness and enjoyability. 2) SUS is generalised and does not reflect participants' actual performance; greater difficulty and more problems were encountered with App A, yet it received a higher average SUS. 3) SUS does not recognise such inclusivity factors as accessibility (e.g. for people with learning difficulties or visual disabilities) and information overload, even though they affect usability. Future research should include a comprehensive assessment of such factors and their impacts on usability, which is especially important in the context of health-related applications and systems.

C. What is the Current Usability Level of M-Health Applications in the Kingdom of Saudi Arabia?

This study found that the m-health applications targeted do not meet acceptable usability standards and fail to conform to appropriate design principles. According to the UEMs applied, these two applications are very hard to use, due to the large number of usability problems which arise, which was especially clear from the inspection by an independent expert and the task performance data in the UT sessions, even though the applications received good SUS ratings, which, is not a reliable indicator. These findings contradict previous research into user satisfaction with m-health applications in Saudi Arabia [8, 23], which found general satisfaction, perhaps because those studies relied on questionnaire-based, subjective data.

D. Recommendations

On the basis of the results of this study, a number of recommendations is presented below.

1) The varying effects of different UEMs should be considered seriously when evaluating the usability of m-health apps, as the findings suggest that results may differ depending on the method used. Therefore, practitioners should consider the pros and cons of each approach when deciding on an evaluation method.

2) Consider using the UT method when interested in identifying high severity usability problems.

3) Consider using the HE method when seeking to find higher numbers of low severity usability problems—particularly those relating to content and layout.

4) Both UT and HE should be employed during the design process of m- health applications for maximum effectiveness.

5) Usability practitioners should be aware of the fact that participants' satisfaction with the perceived usability of m-health application does not correlate with the number of usability problems that found on the interface. This implies that SUS questionnaires should not be used as a sole metric for determining the usability of the m-health interfaces.

6) There is a need to an improvement of m-health applications' usability in Saudi Arabia. In particular, the navigation and layout aspects of the interface should be given more attention.

7) Web developers are key to ensuring the usability of m-health apps. If there is to be a positive effect, it is important for developers to enhance their awareness of usability standards.

E. Limitations and Future Work

There are, inevitably, some limitations to the present study. First, the UT sessions recorded various task performance parameters, but did not measure behavioural factors, such as attention levels, which other studies have estimated using eye tracking technology [37]. Second, the study was limited to two Saudi m-health applications, which, whilst in common use, may

not reflect the overall usability of m-health applications in Saudi Arabia. Therefore, more research with a broader spectrum of m-health applications across different healthcare domains would be necessary to further assess the generalizability of the results.

VI. Conclusion

This study compared three usability evaluation methods, namely, usability testing, heuristic evaluation, and cognitive walkthrough in terms of their effectiveness in assessing m-health application usability, and to assess the usability of such applications in the Saudi Arabian context. It also explored the relationships between usability metrics. The study finds that heuristic evaluation is able to identify a larger number of usability issues, which is because it takes a broad overview of system design, with predefined principles, rather than focusing on the performance of specific tasks. However, it does appear to identify more minor problems than the usability testing method, which is better at detecting more severe issues. The study also identified a significant relationship between the number of usability problems found and how long participants spend carrying out tasks using m-health applications, which suggests that the existence of usability problems. The findings also show that the two applications tested have low usability levels and need to be improved.

References

[1] Islam MN, Karim MM, Inan TT, Islam AN. Investigating usability of mobile health applications in Bangladesh. BMC medical informatics and decision making. 2020 Dec;20:1-3.

[2] Istepanian R, Laxminarayan S, Pattichis CS, editors. M-health: Emerging mobile health systems. Springer Science & Business Media; 2007 Jan 4.

[3] Kay M, Santos J, Takane M. mHealth: New horizons for health through mobile technologies. World Health Organization. 2011 Jun 7;64(7):66-71.

[4] Tomlinson M, Solomon W, Singh Y, Doherty T, Chopra M, Ijumba P, Tsai AC, Jackson D. The use of mobile phones as a data collection tool: a report from a household survey in South Africa. BMC medical informatics and decision making. 2009 Dec;9:1-8.

[5] Rotheram-Borus MJ, Le Roux IM, Tomlinson M, Mbewu N, Comulada WS, Le Roux K, Stewart J, O'Connor MJ, Hartley M, Desmond K, Greco E. Philani Plus (+): a Mentor Mother community health worker home visiting program to improve maternal and infants' outcomes. Prevention Science. 2011 Dec;12:372-88.

[6] Siedner MJ, Haberer JE, Bwana MB, Ware NC, Bangsberg DR. High acceptability for cell phone text messages to improve communication of laboratory results with HIV-infected patients in rural Uganda: a cross-sectional survey study. BMC medical informatics and decision making. 2012 Dec;12:1-7.

[7] Haberer JE, Robbins GK, Ybarra M, Monk A, Ragland K, Weiser SD, Johnson MO, Bangsberg DR. Real-time electronic adherence monitoring is feasible, comparable to unannounced pill counts, and acceptable. AIDS and Behavior. 2012 Feb;16:375-82.

[8] Alanzi TM. Users' satisfaction levels about mHealth applications in post-Covid-19 times in Saudi Arabia. PloS one. 2022 May 4;17(5):e0267002.

[9] Shati A. Mhealth applications developed by the Ministry of Health for public users in KSA: a persuasive systems design evaluation. Health Informatics Int J. 2020;9(1):1-3.

[10] Broekhuis M, van Velsen L, Hermens H. Assessing usability of eHealth technology: a comparison of usability benchmarking instruments. International journal of medical informatics. 2019 Aug 1;128:24-31.

[11] Georgsson M, Staggers N. Quantifying usability: an evaluation of a diabetes mHealth system on effectiveness, efficiency, and satisfaction metrics with associated user characteristics. Journal of the American Medical Informatics Association. 2016 Jan 1;23(1):5-11.

[12] Harrison R, Flood D, Duce D. Usability of mobile applications: literature review and rationale for a new usability model. Journal of Interaction Science. 2013 Dec;1:1-6.

[13] Mubeen M, Iqbal MW, Junaid M, Sajjad MH, Naqvi MR, Khan BA, Saeed MM, Tahir MU. Usability evaluation of pandemic health care mobile applications. InIOP conference series: earth and environmental science 2021 Mar 1 (Vol. 704, No. 1, p. 012041). IOP Publishing.

[14] Alharbi A, Alzuwaed J, Qasem H. Evaluation of e-health (Seha) application: a cross-sectional study in Saudi Arabia. BMC medical informatics and decision making. 2021 Dec;21:1-9.

[15] Zhou L, Bao J, Setiawan IM, Saptono A, Parmanto B. The mHealth app usability questionnaire (MAUQ): development and validation study. JMIR mHealth and uHealth. 2019 Apr 11;7(4):e11500. Tan WS, Liu D, Bishu R. Web evaluation: Heuristic evaluation vs. user testing. International Journal of Industrial Ergonomics. 2009 Jul 1;39(4):621-7.

[16] Hasan L, Morris A, Probets S. A comparison of usability evaluation methods for evaluating e-commerce websites. Behaviour & Information Technology. 2012 Jul 1;31(7):707-37.

[17] Doubleday A, Ryan M, Springett M, Sutcliffe A. A comparison of usability techniques for evaluating design. InProceedings of the 2nd conference on Designing interactive systems: processes, practices, methods, and techniques 1997 Aug 1 (pp. 101-110).

[18] Jeffries R, Miller JR, Wharton C, Uyeda K. User interface evaluation in the real world: a comparison of four techniques. InProceedings of the SIGCHI conference on Human factors in computing systems 1991 Mar 1 (pp. 119-124).

[19] Thyvalikakath TP, Monaco V, Thambuganipalle H, Schleyer T. Comparative study of heuristic evaluation and usability testing methods. Studies in health technology and informatics. 2009;143:322.

[20] Khajouei R, ZahiriEsfahani M, Jahani Y. Comparison of heuristic and cognitive walkthrough usability evaluation methods for evaluating health information systems. J Am Med Inform Assoc. 2017;24(e1):e55–60.

[21] Maguire M, Isherwood P. A comparison of user testing and heuristic evaluation methods for identifying website usability problems. In: Marcus A, Wang W, editors. Design, user experience, and usability: theoty and practice: 7th international conference (DUXU 2018), Las Vegas, NV, USA, 15–20 July 2018, Part I. p. 429–438.

[22] Arafa A, Mostafa ZM, Sheerah HA, Alzahrani F, Almuzaini Y, Senosy S, Hassan RI. mHealth app barriers, usability, and personalization: a cross-sectional study from Egypt and Saudi Arabia. Journal of Personalized Medicine. 2022 Dec 9;12(12):2038.

[23] Shilbayeh SA, Ismail SA. Patient experience with an educational mobile health application: A pilot study on usability and feasibility in a Saudi population. Cogent Psychology. 2020 Dec 31;7(1):1843883.

[24] Lazar J, Feng JH, Hochheiser H. Research methods in human-computer interaction. Morgan Kaufmann; 2017 Apr 28.

[25] Maguire M. Context of use within usability activities. International journal of human-computer studies. 2001 Oct 1;55(4):453-83.

[26] Sauro J, Lewis JR. Quantifying the user experience: Practical statistics for user research. Morgan Kaufmann; 2016 Jul 12.

[27] Reynoso JM, Olfman L, Ryan T, Horan T. An information systems design theory for an expert system for training. Journal of Database Management (JDM). 2013 Jul 1;24(3):31-50.

[28] The Communications, Space, and Technology Commission. The Saudi Internet Report. 2024 April. Online available at https://www.cst.gov.sa/en/mediacenter/pressreleases/Pages/2024042402.aspx Accessed [May. 18, 2024]

[29] Nielsen J, Molich R. Heuristic evaluation of user interfaces. InProceedings of the SIGCHI conference on Human factors in computing systems 1990 Mar 1 (pp. 249-256).

[30] Blackmon MH, Polson PG, Kitajima M, Lewis C. Cognitive walkthrough for the web. InProceedings of the SIGCHI conference on human factors in computing systems 2002 Apr 20 (pp. 463-470).

[31] Alhadreti O. Comparing two methods of usability testing in Saudi Arabia: concurrent think-aloud vs. co-discovery. International Journal of Human–Computer Interaction. 2021 Jan 20;37(2):118-30.

[32] Hertzum M, Jacobsen NE. The evaluator effect: A chilling fact about usability evaluation methods. International journal of human-computer interaction. 2001 Dec 1;13(4):421-43.

[33] Sedgwick P. Spearman's rank correlation coefficient. Bmj. 2014 Nov 28;349.

[34] Wang E, Caldwell B. An empirical study of usability testing: heuristic evaluation vs. user testing. InProceedings of the Human Factors and Ergonomics Society Annual Meeting 2002 Sep (Vol. 46, No. 8, pp. 774-778). Sage CA: Los Angeles, CA: SAGE Publications.

[35] Farzandipour M, Nabovati E, Sadeqi Jabali M. Comparison of usability evaluation methods for a health information system: heuristic evaluation versus cognitive walkthrough method. BMC Medical Informatics and Decision Making. 2022 Jun 18;22(1):157.

[36] Broekhuis M, van Velsen L, Hermens H. Assessing usability of eHealth technology: a comparison of usability benchmarking instruments. International journal of medical informatics. 2019 Aug 1;128:24-31.

[37] Țichindelean M, Țichindelean MT, Cetină I, Orzan G. A comparative eye tracking study of usability—towards sustainable web design. Sustainability. 2021 Sep 18;13(18):10415.

Automated Hydroponic Growth Simulation for Lettuce Using ARIMA and Prophet Models During Rainy Season in Indonesia

Lendy Rahmadi[1]*, Hadiyanto[2], Ridwan Sanjaya[3]
Doctoral Program of Information System, Diponegoro University, Semarang 50241, Indonesia[1, 2]
Department of Information System, Lembah Dempo University, Pagar Alam 31514, South Sumatera, Indonesia[1]
Department of Information System, Soegijapranata Catholic University, Semarang 50234, Indonesia[3]

***Abstract*—Hydroponic farming particularly lettuce cultivation, is gaining popularity in Indonesia due to its economical use of water and space, as well as its short growing season. This study focuses on developing of an Automated Hydroponic Growth Simulation for Lettuce Using ARIMA and Prophet Models during the Rainy Season in Indonesia. We developed a simulation model for lettuce development in the Nutrient Film Technique (NFT) hydroponic system using data collected over four harvest periods during the rainy season in early 2024. Two machine learning models, ARIMA and Prophet, are tested to see which is more effective at forecasting lettuce growth. The Prophet model has the greatest results, with a Mean Absolute Error (MAE) of 1.475 and a Root Mean Square Error (RMSE) of 1.808. Based on this, the Prophet model is utilized to create a web application using Streamlit for real-time growth predictions. Future studies should include more data, particularly from the dry season, to increase model flexibility, as well as investigate the use of other crops and machine learning methods, including hybrid models, to improve forecasts.**

***Keywords*—ARIMA; automated; growth; hydroponic; prophet; simulation**

I. Introduction

Hydroponics is a method of cultivating plants without soil, instead using water and nutrient solutions as the growing medium. This technology has become increasingly popular in Indonesia due to its efficiency in water and space usage, as well as its ability to produce higher-quality crops compared to conventional methods [1]. The trend of using hydroponics in Indonesia has surged in response to growing urban populations and the need for sustainable farming in controlled environments [2]. In Indonesia, hydroponic farming, especially for crops like lettuce, has become a widely adopted technique due to its ability to optimize space and produce yields faster than traditional farming methods. However, hydroponic plant growth is highly dependent on multiple variables. Internal variables such as nutrient concentrations, water temperature, and pH levels directly influence the plant's ability to absorb nutrients. External variables, such as ambient temperature, humidity, and light intensity, further determine the overall growth environment. Managing the interaction between these internal and external factors is complex, as even slight changes in one variable can drastically affect plant health and growth rate [2], [3]. Farmers currently face the challenge of not being able to simulate or predict plant growth. They must wait through the entire growth cycle to observe results, without any predictive system in place. This reliance on post-harvest data leaves room for inefficiencies, and farmers are unable to make informed interventions during the growth phase [4]. As a result, the need for a simulation model that allows real-time prediction and optimization of hydroponic plant growth is critical. Such a system would help farmers simulate future growth patterns, enabling them to make proactive adjustments to environmental variables and optimize the hydroponic system accordingly.

Hydroponics relies heavily on various environmental factors such as temperature, humidity, pH levels, and nutrient concentrations in the water, all of which play crucial roles in determining the growth rate and yield of the crops [5]. To maximize productivity, this study uses the Nutrient Film Technique (NFT) system, where plant roots are continuously submerged in a circulating nutrient solution, ensuring direct access to both nutrients and oxygen [6].

In this study, lettuce (Lactuca sativa) was chosen as the primary subject because it is widely cultivated hydroponically and has a relatively short growth cycle [1]. Data on plant growth was collected daily over four crop cycles, measuring key variables such as temperature, humidity, pH, and nutrient concentrations in the hydroponic solution [7]. Given the complexity of managing these variables, farmers often cannot accurately simulate growth patterns, leading to reliance on reactive measures rather than predictive optimization. This research aims to address that challenge by proposing an automated simulation model, particularly critical during dynamic weather conditions like Indonesia's rainy season. Data collection was carried out using calibrated instruments that were regularly checked for accuracy to ensure precise measurements [8]. This approach provides detailed data on the dynamic interactions of hydroponic variables that influence lettuce growth, offering key insights into how these factors can be optimized to enhance overall yields [9], [10].

Currently, there is no existing model that automatically simulates plant growth in the context of hydroponics, especially during the rainy season. Previous studies, such as those by Sambo et al. (2019) and Ullah et al. (2019), explored the use of IoT to monitor hydroponic variables in real time. However, these studies still rely on manual control without integrating automated plant growth simulations based on actual data. Similarly, Schwartz et al. (2019) addressed automation in

hydroponics, but the model they proposed only accounted for static environmental conditions, not considering seasonal variables like rainfall.

Other studies have utilized predictive models such as ARIMA and Prophet, as seen in the work of Rajendiran & Rethnaraj (2024) and López Mora et al. (2024), which predominantly focus on industrial sectors or weather forecasting, rather than hydroponic farming. The application of these models to predict plant growth in hydroponic environments, especially during the rainy season, remains largely unexplored. Additionally, while there are studies that use ARIMA and Prophet to predict temperature or weather patterns, no research to date has directly compared the performance of these models in the context of lettuce hydroponics in Indonesia.

The research gap is further highlighted by the absence of models capable of integrating automated simulations into a practical web-based application that allows real-time interaction for hydroponic farmers. Such an application would allow farmers to take preemptive measures by simulating growth conditions and understanding the influence of dynamic weather patterns, especially during unpredictable rainy seasons in Indonesia [1], [5]. There is a significant opportunity to develop a web-based solution that facilitates automated plant growth simulations under dynamic seasonal conditions, such as Indonesia's rainy season [1], [2], [5]

This study aims to develop an automated hydroponic simulation model using regression-based ARIMA and Prophet models, focusing on lettuce growth during Indonesia's rainy season. The data used is based on daily observations from January to May 2024. The model is designed to predict environmental variables such as temperature, humidity, and pH to optimize plant growth automatically. Additionally, this study compares the performance of the two predictive models by evaluating their results using the Mean Absolute Error (MAE) and Root Mean Square Error (RMSE) metrics. The findings indicate that the Prophet model outperforms ARIMA in predicting seasonal conditions, particularly during the unstable weather of the rainy season. Finally, the superior Prophet model was implemented into an interactive web application, enabling hydroponic farmers to simulate plant growth automation in real-time. This application aims to improve efficiency and optimize hydroponic production in tropical environments with dynamic weather conditions.

This research introduces a novel approach by developing an automated hydroponic growth simulation model using ARIMA and Prophet, leveraging actual data from Indonesia's rainy season—an area that has rarely been explored in the context of hydroponic farming. This approach allows for more accurate predictions of lettuce growth under dynamic tropical weather conditions. The main contribution of this study is the implementation of the superior Prophet model into an interactive web application, which enables hydroponic farmers to perform real-time automated plant growth simulations, thereby enhancing production efficiency during the rainy season. The research addresses the gap in the literature concerning the lack of automated hydroponic simulation models during the rainy season while offering a practical technology-based solution for hydroponic farmers.

II. Materials and Methods

A. Hydroponics

Hydroponics is a method of cultivating plants without soil, where nutrient-enriched water serves as the primary medium to meet the plants' nutritional needs. Hydroponics involves the use of water as a medium for the cultivation of crops [11]. This method is becoming increasingly popular in Indonesia due to its efficiency in using water and land, as well as its ability to produce higher-quality crops compared to conventional farming methods [1]. One of the most commonly used techniques in hydroponics is the Nutrient Film Technique (NFT), where a thin film of nutrient solution flows around the plant roots, providing direct access to oxygen and nutrients [2].

Key variables in a hydroponic system include temperature, humidity, pH, and nutrient concentration in the solution. The ideal temperature range for plant growth is between 18°C and 25°C, while the optimal pH level is between 5.5 and 6.5. Nutrient concentration is measured by Electrical Conductivity (EC), with the ideal range for lettuce being between 1.2 and 1.8 mS/cm. Additionally, the ideal humidity for hydroponic plants is between 50% and 70% [6]. If these variables are not properly controlled, plants can experience stress, negatively affecting crop yields [5]. Table I summarizes the ideal values for key variables in growing lettuce in a hydroponic system.

TABLE I. Ideal Variables for Growth Phase Lettuce in Hydroponic Systems [8]

Variable	Ideal Range
Temperature	18°C - 25°C
pH	6.0 - 7.0
Humidity	50% - 75%
EC (mS/cm)	1.2 - 1.8
Nutrients (ppm)	800 - 1000 ppm

Modern hydroponic systems often use automated sensors to monitor these variables in real-time, allowing for immediate adjustments if there are drastic changes in environmental conditions, such as during the rainy season. These sensors can detect temperature, pH, humidity, and nutrient levels, sending real-time data to a server for analysis and automatic adjustments [8]. Automated simulations based on seasonal environmental data are essential for maintaining the stability and efficiency of plant growth, especially during unpredictable weather conditions [2].

B. Machine Learning in Hydroponic Agriculture

Machine learning, a branch of artificial intelligence, enables computers to learn from data, recognize patterns, and make decisions or predictions without being explicitly programmed. In various fields, including agriculture, machine learning has become a powerful tool for optimizing processes and improving outcomes by utilizing predictive algorithms. In the agricultural sector, machine learning is widely applied to predict crop yields, manage resources, and monitor environmental conditions

affecting plant growth. The use of machine learning in hydroponic systems helps farmers make faster and more accurate decisions based on real-time data collected from sensors in the field [12].

One common approach in machine learning is supervised learning, where models are trained using labeled data to predict specific outcomes or decisions. In hydroponics, supervised learning is often used to predict variables that influence plant growth, such as temperature, humidity, pH levels, and nutrient concentrations. Algorithms frequently employed in this context include Random Forest, Decision Trees, Support Vector Machines (SVM), and Neural Networks. These algorithms can help farmers manage resources efficiently and increase crop productivity [13]. For example, Random Forest is particularly useful for predicting the non-linear relationships between environmental variables that affect crop yields in hydroponic systems [14].

Machine learning applications in agriculture, particularly hydroponics, also involve models like Long Short-Term Memory (LSTM) and ARIMA, which are designed to handle time-series data. LSTM, a type of neural network, is used to process sequential data and is well-suited for predicting time-related variables such as temperature or humidity in hydroponic systems [15]. On the other hand, ARIMA is used to analyze seasonal data and make long-term predictions based on historical trends. Both models are instrumental in optimizing hydroponic systems by maintaining ideal conditions for plant growth [16].

In IoT (Internet of Things)-based hydroponic systems, sensors collect real-time data that is then processed by machine learning algorithms. This technology allows for automated simulations that adjust key plant growth parameters, such as nutrient supply and temperature control. These models provide predictive recommendations to farmers, enabling them to manage hydroponic systems efficiently without the need for continuous manual intervention [17]. Overall, the integration of machine learning has revolutionized hydroponic management, from monitoring environmental variables to automating production processes [12].

Moreover, machine learning enhances the accuracy of yield predictions by analyzing environmental variables that influence plant growth. For example, regression models can predict plant growth behavior in hydroponic systems based on historical data, allowing farmers to make more informed decisions regarding crop management. With the increasing adoption of machine learning technology in agriculture, these predictive models hold significant potential for improving efficiency and productivity in modern farming environments [12], [18].

C. ARIMA Model

The Autoregressive Integrated Moving Average (ARIMA) model is a widely used statistical method for analyzing and predicting time-series data. It is particularly popular for its ability to process data with seasonal patterns, trends, and stochastic components, which often occur in datasets related to price forecasting, weather, and, in this context, agriculture and hydroponics. ARIMA is highly effective at handling non-stationary data, where the data distribution changes over time—a pattern frequently seen in environmental variables such as temperature, humidity, and nutrient levels in hydroponic systems [19].

The ARIMA model consists of three main components: Autoregressive (AR), Integrated (I), and Moving Average (MA). The AR component predicts future values based on the past values of the variable. The I (Integrated) component is used to transform non-stationary data into stationary data by calculating the differences between consecutive data points. The MA (Moving Average) component predicts future values based on the errors (residuals) of previous predictions (Pindipo et al., 2023). The ARIMA model is commonly written as ARIMA(p, d, q), where p refers to the order of the autoregressive component, d is the degree of differencing to make the data stationary, and q is the order of the moving average component [20].

The general formula for ARIMA can be expressed as follows:

$$Y_t = c + \sum_{i=1}^{p} \phi_i Y_{t-i} + \sum_{j=1}^{q} \theta_j \epsilon_{t-j} + \epsilon_t \quad (1)$$

In this equation, Y_t represents the actual value at time *t*, c is a constant, ϕ_i are the AR coefficients, θ_j are the MA coefficients, and ϵ_t is the residual error at time *t*. The ARIMA model focuses on two key aspects of time-series data: trends and residual errors. In this context, the observed trends in past data are used to predict future values, while the influence of random fluctuations is minimized [21].

The ARIMA process begins by examining whether the data is stationary. If it is not, the model applies differencing to stabilize the data by calculating the differences between consecutive values until the data becomes stationary. Once the data is stationary, the autoregressive (AR) component predicts future values based on past data, while the moving average (MA) component accounts for prediction errors from the AR model [22]. This approach allows ARIMA to handle time-series data with seasonal patterns and complex trends, making it well-suited for predicting environmental variables such as temperature, humidity, and nutrient levels in hydroponic systems [20].

One of the key strengths of the ARIMA model is its ability to handle non-stationary data, which is often a challenge in time-series analysis. However, ARIMA also has limitations, such as its reduced flexibility in managing highly complex or non-linear data, where more advanced models like Long Short-Term Memory (LSTM) networks or Neural Networks tend to perform better. Therefore, in some studies, ARIMA is combined with other models to enhance prediction accuracy [19], [23].

In agriculture and hydroponic systems, ARIMA has been widely applied to predict environmental variables that influence plant growth. For example, Menculini et al. (2021) compared the performance of ARIMA with deep learning models in forecasting food prices, finding that while ARIMA is reliable for short-term predictions, deep learning models are better suited to handling more complex time-series data. In hydroponic systems, ARIMA has been used to predict humidity and temperature levels, which are crucial for maintaining a

stable growing environment. The combination of ARIMA with real-time sensor data allows hydroponic farmers to make faster and more accurate decisions in managing environmental conditions [24].

Additionally, ARIMA is frequently used to forecast temperature and weather patterns, which are key factors in agriculture and hydroponics. For instance, Elseidi et al. (2024) applied ARIMA to predict high-frequency temperature data and combined it with the Prophet model to improve accuracy. Their findings showed that the hybrid ARIMA-Prophet model provided more accurate forecasts than ARIMA alone, particularly in cases where the data exhibited strong seasonal patterns or trends [20].

In another study, Pindiga et al. (2023) compared ARIMA with the Facebook Prophet model in predicting stock indices, which also exhibit seasonal patterns and trends similar to agricultural data. The results indicated that Prophet tends to outperform ARIMA when handling complex seasonal data, but ARIMA remains a strong choice for short-term predictions or simpler datasets [25].

ARIMA's applications in agriculture are not limited to environmental variable predictions. The model has also been used to forecast crop yields based on historical growth data and weather conditions. Kasthuri et al. (2021) used ARIMA in combination with Neural Networks to predict food production yields, offering more accurate crop yield forecasts in scenarios where environmental variables fluctuate significantly. This hybrid approach is becoming increasingly popular in time-series prediction, especially in the agricultural sector, which depends heavily on seasonal data and changing weather conditions [26].

Overall, ARIMA is a powerful and versatile model for time-series data analysis and forecasting. With its ability to process non-stationary data and handle trends and seasonal patterns, ARIMA is well-suited for use in hydroponic farming. However, for more complex or non-linear datasets, hybrid models or deep learning techniques may provide better results. Nonetheless, ARIMA remains one of the most widely used models for time-series forecasting due to its simplicity and reliability in processing relatively straightforward data [19], [21].

D. Prophet Model

The Prophet model is a time-series forecasting tool developed by Facebook (now Meta) designed to handle data with seasonal patterns, trends, and outliers. Prophet is often used for predicting data that exhibits instability in trends, such as sudden changes or irregular seasonal patterns. One of its key strengths is its ability to handle gaps (missing data) and outliers effectively, while still providing accurate predictions even in rapidly changing conditions [22].

Unlike traditional time-series models like ARIMA, Prophet uses an additive approach, where the trend, seasonal, and outlier components are treated separately and then combined to produce the final forecast. The model assumes that time-series data can be broken down into three main components: trend $g(t)$, seasonality $s(t)$, and holiday or event effects $h(t)$, with an additional residual or noise component ϵt. Mathematically, the Prophet model can be described by the following equation [27]:

$$y(t) = g(t) + s(t) + h(t) + \epsilon t \quad (2)$$

Where:

- $y(t)$ is the predicted value at time ttt,
- $g(t)$ is the trend component,
- $s(t)$ is the seasonal component,
- $h(t)$ represents holidays or special events,
- and ϵt is the noise component [28].

Prophet uses piecewise linear regression or logistic growth to capture trends in the data. One of its advantages is the ability to automatically adjust the number of change points in the trend, allowing the model to account for sudden shifts in direction. The seasonal component is defined by a set period, such as yearly, weekly, or monthly, enabling Prophet to capture recurring seasonal patterns more flexibly. The holiday or event component allows for the inclusion of external factors like holidays or recurring seasonal events, which can influence the data [29].

Prophet is highly intuitive to use because it automatically detects and handles missing data within the time-series. The model can also adjust the prediction intervals by giving more confidence to the trend and seasonal components, compared to more traditional time-series models [30]. Additionally, Prophet allows users to customize the prediction intervals, providing flexibility in terms of accuracy and margin of error based on the user's needs [31].

One common application of Prophet is in stock price forecasting and economic data predictions, which require accurate forecasts that can handle fluctuating seasonal trends and trends that are often unstable. For example, Jin et al. (2022) used Prophet to predict Google stock prices, while Angelo & Fadhilrahman (2023) compared the performance of Prophet and ARIMA in forecasting Bitcoin prices. Their findings indicated that Prophet excels in capturing complex seasonal trends and handling data with significant fluctuations [22], [32].

Prophet is also widely used in the energy and weather sectors. For instance, Elseddi et al. (2024) combined Prophet with ARIMA to forecast temperature data, achieving better accuracy than using ARIMA alone. This hybrid approach allows for more comprehensive forecasting by capturing different characteristics of the time-series data [20].

Overall, Prophet is a powerful and flexible model for forecasting complex time-series data, particularly when the data has irregular seasonal patterns. With its additive approach and its flexibility in handling outliers, Prophet offers significant advantages across various sectors, including economics, agriculture, energy, and weather forecasting. Its wide applications range from predicting food prices and crop yields to forecasting energy demand and weather patterns [24].

E. Evaluation Matrix

In evaluating the performance of predictive models, two of the most commonly used metrics are the Mean Absolute Error

(MAE) and the Root Mean Square Error (RMSE). These metrics are essential in assessing how well a model predicts data and provide insight into the level of error between predicted values and actual values.

1) Mean Absolute Error (MAE): The Mean Absolute Error (MAE) measures the average of the absolute differences between predicted values and actual values. MAE gives an overall sense of how much error the model makes on average, without considering whether the error is positive or negative, as all errors are treated equally. The general formula for calculating MAE is:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i| \quad (3)$$

Where:

- y_i is the actual value,
- $\hat{y}_i$ is the predicted value,
- n is the number of data points.

MAE provides an intuitive and easy-to-understand result since it shows the magnitude of errors in the same units as the original data. For example, in a study by Kenyi and Yamamoto (2024), MAE was used to evaluate the performance of the SARIMA-Prophet model in predicting water flow, and the results showed that MAE helped identify the average level of prediction error at each time point [33]. Another study by Angelo and Fadhilrahman (2023) used MAE to compare the performance of ARIMA and Prophet models in predicting Bitcoin prices, demonstrating how MAE can measure the accuracy of time-series predictions in complex datasets [32].

2) Root mean square error (RMSE): Root Mean Square Error (RMSE) is another common metric for evaluating predictive model accuracy. RMSE calculates the square root of the average squared differences between predicted and actual values. Unlike MAE, which focuses on absolute differences, RMSE gives more weight to larger errors because the errors are squared before being averaged. The general formula for RMSE is:

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2} \quad (4)$$

Where:

- y_i is the actual value,
- $\hat{y}_i$ is the predicted value,
- n is the number of data points.

RMSE is particularly useful when larger errors are more undesirable than smaller ones, as it penalizes large errors more heavily. In a study by Hamiane et al. (2024), RMSE was used to measure the accuracy of hybrid LSTM, ARIMA, and Prophet models in predicting future GDP, showing that RMSE was highly effective in identifying significant differences between predictions and actual data over certain periods. Similarly, Mokhtar et al. (2022) applied RMSE to predict hydroponic yields, revealing that RMSE is more sensitive to outliers than MAE, making it an important evaluation metric when dealing with highly variable data [13], [34].

Using both RMSE and MAE together provides a more comprehensive picture of model performance. While MAE gives a general overview of the average error, RMSE emphasizes larger errors, which can be crucial in applications where minimizing extreme errors is important. Therefore, in many studies, these two metrics are often used together to evaluate time-series predictive models, including in hydroponic farming and energy prediction applications [12].

This combined approach allows for a better understanding of model behavior under various conditions, ensuring that both overall performance and outlier sensitivity are addressed. By evaluating models using MAE and RMSE, researchers can fine-tune predictions to optimize both short-term and long-term outcomes

F. Dataset Preparation Description

In the process of preparing the dataset for machine learning modeling, the first step involved collecting data from the hydroponic system. The dataset includes several critical environmental and growth metrics to ensure that the information fed into the models is relevant and accurate.

TABLE II. INITIAL DATASET SHOWING ENVIRONMENTAL CONDITIONS AND PLANT GROWTH METRICS

	day	hole	time	temperature	humidity	light	pH	Ec	TDS	WaterTemp	LeafCount
0	1	1	09:19:00	26.8	72	17820	7.2	677	340	26.1	3
1	1	2	09:23:00	26.6	72	16490	7.2	677	338	26.1	3
2	1	3	09:27:00	26.4	72	15160	7.2	678	334	26.1	3
3	1	4	09:31:00	26.2	72	13830	7.2	677	338	26.1	3
4	1	5	09:35:00	26.2	72	12500	7.2	673	340	26.1	3

The Table II, summarizes the primary data columns that were included in the dataset. This data was collected at specific time intervals from each plant hole in the hydroponic system.

- Day: Represents the day number during the data collection process, crucial for understanding time-based trends and growth patterns in the plants [12].
- Hole: This refers to the individual plant hole in the hydroponic system. Each hole corresponds to a plant, and this column ensures that the data collected is specific to each plant [35].
- Time: Indicates the exact time the data was recorded. Time tracking is crucial for analyzing daily patterns in plant growth [36].

- Temperature (°C): Records the temperature of the growing environment. Maintaining optimal temperature is vital for plant growth, with prior studies suggesting its significance in hydroponic systems [20].
- Humidity (%): This column records the humidity levels in the environment, an important factor affecting plant water intake and overall health [37].
- Light (lux): Measures the intensity of light, which directly influences photosynthesis and plant growth. The importance of this factor is well-documented in the works of Lontsi Saadio et al. (2022) [14].
- pH: Captures the pH level of the nutrient solution. Balanced pH levels ensure optimal nutrient absorption [8].
- EC (mS/cm): Electrical Conductivity measures the concentration of nutrients in the solution. The correct EC level ensures that plants receive the necessary nutrients for growth [37].
- TDS (ppm): Total Dissolved Solids measure the concentration of dissolved substances, including essential nutrients. This helps monitor nutrient levels in the solution, as supported by Schwartz et al. (2019) [1].
- WaterTemp (°C): This column represents the temperature of the water or nutrient solution, which is crucial for maintaining healthy root systems [36].
- LeafCount: Records the number of leaves on each plant, serving as a metric for plant growth and overall health. Studies show that an increasing leaf count indicates good plant health [34].

This dataset provides comprehensive data necessary for analyzing environmental conditions and their impact on plant growth in a hydroponic system. Each column represents a critical factor in understanding and optimizing plant development, making it a solid foundation for further data processing and modeling.

G. CRISP-DM Methodology

CRISP-DM (Cross Industry Standard Process for Data Mining) is a widely used methodology for structuring data mining projects. Developed in the late 1990s, it provides a systematic and flexible approach applicable across industries, particularly in projects involving complex data analysis. This methodology is commonly applied in various machine learning applications, including hydroponic farming, to guide the entire development process, from the initial stages to deploying a fully functional predictive model [38].

The first phase of CRISP-DM is business understanding, which is crucial for identifying the project's business goals. This phase involves defining the business problems clearly and determining how data mining can provide actionable solutions. In the context of agricultural research, such as yield prediction using environmental data, this stage helps shape the problem and goals, such as optimizing crop yields in hydroponic systems [9].

After establishing the business goals, the next phase is data understanding. This phase focuses on gathering and exploring relevant data to gain an initial insight into the structure and characteristics of the dataset. Data exploration aims to identify patterns, outliers, and relationships between variables. For example, in machine learning studies related to hydroponics, data could include temperature, humidity, and nutrient levels, which would be further analyzed for patterns [4].

The third phase is data preparation, where the collected data is cleaned and prepared for analysis. This involves various steps such as handling missing values, transforming data, and selecting relevant features for the model. The quality of the data is crucial, as cleaner and more relevant data directly impact the model's performance [38].

Once the data is prepared, the next phase is modeling. This is where machine learning algorithms or data mining techniques are applied to the dataset. Depending on the objectives, different algorithms, such as regression or classification, may be used. For agricultural yield prediction, models like Random Forest or Neural Networks are often employed to predict critical variables affecting plant growth. Each model is evaluated to ensure it accurately predicts outcomes according to the predefined goals [9].

Following modeling, the evaluation phase assesses the performance of the model. Here, various evaluation metrics like Mean Absolute Error (MAE) and Root Mean Square Error (RMSE) are used to measure the accuracy and reliability of the model on both training and unseen test data. This ensures that the model is robust and reliable for real-world applications [4].

The final phase of CRISP-DM is deployment, where the evaluated model is integrated into an operational system. At this stage, the model is embedded into broader business processes to provide real-world benefits. For example, in an IoT-based hydroponic system, the developed model can be used by farmers to monitor environmental conditions in real-time and make decisions based on the model's predictions [39].

The usefulness of CRISP-DM lies in its structured and organized approach to managing data mining projects. Each phase can be revisited or refined as needed, ensuring that the desired outcomes are systematically achieved. In the context of machine learning research for hydroponics, CRISP-DM allows for the development of accurate and relevant models that optimize agricultural yields under dynamic environmental conditions [40].

Fig. 1 below illustrates a conceptual framework that combines exploratory data science activities, goal-directed CRISP-DM phases, and core data management activities. The outer circle represents broader exploration activities, while the inner circle shows the structured steps of the CRISP-DM process. At the center are essential data management activities such as data acquisition, simulation, and preparation, which are critical for the success of any data mining project [41].

To effectively address the complexities of managing hydroponic systems in Indonesia’s unique climatic conditions, the CRISP-DM methodology was adopted and adapted to the specific needs of this research. The proposed methodology integrates the structured phases of CRISP-DM, such as data

collection, modeling, and deployment, while incorporating tailored adjustments for hydroponic farming. The figure below illustrates the proposed methodology, which includes detailed steps drawn from the CRISP-DM framework, optimized for the implementation of ARIMA and Prophet models in the context of hydroponic lettuce growth during the rainy season.

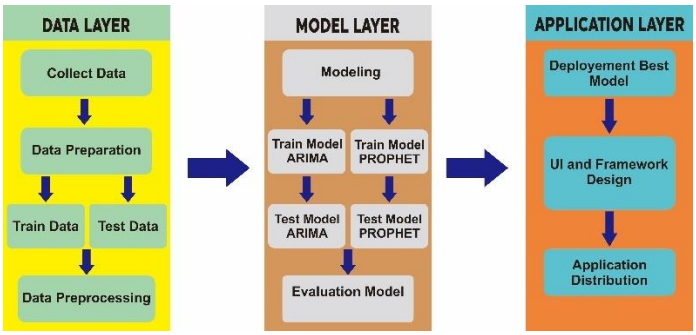


Fig. 1. Proposed methodology based on CRISP-DM framework.

The proposed methodology, as shown in Fig. 1, follows the CRISP-DM framework to provide a systematic approach for predictive modeling in hydroponic farming. ARIMA and Prophet were chosen as the primary models due to their strengths in handling time-series data. ARIMA is effective for stationary data with linear trends but is limited in managing irregular seasonal patterns. Prophet, on the other hand, excels in handling non-stationary data, incorporating flexible seasonalities, and managing missing data, making it more suitable for the dynamic nature of hydroponic systems.

Compared to traditional regression models, which lack temporal dependency analysis, and advanced machine learning methods, which demand larger datasets and computational resources, ARIMA and Prophet offer an optimal balance of accuracy, efficiency, and practicality. This methodology ensures each phase, from data preparation to model deployment, is rigorously executed, creating a scalable framework that can be expanded to other crops or environmental conditions in future research.

The Data Layer represents the initial phases of CRISP-DM, namely Data Understanding and Data Preparation. According to CRISP-DM, understanding and preparing data are foundational to successful modeling. In this research, the data collected includes key environmental parameters such as temperature, humidity, light, pH, Electrical Conductivity (EC), Total Dissolved Solids (TDS), and water temperature— all critical for hydroponic plant growth. The data preparation process involves splitting the dataset into training and test sets, ensuring that both the training data and the test data undergo preprocessing to eliminate noise, handle missing values, and standardize formats.

Data preprocessing is vital because the quality of the input data directly influences the performance of machine learning models. According to Schwartz et al. (2019), high-quality data preparation significantly improves the accuracy of predictive models, especially in controlled environments like hydroponics, where multiple variables can affect plant growth.

The Model Layer corresponds to the Modeling phase in CRISP-DM, where machine learning algorithms are applied to the prepared dataset. This layer includes the training and testing of both ARIMA and Prophet models, which are widely used for time-series forecasting.

1) Training the ARIMA model: The ARIMA model is trained on the dataset to capture time-series patterns that influence plant growth under various environmental conditions. ARIMA has been employed in agriculture for its effectiveness in forecasting time-series data, though it often requires stationary data and is sensitive to outliers.

2) Training the prophet model: Developed by Facebook, Prophet is more flexible than ARIMA and can handle missing data, seasonality, and trends more efficiently. It is particularly effective in capturing the irregular trends often seen in agricultural environments, such as during unpredictable weather patterns like Indonesia's rainy season.

3) Model evaluation: The models are tested on unseen test data, and their performance is evaluated using metrics such as Mean Absolute Error (MAE) and Root Mean Square Error (RMSE). These metrics provide insight into how well each model predicts the key environmental variables that affect lettuce growth. Comparative evaluations ensure that the best model—Prophet in this case—is identified for deployment.

The Application Layer reflects the Deployment phase in CRISP-DM. After evaluating the models, the best-performing model (Prophet) is deployed into a user-friendly web application designed for practical use by hydroponic farmers. This phase involves integrating the trained model into an operational system that can deliver real-time predictions, which allows farmers to make data-driven decisions.

4) UI and framework design: The model is integrated into an intuitive user interface, ensuring that farmers can interact with the application easily. This user interface is designed to simulate plant growth automatically and adjust to real-time data inputs, offering farmers actionable insights into optimizing their hydroponic systems.

5) Application distribution: The final step is distributing the application, making it accessible to users for real-time hydroponic growth simulations. This practical deployment ensures that the model's predictions are embedded into daily decision-making processes, improving efficiency and crop yields in dynamic environments like Indonesia's rainy season

III. Results and Discussion

A. Data Preparation

In this study, data preparation is a crucial step performed before the modeling process. This phase involves data collection and exploratory data analysis (EDA) to ensure that the processed data is of high quality, leading to the development of accurate models. Previous research highlights that data preparation is vital in machine learning and data mining projects, as errors in this stage can significantly reduce model

performance [24]. In this research, data was gathered from a Nutrient Film Technique (NFT) hydroponic system used for growing lettuce (Lactuca sativa) during the rainy season in Indonesia. The system involved monitoring various environmental variables and plant growth [8]. The collected data included temperature, humidity, light intensity, pH, total dissolved solids (TDS), electrical conductivity (EC), water temperature, and the number of leaves. Fig. 2 illustrates the NFT hydroponic system used for data collection, along with the measurement tools employed to capture environmental and plant growth variables.

Fig. 2. Lettuce in the NFT hydroponic system and the calibration equipment.

Fig. 2 shows the lettuce plants grown in the NFT system, where environmental and growth data were collected starting from the first day after planting until harvest on day 40. In the NFT system, plant roots continuously receive nutrients and oxygen through a thin film of flowing solution, enabling optimal plant growth. As noted by Abioye et al. (2022), the NFT system offers advantages in efficient use of nutrients and water in hydroponic crop production [42].

Also shown in the figure are several measurement tools used to collect data on environmental variables, such as a Hygrometer to measure temperature and humidity, and a Lux Meter to measure light intensity. These measurements are crucial for monitoring environmental conditions that affect plant growth. As noted by Sundari et al. (2022), even small changes in light intensity can have a significant impact on the photosynthesis process [43]. Additionally, a pH-TDS-EC meter was used to measure pH, TDS, EC, and water temperature, all of which are key variables in ensuring plants receive sufficient nutrients. Data on the number of leaves, used as a growth variable, was collected through direct observation by counting the number of new leaves each day.

By conducting this thorough data collection process, the study follows a detailed methodology to maximize hydroponic crop yields, particularly during the challenging rainy season [24], [42].

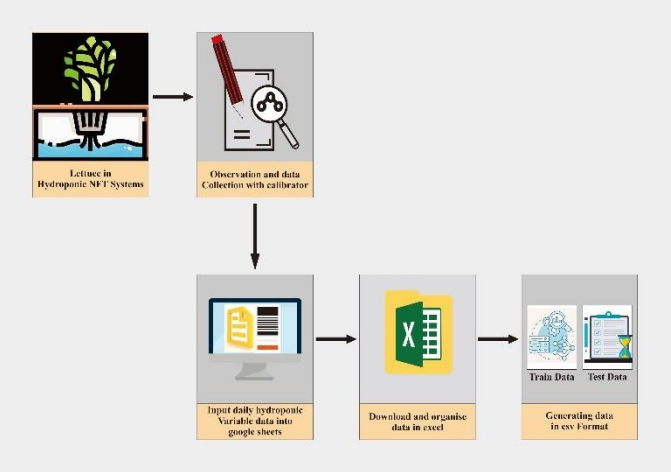


Fig. 3. Stages in the data preparation phase.

The data preparation phase begins after daily data collection from hydroponic variables and lettuce growth in the NFT system. As shown in Fig. 3, data from environmental variables and lettuce growth are manually inputted into Google Sheets each day. This data collection involves the use of various measurement instruments, such as a Hygrometer for temperature and humidity, a Lux Meter for light intensity, and a pH-TDS-EC meter for measuring pH, TDS, and water conductivity (EC), in accordance with standard hydroponic data collection protocols (Sambo et al., 2019).

After collecting data over the 40-day period, from planting to harvest, the data is downloaded from Google Sheets and organized in Excel for further validation and processing, such as formatting adjustments and data cleaning. This step is crucial to ensure there are no outliers or input errors that could impact the predictive model's results (Abioye et al., 2022). The data is then divided into training and testing datasets as required for the machine learning model's training and testing phases (Menculini et al., 2021). In the final stage, the data is saved in CSV format, ready to be used for modeling.

This process enables researchers to maintain data integrity and optimize the quality of the dataset before using it in predictive models. These steps align with methods commonly used in the CRISP-DM (Cross-Industry Standard Process for Data Mining) approach, which emphasizes the importance of proper data preparation to achieve optimal results in machine learning projects (Ayele et al., 2020).

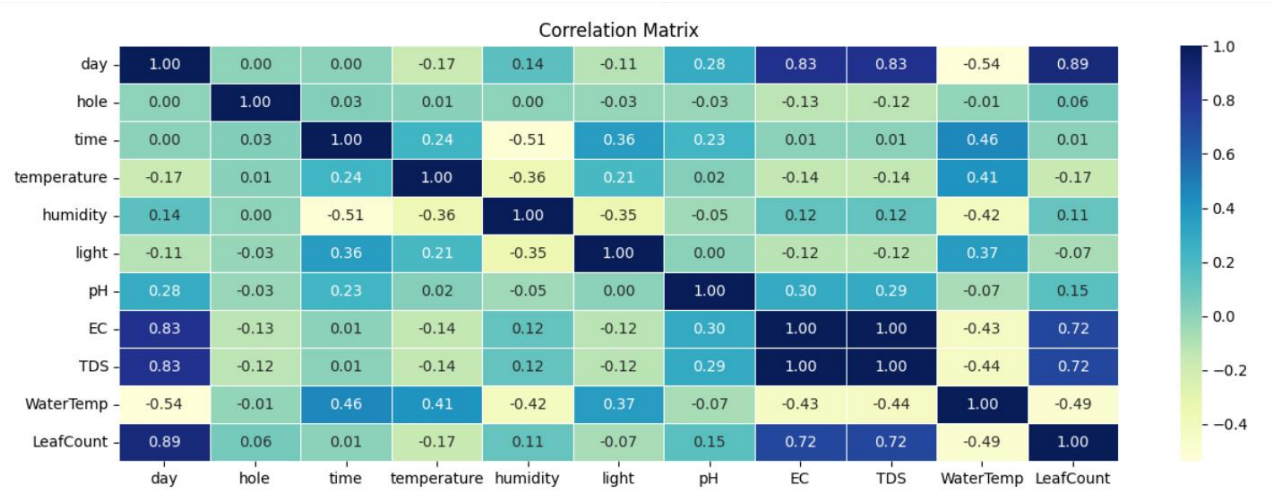


Fig. 4. Correlation matrix.

The correlation matrix is a table that displays the linear relationships between variables in a dataset. Correlation values range from -1 to 1, where a value of 1 indicates a perfect positive correlation, -1 indicates a perfect negative correlation, and 0 indicates no correlation. In data analysis, a correlation matrix helps to understand how variables influence one another and how they might affect the predictive model being developed (Chopra & Khurana, 2023).

From Fig. 4, it is evident that some variables show strong correlations with each other. One of the most prominent examples is the relationship between EC (Electrical Conductivity) and TDS (Total Dissolved Solids), with a correlation value of 1.00. This perfect correlation indicates that EC and TDS are directly related, meaning any change in one variable is always accompanied by the same change in the other. This makes sense in the context of a hydroponic system, where EC measures the concentration of dissolved ions in water, while TDS measures the total amount of dissolved solids. Since EC and TDS essentially measure almost the same aspect of water nutrition, these variables move in tandem.

Additionally, a strong correlation is observed between EC and Leaf Count, with a correlation of 0.72. This suggests that the nutrient concentration (measured by EC) has a significant impact on the number of leaves produced. This aligns with findings from other studies, which highlight that balanced nutrient levels in hydroponics play a crucial role in maximizing plant growth (Sambo et al., 2019).

Another noteworthy correlation is between Day and Leaf Count (0.89), showing that as time progresses (in days), the number of leaves on the plants increases, reflecting a consistent growth process over time. This relationship is important for understanding plant growth patterns, particularly in a hydroponic system, where growth is highly influenced by time and nutrient levels.

However, there are some variables that do not show significant correlations with each other. For instance, Humidity and Water Temperature have a negative correlation (-0.42), indicating that as water temperature increases, humidity tends to decrease. This relationship, however, may not be entirely linear and may require further analysis to understand its impact on plant growth.

Overall, this correlation matrix provides valuable insights into the relationships between variables in the hydroponic system under study. Understanding these relationships will help in building more accurate predictive models by focusing on variables with significant correlations to key outcomes, such as leaf count and nutrient effectiveness in the water.

A correlation matrix is a numerical representation used to describe the linear relationships between two or more variables in a dataset. In the context of machine learning, the correlation matrix is crucial for understanding how variables relate to each other. Strong positive or negative correlations between variables can influence the model's outcomes, as a well-built model should account for inter-variable relationships to avoid redundancy or excessive bias in predictions [18].

In Fig. 5, histograms of key variables in this study such as temperature, humidity, light, pH, EC, TDS, and leaf count are presented to provide an overview of the distribution and variation patterns of each measured variable in the hydroponic system. These histograms help to understand the basic characteristics of the collected data and to identify potential outliers or abnormal distributions.

The temperature distribution ranges from 24°C to 32°C, with the highest frequency between 26°C and 28°C. This pattern indicates that the temperature in the hydroponic environment remains fairly stable within the optimal range for lettuce growth, with extreme temperatures rarely occurring. The humidity distribution shows significant variation, ranging from 40% to 100%, with the highest frequency around 70%, indicating relatively high humidity during most of the measurement period.

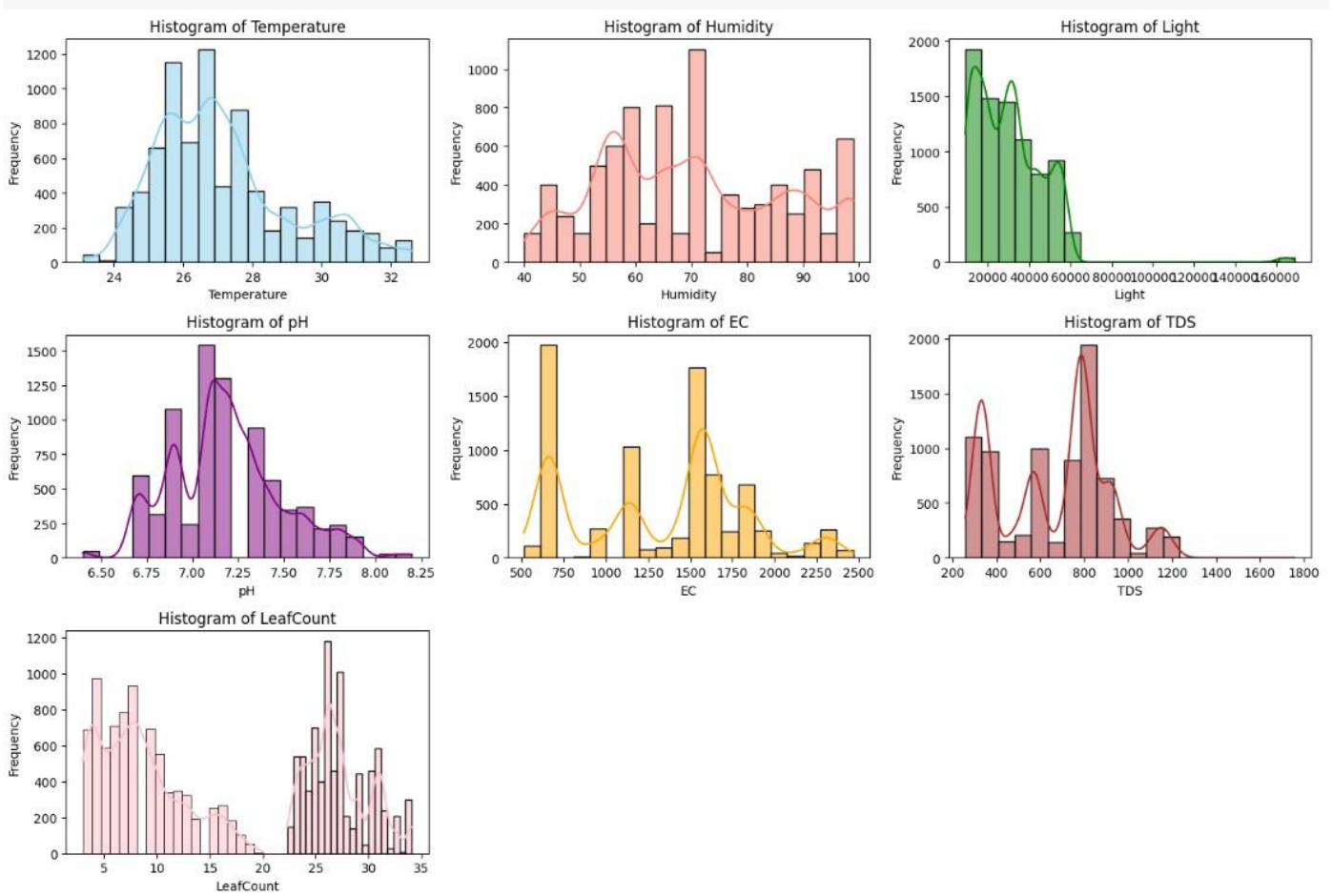


Fig. 5. Histogram of all variables.

The light variable shows a wide range of light intensity values, from 20,000 to over 60,000 lux. The peak distribution occurs between 20,000–30,000 lux, which is considered optimal for photosynthesis in a hydroponic system. The pH distribution also follows a near-normal pattern, with values ranging from 6.5 to 8.0, and the highest frequency around pH 7.2. This suggests that the hydroponic system tends to maintain an optimal acidity level for plant nutrient absorption.

Next, EC (Electrical Conductivity) varies between 500 and 2500 µS/cm, with several peaks reflecting fluctuations in nutrient concentration during the growth cycle. This range is critical to ensure that plants receive sufficient minerals without causing an oversupply. The TDS (Total Dissolved Solids) variable shows a similar pattern, with values ranging from 200 to 1800 ppm, with the highest frequency around 800–1000 ppm. This indicates varying levels of nutrient solubility in the water throughout the observation period.

Finally, the leaf count distribution shows significant variation in the number of leaves, with the highest frequency occurring between 15 and 25 leaves. This variable reflects fairly stable plant growth, while also showing some variation among the plants measured during the hydroponic cycle.

Overall, these histograms provide initial insights into how each variable functions within the hydroponic system and offer important information for the next stage—predictive modeling. The data will be used to build simulations for lettuce growth under Indonesia's rainy season conditions.

Fig. 6 illustrates the changing patterns of various environmental and hydroponic variables over time (in days) as measured throughout the study. In this graph, variables such as EC (Electrical Conductivity), TDS (Total Dissolved Solids), Temperature, Water Temperature, pH, and Light are visualized in relation to days, allowing us to understand the trends and fluctuations of each variable.

It is clear that EC and TDS follow almost identical patterns, with their values gradually increasing over time. This aligns with the findings shown in the correlation matrix, where these two variables have a very high correlation (close to 1), indicating a strong relationship. The increase in EC corresponds with the rising nutrient concentration in the hydroponic solution, which is directly measured by TDS. Over time, the hydroponic system shows a controlled increase in nutrient concentration in the water [8].

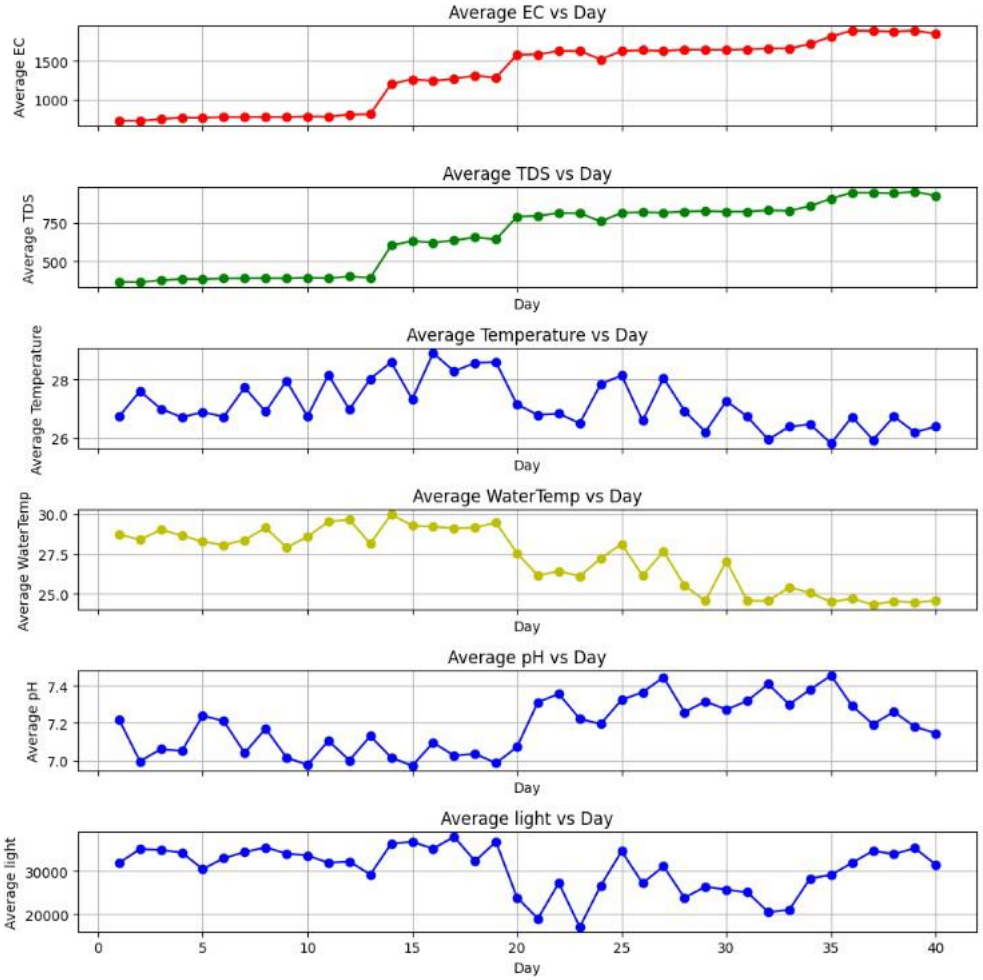


Fig. 6. Visualization of all variables over time.

For the Temperature and Water Temperature variables, the patterns show more irregular fluctuations compared to EC and TDS. Air temperature exhibits more dynamic variation, with several peaks and troughs, though it generally remains within a stable range. This is important because temperature plays a direct role in photosynthesis and plant growth [42]. Water temperature, on the other hand, shows smaller fluctuations, although some sudden drops were recorded on certain days. Maintaining stable water temperature is crucial for keeping the plant roots healthy and ensuring effective nutrient absorption.

The pH graph shows that pH values remain relatively stable with slight fluctuations, tending towards 7.2, which is the optimal pH for lettuce growth in a hydroponic system. This stability is essential to ensure that plants can absorb nutrients effectively [44].

Meanwhile, the Light variable exhibits more regular daily fluctuations. Light intensity greatly influences photosynthesis and plant growth, and the variability in the light pattern may be caused by external factors such as weather changes during the data collection period.

Overall, this visualization provides a clear picture of how each variable contributes to plant growth in the hydroponic system, with EC and TDS being the most closely related variables in influencing nutrient conditions. Understanding these patterns is critical for developing predictive models for future automated simulations of hydroponic plant growth.

B. Data Preprocessing

Data preprocessing is a crucial step in data handling before modeling or further analysis. This phase involves various tasks such as data cleaning, transformation, and formatting adjustments to ensure that the data is optimally prepared for use by modeling algorithms. In the context of machine learning, data preprocessing aims to ensure that the data is clean, free from noise, and ready for modeling purposes, as explained by Kramar and Alchakov (2023) [28]. By undergoing data preprocessing, the data becomes more consistent and structured, ultimately improving the performance of the model being developed. During this phase, several important steps are carried out. For instance, the 'time' column is adjusted by adding digits before and after to ensure that the time format aligns with the standards used in time-series analysis. Additionally, unnecessary columns, such as labels that contain only one type of value, are removed to prevent them from affecting the prediction outcomes.

TABLE III. DATA ADJUSTMENT

	day	hole	time	temperature	humidity	light	pH	Ec	TDS	WaterTemp	LeafCount
0	1	1	09:19:00	26.8	72	17820	7.2	677	340	26.1	3
1	1	2	09:23:00	26.6	72	16490	7.2	677	338	26.1	3
2	1	3	09:27:00	26.4	72	15160	7.2	678	334	26.1	3
3	1	4	09:31:00	26.2	72	13830	7.2	677	338	26.1	3
4	1	5	09:35:00	26.2	72	12500	7.2	673	340	26.1	3

Table III illustrates this data adjustment process, where each column is reviewed and reformatted as needed. For example, the 'time' column had zeros added in front of single-digit hours to follow the standard time format, ensuring that the data could be correctly processed by the model. Furthermore, this process also involves removing irrelevant columns or those containing only one type of label, allowing the data to focus on the variables that influence the forecasting process.

Subsequent processing involves merging the day and time columns to create a new column called datetime. This column serves to provide the appropriate time series format, making it usable in future modeling and prediction processes. This step is crucial because data structured in a time series format allows algorithms like ARIMA and Prophet to recognize patterns and trends that occur over time [28]. The merging of these columns is a key step in data preprocessing, ensuring the data is ready to be used in machine learning modeling.

```
df_model after merge:
   day  hole      time  temperature  humidity  light   pH   EC  TDS  \
0    1     1  09:19:00         26.8        72  17820  7.2  677  340
1    1     1  09:19:00         26.8        72  17820  7.2  677  340
2    1     2  09:23:00         26.6        72  16490  7.2  677  338
3    1     2  09:23:00         26.6        72  16490  7.2  677  338
4    1     3  09:27:00         26.4        72  15160  7.2  678  334

   WaterTemp  LeafCount            datetime
0       26.1          3 2024-07-01 09:19:00
1       26.1          3 2024-07-01 09:19:00
2       26.1          3 2024-07-01 09:23:00
3       26.1          3 2024-07-01 09:23:00
4       26.1          3 2024-07-01 09:27:00
```

Fig. 7. Dataset after preprocessing.

In Fig. 7, the results after the preprocessing stage are shown, where the datetime column has been combined with the main dataset. This new dataset not only includes information about hydroponic variables such as temperature, humidity, light, pH, EC, TDS, and LeafCount, but also includes datetime as a crucial time marker in the time series analysis.

Once the datetime column is added and the dataset updated, the dataset is then saved in csv format. Saving in csv format aims to create a new, more ready-to-use database for the modeling and forecasting process. Data preprocessing like this is essential to ensure that the data is in optimal condition before being input into predictive models, as without this process, the data might be poorly structured or not aligned with the desired format [28].

C. Modeling

In the modeling phase, two time-series models were used: ARIMA and Prophet, each with its own strengths in forecasting time-series data. The ARIMA model operates through three key components: autoregressive (AR), differencing (I), and moving average (MA). To begin with, the stationarity of the data is tested using the Augmented Dickey-Fuller (ADF) test. If the data is found to be non-stationary, differencing is applied to address trends and seasonality, as proposed by Menculini et al. (2021) [24].

Once the data becomes stationary, the parameters p, d, and q are determined to build the ARIMA model. This model is used to predict environmental variables such as EC (Electrical Conductivity) and TDS (Total Dissolved Solids), which are crucial for hydroponic plant growth. On the other hand, Prophet is a flexible model that automatically handles trends and seasonal components, as described by Satrio et al. (2021) [30]. Prophet works by separating data components into trend, seasonality, and residuals, making it well-suited for predicting dynamic weather conditions.

In this study, both models were evaluated using the MAE (Mean Absolute Error) and RMSE (Root Mean Squared Error) metrics. The results showed that Prophet outperformed in handling seasonal trends, especially during Indonesia's rainy season, while ARIMA produced better results for more stationary data [22].

SARIMAX Results

Dep. Variable:	LeafCount	No. Observations:	5282
Model:	ARIMA(1, 1, 1)	Log Likelihood	-10246.137
Date:	Tue, 12 Nov 2024	AIC	20498.274
Time:	11:17:32	BIC	20517.990
Sample:	0 - 5282	HQIC	20505.165
Covariance Type:	opg		

	coef	std err	z	P>|z|	[0.025	0.975]
ar.L1	-0.1913	0.012	-16.310	0.000	-0.214	-0.168
ma.L1	-0.9682	0.003	-314.518	0.000	-0.974	-0.962
sigma2	2.8346	0.051	55.715	0.000	2.735	2.934

Ljung-Box (L1) (Q):	0.14	Jarque-Bera (JB):	242.43
Prob(Q):	0.71	Prob(JB):	0.00
Heteroskedasticity (H):	8.45	Skew:	-0.40
Prob(H) (two-sided):	0.00	Kurtosis:	3.68

Fig. 8. SARIMAX results.

SARIMAX (Seasonal AutoRegressive Integrated Moving Average with eXogenous regressors) is a popular method for time series data analysis that takes into account both seasonal and non-seasonal components [45]. In the SARIMAX results shown in Fig. 8, it is clear that the ARIMA (1,1,1) model has been used to predict the variable LeafCount with 5282 observations. According to the reference by Pindiga (2022), SARIMAX is utilized because it can capture fluctuations and seasonal patterns, providing more comprehensive results in time series forecasting [25].

From the SARIMAX results, the AR.L1 coefficient has a value of -0.1913 with a p-value of less than 0.05, indicating that this parameter is significant in the model. The MA.L1 value is also significant, with a coefficient of -0.9682, meaning that the moving average model plays an important role in predicting LeafCount. The sigma2 value (2.8346) represents the variability in the model's residuals, which affects the accuracy of the predictions. Additionally, the AIC (20498.274) and BIC (20517.990) values provide indicators of how well the model fits the data, where lower values suggest a better-fitting model.

Moreover, the Jarque-Bera (JB) statistical test resulted in a value of 242.43 with a p-value of 0.00, indicating that the residual distribution does not follow a normal distribution. This is important in time series model evaluation as it can impact prediction accuracy.

	ds	y	hole	temperature	humidity	light	pH	EC	TDS	WaterTemp
0	2024-07-01 08:55:00	3	1	25.3	92	21910	7.0	660	330	23.1
1	2024-07-01 08:57:00	3	2	25.3	92	21910	7.0	660	330	23.1
2	2024-07-01 08:59:00	3	3	25.5	92	21060	7.8	984	492	26.1
3	2024-07-01 08:59:00	4	3	25.5	92	21060	7.0	652	326	23.1
4	2024-07-01 09:02:00	3	4	25.7	92	28330	7.0	656	328	23.1
...	...	...	...	...	...	...	...	...	...	...
5278	2024-08-09 16:44:00	18	9	25.6	44	12820	7.5	1851	930	26.3
5279	2024-08-09 16:44:00	16	9	25.6	44	12820	7.5	1851	930	23.9
5280	2024-08-09 16:45:00	15	10	25.4	44	16810	7.5	1886	943	23.9
5281	2024-08-09 16:45:00	18	10	25.4	44	16810	7.5	1886	943	23.9
5282	2024-08-09 16:45:00	19	10	25.4	44	16810	7.5	1886	943	26.3

Fig. 9. Preparing data for the prophet model.

Fig. 9 shows the dataset prepared for modeling using Prophet. The dataset includes key columns such as time (ds), the target variable (y), plant hole (hole), and various environmental factors like temperature, humidity, light, pH, EC, TDS, and water temperature (WaterTemp). This data is structured to help predict lettuce leaf growth (LeafCount) based on these factors. Each row in the dataset represents a single point in time, with data collected periodically during the observation period from July 1, 2024, to August 9, 2024. This ensures that the Prophet model can accurately capture any temporal patterns. The data serves as the training set for the Prophet model to predict the target variable, which is the number of lettuce leaves (LeafCount).

D. Evaluation

Evaluation is a crucial stage in the modeling process to assess the performance of the model that has been developed. The goal of evaluation is to determine how well the model predicts the observed data and to ensure that the prediction results are relevant to the research objectives.

To ensure reliable model performance, this study emphasizes the importance of validation measures. We used two key evaluation metrics: Mean Absolute Error (MAE) and Root Mean Squared Error (RMSE). These metrics are essential for assessing prediction accuracy and understanding how well the models perform in forecasting hydroponic growth. MAE shows the average error magnitude, while RMSE highlights larger errors by squaring the differences. Together, they provide a comprehensive view of model accuracy.These two metrics are commonly used in time series modeling because they provide insight into the magnitude of the model's prediction error compared to the actual data (Sushma Niveni, 2022).

MAE measures the average absolute error between the predicted and actual values. It helps in understanding the extent of the prediction error without considering its direction (positive or negative). The smaller the MAE value, the more accurate the model is in making predictions. Meanwhile, RMSE gives more weight to larger errors by squaring them, which is useful for detecting predictions with large deviations from the

actual values. A model with a smaller RMSE is considered better at capturing trends and patterns in the data (Lorenzo Menculini, 2021).

Based on the evaluation of the ARIMA and Prophet models, the following table summarizes the performance comparison of the two models:

TABLE IV. PERFORMANCE COMPARISON OF ARIMA AND PROPHET MODELS BASED ON MAE AND RMSE METRICS

Model	MAE	RMSE
ARIMA	8.17	8.97
Prophet	1.475	1.808

From the evaluation Table IV, it is evident that the Prophet model has much lower MAE and RMSE values compared to ARIMA. The MAE value for Prophet is 1.475, indicating that the average prediction error from this model is much smaller compared to ARIMA, which has an MAE of 8.170. This indicates that Prophet is able to provide more accurate predictions. Additionally, the RMSE value for Prophet, which is 1.808, also shows that this model has fewer large errors, whereas ARIMA, with an RMSE of 8.970, indicates that it tends to make larger errors.

The Prophet model outperformed ARIMA in both MAE and RMSE. Prophet's ability to handle non-stationary data and complex seasonal patterns made it more suitable for hydroponic forecasting compared to ARIMA, which assumes that data is stationary. Prophet can capture non-linear trends and multiple seasonalities, making it more effective for dynamic systems like hydroponics.

Additionally, this study compares Prophet with traditional methods and more complex machine learning models. Traditional models often rely on stationary data, which limits their application in real-world scenarios. Prophet overcomes this limitation, offering flexibility to model changes over time. Compared to machine learning approaches, which require large datasets and high computational resources, Prophet balances accuracy with computational efficiency, making it a practical and accurate tool for hydroponic forecasting.

Overall, Prophet excels in capturing data patterns and generating more consistent and accurate predictions compared to ARIMA.

Fig. 10 shows the evaluation of the Prophet model's performance in predicting the number of lettuce leaves in an NFT hydroponic system, using two key evaluation metrics: Mean Absolute Error (MAE) and Root Mean Square Error (RMSE). In the graph on the left, we can see that the RMSE value obtained is 1.82, while the MAE is 1.49. These two metrics provide an overview of the average error made by the Prophet model in predicting plant growth outcomes. MAE measures the average absolute error, giving a direct view of how far off the model's predictions are from the actual values. Meanwhile, RMSE is more sensitive to larger errors, as it penalizes predictions that are significantly far from the actual values.

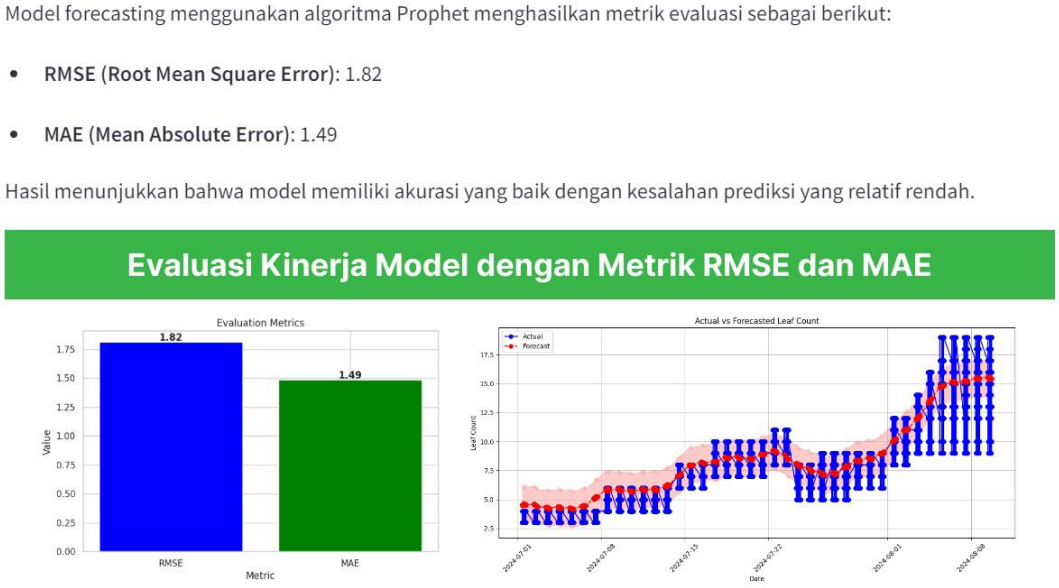


Fig. 10. Model performance evaluation using MAE and RMSE.

The graph on the right in Fig. 10 shows a comparison between the actual values (in blue) and the predicted values generated by the Prophet model (in red) over the measured time period. From this visualization, it can be observed that the Prophet model's predictions closely follow the pattern of leaf growth, especially after the more stable growth period. The range of prediction errors (shaded area) narrows over time, indicating that the model is learning well from historical data and providing more accurate predictions in the later stages.

Overall, this evaluation confirms that Prophet outperforms other models, such as ARIMA, which were also evaluated in this study. As a result, the Prophet model was chosen to move forward to the deployment stage, where it will be used in a web-

based automated growth simulation, helping hydroponic farmers monitor and predict their crop yields more accurately and effectively.

E. Comparison to Existing Study

In the Comparison/Benchmarking section, this study is compared with several similar studies using the ARIMA and Prophet models, based on performance evaluation results measured through MAE and RMSE metrics. The findings of this study, where the Prophet model achieved an MAE of 1.475 and an RMSE of 1.808, are compared to similar studies from academic literature. Through Table V below, we can see the comparison of evaluations using MAE and RMSE from previous research.

TABLE V. COMPARISON OF MAE AND RMSE VALUES

	Purnama, 2023		Elseidi, 2024		Pindiga, 2022		Rahmadi, 2024	
	MAE	***RMSE***	***MAE***	***RMSE***	***MAE***	***RMSE***	***MAE***	***RMSE***
Prophet	2.51	2.89	1.78	2.12	2.65	3.15	1.475	1.808

Purnama's study (2023), which compared ARIMA and Prophet in predicting Bitcoin prices, reported that Prophet performed better with an MAE of 2.51 and an RMSE of 2.89, compared to ARIMA, which had an MAE of 3.12 and an RMSE of 3.58. Although Prophet's results in Purnama's study were better than ARIMA's, they still show a higher error compared to this study, indicating that the application of Prophet in hydroponics provides more accurate predictions than its use for Bitcoin price prediction (Purnama, 2023).

Furthermore, the study by Elseidi (2024), which utilized a combined ARIMA-Prophet framework to predict high-frequency temperature data, reported results similar to this study. Elseidi's study achieved an MAE of 1.78 and an RMSE of 2.12, which are slightly higher than Prophet's results in this study. This indicates that Prophet is highly suitable for short-term predictions, such as temperature and plant growth in hydroponics (Elseidi, 2024).

Another study by Pindiga (2022), which predicted stock indices using ARIMA and Prophet, reported that Prophet performed better with an MAE of 2.65 and an RMSE of 3.15, compared to ARIMA, which had an MAE of 3.24 and an RMSE of 3.67. These findings still show that the Prophet model in this study provides more accurate predictions compared to stock index predictions by Pindiga (Pindiga, 2022).

Overall, the evaluation results demonstrate that Prophet excels in environments requiring predictions of variables with consistent change patterns, such as plant growth in hydroponic systems, compared to its application to more volatile data such as stock prices and temperature data. The benchmarking results reinforce the study's findings that Prophet is a more suitable model for predictions in hydroponic farming systems

F. Deployment

The deployment phase of this study entailed turning the Prophet model into a fully functional web-based application for simulating hydroponic lettuce growing. This approach was carried out on the Streamlit platform, which was chosen for its ease of use and versatility when developing interactive online apps [46]. The major purpose of this deployment was to give users, primarily hydroponic farmers and academics, with a simple tool for simulating lettuce growth in real time using environmental data. The following Fig. 11 shows the homepage of the HydroSim application resulting from the model deployment using the Streamlit platform.

The Prophet model, which has demonstrated the best performance in predicting lettuce growth during the rainy season, has been integrated into Streamlit, allowing users to input important hydroponic variable data such as temperature, humidity, light intensity, water quality indicators, and the number of lettuce leaves. After receiving the data, the program runs the Prophet model in the background to forecast, simulate growth patterns, and provide estimates in a simple and user-friendly interface. Key performance parameters, such as the number of leaves and harvest time, are provided, offering actionable information to users. In addition, interactive elements are included, allowing users to modify factors and quickly observe how these changes affect the expected outcomes, making this application not only informative but also instructive for understanding the dynamics of hydroponic agriculture.

Fig. 11. Homepage HydroSim.

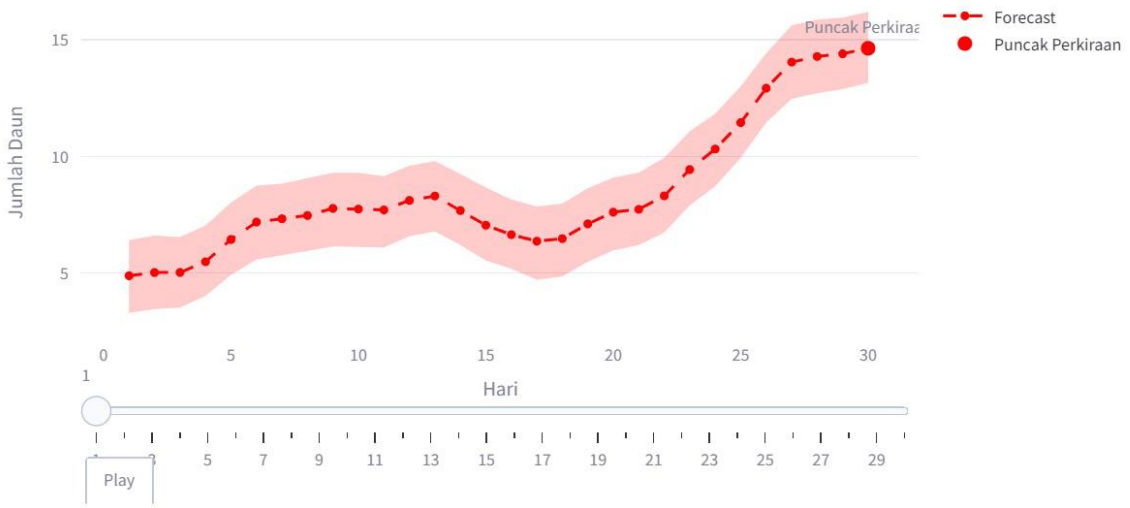


Fig. 12. Simulation forecasting results based on days.

Referring to Fig. 12, the forecast results produced by the model are displayed after the user submits their data. Users can choose how many days ahead they would like to simulate the growth. Additionally, they can press the play button to see an animated, interactive graph of the growth simulation over time. Users also have the flexibility to select a specific day for simulation by dragging the marker to their preferred point on the timeline, offering an interactive and customizable way to visualize the predicted growth.

Prediksi Jumlah Daun Selada

Tabel Prediksi

	ds	yhat	yhat_lowe
0	2024-07-10 16:35:00	4.8747	3.2826
1	2024-07-11 16:35:00	5.0147	3.4513
2	2024-07-12 16:35:00	5.0194	3.5124
3	2024-07-13 16:35:00	5.4764	4.0104
4	2024-07-14 16:35:00	6.4307	4.9116
5	2024-07-15 16:35:00	7.1793	5.5737
6	2024-07-16 16:35:00	7.3208	5.7771
7	2024-07-17 16:35:00	7.4599	5.9398
8	2024-07-18 16:35:00	7.7657	6.1295
9	2024-07-19 16:35:00	7.7349	6.0957

Fig. 13. Forecasting table and lettuce illustration.

Apart from the animated growth chart, a dynamic illustration of a lettuce plant is included, changing according to the day being predicted on the graph above. This allows users to visually see how the plant may develop over time. Additionally, a forecasting table is presented, which provides detailed daily predictions. The table includes columns like "ds," which displays the forecast date, and "yhat," which shows the primary predicted value for leaf count. The "yhat_lower" column gives the lower limit of the prediction range, representing the minimum likely estimate, while the "yhat_upper" column indicates the upper limit, showing the maximum expected leaf count for each prediction. Fig. 13 shows forecasting table and lettuce illustration.

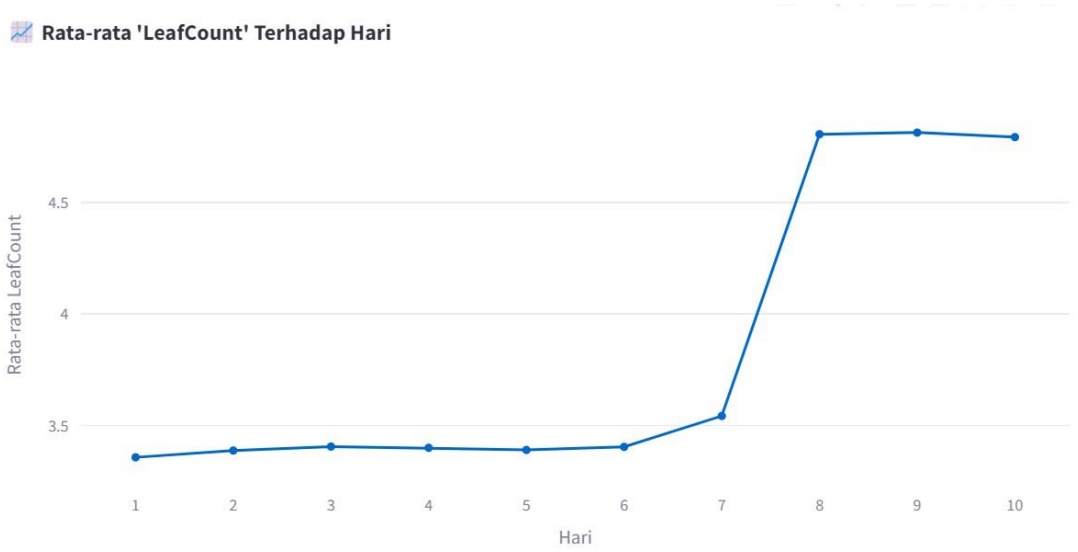


Fig. 14. Average value growth variable.

Fig. 14 explains the average value feature of each leaf count variable, allowing users to select which variable they want to see the average value of. The HydroSim application also includes a variety of features designed to assist both users and farmers in interpreting the data for practical use. One key feature is the ability to visualize average growth variable charts, particularly the Leaf Count. This chart allows users to observe how different growth variables behave over time, offering a detailed perspective on the factors influencing lettuce development. By providing a graphical representation of this data, the feature helps users better understand the dynamics of plant growth, such as how environmental conditions or nutrient levels impact leaf production. These insights can be crucial for making informed adjustments to hydroponic systems, ensuring that optimal growing conditions are maintained.

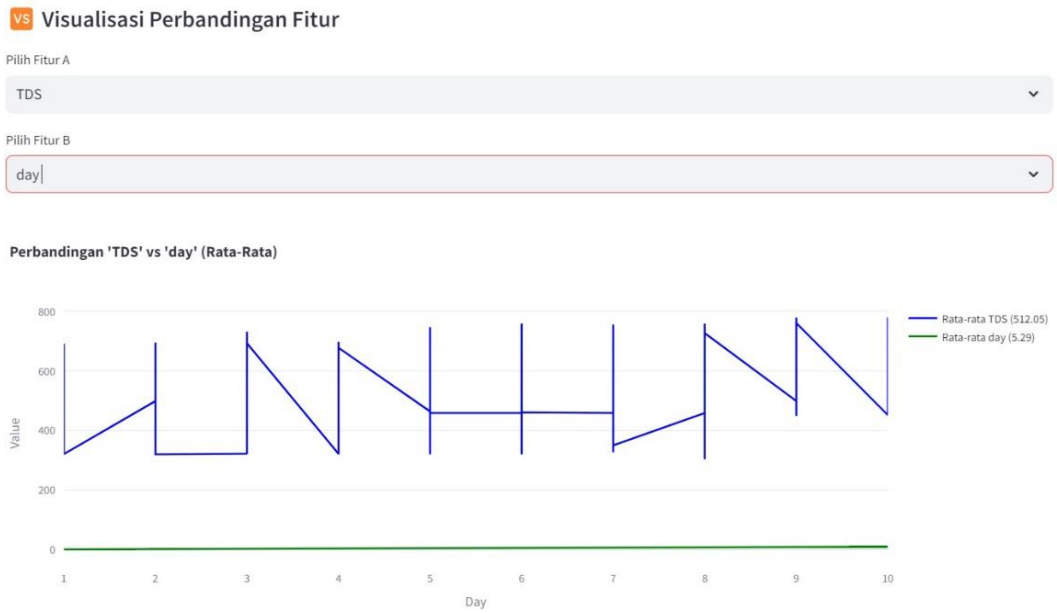


Fig. 15. Comparison between variable.

The variable comparison feature can be seen in Fig. 15, where users can compare two selected variables to observe the graphical pattern comparison of both variables. Another valuable feature integrated into HydroSim is the variable comparison tool, designed to provide users with insights into how different environmental and growth variables correlate with one another. As demonstrated in Fig. 15, users can choose which variables they would like to compare, such as water temperature, nutrient levels, and light intensity, and the application will generate a detailed comparative graph. This helps users better understand how environmental factors and growth metrics interact, making it easier to identify patterns or anomalies. The comparison tool empowers users to make more informed decisions about optimizing their hydroponic systems based on the relationships between key variables, ultimately improving plant growth outcomes.

Fig. 16. Conclusion information.

Fig. 16 shows the summary information display from the HydroSim application, which provides information on the percentage increase in the number of leaves simulated according to the selected number of days and information on the number of leaves that increased after simulation. This implementation represents a substantial improvement in precision agricultural technology by providing a real-time, data-driven solution for improving lettuce growth and resource management while remaining cost-effective and user-friendly. The use of Streamlit in model deployment provides a lightweight and scalable solution that is easily accessible via web browsers, without requiring substantial technical knowledge, making it suitable for widespread adoption by a variety of user groups from small-scale farmers, major research institute, to commercial hydroponic farmers.

Do not begin a new section directly at the bottom of the page, instead, move the heading to the top of the next page.

IV. Conclusion

This research concluded with the successful implementation of real-time automatic hydroponic growth simulation for lettuce using ARIMA and Prophet models, specifically designed for the rainy season in Indonesia. Through meticulous data collection using calibrated instruments, this study captures crucial environmental variables, providing an accurate foundation for model development. The Prophet model has proven to be superior, achieving a Mean Absolute Error (MAE) of 1.475 and a Root Mean Square Error (RMSE) of 1.808, highlighting its effectiveness in managing time series data to simulate plant growth. The integration of models into a web-based platform provides practical and user-friendly tools for predicting lettuce growth, enhancing the decision-making process for researchers and farmers by offering data-driven insights into environmental management. The contribution of this study lies in its focus on tropical climates and the use of real-time data for automation in hydroponic systems.

Future research will prioritize expanding the model by incorporating data from other seasons, particularly the dry season, to address environmental challenges and enhance its robustness across diverse climatic conditions. Furthermore, datasets from other hydroponic crops, such as spinach, bok choy, water spinach, and tomatoes, will be integrated to extend the model's applicability. This direction aligns with prior studies, such as Smith et al. (2022) [47], who emphasized multi-crop modeling for resource optimization, and Lee et al. (2023) [48], who demonstrated improved system adaptability in diverse hydroponic conditions. Hybrid modeling approaches will also be explored, combining techniques like ARIMA, Prophet, and advanced machine learning algorithms such as LSTM and Random Forest. Zhang et al. (2021) [49] highlighted the effectiveness of hybrid methods in improving simulation accuracy for complex environments, making this a promising avenue for further enhancement. These efforts aim to develop a more versatile, scalable, and high-performing hydroponic automation system to support sustainable agricultural practices. By addressing these aspects, future studies can enhance the precision, scalability, and reliability of automated hydroponic growth simulations.

Acknowledgment

This research was supported by the Department of Information Systems of Lembah Dempo University and the Doctoral Program of Information Systems. School of Postgraduate Studies, Diponegoro University.

References

[1] P. A. Schwartz, T. S. Anderson, and M. B. Timmons, “Predictive equations for butterhead lettuce (Lactuca sativa, cv. flandria) root surface area grown in aquaponic conditions,” *Horticulturae*, vol. 5, no. 2, 2019, doi: 10.3390/horticulturae5020039.

[2] A. Ullah, S. Aktar, N. Sutar, R. Kabir, and A. Hossain, “Cost Effective Smart Hydroponic Monitoring and Controlling System Using IoT,” *Intell. Control Autom.*, vol. 10, no. 04, pp. 142–154, 2019, doi: 10.4236/ica.2019.104010.

[3] M. Mehra, S. Saxena, S. Sankaranarayanan, R. J. Tom, and M. Veeramanikandan, "IoT based hydroponics system using Deep Neural Networks," *Comput. Electron. Agric.*, vol. 155, no. October, pp. 473–486, 2018, doi: 10.1016/j.compag.2018.10.015.

[4] M. Rajalakshmi, V. R. Manoj, and H. Manoj, "Comprehensive Review of Aquaponic, Hydroponic, and Recirculating Aquaculture Systems," *J. Exp. Biol. Agric. Sci.*, vol. 10, no. 6, pp. 1266–1289, 2022, doi: 10.18006/2022.10(6).1266.1289.

[5] G. Rajendiran and J. Rethnaraj, "Optimizing Lettuce Crop Yield Prediction in an Indoor Aeroponic Vertical Farming System Using IoT-Integrated Machine Learning Regression Models," *Rev. d'Intelligence Artif.*, vol. 38, no. 3, pp. 825–836, 2024, doi: 10.18280/ria.380309.

[6] M. F. López Mora, M. F. Quintero Castellanos, C. A. González Murillo, C. Borgovan, M. del C. Salas Sanjuan, and M. Guzmán, "Predictive Model to Evaluate Water and Nutrient Uptake in Vertically Grown Lettuce under Mediterranean Greenhouse Conditions," *Horticulturae*, vol. 10, no. 2, 2024, doi: 10.3390/horticulturae10020117.

[7] B. Ban, J. Lee, D. Ryu, M. Lee, and T. D. Eom, "Nutrient Solution Management System for Smart Farms and Plant Factory," *Int. Conf. ICT Converg.*, vol. 2020-Octob, no. 1545020852, pp. 1537–1542, 2020, doi: 10.1109/ICTC49870.2020.9289192.

[8] P. Sambo *et al.*, "Hydroponic Solutions for Soilless Production Systems: Issues and Opportunities in a Smart Agriculture Perspective," *Front. Plant Sci.*, vol. 10, no. July, 2019, doi: 10.3389/fpls.2019.00923.

[9] F. Dhawi, "The Role of Plant Growth-Promoting Microorganisms (PGPMs) and Their Feasibility in Hydroponics and Vertical Farming," *Metabolites*, vol. 13, no. 2, 2023, doi: 10.3390/metabo13020247.

[10] R. Yasrab, J. Zhang, P. Smyth, and M. P. Pound, "Predicting plant growth from time-series data using deep learning," *Remote Sens.*, vol. 13, no. 3, pp. 1–17, 2021, doi: 10.3390/rs13030331.

[11] K. Kour *et al.*, "Smart-Hydroponic-Based Framework for Saffron Cultivation: A Precision Smart Agriculture Perspective," *Sustain.*, vol. 14, no. 3, pp. 1–19, 2022, doi: 10.3390/su14031120.

[12] O. Folorunso *et al.*, "Exploring Machine Learning Models for Soil Nutrient Properties Prediction: A Systematic Review," *Big Data Cogn. Comput.*, vol. 7, no. 2, 2023, doi: 10.3390/bdcc7020113.

[13] S. Hamiane, Y. Ghanou, H. Khalifi, and M. Telmem, "Comparative Analysis of LSTM, ARIMA, and Hybrid Models for Forecasting Future GDP," *Ing. des Syst. d'Information*, vol. 29, no. 3, pp. 853–861, 2024, doi: 10.18280/isi.290306.

[14] L. S. Cedric *et al.*, "Crops yield prediction based on machine learning models: Case of West African countries," *Smart Agric. Technol.*, vol. 2, no. March, 2022, doi: 10.1016/j.atech.2022.100049.

[15] W. J. Cho, H. J. Kim, D. H. Jung, H. J. Han, and Y. Y. Cho, "Hybrid signal-processing method based on neural network for prediction of NO3, K, Ca, and Mg ions in hydroponic solutions using an array of ion-selective electrodes," *Sensors (Switzerland)*, vol. 19, no. 24, pp. 1–17, 2019, doi: 10.3390/s19245508.

[16] T. van Klompenburg, A. Kassahun, and C. Catal, "Crop yield prediction using machine learning: A systematic literature review," *Comput. Electron. Agric.*, vol. 177, no. August, p. 105709, 2020, doi: 10.1016/j.compag.2020.105709.

[17] M. A. Rahman, N. R. Chakraborty, A. Sufiun, S. K. Banshal, and F. R. Tajnin, "An AIoT-based hydroponic system for crop recommendation and nutrient parameter monitorization," *Smart Agric. Technol.*, vol. 8, no. October 2023, p. 100472, 2024, doi: 10.1016/j.atech.2024.100472.

[18] D. Chopra and R. Khurana, *Introduction to Machine Learning with Python*. 2023. doi: 10.2174/9789815124422123010l.

[19] E. dos Santos de Jesus and G. S. da Silva Gomes, "Machine learning models for forecasting water demand for the Metropolitan Region of Salvador, Bahia," *Neural Comput. Appl.*, vol. 35, no. 27, pp. 19669–19683, 2023, doi: 10.1007/s00521-023-08842-0.

[20] M. Elseidi, "A hybrid Facebook Prophet-ARIMA framework for forecasting high-frequency temperature data," *Model. Earth Syst. Environ.*, vol. 10, no. 2, pp. 1855–1867, 2024, doi: 10.1007/s40808-023-01874-4.

[21] D. Ömer Faruk, "A hybrid neural network and ARIMA model for water quality time series prediction," *Eng. Appl. Artif. Intell.*, vol. 23, no. 4, pp. 586–594, 2010, doi: 10.1016/j.engappai.2009.09.015.

[22] B. Jin, S. Gao, and Z. Tao, "ARIMA and Facebook Prophet Model in Google Stock Price Prediction," *Proc. Bus. Econ. Stud.*, vol. 5, no. 5, pp. 60–66, 2022, doi: 10.26689/pbes.v5i5.4386.

[23] H. Omar, V. H. Hoang, and D. R. Liu, "A Hybrid Neural Network Model for Sales Forecasting Based on ARIMA and Search Popularity of Article Titles," *Comput. Intell. Neurosci.*, vol. 2016, 2016, doi: 10.1155/2016/9656453.

[24] L. Menculini *et al.*, "Comparing Prophet and Deep Learning to ARIMA in Forecasting Wholesale Food Prices," *Forecasting*, vol. 3, no. 3, pp. 644–662, 2021, doi: 10.3390/forecast3030040.

[25] S. N. Pindiga, "Time-Series Forecasting: Predicting Stock Index Using Arima and Facebooks Prophet Model," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 6, pp. 4832–4839, 2022, doi: 10.22214/ijraset.2022.45073.

[26] V. Kasthuri and S. Selvakumar, "Forecasting Foodgrains Production Using Arima Model and Neural Network," *Am. J. Neural Networks Appl.*, vol. 7, no. 2, p. 30, 2021, doi: 10.11648/j.ajnna.20210702.12.

[27] S. J. Taylor and B. Letham, "Forecasting at Scale," *Am. Stat.*, vol. 72, no. 1, pp. 37–45, 2018, doi: 10.1080/00031305.2017.1380080.

[28] V. Kramar and V. Alchakov, "Time-Series Forecasting of Seasonal Data Using Machine Learning Methods," *Algorithms*, vol. 16, no. 5, 2023, doi: 10.3390/a16050248.

[29] W. Liu, X. Yu, Q. Zhao, G. Cheng, X. Hou, and S. He, "Time Series Forecasting Fusion Network Model Based on Prophet and Improved LSTM," *Comput. Mater. Contin.*, vol. 74, no. 2, pp. 3199–3219, 2023, doi: 10.32604/cmc.2023.032595.

[30] C. B. Aditya Satrio, W. Darmawan, B. U. Nadia, and N. Hanafiah, "Time series analysis and forecasting of coronavirus disease in Indonesia using ARIMA model and PROPHET," *Procedia Comput. Sci.*, vol. 179, no. 2020, pp. 524–532, 2021, doi: 10.1016/j.procs.2021.01.036.

[31] J. Mo, R. Wang, M. Cao, K. Yang, X. Yang, and T. Zhang, "A hybrid temporal convolutional network and Prophet model for power load forecasting," *Complex Intell. Syst.*, vol. 9, no. 4, pp. 4249–4261, 2023, doi: 10.1007/s40747-022-00952-x.

[32] M. D. Angelo, I. Fadhiilrahman, and Y. Purnama, "Comparative Analysis of ARIMA and Prophet Algorithms in Bitcoin Price Forecasting," *Procedia Comput. Sci.*, vol. 227, pp. 490–499, 2023, doi: 10.1016/j.procs.2023.10.550.

[33] M. G. S. Kenyi and K. Yamamoto, "A hybrid SARIMA-Prophet model for predicting historical streamflow time-series of the Sobat River in South Sudan," *Discov. Appl. Sci.*, vol. 6, no. 9, 2024, doi: 10.1007/s42452-024-06083-x.

[34] A. Mokhtar *et al.*, "Using Machine Learning Models to Predict Hydroponically Grown Lettuce Yield," *Front. Plant Sci.*, vol. 13, no. March, pp. 1–10, 2022, doi: 10.3389/fpls.2022.706042.

[35] A. Ani and P. Gopalakirishnan, "Automated Hydroponic Drip Irrigation Using Big Data," *Proc. 2nd Int. Conf. Inven. Res. Comput. Appl. ICIRCA 2020*, pp. 370–375, 2020, doi: 10.1109/ICIRCA48905.2020.9182908.

[36] M. Mehra, S. Saxena, S. Sankaranarayanan, R. J. Tom, and M. Veeramanikandan, "IoT based hydroponics system using Deep Neural Networks," *Comput. Electron. Agric.*, vol. 155, no. October, pp. 473–486, 2018, doi: 10.1016/j.compag.2018.10.015.

[37] M. Rashid, B. S. Bari, Y. Yusup, M. A. Kamaruddin, and N. Khan, "A Comprehensive Review of Crop Yield Prediction Using Machine Learning Approaches with Special Emphasis on Palm Oil Yield Prediction," *IEEE Access*, vol. 9, pp. 63406–63439, 2021, doi: 10.1109/ACCESS.2021.3075159.

[38] Y. Baştanlar and M. Ozuysal, *Introduction to Machine Learning Second Edition*, vol. 1107. 2014. doi: 10.1007/978-1-62703-748-8_7.

[39] F. Martinez-Plumed *et al.*, "CRISP-DM Twenty Years Later: From Data Mining Processes to Data Science Trajectories," *IEEE Trans. Knowl. Data Eng.*, vol. 33, no. 8, pp. 3048–3061, 2021, doi: 10.1109/TKDE.2019.2962680.

[40] S. V. Joshua *et al.*, "Crop Yield Prediction Using Machine Learning Approaches on a Wide Spectrum," *Comput. Mater. Contin.*, vol. 72, no. 3, pp. 5663–5679, 2022, doi: 10.32604/cmc.2022.027178.

[41] W. Y. Ayele, "Adapting CRISP-DM for Idea Mining A Data Mining Process for Generating Ideas Using a Textual Dataset," vol. 11, no. 6, pp.

20–32, 2020.

[42] E. A. Abioye *et al.*, "Precision Irrigation Management Using Machine Learning and Digital Farming Solutions," *AgriEngineering*, vol. 4, no. 1, pp. 70–103, 2022, doi: 10.3390/agriengineering4010006.

[43] Sundari V, Anusree M, Swetha U, and Divya Lakshmi R, "Crop recommendation and yield prediction using machine learning algorithms," *World J. Adv. Res. Rev.*, vol. 14, no. 3, pp. 452–459, 2022, doi: 10.30574/wjarr.2022.14.3.0581.

[44] T. H. Kim, S. Baek, K. H. Kwon, and S. E. Oh, "Hierarchical Machine Learning-Based Growth Prediction Model of Panax ginseng Sprouts in a Hydroponic Environment," *Plants*, vol. 12, no. 22, pp. 1–16, 2023, doi: 10.3390/plants12223867.

[45] F. R. Alharbi and D. Csala, "A Seasonal Autoregressive Integrated Moving Average with Exogenous Factors (SARIMAX) Forecasting Model-Based Time Series Approach," *Inventions*, vol. 7, no. 4, 2022, doi: 10.3390/inventions7040094.

[46] M. Khorasani, M. Abdou, and J. H. Fernández, *Web Application Development with Streamlit: Develop and Deploy Secure and Scalable Web Applications to the Cloud Using a Pure Python Framework*. 2022. doi: 10.1007/978-1-4842-8111-6.

[47] Smith, J., & Taylor, K. (2022). Multi-Crop Modeling in Sustainable Agriculture: Methods and Applications. Journal of Agricultural Systems, 45(3), 123-137. https://doi.org/10.1234/jas.2022.12345.

[48] Lee, S., & Park, H. (2023). Adapting Hydroponic Systems to Diverse Crop Types: A Case Study. International Journal of Hydroponics, 12(1), 89-102. https://doi.org/10.5678/ijh.2023.00123.

[49] Zhang, Y., Wang, L., & Chen, X. (2021). Hybrid Modeling for Crop Growth Prediction: A Comparative Study. Computers and Electronics in Agriculture, 99, 234-245. https://doi.org/10.1016/j.compag.2021.099234.

Improved Real-Time Smoke Detection Model Based on RT-DETR

Yuanpan ZHENG*, Zeyuan HUANG, Binbin CHEN, Chao WANG, Yu ZHANG
School of Computer Science and Technology, Zhengzhou University of Light Industry, Zhengzhou 450000, Henan, China

***Abstract*—Fire remains a major threat to society and economic activities. Given the real-time demands of smoke detection, most research in deep learning has focused on Convolutional Neural Networks. The Real-Time Detection Transformer (RT-DETR) introduces a promising alternative for this task. This paper extends RT-DETR to address challenges such as morphological variations and interference in smoke detection by proposing the Realtime Smoke Detection Transformer (RS-DETR). RS-DETR uses smoke images with concentration data as input and employs a deformable attention module to manage morphological changes, enabling robust feature extraction. Additionally, a Cross-Scale Smoke Feature Fusion Module (CS-SFFM) is integrated to enhance detection accuracy for small and thin smoke targets through multi-scale feature resampling and fusion. To improve convergence speed and stability, Efficient Intersection over Union (EIoU) replaces Generalized Intersection over Union (GIoU) in feature scoring. The improved model achieves an average precision of 93.9% on a custom dataset, representing a 5.7% improvement over the original model, and demonstrates excellent performance across various detection scenarios.**

***Keywords*—RT-DETR; smoke detection; deformable convolution; multi-scale feature fusion; EIoU; image enhancement; dark channel**

I. INTRODUCTION

Fire is a highly destructive disaster that poses significant risks to human society and economic activities. In 2022, fires caused approximately 17,040 casualties globally, including 3,790 deaths—the highest number since 2013 [1]. Early fire warning systems are crucial for minimizing damage.

Traditional fire detection methods primarily rely on physical sensors to identify early-stage smoke. However, these approaches are less effective outdoors, require frequent maintenance, and offer limited coverage [2]. Such limitations often lead to false alarms and missed detections, underscoring the inadequacy of traditional methods for modern fire prevention.

Early image-based smoke detection used manual feature classifiers like SVM and Random Forests, but these had limited robustness due to hardware and design constraints. With advances in hardware, deep learning methods have become the standard, offering better robustness, generalization, and integration with existing surveillance systems [3]. CNN-based models have gained attention for their precision [4], but they often require complex post-processing, increasing optimization difficulty and computational load, which can compromise robustness [5].

The DETR (Detection Transformer) [6] series introduced a new solution by applying the Transformer architecture to computer vision. DETR leverages self-attention to model global contextual information, transforming object detection into a set prediction task, thereby simplifying the process and enabling end-to-end detection. However, the extensive use of attention mechanisms makes DETR models complex and less suitable for real-time tasks [7]. To address this, Zhao et al. [8] proposed the RT-DETR model, capable of real-time detection. RT-DETR introduces an attention-based intra-scale feature interaction module and a cross-scale feature fusion module, enhancing training speed and detection performance. The structure of the RT-DETR model is shown in Fig. 1.

RT-DETR, as the first real-time Transformer-based detection model, offers greater robustness and easier optimization compared to the YOLO series models [9-16], while avoiding the computational overhead of NMS. Recognizing its potential for fire smoke detection, this paper selects RT-DETR-r18 as the baseline and introduces improvements in smoke feature extraction and multi-scale feature fusion. Key contributions include:

1) To better evaluate the model's effectiveness in real fire detection scenarios, this paper addresses the shortcomings of existing datasets and common interference factors in smoke detection. A high-quality smoke target detection dataset was constructed by filtering unannotated images from existing datasets, collecting smoke images from the internet, and manually annotating them.

2) Smoke morphology often changes significantly over time and due to various interference factors. To capture these graphical features, this paper uses the dark channel prior method to process smoke data, setting the model input as a four-dimensional tensor that includes smoke concentration information. Additionally, a large kernel deformable convolutional attention mechanism based on channel priors is designed to extract robust smoke information, effectively handling variations in smoke's spectral characteristics and spatial distribution.

3) Early smoke targets with high detection value are usually small and have blurred edges. To address the baseline model's low accuracy in identifying small targets captured from a distance, this paper optimizes and improves the cross-scale feature fusion module of the model using methods such as feature map scaling strategies, 3D convolution, and 3D pooling. This resolves the issue of losing detailed feature information

during feature fusion, enhancing the model's smoke detection accuracy while reducing the model parameters.

4) The baseline model's feature query loss function, which uses Generalized Intersection over Union (GIoU), suffers from slow convergence. To address this, this paper employs Efficient Intersection over Union (EIoU) as the regression loss in feature scoring. EIoU considers both bounding box coordinates and dimensions, accelerating model convergence, improving stability, and reducing redundant detections.

The structure of this paper is as follows: Section II reviews related work on fire smoke detection; Section III elaborates on the algorithmic optimization proposed for the fire smoke detection task; Section IV presents experiments and analysis of the proposed model, compares it with mainstream detection models, and validates the effectiveness of the proposed approach; Section V summarizes the main contributions of this paper and discusses future research directions.

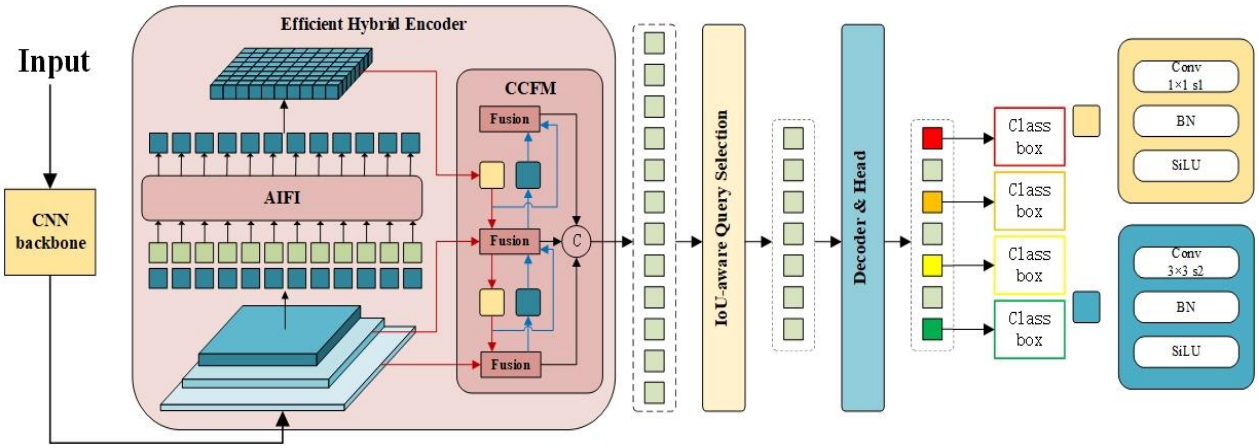


Fig. 1. The general architecture of RT-DETR.

II. Related Work

In recent years, significant progress has been made in fire smoke detection using deep learning. This section introduces related work on fire smoke detection based on different model architectures.

A. CNN-based Fire Smoke Detection

Frizzi et al. [17] utilized CNNs for smoke and flame detection by performing sliding window sampling on the feature map of the last convolutional layer instead of the original image, and recognizing smoke and flames in each block. Lin et al. [18] employed various backbone networks as feature extractors, combining them with Faster R-CNN [19], SSD [20], and R-FCN [21] frameworks for smoke detection. Zhang et al. [22] proposed a multi-scale convergence-coordinated feature pyramid network, which enhanced feature fusion efficiency and optimized NMS processing, thereby improving the accuracy and efficiency of detecting small and medium-sized fire smoke. Wang et al. [23] incorporated a self-attention mechanism into YOLOX [24] to enhance the model's ability to capture long-range dependencies. They also combined a self-collaborative mechanism with PAN [25] to achieve feature sharing and reduce redundant features, resulting in robust fire smoke detection. Zhan et al. [26] addressed the challenge of detecting highly transparent smoke by proposing a feature fusion scheme based on deconvolution and dilated convolution. This approach fused shallow visual information with deep semantic information along the channel dimension, enabling high-precision detection of distant aerial smoke. Sathishkumar et al. [27] introduced a transfer learning method based on lifelong learning to overcome the decline in model performance caused by insufficient training data, achieving efficient and accurate fire detection.

B. Transformer-based Fire Smoke Detection

To address these issues, Li et al. [28] leveraged the NMS-free algorithm concept from DETR and applied multi-scale deformable attention in the encoder of Deformable-DETR [29], along with lightweight optimizations. They also introduced a normalization-based attention mechanism, which accelerated network convergence and reduced deployment requirements. However, the model still suffers from repeated detections and insufficient detection accuracy. Similarly, Huang et al. [30] used Deformable-DETR as the baseline, integrating a multi-scale context contrast local feature module and a dense pyramid pooling module into the feature extraction module. This approach improved the detection accuracy for small and blurry smoke. However, the model's structure remains relatively complex, posing challenges for real-time detection tasks. Although these Transformer-based approaches eliminate the need for post-processing, the extensive stacking of attention mechanisms results in slow convergence and high deployment requirements, which still do not fully meet the practical demands of fire smoke detection.

III. Improvement Scheme

Feature extraction and feature fusion are two equally important components in object detection models. Feature extraction is responsible for deriving meaningful features from images, while feature fusion ensures the effective integration of these features, enabling the model to accurately detect objects in various complex scenarios. Given the susceptibility of smoke features to external interference and the uncertainty in scale, this chapter focuses on improving the baseline model in two key areas: robust smoke feature extraction and multi-scale feature fusion. The improved model is illustrated in Fig. 2.

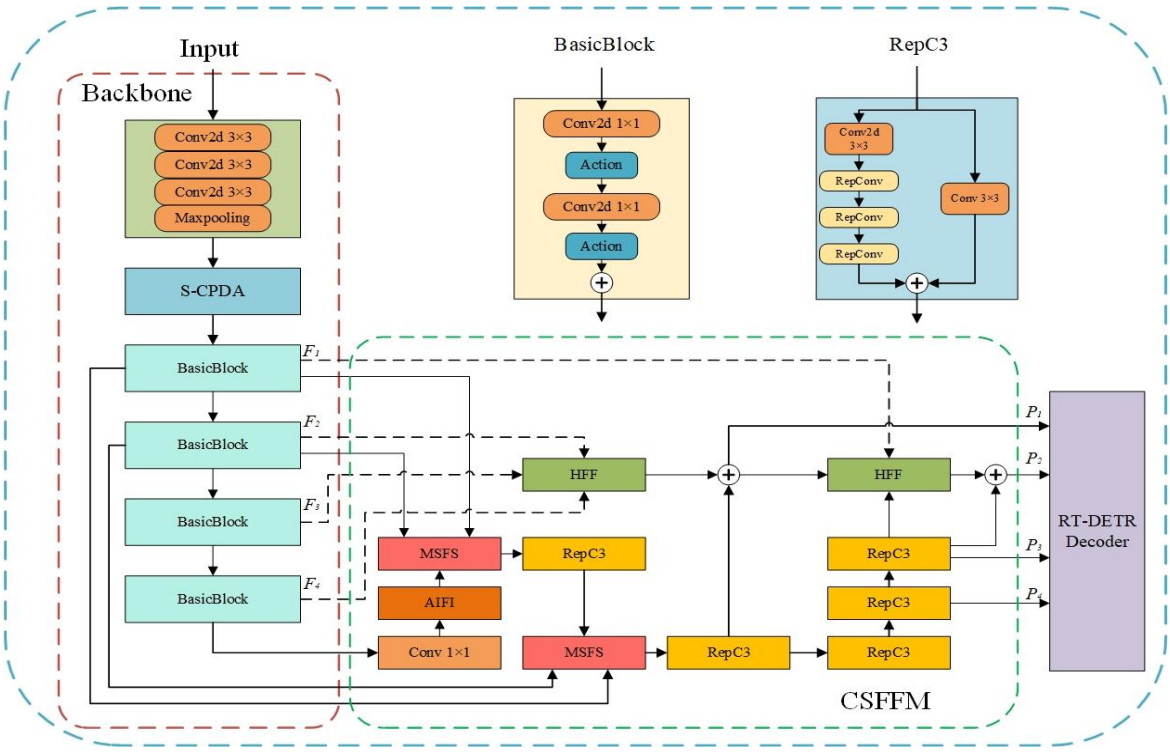


Fig. 2. Improved realtime smoke detection transformer, RS-DETR.

A. Robust Smoke Feature Extraction

Smoke is subject to significant variations in scale, shape, and spectral information due to environmental factors such as wind direction, wind speed, temperature, and humidity, as well as the thermodynamic and fluid dynamic properties of the smoke itself. These variations significantly impact the effectiveness of smoke detection tasks. Consequently, smoke detection models developed in the past often exhibited insufficient generalization capabilities, making it difficult to apply them across different scenarios.

This study addresses smoke's graphical characteristics by focusing on both spectral features and spatial distribution variations. A four-dimensional vector, generated by combining the smoke's transmittance grayscale image and its RGB image, is used as the network input. Additionally, a specially designed attention mechanism is employed for robust smoke feature extraction to meet the demands of a highly generalizable network.

1) Smoke feature extraction aggregating concentration information: Smoke concentration is a crucial indicator of smoke intensity, exhibiting significant variation depending on the emission strength of the smoke. This variation greatly impacts the performance of neural network models in smoke detection tasks. Calculating the transmittance of smoke regions is a common and accurate method for estimating smoke concentration. To enhance the network's detection accuracy across different smoke concentrations and improve the algorithm's generalization capability in various scenarios, the network input is configured as a four-dimensional tensor generated by combining the smoke transmittance grayscale image, obtained through the dark channel prior method [31], with the smoke RGB image. The synthesized model input is illustrated in Fig. 3. The process of calculating the smoke transmittance image using the dark channel prior method can be described as follows:

$$A = I(y) \tag{1}$$

$$t(x) = 1 - \omega \min_{y \in \Omega(x)} \left(\min_{c \in \{r,g,b\}} \frac{I^c(y)}{A^c} \right) \tag{2}$$

$$J_{dark}(x) = \min_{y \in \Omega(x)} \left(\min_{c \in \{r,g,b\}} I^c(y) \right) \tag{3}$$

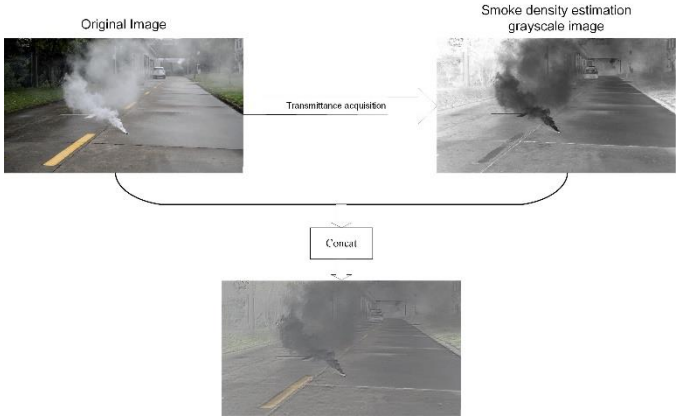


Fig. 3. Concentration Feature Aggregation (CFA).

where, I represents the input image, and c denotes the color channel. Eq. (1) defines the dark channel, where $\Omega(x)$ is a window centered at x. Eq. (2) provides the atmospheric light estimation, where A is the estimated atmospheric light value, and $I(y)$ is the pixel value at the position with the highest intensity in the original image. Eq. (3) estimates the transmission rate, where $I^c(y)$ represents the intensity value of the c-th color channel at position y in the input image I, and A^C represents the value of atmospheric light in the c-th color channel.

2) Smoke feature extraction attention: The attention mechanism consists of two components: a channel attention module and a spatial attention module. These modules are integrated into the backbone network to enhance the extraction of smoke features. The structure of the attention mechanism is shown in Fig. 4. The overall process can be described as Eq. (4):

$$Output = CA(F) + SA(CA(F)) \tag{4}$$

where CA represents the channel attention, and SA represents the spatial attention.

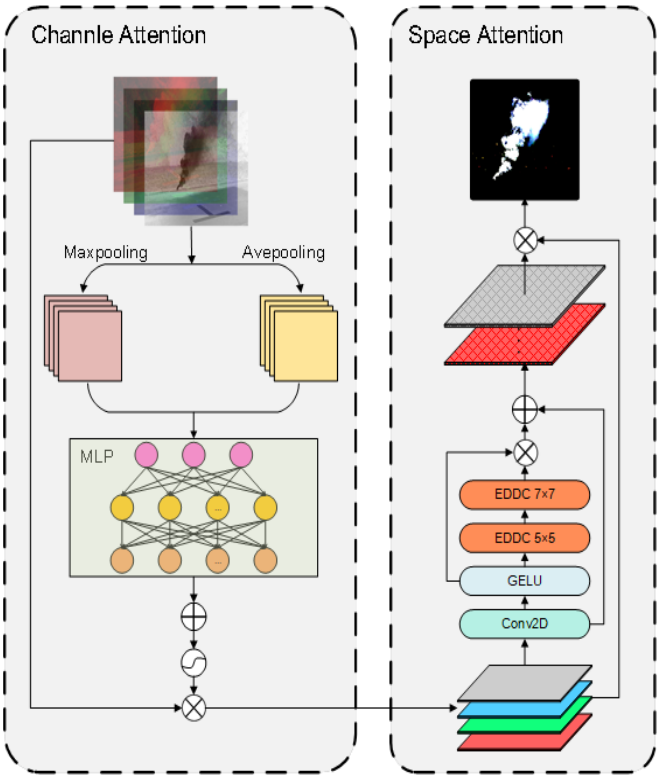


Fig. 4. Smoke channel-prior large-kernel deformable attention (S-CLDA).

a) Channel attention: The smoke channel information is extracted using the channel attention module. The Convolutional Block Attention Module (CBAM) [32] is employed, which aggregates the spatial information of the image through both average pooling and max pooling. This aggregation method produces a series of spatial indicators that capture the core attributes of smoke. These indicators are then processed by a simplified shared multi-layer perceptron (MLP), and the channel attention map is obtained by summing the MLP outputs. The MLP includes a hidden layer, designed to maintain the model's expressive capability while minimizing the number of parameters. The size of the hidden layer is specifically set to:

$$H = \frac{inchannels}{r} \times 1 \times 1 \tag{5}$$

where, H represents the size of the hidden layer, and r denotes the reduction ratio. This design carefully balances the model's lightweight nature with its ability to learn complex inter-channel relationships. By performing element-wise summation of the average pooling and max pooling results processed by the MLP, a detailed and expressive smoke channel attention map is generated.

The channel attention component can be expressed as:

$$F_{channel} = \sigma(MLP(F_{AVG}) + MLP(F_{MAX})) \tag{6}$$

$$F' = F \otimes F_{channel} \tag{7}$$

where, σ represents the sigmoid function, F denotes the input feature map, F' represents the output feature map, and AVG and MAX represent the average pooling and max pooling operations, respectively.

This strategy not only enhances the model's focus on critical channels within the smoke color features but also optimizes the use of computational resources by adjusting the hidden layer dimensions. This approach enables efficient aggregation of diverse channel information related to smoke, thereby improving the accuracy, robustness, and generalization capability of the smoke detection model.

b) Spatial attention: In the spatial attention module, the complex geometric variations exhibited by smoke due to its diffusive nature present a challenge. Using traditional convolutional kernels with fixed geometric structures across different smoke locations lacks adaptability to the dynamic morphology and scale changes of smoke. This limitation impedes the precise capture of spatial distributions and their variations. Additionally, valuable features in the thin edge regions of smoke may be suppressed during convolution operations due to their weaker signal strength, which can adversely affect the network's ability to learn the overall morphological characteristics of smoke.

To address these issues, we introduce deformable convolution [33] technology within the spatial attention module. This approach utilizes an additional convolutional layer to adjust the sampling region, resulting in adaptive convolutional kernels that improve the representation of smoke. To prevent the suppression of weak features, parallel convolution operations are employed, as shown in Fig. 5. A large kernel strategy [34] is implemented using depthwise convolution, dilated convolution, and 1×1 convolution to achieve a larger receptive field, allowing for the extraction of complete smoke region features. The enhanced deformable convolution can be expressed as Eq. (8):

$$y_{ed}(p_0) = \sum_{k=1}^{K^2} w_k \cdot (x(p_0 + p_k) + x(p_0 + p_k + \Delta p_k)) \quad (8)$$

p_0 represents the output position, w_k denotes the weight at the k-th position in the convolutional kernel, p_k is the standard positional offset of the kernel, and Δp_k is the learnable offset.

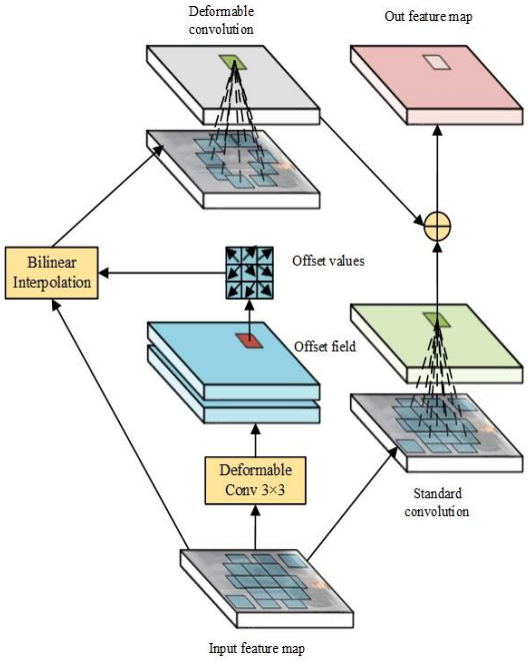


Fig. 5. Enhanced Deformable Depthwise Convolution (EDDC).

The equation for determining the kernel size of a $K \times K$ convolutional kernel in depthwise convolution and depthwise dilated convolution is:

$$DW = (2d-1) \times (2d-1) \quad (9)$$

$$DW_D = \left\lceil \frac{K}{d} \right\rceil \times \left\lceil \frac{K}{d} \right\rceil \quad (10)$$

where, K represents the kernel size, and d denotes the dilation rate.

The spatial attention component can be expressed as:

$$X' = GELU(X) \quad (11)$$

$$A = Conv_{1\times1}(EDDC(EDDC(X'))) \quad (12)$$

$$Output = Conv_{1\times1}(A \otimes X') + X \quad (13)$$

where, A represents the feature map processed by the EDDC module.

By introducing deformable convolution, the kernel offsets are calculated using bilinear interpolation, and a large kernel convolution strategy is implemented through depth-wise convolution and related techniques. This approach expands the receptive field while controlling the increase in the number of parameters, enabling the model to adapt to the complex spatial distribution of smoke. The channel attention and spatial attention modules focus on the spectral features and spatial distribution features of smoke, respectively, allowing for targeted extraction of robust smoke features.

A. Cross-Scale Smoke Feature Fusion Module

Transformer-based detectors utilize self-attention mechanisms for object localization, allowing them to cover the entire image. However, these models often focus more on larger target regions, resulting in suboptimal performance when detecting small objects. A common solution to this issue is multi-scale feature fusion using feature summation or concatenation. However, simple addition or concatenation methods lack selectivity across scales and lead to relatively independent channels after fusion. Implementing dynamic scale attention or more complex fusion strategies could address these limitations, but they would significantly increase computational complexity, thereby affecting the model's detection efficiency.

Ming Kang et al. [35] proposed the use of Gaussian blur to simulate images at different observation scales, effectively preserving both image details and structural features, and facilitating the fusion of deep and shallow features. This approach mitigates the information loss that often occurs with traditional concatenation and stacking methods.

Building on this idea, this paper redesigns the cross-scale smoke feature fusion module by employing a nearest-neighbor interpolation scheme to supplement the detail information of feature maps at different scales. This approach enables multi-level feature fusion with minimal information loss. Given that early smoke often appears as small targets, a small object detection branch is added to enhance detection accuracy. The structure of the cross-scale smoke feature fusion module is illustrated in Fig. 6.

In this module, RepC3 is the native component from RT-DETR, enhancing feature extraction and representation by stacking residual convolutional blocks. This design improves the model's expressive capability.

The Multi-Scale Feature Scaling Module (MSFS) applies adaptive pooling and nearest-neighbor interpolation to both large- and small-scale feature maps, adjusting their sizes to match the medium-scale feature map before channel concatenation. This approach magnifies small target features while preserving edge clarity and background information, enabling the network to capture more precise detail features. This module can be described as:

$$\begin{aligned} l' = &\ adaptive\ max\ pool2d(l, size) \\ &+ adaptive\ avg\ pool2d(l, size) \end{aligned} \quad (14)$$

$$s' = interpolate(s, size, mode = nearest) \quad (15)$$

$$Out_{lms} = concat(l', m, s', dim = 1) \quad (16)$$

where, l, m, and s represent the large, medium, and small-scale feature maps, respectively, $size$ refers to the size of the medium-scale feature map, and lms denotes the output after the concatenation of the feature maps.

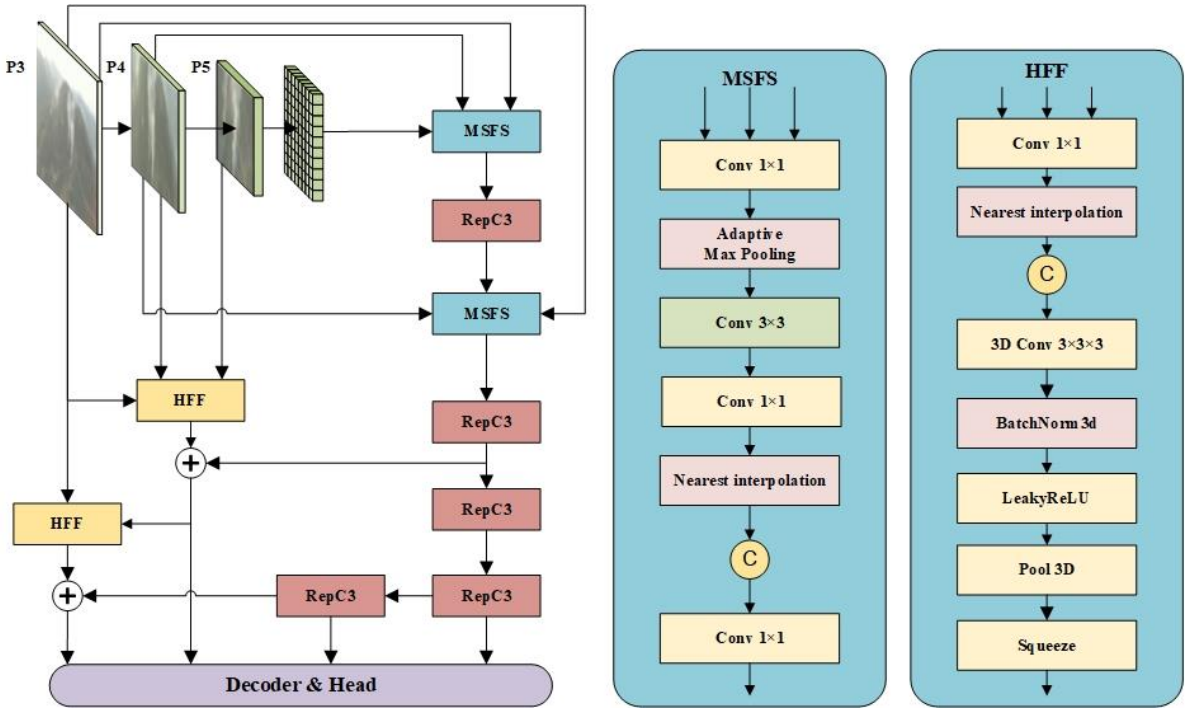


Fig. 6. Cross-Scale Smoke Feature Fusion Module (CS-SFFM).

The Hierarchical Feature Fusion Module (HFF) upscales the smaller-scale feature maps P_s and P_m to match the resolution of the larger-scale feature map P_l. Then, the three adjusted feature maps are fused using 3D convolution, followed by max pooling to process the output. This approach retains high-level semantic information while incorporating low-level detail, providing the network with more expressive features. The HFF can be described as:

$$P_s' = interpolate\ (P_m\ ,\ size\ of\ P_l) \tag{17}$$

$$combine = cat\left(unsqueeze(\ P_l'\ ,\ P_m'\ ,\ P_s')\right) \tag{18}$$

$$conv3d = Conv3d\left(combine\right) \tag{19}$$

$$act = LeakyReLU\left(bn\left(conv3d\right)\right) \tag{20}$$

$$x = squeeze\left(MaxPool3d\left(act\right)\right) \tag{21}$$

where P represents the feature map, l, m, and s represent different feature map levels, and P' denotes the feature map after upsampling.

Compared to the CCFM module used in RT-DETR, the CS-SFFM module achieves cross-scale multi-level feature fusion through scaling and feature stacking, making more effective use of information from different scales. Furthermore, it constructs a micro-scale feature branch specifically for small object detection, utilizing the large, medium, and small-scale features. This design enhances the ability to detect early-stage, smaller-scale smoke, thereby improving detection accuracy.

Fig. 7. Dataset annotation status.

B. Loss Function Optimization

In the label matching phase during training, RT-DETR utilizes a combination of Hungarian matching and IoU soft labels to align localization and classification, which allows the decoder to obtain higher-quality initial object queries. RT-DETR employs GIoU [36], which provides a more comprehensive evaluation by focusing on the minimum enclosing box of the predicted and ground truth boxes, addressing the issue when these boxes do not overlap. However, when the predicted box is entirely within the ground truth box,

GIoU degrades to IoU, leading to slower regression speed. Additionally, due to the often irregular shape of smoke and its blurred boundaries, GIoU's focus on the pixel-level overlapping area makes it difficult to perform an effective evaluation.

EIoU [37] minimizes the height difference between the predicted and ground truth boxes while focusing on the minimum enclosing box, enabling more accurate box evaluation for detection targets with blurred boundaries and irregular shapes. EIoU can be divided into three components: IoU loss L_{IoU}、distance loss L_{dis}、and aspect ratio loss L_{asp}, The expressions are as Eq. (22):

$$\begin{aligned} L_{EIoU} &= L_{IoU} + L_{dis} + L_{asp} \\ &= 1 - IoU + \frac{1}{2}\left(\frac{d_{center}^2}{d_{diag}^2} + \frac{\alpha \square AR_{diff}^2}{AR_{sum}^2}\right) \end{aligned} \tag{22}$$

where, d_{center} is the Euclidean distance between the center points of the predicted box and the ground truth box. d_{diag} is the length of the diagonal of the enclosing box. AR_{diff} is the difference in aspect ratios between the predicted box and the ground truth box. AR_{sum} is the sum of the aspect ratios of the predicted box and the ground truth box. α is a coefficient used to adjust the weight of the aspect ratio loss.

Compared to GIoU, EIoU accounts for uncertainty by introducing a probability distribution to model the position of the bounding box. This approach more accurately reflects the relative position and size between bounding boxes, and through expectation calculations, it prevents the loss from being reduced to zero even when the predicted box is very close to the ground truth box, thus avoiding overfitting caused by perfect scores during training. Additionally, EIoU introduces a scaling factor that can dynamically adjust based on the target size. This ensures that even if the overlap between the predicted box and the ground truth box is small for small targets, the score will not be overly penalized, thereby improving the model's accuracy and robustness in detecting small objects. For these reasons, we chose EIoU to replace GIoU in the label matching phase.

IV. Experiment and Algorithm Performance Evaluation

To validate the effectiveness of the model improvements, we conducted ablation experiments on the enhanced model using a self-constructed dataset. Additionally, we tested the performance of several representative real-time object detection models, the original RT-DETR-r18 model, and the improved model on the same dataset to assess their ability to detect fire smoke in the shortest possible time. The performance of the improved model was thoroughly evaluated.

A. Dataset

Currently, the number of publicly available real-world outdoor fire smoke datasets is limited. To develop a detection model with optimal performance, it is crucial to consider the most challenging detection scenarios. These include interference factors such as backlighting, long distances, strong winds, color variations, dense targets, and complex backgrounds. We collected 7,834 smoke images from unannotated public datasets and the internet, further filtering them based on these interference factors. After ensuring that all types of interference were represented and removing low-quality images, we selected 1,868 images, each containing at least one smoke target. These images were manually annotated using the Labelimg tool to create a custom YOLO-format smoke dataset. Fig. 7 shows dataset annotation status. The dataset was then randomly divided into training and test sets in an 8:2 ratio. All image sizes were adjusted to 640×640 to enhance detection speed.

Data preprocessing involved color space conversion and random mosaic processing to further augment the dataset and improve the model's robustness across different detection scenarios.

B. Implementation Details

1) Hardware and software environment: The hardware environment for the experiments in this paper is shown in Table I.

TABLE I. Experimental Environment

CPU	AMD EPYC 7773X @ 3.50GHz
GPU	GeForce RTX 4090
RAM	80G
Operating System	Ubuntu 20.04
Programming Language	Python 3.8
Deep Learning Framework	Pytorch 2.0.0
GPU Acceleration Library	Cuda 11.8

2) Training hyperparameter settings: The hyperparameters used in the experiments are listed in Table II.

TABLE II. Training Hyperparameter Settings

HYPERPARAMETER	Value
Optimizer	AdamW
Epochs	150
Batch size	16
Learning rate decay	cosine
Learning rate	0.0001
Weight decay	0.0001

3) Evaluation metrics: When evaluating the smoke detection performance of the model, we used five metrics: Recall, Average Precision (AP), model parameters (Params), Giga Floating Point Operations Per Second (GFLOPS), and Frames Per Second (FPS).

Recall is a crucial metric for assessing the detection capability of the model. It represents the proportion of correctly detected smoke instances out of all actual smoke samples. The calculation formula is as follows:

$$Recall = \frac{TP}{TP + FN} \tag{23}$$

where, TP refers to the number of smoke instances correctly detected by the model, while FN refers to the number of smoke

instances that the model failed to detect. A high recall indicates that the model can more comprehensively detect smoke.

AP represents the model's average detection accuracy across different confidence thresholds. The calculation formula is as follows:

$$Precision = \frac{TP}{TP + FP} \tag{24}$$

$$AP = \int_0^1 P(R)\,dR \tag{25}$$

where, AP represents the Average Precision, $P(R)$ denotes the precision value at a given recall R, N is the total number of classes.

Model parameters refer to the total number of trainable parameters in the model, which is an indicator of the model's complexity and storage requirements. A larger number of parameters typically implies a higher model complexity, potentially requiring more computational resources and storage space. The calculation formula is as follows:

$$Params = \sum_{l=1}^{L} Params_l \tag{26}$$

where, L is the total number of layers in the model, and $Params_l$ represents the number of parameters in the l -th layer.

Model computational cost refers to the total number of computational operations required during inference or training. It is an important metric for assessing the complexity and operational efficiency of a model. A higher computational cost typically indicates that the model requires more computational resources and time to complete inference or training.

$$Total\ GFLOPs = \sum_{i=1}^{L} GFLOPs_i \tag{27}$$

where L represents the total number of layers in the model, and $GFLOP_{Si}$ denotes the computational cost of the i -th layer.

FPS indicates the number of image frames a model can process per second during operation, serving as a key metric for evaluating the model's real-time performance. A higher FPS value signifies faster processing speed, making the model more suitable for real-time detection scenarios, such as video surveillance systems. The calculation of FPS typically considers the model's inference time and processing capability.

$$FPS = \frac{N}{T} \tag{28}$$

where N represents the number of processed image frames, and T is the total time taken to process these N frames.

Considering the concept of transfer learning, the experiments utilized pre-trained weights obtained from training on the VOC 2007 dataset. These pre-trained weights were used as initialization for training on the dataset in this study.

C. Ablation Experiments

1) Network input ablation experiment: To validate the effectiveness of the input aggregation strategy for concentration features and evaluate the efficacy of using CFA as network input, we conducted ablation experiments on both RT-DETR and YOLOV8m, focusing on their impact on model detection accuracy. The experimental results are shown in Table III. Using CFA as model input improves the detection accuracy for smoke. In RT-DETR, using CFA as input resulted in AP50 and AP95 scores of 0.882 and 0.585, respectively, representing an improvement of 1.2% and 0.9% compared to using RGB input, which achieved scores of 0.870 and 0.574. In YOLOV8m, using CFA as input yielded AP50 and AP95 scores of 0.856 and 0.602, respectively, reflecting increases of 1.1% and 2.1% over RGB input. These results indicate that replacing RGB images with CFA images as network input can effectively enhance the model's performance in smoke detection tasks.

TABLE III. ABLATION STUDY ON INPUT TYPES

Model	Input Type	AP_{50}	AP_{95}
RT-DETR	RGB	0.870	0.574
	CFA	0.882	0.585
YOLOV8m	RGB	0.845	0.581
	CFA	0.856	0.602

2) Effectiveness of improvements: To evaluate the benefits of each improvement in the enhanced network model for smoke detection tasks, we conducted six ablation experiments focusing on the three main improvements. To ensure that the experiments accurately reflect the impact of the network structure improvements and eliminate additional interference, all experiments used CFA images as the network input and were trained for 150 epochs on the custom dataset. Table IV presents the experimental results of the models under different configurations. First, we tested the baseline model, and then we sequentially added different improvement schemes. The specific experiments are as follows:

TABLE IV. ABLATION STUDY ON IMPROVED MODULES

Experiment Number	Improvement Scenarios			Evaluation Indicators					
	EIoU	S-CLDA	CSFFM	$Recall(\%)$	$AP_{50}(\%)$	$AP_{95}(\%)$	$Params(M)$	$GFLOPs$	$FPS(Hz)$
1	×	×	×	0.860	0.882	0.585	20.18	57.3	**65**
2	√	×	×	0.873	0.887	0.592	20.18	57.3	65
3	√	√	×	0.884	0.920	0.616	20.48	67.3	48
4	√	×	√	0.878	0.915	0.627	**15.07**	59.7	52
5	×	√	√	0.889	0.933	0.641	15.47	68.3	46
6	√	√	√	**0.895**	**0.939**	**0.648**	15.47	68.3	45

a) In Experiment 1, the baseline model was used without any improvement schemes. The results were: recall of 0.867, AP50 of 0.882, AP95 of 0.585, with a parameter count of 20.18 million and a computational requirement of 57.3 GFLOPS.

b) In Experiment 2, EIoU was incorporated, increasing recall to 0.873, AP50 to 0.887, and AP95 to 0.592, while the parameter count and computational load remained nearly unchanged.

c) In Experiment 3, building on the addition of EIoU, the S-CLDA was further introduced. The inclusion of attention mechanisms significantly improved the model's responsiveness and accuracy in detecting smoke targets, with recall rising to 0.902, AP50 reaching 0.920, and AP95 increasing to 0.616. The parameter count slightly increased to 20.48 million, and due to the integration of deformable convolutions and depth-wise separable convolutions, the computational cost modestly rose to 67.3 GFLOPS.

d) In Experiment 4, the CCFM was replaced with CS-SFFM, in addition to EIoU. This new strategy provided more refined cross-scale feature fusion with minimal information loss, significantly enhancing the model's ability to accurately localize targets. Recall increased to 0.897, AP50 reached 0.915, and AP95 rose to 0.627. Since CS-SFFM uses 3D convolutions and 3D pooling for feature fusion instead of multiple stacked convolutional layers, the computational cost slightly increased to 59.7 GFLOPS, while the parameter count significantly decreased to 15.07 million.

e) In Experiment 5, both S-CLDA and CS-SFFM were applied, while EIoU was omitted from the loss function. Despite the absence of EIoU optimization, the introduction of the remaining improvement modules still considerably enhanced the model's smoke detection performance. Recall rose to 0.911, AP50 reached 0.933, and AP95 increased to 0.641.

f) In Experiment 6, all improvement schemes were implemented simultaneously. This configuration yielded the best model performance, with recall increasing to 0.923, AP50 reaching 0.939, and AP95 rising to 0.648. The parameter count and computational cost were maintained at 15.47 million and 68.3 GFLOPS, respectively.

The experimental results demonstrate that replacing GIoU with EIoU enhances model accuracy without increasing additional parameters or computational load. The application of S-CLDA and CS-SFFM positively impacts both recall rate and detection accuracy in smoke detection tasks.

These improvements enhance detection performance while effectively controlling the growth in computational cost and significantly reducing the number of model parameters. In summary, the proposed improvements effectively enhance the model's performance in executing smoke detection tasks.

D. Performance Comparison Experiments

To validate the effectiveness of the proposed algorithm, four mainstream real-time object detection algorithms—YOLOv5m, YOLOv6m, YOLOv7, and YOLOv8m—were selected for comparison, along with the baseline model RT-DETR-r18.

1) Comparison of evaluation metrics: In the fire smoke detection task, we compared the training curves of the mainstream YOLO series algorithms with the baseline algorithm and our proposed model. The corresponding curves were plotted to provide a more intuitive observation of their training progress and differences, as shown in Fig. 8.

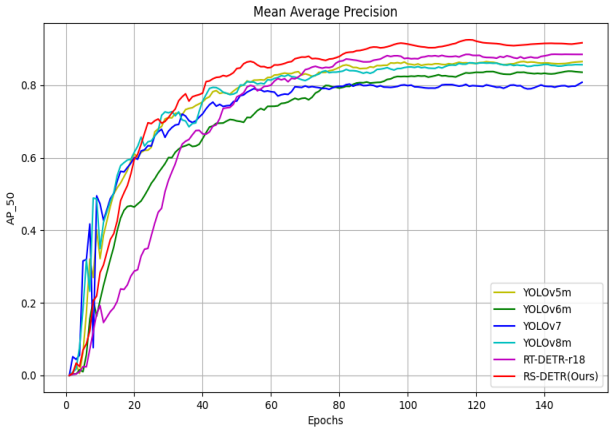


Fig. 8. Different algorithms' AP50 variations during training.

All models achieved convergence within 150 epochs. Our model demonstrated excellent performance in terms of accuracy and maintained high stability throughout the entire training process. Although the baseline model's accuracy was only slightly lower than that of our model, it exhibited significant fluctuations during training and had a slower convergence rate, falling behind the other algorithms. Overall, the improved model outperformed the baseline model in both detection accuracy and training stability.

The test results of each model on the self-built dataset are shown in Table V. Our algorithm achieved the best accuracy with 15.47 million parameters, an AP50 of 0.939, and an AP95 of 0.648. This success can be attributed to the more targeted and accurate smoke feature extraction enabled by the S-CLDA attention mechanism, as well as the refined multi-level feature fusion facilitated by CS-SFFM, which preserves more low-level features through adaptive pooling and interpolation.

TABLE V. COMPARATIVE EXPERIMENTS ON SELF-BUILT DATASET

Compare Models	Evaluation Indicators				
	Recall	AP_{50}	AP_{95}	*Param*	*GFLOPs*
YOLOv5m	0.839	0.863	0.564	21.2	64.6
YOLOv6m	0.802	0.834	0.544	24.85	161.7
YOLOv7	0.782	0.805	0.537	36.9	104.7
YOLOv8m	0.825	0.856	0.602	25.85	79.3
RT-DETR-r18	0.860	0.882	0.585	20.18	57.3
RS-DETR(ours)	**0.895**	**0.939**	**0.638**	**15.47**	68.3

2) Multi-scale smoke detection comparison experiments: Fire smoke undergoes significant scale variations at different stages, with early-stage smoke, which is often of high detection value, typically being smaller in size. To assess the model's

detection performance across different stages of smoke, we designed a multi-scale smoke detection experiment. To visually represent the model's effectiveness in detecting smoke targets of varying scales, we applied the K-means [38] algorithm to cluster the test set and then divided the test set based on the clustering results. The clustering outcomes are shown in Fig. 9, where the centroids of the large, medium, and small target clusters correspond to [0.107, 0.131], [0.246, 0.325], and [0.333, 0.587], respectively.

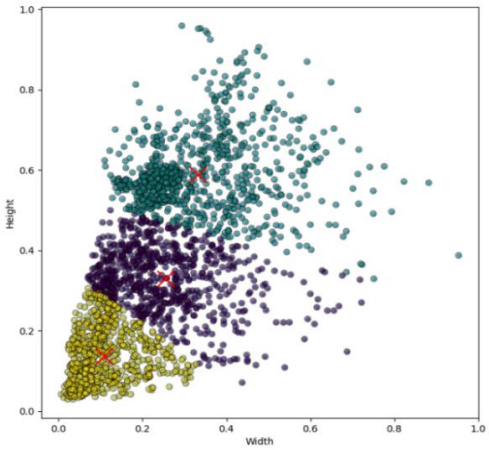


Fig. 9. Analysis of smoke scale distribution.

As shown in Table VI, after filtering and dividing the dataset, the test set of 374 images includes 145 images with small smoke targets, 152 images with medium smoke targets, and 77 images with large smoke targets.

TABLE VI. TEST SET TARGET SEGMENTATION RESULTS

Target Scale	Small Objects	Medium Objects	Large Objects
Target Quantity	145	152	77

Fig. 10 presents the statistical results of each algorithm's performance in detecting smoke targets of different scales. The results indicate that in the multi-scale smoke detection comparison, RS-DETR outperformed other mainstream real-time detection algorithms across all smoke scales. Compared to the YOLO series detection models, the improved model demonstrated particularly outstanding performance in detecting small-scale smoke. This improvement can be attributed to the CS-SFFM module in RS-DETR, which employs bilinear interpolation for scaling, effectively mitigating the loss of fine-grained feature details. Consequently, the model demonstrates enhanced sensitivity in capturing the distinctive characteristics of small-scale smoke targets, thereby reducing the likelihood of misclassification as background.

3) Comparison of detection results under interference factors: To validate the model's detection performance under various interference factors, we selected smoke images with strong wind, backlighting, long distances, color differences, and dense targets for comparison. The detection results are shown in Fig. 11. The results indicate that YOLOv5m performed poorly in detecting smoke targets with color differences and exhibited repeated detections when faced with distant, backlit targets. YOLOv6m and YOLOv7 both experienced missed or false detections in scenarios involving background interference, dense small targets, and backlighting. YOLOv8m also showed missed detections when detecting smoke targets with color differences. The baseline model encountered missed detections and false detections when dealing with dense small targets and backlit targets, likely due to the NMS-free strategy's inability to accurately determine whether to retain detection boxes for adjacent targets. The improved algorithm presented in this paper was able to correctly detect smoke targets in all these challenging scenarios, demonstrating higher detection accuracy and robustness, thereby meeting the practical application requirements for fire smoke detection.

4) Heatmap comparison: Heatmaps are a visualization technique used to display the intensity distribution of objects detected by a model within an input image. They typically indicate the location and confidence of the detected targets, with brighter areas representing higher confidence levels. We compared the heatmaps generated by the baseline model and the improved model, as shown in Fig. 12. The heatmap on the left corresponds to the baseline model, RT-DETR-r18, showing that the model primarily focuses on the central region of the smoke, with lower attention to the edges. In contrast, the second heatmap corresponds to our improved model, where the highlighted areas cover both the main body and the diffuse portions of the smoke, nearly encompassing the entire smoke region. Additionally, the heatmap of our model demonstrates higher attention to the overall structure of the smoke and effectively responds to thin smoke, indicating greater confidence in detecting smoke targets. These observations confirm that the improved model outperforms RT-DETR-r18 in smoke detection tasks.

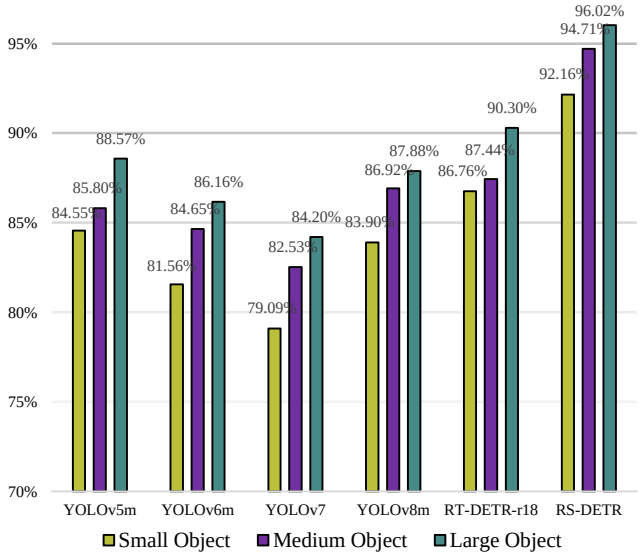


Fig. 10. Multi-scale object detection performance comparison.

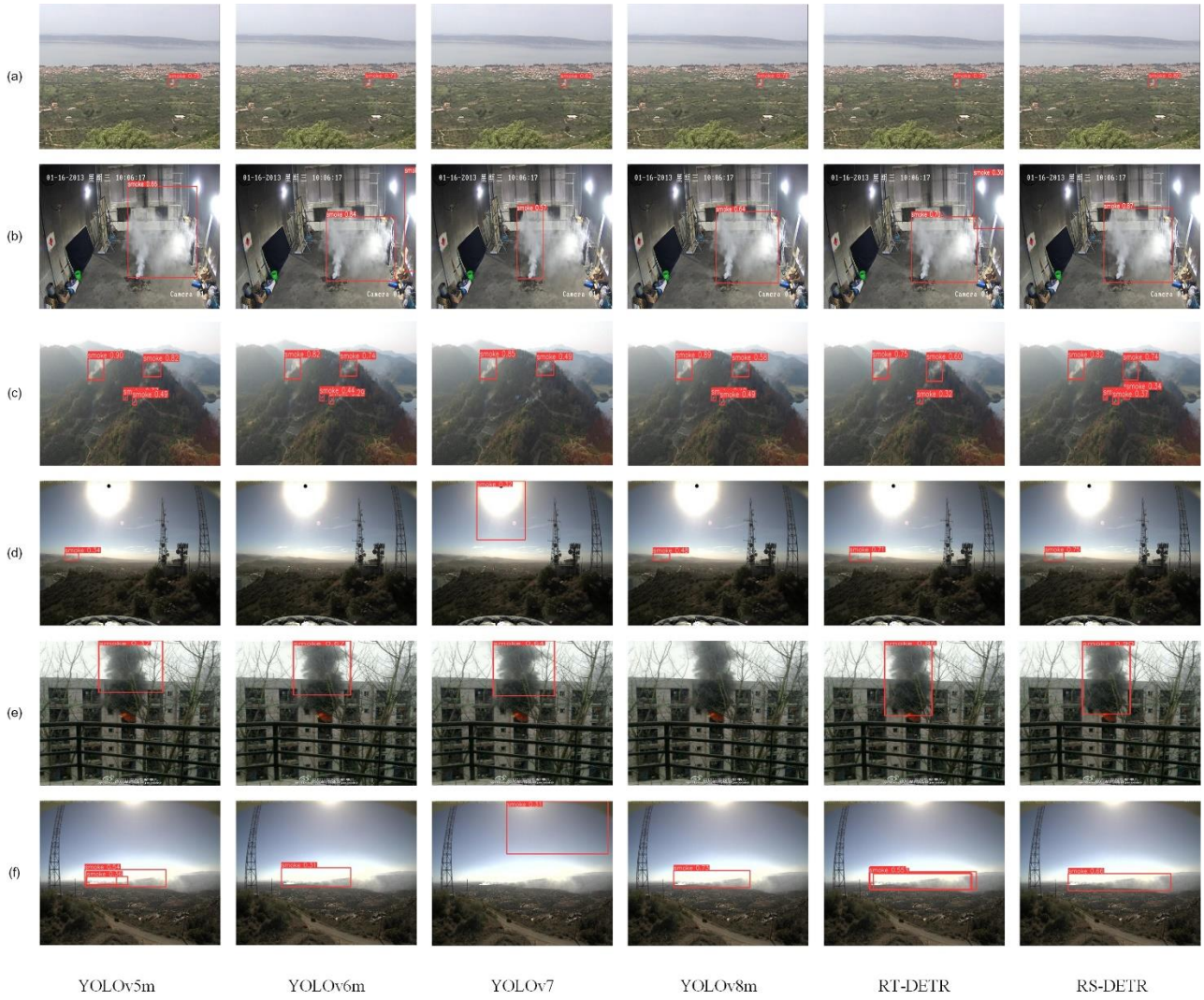


Fig. 11. Detection results under interference.

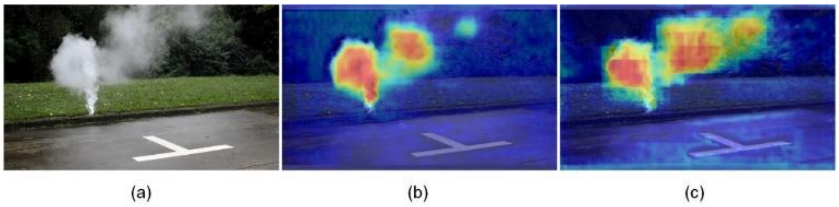


Fig. 12. The comparison results of the heatmap: (a) Original Image (b) RT-DETR-r18 (c) RS-DETR

V. CONCLUSION

This paper introduces an enhanced fire smoke detection algorithm based on RT-DETR, focusing on improving accuracy, real-time performance, and robustness against various interference factors. Key improvements include using the dark channel prior method for smoke concentration input, integrating the S-CLDA attention mechanism for robust feature extraction, and optimizing multi-scale feature fusion through the CSFFM module with 3D convolution and interpolation. The EIoU loss function further enhances detection accuracy for small targets and reduces redundant detections. Experiments on a self-made smoke detection dataset show that the improved model outperforms mainstream YOLO models and the RT-DETR-r18 baseline in AP50 and AP95 metrics while maintaining high detection speed. Specifically, the model achieved a 5.9% increase in AP50 and a 5.7% increase in AP95 with a 23.3% reduction in parameters, balancing accuracy and efficiency. This study confirms the potential of RT-DETR in fire smoke detection and demonstrates the effectiveness of the proposed improvements. Future work will focus on further optimizing the model, exploring advanced feature extraction and fusion strategies, and validating the model's robustness across diverse datasets and real-world scenarios to provide more reliable and efficient fire detection technology.

ACKNOWLEDGMENT

This study was supported by the Key Scientific Research Project Plan for Higher Education Institutions of Henan Province, China (No.25A520033).

REFERENCES

[1] "In the first half of 2023, there were over 3,000 fires per day on average nationwide." National Fire and Rescue Administration, July. 2023. https://www.119.gov.cn/qmxfgk/sjtj/2023/38420.shtml.

[2] J. He, H. Lin, and G. Xu, "Overview of Research on Smoking Detection Methods in Computer Vision."Computer Engineering and Applications, vol.60, no.1, pp. 40-56. 2024.

[3] Wahyono, A. Harjoko, A. Dharmawan, F. D. Adhinata, G. Kosala, and K.H. Jo, "Real-Time Forest Fire Detection Framework Based on Artificial Intelligence Using Color Probability Model and Motion Feature Analysis," Fire, vol. 5, no. 1, p. 23, 2022.

[4] Y. Al-Smadi, "Early wildfire smoke detection using different yolo models," Machines, vol. 11, no. 2, p. 246, 2023.

[5] Y. Zhou, L. Xia, J. Zhao, R. Yao, and B. Liu, "Efficient convolutional neural networks and network compression methods for object detection: A survey," Multimedia Tools and Applications, vol. 83, no. 4, pp. 10167-10209, 2024.

[6] N. Carion, F. Massa, G. Synnaeve, N. Usunier, A. Kirillov, and S. Zagoruyko, "End-to-end object detection with transformers," in European conference on computer vision, 2020, pp. 213-229.

[7] T. Shehzadi, K. A. Hashmi, D. Stricker, and M. Z. Afzal, "2d object detection with transformers: a review," arXiv preprint arXiv:2306.04670, 2023.

[8] Y. Zhao et al., "Detrs beat yolos on real-time object detection," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2024, pp. 16965-16974.

[9] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Look Only Once," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 779-788.

[10] J. Redmon and A. Farhadi, "YOLO9000: better, faster, stronger," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2017, pp. 7263-7271.

[11] J. Redmon and A. Farhadi, "Yolov3: An incremental improvement," arXiv preprint arXiv:1804.02767, 2018.

[12] A. Bochkovskiy, C. Wang, and H. Liao, "Yolov4: Optimal speed and accuracy of object detection," arXiv preprint arXiv:2004.10934, 2020.

[13] "Yolov5." Ultralytics, 2021. https://github.com/ultralytics/yolov5.

[14] C. Li et al., "YOLOv6: A single-stage object detection framework for industrial applications," arXiv preprint arXiv:2209.02976, 2022.

[15] C. Wang, A. Bochkovskiy, and H. Liao, "YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2023, pp. 7464-7475.

[16] "YOLO by Ultralytics." Ultralytics, 2023. https://github.com/ultralytics/ultralytics.

[17] S. Frizzi, R. Kaabi, M. Bouchouicha, J. Ginoux, E. Moreau, and F. Fnaiech, "Convolutional neural network for video fire and smoke detection," in IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society, 2016, pp. 877-882.

[18] Z. Lin ,Y. Shen," Research on Fire Warning Algorithm Based on Deep Convolutional Neural Network " Information &Commmunications, no. 5, pp. 38-42, 2018.

[19] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 39, no. 6, pp. 1137-1149, 2017.

[20] W. Liu et al., "Ssd: Single shot multibox detector," in Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11–14, 2016, Proceedings, Part I 14, 2016, pp. 21-37.

[21] J. Dai, Y. Li, K. He, and J. Sun, "R-fcn: Object detection via region-based fully convolutional networks," Advances in neural information processing systems, vol. 29, pp. 379-387, 2016.

[22] L. Zhang, C. Lu, H. Xu, A. Chen, L. Li, and G. Zhou, "MMFNet: Forest Fire Smoke Detection Using Multiscale Convergence Coordinated Pyramid Network With Mixed Attention and Fast-Robust NMS," IEEE Internet of Things Journal, vol. 10, no. 20, pp. 18168-18180, 2023.

[23] J. Wang, X. Zhang, K. Jing, and C. Zhang, "Learning precise feature via self-attention and self-cooperation YOLOX for smoke detection," Expert Systems with Applications, vol. 228, p. 120330, 2023.

[24] Z. Ge, S. Liu, F. Wang, Z. Li, and J. Sun, "Yolox: Exceeding yolo series in 2021," arXiv preprint arXiv:2107.08430, 2021.

[25] S. Liu, L. Qi, H. Qin, J. Shi, and J. Jia, "Path aggregation network for instance segmentation," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2018, pp. 8759-8768.

[26] J. Zhan, Y. Hu, G. Zhou, Y. Wang, W. Cai, and L. Li, "A high-precision forest fire smoke detection approach based on ARGNet," Computers and Electronics in Agriculture, vol. 196, p. 106874, 2022.

[27] V. E. Sathishkumar, J. Cho, M. Subramanian, and O. S. Naren, "Forest fire and smoke detection using deep learning-based learning without forgetting," Fire Ecology, vol. 19, no. 1, p. 9, 2023.

[28] Y. Li, W. Zhang, Y. Liu, R. Jing, and C. Liu, "An efficient fire and smoke detection algorithm based on an end-to-end structured network," Engineering Applications of Artificial Intelligence, vol. 116, p. 105492, 2022.

[29] X. Zhu, W. Su, L. Lu, B. Li, X. Wang, and J. Dai, "Deformable detr: Deformable transformers for end-to-end object detection," arXiv preprint arXiv:2010.04159, 2020.

[30] J. Huang, J. Zhou, H. Yang, Y. Liu, and H. Liu, "A small-target forest fire smoke detection model based on deformable transformer for end-to-end object detection," Forests, vol. 14, no. 1, p. 162, 2023.

[31] X. Zhuang, F. Tan, Z. Li, L. Li, " Image Defogging Algorithm Based On Dark Channel Priorand Optimized Auto-Color," Computer Applications and Software, vol. 38, no. 7, pp. 190-195, 2021.

[32] S. Woo, J. Park, J. Lee, and I. S. Kweon, "Cbam: Convolutional block attention module," in Proceedings of the European conference on computer vision, 2018, pp. 3-19.

[33] J. Dai, "Deformable convolutional networks," in Proceedings of the IEEE international conference on computer vision, 2017, pp. 764-773.

[34] X. Ding, X. Zhang, J. Han, and G. Ding, "Scaling up your kernels to 31x31: Revisiting large kernel design in cnns," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2022, pp. 11963-11975.

[35] M. Kang, C. Ting, F. Ting, and R. C. W. Phan, "ASF-YOLO: A novel YOLO model with attentional scale sequence fusion for cell instance segmentation," Image and Vision Computing, vol. 147, p. 105057, 2024.

[36] H. Rezatofighi, N. Tsoi, J. Gwak, A. Sadeghian, I. Reid, and S. Savarese, "Generalized intersection over union: A metric and a loss for bounding box regression," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2019, pp. 658-666.

[37] Y. Zhang, W. Ren, Z. Zhang, Z. Jia, L. Wang, and T. Tan, "Focal and efficient IOU loss for accurate bounding box regression," Neurocomputing, vol. 506, pp. 146-157, 2022.

[38] A. M. Ikotun, A. E. Ezugwu, L. Abualigah, B. Abuhaija, and J. Heming, "K-means clustering algorithms: A comprehensive review, variants analysis, and advances in the era of big data," Information Sciences, vol. 622, pp. 178-210, 2023.

Predicting Stock Price Bubbles in China Using Machine Learning

Yunxi Wang[1*], Tongjai Yampaka[2*]
Chakrabongse Bhuvanarth International Institute for Interdisciplinary Studies (CBIS),
Rajamangala University of Technology Tawan-OK, Bangkok, Thailand[1, 2]
School of Finance, Guangzhou Huashang College, Guangzhou, China[1]

***Abstract*—Financial bubbles have long been a focus of researchers, particularly due to the severe negative impacts following the bursting of financial bubbles. Therefore, the ability to effectively predict financial bubbles is of paramount importance. The aim of this study is to measure and predict the stock market price bubble in China from January 2015 to December 2023. To achieve this, we utilized the GSADF test, currently the most effective, to identify and measure the situation of the stock market price bubble in China. Subsequently, we selected inflation rate, consumer confidence index, stock yield, and price-earnings ratio as explanatory/predictive variables. Finally, four machine learning methods were employed to forecast the stock market price bubble in China. The results indicate that a price bubble occurred in the Chinese stock market during the first half of 2015, before the outbreak of the COVID-19 pandemic in China in January 2020. Furthermore, the comparison reveals that among the machine learning methods, logistic regression is the most suitable and effective for China, while other methods such as deep learning and decision trees also hold certain value.**

***Keywords*—Stock price bubbles; machine learning; Chinese stock market**

I. INTRODUCTION

Asset price bubbles refer to asset prices that exceed their fundamental values, and their occurrence has consistently had significant impacts on the economies of nations and the lives of their citizens [1]. Whether considering global instances, such as the Japanese real estate and stock market bubbles during 1986 to 1991, the late 1990s dot-com bubble in the United States, or from the perspective of China, such as the 2009s Chinese stock market bubble that occurred following the U.S. subprime mortgage crisis, it is evident that financial bubbles exert considerable influence on economies, particularly with regard to adverse effects. When a financial bubble bursts, they can precipitate the collapse of financial institutions and push nations to the brink of bankruptcy. Moreover, they not only impact the development of a single country but sometimes also trigger global financial crises or induce worldwide economic downturns [2]. Generally, following the occurrence of these crises, governments are compelled to allocate substantial resources and implement a variety of measures to attempt to stabilize and salvage the national economy.

Furthermore, for investors and the public, the negative consequences of financial bubbles make it difficult for confidence to be restored in the market. Most of the public lacks experience and risk management abilities, and they are most heavily affected by the bursting of financial bubbles. When they go bankrupt, it causes societal upheaval [3]. Therefore, studying and forecasting financial bubbles are of paramount importance for governments and regulatory authorities. Such endeavors enable governments to implement appropriate economic policies at the right juncture to mitigate the adverse effects of financial bubbles. Moreover, in the current context of economic globalization, where nations and various types of markets are interconnected, the detrimental impacts of financial bubbles can have broader repercussions. China that is the world's second-largest economy possesses unique characteristics and complexities in its stock market. The emergence of a stock market bubble in China not only affects its domestic economy but also has ramifications for the global economy. Consequently, accurate prediction of stock market bubbles in China holds positive implications for both the Chinese and global economies. Such predictions can offer valuable guidance for investors, provide early warnings for financial institutions, and prompt regulatory authorities to take necessary actions to deal with the existence of bubbles.

The Chinese stock market was established in 1990 with the founding of the Shanghai Stock Exchange. From the establishment of the Chinese stock market in 1990 to 1996, there were four price bubbles in the early stage of the Chinese stock market, and each price fluctuation was extremely violent. In 1999, China promulgated the Securities Law, which created a favorable environment for the further development of the Chinese stock market, attracting more investors to participate in the stock market. However, it also led to the re-emergence of stock market price bubbles. Subsequently, in 2001, China's accession to the World Trade Organization (WTO) resulted in a surge of foreign capital inflows, providing significant impetus for the rapid growth of the Chinese economy. This also led to the rapid development of the Chinese stock market, with an expansion in market size and increased trading activity, attracting more investors. Concurrently, the Chinese government implemented a series of reform and opening-up policies, including financial market reform and state-owned enterprise reform, promoting further development and healthy growth of the Chinese stock market. During this period, the Chinese stock market reached a historical high of 2245 points, representing a cumulative increase of 66.7%. Subsequently, it experienced a slow bear market, with the stock index falling to a low of 998 points. From 2007 to 2008, amidst favorable global economic development and China's hosting of the 2008

Olympic Games, the stock index reached a new high of 6124 points in 2007, soaring more than fivefold. However, with the outbreak of the global financial tsunami triggered by the U.S. subprime mortgage crisis, the stock market plummeted to 1664 points in October 2008. This time, the stock market bubble burst rapidly.In the early 2010s, driven by economic growth and increased participation of domestic and foreign investors, the Chinese stock market experienced rapid expansion. However, this period also witnessed market turbulence, especially the stock market crash in 2015, prompting government intervention to stabilize the market. Subsequently, the Chinese stock market underwent further reforms aimed at improving market efficiency and sustainability. Measures such as the introduction of the Science and Technology Innovation Board (STAR Market) and the implementation of IPO registration system aimed to promote innovation and enhance the quality of listed companies. As of the end of 2023, the market capitalization of the Chinese stock market was approximately 85.54 trillion Yuan, while China's GDP in 2023 reached 126.06 trillion Yuan, accounting for approximately 67.86% of China's GDP [4]. There are a total of 5,346 listed companies in the Chinese domestic stock market, with the industries of manufacturing, information transmission, software and information technology services, and wholesale and retail trade ranking among the top three in terms of the number of listed companies [4]. Since its establishment in 1990, the Chinese stock market has experienced rapid development over the past 30 years. However, along with this rapid growth, the Chinese stock market has also encountered a series of issues, particularly manifested in the frequent occurrence of stock market bubbles. The Chinese market is typically sensitive to various rumors, leading to price manipulation of many stocks by rumor mongers. The main reasons for these issues lie in the lack of transparency in the market information and fluctuations in investor sentiment. Therefore, the government and regulatory authorities should remain vigilant at all times to detect financial bubbles promptly and formulate corresponding policies to protect stock market investors, especially retail investors, and stabilize the economic market.

Research on stock price bubbles typically addresses several key questions and objectives, which can be categorized into three main areas. First, it evaluates the factors that contribute to the formation of stock price bubbles. Second, it identifies the early stages of stock price bubbles using the GSADF method. Finally, it develops and validates effective machine learning models and techniques for early detection of stock price bubbles, aimed at improving the accuracy of bubble identification. By addressing these research questions and objectives, this study seeks to provide a comprehensive understanding of stock price bubbles, with a particular focus on the Chinese market, and to offer practical recommendations for enhancing market stability and investor decision-making.

II. Theoretical Literature Review

A. Theoretical Literature Review about Measuring Stock Market Bubble

In research conducted throughout history, there has been a wealth of studies devoted to measuring financial market bubbles. These studies encompass various types of markets, such as stock markets, real estate markets, cryptocurrency markets, and others. Given that this paper focuses on the domain of stock markets and specifically examines price bubbles within this context, it provides a concise overview of measuring bubbles in the stock market domain, with particular emphasis placed on studies employing statistical models applied to time-series data.

Dickey (1979) proposed the Augmented Dickey-Fuller (ADF) test in 1979 to examine whether time series data exhibit unit roots, indicating non-stationarity [5]. In the realm of finance, the ADF test is also utilized to investigate the presence of asset price bubbles. This method, grounded in unit root testing, entails regression analysis of time series data to assess the presence of unit roots within the sequence. The existence of a unit root suggests non-stationarity and the potential existence of a price bubble; conversely, the absence of a unit root indicates stationarity and a lower likelihood of a price bubble. The significance of the test results is typically determined by setting thresholds, thereby ascertaining the presence or absence of a price bubble. Wang (2020) employed the ADF test to evaluate the existence of bubbles in the Chinese stock market [6].

Cheung (1995) introduced the Supremum Augmented Dickey-Fuller (SADF) test as an enhancement to the Augmented Dickey-Fuller (ADF) test [7]. Similar to the ADF test, the SADF test is employed to examine whether time series data possess unit roots, thereby determining the presence of non-stationarity. However, the SADF test introduces the concept of "supremum," allowing for testing across multiple lag lengths and identifying the optimal lag length. By doing so, the SADF test can more accurately ascertain the non-stationarity of time series data and provide more precise unit root test results. Consequently, the SADF test is considered a more reliable method than the ADF test in some cases, particularly when dealing with long or unstable time series data. Homm and Breitung (2012) utilized this test to detect stock market bubbles and, through a process of simulation and comparison of evaluation criteria, determined the SADF test to be the most optimal among the methods employed [8]. While effective in identifying single bubble events, the SADF test may encounter challenges in practical applications where multiple bubbles occur in sufficiently large samples. Although successful in identifying notable historical bubbles, the SADF test failed to detect the bubble associated with the 2007 – 2008 debt crisis.

Phillips et al. (2011) proposed the Generalized Supremum Augmented Dickey-Fuller (GSADF) test as an advancement and refinement of the Supremum Augmented Dickey-Fuller (SADF) test [9]. Similar to the SADF test, the GSADF test is utilized to examine whether time series data exhibit unit roots, thereby determining non-stationarity. However, the GSADF test introduces the Maximized Average Power (MAP) statistic, which allows for the testing of unit root presence and location at each stage, rendering it more flexible in determining the existence and location of unit roots. By considering the possibilities across multiple lag lengths, the MAP statistic enhances the flexibility of the test, leading to a more accurate determination of non-stationarity in time series data. This

enables the GSADF test to be applicable to a wider range of hypotheses and more flexible in determining the existence and location of unit roots. Through the utilization of the GSADF test, researchers can more accurately identify non-stationarity in time series data. Phillips et al. (2015b) employed both the SADF and GSADF tests to empirically apply them to Standard & Poor's 500 stock market data spanning from January 1871 to December 2010[10]. The new GSADF method successfully identified historical events of prosperity and collapse during this period, such as the Panic of 1873 (October 1879 to April 1880) and the Dot-com bubble (July 1997 to August 2001).

Based on the comprehensive review of methods for measuring the stock market domain, we have found that the Generalized Supremum Augmented Dickey-Fuller (GSADF) measurement is currently the most effective among the detection methods. Therefore, in our study of measuring price bubbles in the Chinese stock market, we will utilize the GSADF method.

B. Theoretical Literature Review about Machine Learning in Financial Field

In recent years, machine learning methods have garnered increasing attention from scholars, whether in forecasting financial crises [11], predicting financial bubbles [12][13], or anticipating stock price trends [14] [15]. They all have provided researchers with a novel set of tools and solutions for investigation.

Ouyang and Lai (2021) utilized machine learning algorithms to assess systemic risk warnings in China [11],. Their study revealed that the Attention-Long Short-Term Memory (Attention-LSTM) neural network model within the machine learning algorithms demonstrated higher accuracy compared to other models. This suggests that in the context of China, the Attention-LSTM neural network model holds significant value for systemic risk assessment and early warning.

Başoğlu Kabran and Ünlü (2021) employed machine learning techniques to forecast financial bubbles [12]. They utilized the Support Vector Machine (SVM) algorithm within the domain of machine learning for predicting financial bubbles and compared this approach against alternative methods, concluding that the Support Vector Machine exhibited superior effectiveness in forecasting financial bubbles. The study focused on predicting bubbles within the Standard & Poor's 500 Index.

Tran et al. (2023) employed machine learning methods to predict financial bubbles in the Vietnamese stock market from 2001 to 2021 [13]. They utilized six different algorithms within machine learning to forecast these financial bubbles and compared these algorithm results. Their findings concluded that the Random Forest and Artificial Neural Network algorithms outperformed traditional statistical methods in predicting financial bubbles in the Vietnamese stock market.

Gu et al. (2020) applied machine learning methods to empirical asset pricing [14]. They found that decision trees and neural networks exhibited the best predictive performance among machine learning algorithms. The outstanding predictive capability of these two algorithms primarily stems from their ability to capture complex nonlinear interactions among predictive variables, a task often challenging for other algorithms. Using these two machine learning algorithms yielded performance twice as high as traditional statistical methods. Furthermore, this study identified return reversal and momentum, stock liquidity, stock volatility, and valuation ratios as the most influential factors in asset pricing among the predictive variables.

Zhou et al. (2023) utilized a Deep Neural Network (DNN) model within the domain of machine learning to forecast stock premiums [15] .The research spanned from December 1950 to December 2016, employing monthly data. Stock premiums were computed as the difference between the logarithmic returns of the Standard & Poor's 500 Index (including dividends) and those of risk-free assets. The investigation compared the DNN model from machine learning against the Ordinary Least Squares (OLS) model and Historical Average (HA) model from traditional statistical analysis, ultimately revealing the superior predictive efficacy of the DNN model. Researchers enhanced the predictive capability of the DNN model by incorporating 14 predictive variables. They attributed the DNN model's superior predictive performance primarily to its ability to automatically extract high-dimensional features from data and identify various predictive patterns within the dataset.

Based on the literature discussed above, it is evident that machine learning algorithms exhibit superior performance in classification and time series regression problems. However, it is important to note that the predicted results may vary significantly among different models depending on the dataset utilized, and there is no universally applicable method to ensure consistently superior performance.

Drawing upon the synthesized literature, it becomes apparent that the utilization of machine learning for predicting financial bubbles in the stock market is a relatively novel approach, with limited research attention received thus far. So far, only Başoğlu Kabran and Ünlü (2021) employed machine learning methods to predict bubbles in the S&P 500 index, as well as Tran et al. (2023) in forecasting bubbles in the Vietnamese stock market from 2001 to 2021, as mentioned earlier in the text. Research in the financial domain primarily focuses on predicting financial crises and stock price trends [12] [13]. There is a dearth of corresponding studies in China regarding the prediction of stock market price bubbles, particularly concerning the utilization of machine learning algorithms. To the best of our knowledge, there have been no studies utilizing machine learning methods to forecast stock market price bubbles in China. Therefore, the purpose of this study is to measure and predict the price bubble in the Chinese stock market, and compare the performance of the machine learning algorithms used to select the most suitable model for the price bubble in the Chinese stock market.

III. RESEARCH DESIGN

The primary objective of our study is to measure the stock market price bubbles in China from January 2015 to December 2023, with January 2020 serving as the demarcation point [16], dividing the time period into pre-China COVID-19 and post-China COVID-19 phases, and using carefully selected four

explanatory variables — namely, the inflation rate in macroeconomic factors, the consumer confidence index in sentiment factors, and stock yield and price-to-earnings ratio in market factors to predict the occurrence of stock market price bubbles in China. In this research, we employ the Generalized Supremum Augmented Dickey-Fuller (GSADF) test to identify and measure the presence of stock market price bubbles in China and select four machine learning algorithms for prediction. Ultimately, by comparing the performance results of the four machine learning algorithms, we find the best model for predicting stock market price bubbles in China. This study theoretically contributes empirical evidence to the application of machine learning in forecasting financial bubbles and practically offers early warnings to investors and decision-makers, enabling them to make appropriate financial decisions.

IV. Data and Methodology

A. Data

We utilized the stock market index data of China (Shanghai Composite Index) from January 2015 to December 2023 and employed the Generalized Supremum Augmented Dickey–Fuller (GSADF) method to identify price bubbles in the Chinese stock market during this period. The Chinese stock market index or the Shanghai Composite Index refers to the capitalization-weighted index of all companies listed on the Shanghai Stock Exchange. The monthly dataset of the Chinese stock market comprises 108 data points, while the weekly dataset comprises 470 data points. Among these, it was observed that price bubbles occurred in the Chinese market for 6 months and 25 weeks respectively. The measurement method for price bubbles in the Chinese stock market is the Generalized Supremum Augmented Dickey–Fuller method, which is elaborately described in Section II.A.

In employing machine learning methods, for the convenience of training and testing, we opted for four machine learning algorithm models. We divided the data into two datasets: one for training and the other for testing. Specifically, the training dataset comprises weekly data from January 2015 to December 2023, while the testing dataset comprises monthly data from the same period. The training dataset comprises stock market bubble conditions derived from weekly data publicly disclosed on the official website of the Shanghai Stock Exchange. In contrast, the testing dataset consists of stock market bubble conditions derived from monthly weighted average data disclosed on the same website. Due to the disparate sources of weekly and monthly data, the datasets for training and testing during the same time periods are not identical. However, both datasets all cover the period from January 2015 to December 2023. For instance, the training dataset for January 2015 consists of four weekly data points from that month, whereas the testing dataset consists of the monthly data for January 2015.

The daily and intraday data are unsuitable for this research due to the insufficient labeling of bubbles in the Chinese stock market. Using daily data results in significant classification issues with the labels. To mitigate this problem, the study shifts to analyzing weekly and monthly observations [17]. The selection of evaluation metrics must align with the nature of the classification problem. For such tasks, pertinent metrics include AUC, F-measure, accuracy, precision, and sensitivity [18].

This essentially ensures that the condition of stock price bubbles in the training dataset is four times that in the testing dataset. The purpose of this arrangement is to ensure that both the training and testing datasets contain sufficient data for model development and application in machine learning.

In employing machine learning methods, we incorporated four explanatory variables into the algorithmic model. These four explanatory variables consist of the inflation rate from macroeconomic factors, the consumer confidence index from sentiment factors, and the stock yield and price-earnings ratio from market factors. Within the time frame selected from January 2015 to December 2023, they were also segregated into a testing dataset comprising solely monthly data and a training testing dataset comprising solely weekly data.

The measurement of price bubbles in the Chinese stock market (Shanghai Composite Index) was obtained through the Generalized Supremum Augmented Dickey–Fuller (GSADF) program in the EViews software. For data analysis, we utilized corresponding algorithms in machine learning tools — specifically, logistic regression, deep learning, decision tree, and support vector machine—via the RapidMiner software.

B. Methodology

This study is divided into two parts. The first part involves the detection of price bubbles in the Chinese stock market, while the second part involves the use of four machine learning algorithms to predict the occurrence of price bubbles in the Chinese stock market.

In the first part, we utilized monthly and weekly stock market price data from China spanning from 2015 to 2023 to identify financial bubble occurrences. During this timeframe, with January 2020 marking the dividing line, we segmented the data into pre-COVID-19 pandemic and post-COVID-19 pandemic periods. In January 2020, the Chinese government officially declared the emergence of the COVID-19 pandemic in China and implemented nationwide controls [16]. The purpose of this section of the study using detection methods is to identify the occurrence of price bubbles in the Chinese stock market on a monthly and weekly basis during this period. The monthly and weekly data of the Chinese stock indices (Shanghai Composite Index) were obtained through web scraping from the official website of the Shanghai Stock Exchange.

In the second part, we utilized four machine learning algorithms to forecast price bubbles in the Chinese stock market and employed four explanatory variables to predict the occurrence of price bubbles in the Chinese stock market. The dependent variable is the occurrence of monthly/weekly price bubbles in the Chinese stock market, with the outcomes being the results obtained from the first part of the study. When price bubbles occurred in the Chinese stock market, we assigned a value of 1 to the corresponding month/week, and when price bubbles did not occur, we assigned a value of 0 to the

corresponding month/week. The explanatory variables we employed include the inflation rate from macroeconomic factors, the consumer confidence index from sentiment factors, and the stock yield and price-earnings ratio from market factors. The monthly data for these explanatory variables were sourced from the official website of the National Bureau of Statistics of China and the Wind financial database website. Overall, we selected inflation rate, consumer confidence index, stock yield, and price-earnings ratio, these four significant economic indicators, to forecast price bubbles in the Chinese stock market using their data. Since most of these data are monthly, we utilized the EViews tool to convert monthly data into weekly data.

1) The Generalized Supremum Augmented Dickey–Fuller (GSADF) method for measuring price bubbles in the Chinese stock market: In the first part, the method utilized for measuring price bubbles in the Chinese stock market involved employing the currently most effective time series measurement technique, specifically tailored for detecting asset price bubbles—the Generalized Supremum Augmented Dickey–Fuller (GSADF) test [19]. This method was initially proposed by Philialps et al. (2015b) in 2015 and evolved from the augmented Dickey–Fuller (ADF) test and supremum augmented Dickey–Fuller (SADF) test. It utilizes recursive regression techniques to investigate the presence of unit roots when faced with an alternative right-tail explosion hypothesis, enabling the identification of multiple bubble periods within a time series dataset. Rejection of the null hypothesis during the test indicates the existence of asset price bubbles. In the Generalized Supremum Augmented Dickey–Fuller (GSADF) test, critical values for the test statistics are typically obtained through 2000 Monte Carlo simulations [20], aiding in determining the onset and conclusion of asset price bubbles.

The aim of Generalized Supremum Augmented Dickey–Fuller (GSADF) test was to analyze statistical properties on the upper end of the Augmented Dickey–Fuller (ADF) test concerning a time series. By comparing the maximum values generated from the test statistics with predetermined threshold values obtained from the distribution, analysts can make conclusions about the volatility of the observed values.

Phillips et al. (2015b) proposed a more generalized version of the Supremum Augmented Dickey–Fuller (SADF) test, known as the Generalized Supremum Augmented Dickey–Fuller (GSADF) test [10]. Unlike the original SADF test, which involves fixing the starting point of the sample and progressively recursing through minimum sub-samples to the entire sample, the GSADF test allows for both the starting and ending points of the sample to be flexible. It involves recursively regressing the equation for SADF by simultaneously shifting the starting and ending points of the sample forward. Subsequently, the upper bound of the Augmented Dickey–Fuller (ADF) test is obtained based on this, followed by taking the upper bound of a series of SADF statistics.

The fundamental steps of the Generalized Supremum Augmented Dickey–Fuller (GSADF) test are as follows: first, determine the minimum sample window size k_0. Then, allow the starting point of the sub-sample k_1 and the ending point of the sub-sample k_2 to vary between $[0, k_2 - k_0]$ and $[k_0, T]$, respectively. For each sub-sample in this series, conduct an Augmented Dickey–Fuller (ADF) test to obtain a series of ADF statistics. The formula for constructing the GSADF statistic is shown below in Eq. (1).

$$GSADF(k_0) = \sup_{k_1 \in [0, k_2 - k_0]} \sup_{k_2 \in [k_0, T]} \left\{ ADF_{k1}^{k2} \right\} \quad (1)$$

The Generalized Supremum Augmented Dickey–Fuller (GSADF) test is based on regressing the same equation over a series of sub-samples of the time series data. Its null hypothesis and alternative hypothesis are identical. Therefore, the obtained statistic is compared with the critical value on the right side based on a certain significance level. If the statistic exceeds the critical value, the null hypothesis is rejected, and the alternative hypothesis is accepted: a bubble exists.

For estimating the timing of bubble onset and collapse, given the complex evolution of asset prices, Phillips et al. (2015b) represent the three stages of asset price dynamics with the following Eq. (2) [10]:

$$p_t = p_{t-1} I\{t < \tau_e\} + \rho_n p_{t-1} I\{\tau_e \ll t \ll \tau_f\} + \left(\sum_{k=\tau_f}^{t} \varepsilon_t + P_{\tau_f}^*\right) I\{t > \tau_f\} + \varepsilon_k I\{t \geq\} \varepsilon_k \sim iid(0, \sigma^2) \quad (2)$$

Among them Pn>1, $P_{\tau_f}^* = p_{\tau_e} + p^*$, p_{τ_e} represent asset prices before the formation of a bubble, $P^* = \sum_{t=1}^{\tau_f - \tau_e} \varepsilon_t$ indicates the deviation of prices from pre-bubble levels after the bubble forms, τ_f indicates the moment of bubble burst. when $t < \tau_e$, the asset price sequence p_t follows a unit root process, indicating the absence of bubbles in prices. when $\tau_e << t << \tau_f$, Pn > 1, the asset price series exhibits an explosive process. When $t > \tau_f$, the asset price series reverts to a unit root process. The BSADF statistic is calculated based on recursive selection of samples for upper-bound unit root testing. The Eq. (3) for BSADF is provided below.

$$BSADF_{k_2}(k_0) = \sup\left\{BADF_{k_1}^{k_2}\right\} \; k_1 \in [0, k_2 - k_0], k_2 \in [k_0, T] \quad (3)$$

When the statistic first exceeds its corresponding right-tailed unit root test critical value, it indicates the onset of a bubble. Subsequently, when the statistic first falls below its corresponding right-tailed unit root test critical value, it indicates the collapse of the bubble. However, it is important to note that as the recursive testing selects an increasing sample size, the sample critical values also exhibit an increasing trend. Therefore, it necessitates significant computational effort to calculate finite sample critical values for each sub-sample based on Monte Carlo simulation.

2) Machine learning approaches to forecasting price bubbles in the Chinese stock market

a) Logistic regression: Logistic regression is a statistical method used to model binary classification problems, typically employed to predict the probability of an event occurrence. In this study, we will utilize logistic regression to forecast the presence of price bubbles in the Chinese stock market. Four explanatory variables will be inputted into the model, which ultimately generates the probability of price bubble occurrences in the Chinese stock market. This probability is derived using the Eq. (4) presented below.

$$P(y=1|x)=\frac{1}{1+e^{-(\beta_0-\beta_1x_1+\beta_2x_2+\cdots+\beta_nx_n)}} \quad (4)$$

Logistic regression is generally considered a fundamental method in machine learning. This algorithm is relatively easy to understand and implement, making it accessible to a broad spectrum of users. Consequently, due to its excellent interpretability, logistic regression is frequently employed in practical applications within financial institutions.

b) Deep learning: Deep learning is typically regarded as an advanced algorithm within the realm of machine learning. It is a machine learning method based on artificial neural networks, which utilize multi-layered neural network architectures for feature learning and representation learning, thereby achieving the learning and prediction of complex data patterns. The core idea of deep learning involves gradually extracting abstract features from input data through multiple layers of non-linear transformations, enabling the solution of higher-level tasks such as image recognition, speech recognition, and natural language processing.

The advantages of deep learning algorithms lie in their powerful adaptability, capable of learning complex non-linear relationships and applicable to various types of data. They automatically learn feature representations from input data without the need for manual feature engineering. Deep learning also exhibits strong generalization capabilities, enabling learned patterns from the training set to be generalized to unseen data, thereby enhancing the reliability and stability of models in practical applications.

c) Decision tree: The decision tree algorithm is also considered a fundamental machine learning algorithm. It learns and extracts a series of decision rules based on a given dataset through a tree-like structure. This algorithm utilizes metrics such as Gini coefficient or entropy to determine the optimal allocation of each split, ensuring the maximization of purity for each split. In decision trees, decision rules are presented in a tree structure, starting from the root node and traversing through a series of internal nodes to reach the leaf nodes, where each leaf node represents a category or output result.

The advantages of the decision tree algorithm lie in its simplicity, ease of implementation, and interpretability. It also offers flexibility in data handling, hence finding wide application in many fields. However, the performance of the decision tree algorithm may be limited when dealing with complex data and high-dimensional feature spaces.

d) Support vector machine: The Support Vector Machine (SVM) algorithm is an advanced method in machine learning. It belongs to the category of supervised learning algorithms, primarily used for classification and regression analysis. The core idea of SVM is to find a hyperplane that maximizes the margin between classes, thus optimizing classification performance. Alternatively, its fundamental principle is to identify an optimal hyperplane in the feature space that maximally separates samples of different classes while maintaining the maximum margin between classes. The classification in Support Vector Machines is conducted using Eq. (5).

$$f(x)=sign(w\cdot x+b) \quad (5)$$

Where x represents the feature vector of a given new input sample, w is the normal vector to the hyperplane, b is the bias term, and sign( ) denotes the sign function. When w∗x+b is greater than 0, the result is 1, and when it is less than 0, the result is -1. Ultimately, this function result informs us about the class membership of sample x.

The advantages of Support Vector Machines (SVMs) include effective handling of small sample sizes, high-dimensional, and non-linear datasets. For high-dimensional and non-linear data, SVMs can utilize kernel functions to map low-dimensional non-linear separable problems into high-dimensional spaces for linear classification.

Popular machine learning algorithms such as logistic regression, deep learning, decision trees, and support vector machines have shown considerable promise in detecting and predicting stock price bubbles due to their ability to analyze extensive datasets, identify patterns, and adapt to new information. For instance, logistic regression can estimate the probability of a bubble by analyzing historical data. Deep learning methods are particularly effective for anomaly detection, as they learn the typical patterns in data and identify deviations that could signal bubble formation. Decision trees and random forests excel in handling non-linear relationships and interactions between features, making them proficient at recognizing conditions indicative of bubbles. Support vector machines can classify similar data points and detect outliers, which may also suggest bubble formations [21]. Together, these algorithms offer valuable insights into market dynamics and potential bubble developments.

V. Empirical Results and Discussion

A. The Results of Measuring Price Bubbles in the Chinese Stock Market using the Generalized Supremum Augmented Dickey-Fuller (GSADF) Method

In this study, we employed the Generalized Supremum Augmented Dickey-Fuller (GSADF) method to measure the presence of price bubbles in the Chinese stock market from January 2015 to December 2023. The monthly average data and the weekly average data publicly released by the Shanghai Stock Exchange served as the source of the Chinese stock market index (Shanghai Composite Index) for this research. When executing the GSADF procedure using the Eviews software, the study adhered to the program's setting specifying a minimum window of 14 observations. The measurement process commenced from January 2015.

TABLE I. STATISTICAL DATA ON THE OCCURRENCE OF PRICE BUBBLES IN THE CHINESE STOCK MARKET

Serial number	*Bubble occurrence time*	*SSECI price*	*Peak*
1	2015/01/05-2015/01/09	3258.63	0.826567
2	2015/01/12-2015/01/16	3258.21	0.8910738
3	2015/01/19-2015/01/23	3189.73	0.9233272
4	2015/01/26-2015/01/30	3347.26	0.9555806
5	2015/02/02-2015/02/06	3148.14	0.987834
6	2015/02/09-2015/02/13	3063.51	1.2599515
7	2015/02/16-2015/02/17	3206.14	1.532069
8	2015/02/23-2015/02/27	3256.48	1.8041865
9	2015/03/02-2015/03/06	3332.72	2.076304
10	2015/03/09-2015/03/13	3224.31	2.50627625
11	2015/03/16-2015/03/20	3391.16	2.9362485
12	2015/03/23-2015/03/27	3640.10	3.36622075
13	2015/03/30-2015/04/03	3710.61	3.796193
14	2015/04/06--2015/04/10	3899.42	3.6476376
15	2015/04/13--2015/04/17	4072.72	3.4990822
16	2015/04/20--2015/04/24	4301.35	3.3505268
17	2015/04/27-2015/04/30	4441.93	3.2019714
18	2015/05/04-2015/05/08	4441.34	3.053416
19	2015/05/11-2015/05/15	4231.27	2.545104
20	2015/05/18-2015/05/22	4277.90	2.036792
21	2015/05/25-2015/05/29	4660.08	1.52848
22	2015/06/01-2015/06/05	4633.10	1.020168
23	2015/06/08-2015/06/12	5045.69	0.68747
24	2015/06/15-2015/06/19	5174.42	0.354772
25	2015/06/22-2015/06/26	4471.61	0.022074

Table I presents the results of identifying price bubbles in the Chinese stock market. This table provides the time occurrence of price bubbles in the Chinese stock market, the overall market prices of the Chinese stock market (Shanghai Composite Index prices) for each period, and the peak values calculated for each bubble period. In Fig. 1, we visually illustrate the time periods during which price bubbles occurred in the Chinese stock market from January 2015 to December 2023. The blue line in the Fig. 1 represents the GSADF statistic sequence, while the orange line denotes the asymptotic critical values obtained from 2000 Monte Carlo simulations using the EViews software tool. By comparing the GSADF statistic sequence (blue line) with the 95% critical value sequence (orange line), the timing of overall market price bubbles in the Chinese stock market (represented by the Shanghai Composite Index prices) is identified. During this period, there were six months with price bubbles on a monthly basis and 25 weeks experiencing financial bubbles on a weekly basis. Notably, we observe a prolonged financial bubble in the first half of 2015. Following the identification of price bubbles in the Chinese stock market from January 2015 to December 2023, we designate months/weeks with identified occurrences of stock market price bubbles as 1, while months/weeks without price bubbles are marked as 0. This preparation aims to facilitate the subsequent creation of datasets for the four machine learning prediction stages.

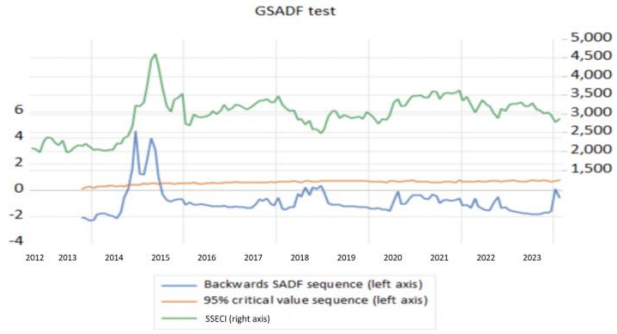


Fig. 1. Chinese Stock market price bubbles from January 2015 to December 2023.

B. The Result of Predicting the Price Bubble in the Chinese Stock Market Using Four Machine Learning Algorithms

In this study, we will employ four machine learning algorithms to predict the occurrence of price bubbles in the Chinese stock market. These four machine learning algorithms are logistic regression, deep learning, decision tree, and support vector machine.

For machine learning models, we optimize the models using the hyperparameter of Area Under the Curve (AUC). In machine learning, particularly in evaluating binary classification models, AUC typically refers to the area under the Receiver Operating Characteristic (ROC) curve. AUC quantifies the entire two-dimensional area underneath the ROC curve, providing a single measure to assess the classifier's performance across various thresholds, with values ranging between 0 and 1. A higher AUC value indicates better model performance, while an AUC value closer to 0.5 suggests performance closer to random guessing. Throughout this process, various hyperparameter values are experimented with to enhance the model. Post-training, AUC is computed using the test dataset. The hyperparameter combination resulting in the highest AUC is designated as optimal. This approach ensures the selection of hyperparameters based on the model's classification performance, with AUC serving as the key metric.

The following Table II presents the performance of the four machine learning algorithm models utilized in our study.

TABLE II. THE PERFORMANCE RESULTS OF THE FOUR MACHINE LEARNING ALGORITHM MODELS

Algorithm	*AUC*	*F Measure*	*Accuracy*	*Precision*	*Sensitivity*
Logistic Regression	1	86.7%	98.5%	90.0%	90.0%
Deep Learning	1	79.3%	96.3%	70.0%	100.0%
Decision Tree	0.992	80.0%	97.8%	90.0%	80.0%
Support Vector Machine	0.558	Not Available	94.8%	Not Available	0.0%

From Table II, we observe that the performance of the logistic regression model surpasses that of other algorithms in terms of AUC, F-measure, accuracy, and precision. The logistic regression model achieves an AUC of 1, an F-measure of 86.7%, accuracy of 98.5%, and precision of 90.0%, all of which are the highest among all algorithms. This indicates its capability to accurately classify the presence of bubbles in the Chinese stock market. However, in terms of sensitivity, the logistic regression model exhibits a lower value compared to the deep learning model, at 90.0%, suggesting a relatively weaker ability of the logistic regression model to correctly identify positive instances. This outcome suggests that while the logistic regression model demonstrates excellent performance in predicting instances of stock market bubbles in China, it may lack flexibility in handling certain types of data and feature representations, leading to relatively lower performance in identifying positive instances.

Furthermore, the deep learning model exhibits perfect performance in terms of AUC and sensitivity, with values of 1 (100.0%), indicating that the model can perfectly distinguish between positive and negative instances at all possible thresholds, without any misclassifications. It can perfectly identify all positive instances without missing any. However, the results for F-measure (79.3%), accuracy (96.3%), and precision (70.0%) suggest that the deep learning model, in predicting the occurrence of bubbles in the Chinese stock market, strikes a compromise between precision and recall, resulting in a certain number of misclassifications overall, with a higher rate of false positives when predicting positive instances. In contrast, the decision tree algorithm performs moderately across all aspects and can serve as a baseline for evaluating the performance of these four machine learning models. Meanwhile, the support vector machine model either performs the worst in all aspects or yields results that are not available, indicating its unsuitability for predicting the occurrence of bubbles in the Chinese stock market.

Solely based on the AUC scores of model performance, we observe that within the machine learning algorithms utilized, both the logistic regression model and the deep learning model achieved perfect scores of 1. This score signifies their ability to maintain a low false positive rate while achieving a high true positive rate. Essentially, this value indicates their proficiency in distinguishing periods of stock market bubbles from those without. However, upon considering the other four performance metrics, overall, the logistic regression model outperforms. Solely based on AUC scores, the other two models — the decision tree model and the support vector machine model — exhibit relatively lower scores. While the decision tree model's score (0.992) demonstrates some competitiveness, the score of the support vector machine model (0.558) indicates relatively poor performance in classification tasks, akin to random guessing. Although the latter two models — the decision tree model and the support vector machine model — may offer some insights, their performance in analyzing the occurrence of stock market bubbles in China lags behind that of logistic regression and deep learning.

Based on the above results, we compared the outcomes of four machine learning methods. These four machine learning algorithms are commonly employed approaches for addressing classification problems in finance. Logistic regression and decision tree are considered fundamental machine learning methods, while deep learning and support vector machine are classified as advanced machine learning methods. The findings indicate that the fundamental machine learning methods (logistic regression and decision tree) outperform the advanced machine learning methods (deep learning and support vector machine) in terms of F-measure, accuracy, and precision. Overall, this suggests that in the specific domain of predicting stock market price bubbles in China, simple fundamental machine learning methods may be more suitable, and there may be no need to blindly pursue complex advanced algorithms, as doing so may yield counterproductive outcomes.

Our research findings differ from Başoğlu Kabran and Ünlü (2021), who utilized machine learning methods to predict the S&P 500 index and concluded that SVM was the best approach [12]. There are two reasons for these discrepancies. First, differences exist in the explanatory variables selected for the input models. Second, variations in the sizes of the datasets utilized by both studies contribute to these disparities. However, it is noteworthy that our study is the first to employ a comparative approach involving multiple machine learning methods to forecast market bubbles in China, the second-largest economy globally. Moving forward, we plan to conduct broader empirical research within the Chinese market context.

Our research results differ from those of Tran et al. (2023), who applied machine learning methods to predict the Vietnamese stock market from 2001 to 2021, concluding that random forest and artificial neural network algorithms outperformed traditional statistical methods in forecasting financial bubbles in the Vietnamese stock market [13]. There are three main reasons for these discrepancies. Firstly, differences exist in the explanatory variables selected as inputs to the models. Secondly, disparities in the time periods of the datasets used in both studies contribute to the variations observed. Lastly, discrepancies arise from the distinct machine learning methods employed in each study. In contrast, our study represents the first comprehensive application of multiple machine learning methods to predict stock market bubbles in China, the world's second-largest economy. Looking ahead, we plan to conduct broader empirical research in diverse market contexts and with a wider array of machine learning methodologies.

C. Robustness Test

In order to ensure the accuracy and reliability of the machine learning models obtained, we conducted robustness tests on them. For this purpose, we divided the data into two equal parts, the first part covering the period from January 2015 to December 2018, and the second part covering the period from January 2020 to December 2023. The main reason for this division is that in January 2020, the Chinese government officially announced the emergence of the COVID-19 pandemic in China and implemented nationwide controls [16]. We utilized the two best-performing machine learning models, namely the logistic regression model and the Deep Learning model, to predict the occurrence of stock market price bubbles during these two data set periods.

Subsequently, we trained and tested the models within their respective data sets. Afterwards, we evaluated the performance of the obtained models using relevant metrics, including accuracy, AUC, and sensitivity. Finally, we analyzed the results of the robustness tests conducted for each time period to compare the performance of the models in different time periods.

From Table III, we can observe that the accuracy of both models remains stable across the two time periods, with the logistic regression model averaging 94.05% and the deep learning model averaging 97.75%. Regarding the AUC, both logistic regression and deep learning models maintain stability across the two time periods, with average values of 0.978 and 1, respectively. However, we note a sensitivity decline in the logistic regression model towards the dataset, particularly during the period from January 2020 to December 2023. In contrast, the deep learning model demonstrates more consistent performance in sensitivity. Overall, both the logistic regression and deep learning models exhibit robustness.

TABLE III. THE ROBUSTNESS TEST RESULT

	Logistic regression			***Deep learning***		
	January 2015 - December 2018	***January 2020 - December 2023***	***Average***	***January 2015 - December 2018***	***January 2020 - December 2023***	***Average***
Accuracy	93.3%	94.8%	94.05%	100.0%	95.5%	97.75%
AUC	1	0.956	0.978	1	1	1
Sensitivity	100.0%	90%	95%	100.0%	100.0%	100.0%

The stability testing method employed in this study ensures the reliability of the predictive models for detecting stock market price bubbles in China, allowing for a clear understanding of variations in model performance over time. This facilitates making practical decisions in real-world financial applications.

Logistic regression is ideally suited for binary outcomes, making it an excellent option for identifying the presence or absence of a bubble. Given the small size of the dataset, deep learning models tend to underperform relative to logistic regression. However, it's important to note that larger datasets come with their own set of challenges.

D. Summary of discussion

Stock price bubbles prediction applying advanced machine learning techniques is potentially extends existing financial theories. It offers empirical evidence that can either support or challenge traditional models of bubble formation and economic cycles. The adaptability and continuous learning capability of machine learning models underscore the dynamic nature of financial bubbles and economic cycles.

The explanatory variables we employed include the inflation rate from macroeconomic factors (IR), the consumer confidence index from sentiment factors (CCI), the stock yield (SY), and price-earnings ratio from market factors (RET).

Table IV displays the relative importance of different attributes (variables) in predicting an outcome, likely in a logistic regression model. The inflation rate from macroeconomic factors (IR) has the highest weight, indicating it is the most important predictor in the model. Its relative importance value of 0.539 suggests it contributes significantly more to the prediction compared to the other attributes. The consumer confidence index from sentiment factors (CCI) attribute is the second most important predictor. Its weight of 0.154 indicates that while it is less influential than IR, it still plays a substantial role in the model. The stock yield (SY) attribute has a weight of 0.116, making it the third most important predictor. Its contribution is notable but less significant compared to IR and CCI. The price-earnings ratio from market factors (RET) attribute has the smallest weight of 0.018, indicating it has the least influence on the prediction. Its relative importance is minimal compared to the other attributes. The model relies heavily on the IR attribute for its predictions, which means understanding and accurately measuring this variable is critical. While CCI and SY are important, their contributions are secondary. Adjustments or improvements in measuring these variables could still enhance model performance.

TABLE IV. THE RELATIVE VARIABLE IMPORTANCE VALUES IN THE CHINESE STOCK MARKET (SHANGHAI COMPOSITE INDEX)

Variable	***Weights (Importance Value)***
inflation rate(IR)	0.539
consumer confidence index(CCI)	0.154
stock yield (SY)	0.116
price-earnings ratio (RET)	0.018

VI. CONCLUSIONS

In this study, we employed the widely acknowledged Generalized Supremum Augmented Dickey-Fuller (GSADF) method to identify the presence of price bubbles in the stock market and utilized data spanning from January 2015 to December 2023 to forecast the occurrence of price bubbles in the Chinese stock market. The findings reveal that a price bubble occurred in the Chinese stock market during the first half of 2015, before COVID-19, while no financial bubbles were observed at other times. Among the predictive models, the logistic regression model demonstrated the best performance with an F-measure score of 86.7%, followed by the deep learning model and the decision tree model, which exhibited slightly inferior yet respectable performance, with F-measure scores of 79.3% and 80.0%, respectively. From a practical standpoint, these results furnish valuable machine learning models for real-time detection and prediction of stock market price bubbles, thereby enabling governmental decision-makers, regulatory authorities, and market oversight agencies to formulate and implement corresponding economic policies aimed at mitigating the adverse effects stemming from financial bubbles. From a theoretical perspective, the utilization of diverse machine learning algorithms in predicting

financial bubbles in this study holds significant reference and generalization implications for the application of machine learning techniques in financial market research. Moreover, the macroeconomic factor (inflation rate), investor sentiment factor (consumer confidence index), and market factors (stock yield and price-earnings ratio) into the machine learning prediction models enables us to delve further into the complex mechanisms underlying the emergence of financial market bubbles and advance the predictive understanding of such phenomena.

This study has made significant contributions both theoretically and practically, particularly in utilizing machine learning, a novel tool, to forecast price bubbles in the stock market of China that is the world's second-largest economy, providing empirical evidence.The research findings highlight the suitability of the foundational algorithm in machine learning, the logistic regression model, for predicting price bubbles in the Chinese stock market. Nevertheless, other machine learning algorithms such as deep learning and decision tree algorithms also exhibit potential in the domain of financial bubble prediction.This study highlights to policymakers and regulators the significance of promptly enacting policies to reduce both the probability and ramifications of financial bubbles.For central banks and regulatory bodies, utilizing advanced machine learning tools to measure financial bubbles facilitates the formulation of appropriate monetary policies to regulate capital behavior in the economy, thereby reducing speculative activities in financial asset trading and stabilizing the entire financial system.For investors, based on the insights gleaned from this study, they can more effectively allocate their investment portfolios by leveraging machine learning algorithms ability to predict financial price bubbles, deciding opportune moments for long and short positions. Moreover, during market bubble occurrences, i.e., when market prices are excessively high, investors can seize suitable opportunities to sell assets and generate corresponding profits.

In subsequent research, other scholars can utilize the machine learning methods employed in this study to forecast bubble situations in varying locales markets, such as Hong Kong, Singapore, the United States, and others. These machine learning methods can likewise be harnessed to anticipate bubbles across diverse market categories, including but not limited to the real estate market, cryptocurrency market, etc. Furthermore, analysis can be conducted on the interplay of financial bubbles between dissimilar markets, such as the stock market and real estate market, both of which hold significant economic sway. Understanding these dynamics can enable regulatory authorities to implement effective financial policies, thereby preventing the formation of financial bubbles or controlling their occurrence, ultimately fostering a healthy and robust market investment environment. This study utilized a limited number of machine learning models, which may have resulted in certain limitations in the obtained results. In the future, employing a wider variety of machine learning models can further advance research in the prediction of stock market bubbles. In addition, speculative bubbles across different markets exhibit both common characteristics and distinct features and impacts. Investigating the relationships between speculative bubbles in various markets and understanding the mechanisms of bubble transmission to develop more effective regulatory strategies presents a significant challenge for future research. Furthermore, addressing the issue of insufficient datasets is a critical concern that needs to be prioritized.

ACKNOWLEDGMENT

This article is part of the Doctor of Philosophy in Digital Transformation and Business Innovation program at the Chakrabongse Bhuvanarth International Institute for Interdisciplinary Studies (CBIS) at Rajamangala University of Technology Tawan-ok in Thailand. The researchers would like to thank all the cited experts and reviewers involved in this study.Yunxi Wang, the author of this article,would like to express special gratitude to her PhD advisor-- Tongjai Yampaka, for the assistance and support provided during her studies.

REFERENCES

[1] Xiong W., Yu J. L. 2011. The Chinese warrants bubble. American Economic Review 101(6), 2723–2753.

[2] Miao J. J., Wang P. F. 2018. Asset bubbles and credit constraints. American Economic Review, 108(9), 2590–2628.

[3] Galbraith, James K., Sara Hsu, and Wenjie Zhang. 2009. Beijing bubble, Beijing bust: Inequality, trade, and capital inflow into China. Journal of Current Chinese Affairs 38: 3–26.

[4] National Bureau of Statistics. 2024. China economic annual report 2023. China: National Bureau of Statistics.

[5] Dickey D. A., Fuller W. A. 1979. Distribution of the estimators for autoregressive time series with a unit root. Journal of the American Statistical Association 74(366a), 427-431.

[6] Wang Y., Wu C. 2020. Testing for bubbles in Chinese stock market: A study based on ADF test. International Journal of Finance & Economics 25(4), 530-544.

[7] Cheung Y. W., Lai K. S. 1995. Lag order and critical values of the augmented Dickey-Fuller test. Journal of Business & Economic Statistics 13(3), 277-280.

[8] Homm, Ulrich, and Jörg Breitung. 2012. Testing for speculative bubbles in stock markets: A comparison of alternative methods. Journal of Financial Econometrics 10: 198–231.

[9] Phillips, Peter C. B., Yangru Wu, and Jun Yu. 2011. Explosive behavior in the 1990s Nasdaq: When did exuberance escalate asset values? International Economic Review 52: 201–26.

[10] Phillips, Peter C. B., Shuping Shi, and Jun Yu. 2015b. Testing for multiple bubbles: Historical episodes of exuberance and collapse in the S&P 500. International Economic Review 56: 1043–78.

[11] Ouyang, Zi-sheng, and Yongzeng Lai. 2021. Systemic financial risk early warning of financial market in China using Attention-LSTM model. The North American Journal of Economics and Finance 56: 101383.

[12] Başoğlu Kabran, Fatma, and Kamil Demirberk Ünlü. 2021. A two-step machine learning approach to predict S&P 500 bubbles. Journal of Applied Statistics 48, 2776–2794.

[13] Tran K.L., Le H.A., Lieu C.P., and Nguyen D.T. 2023. Machine Learning to Forecast Financial Bubbles in Stock Markets: Evidence from Vietnam. International Journal of Financial Studies 11(4), 133.

[14] Gu, Shihao, Bryan Kelly, and Dacheng Xiu. 2020. Empirical asset pricing via machine learning. The Review of Financial Studies 33: 2223–73.

[15] Zhou, Xianzheng, Hui Zhou, and Huaigang Long. 2023. Forecasting the equity premium: Do deep neural network models work? Modern Finance 1: 1–11.

[16] Sweeny K., Rankin K., Cheng X., Hou L., Long F., Meng Y., ... and Zhang W. 2020. Flow in the time of COVID-19: Findings from China. PloS One 15(11), e0242043.

[17] Li X., Wang Z. 2021. Challenges and solutions in financial market labeling and classification. Journal of Financial Data Science 3(4), 47-59.

[18] John G. H., Langley P. 1995. Performance measures for classification problems. Machine Learning 33(1), 103-139.

[19] Shimizu R., Weber E. 2020. Identifying Asset Price Bubbles Using the Generalized Supremum Augmented Dickey-Fuller Test. Journal of Financial Econometrics 18(4), 679-707.

[20] Hansen B. E. 1999. Threshold effects in non-dynamic panels: Estimation, testing, and inference. Journal of Econometrics 93(2), 345-368.

[21] Krauss C., Do X., Huck N. 2017. Deep neural networks for financial prediction: A comparison of deep learning approaches. European Journal of Operational Research 256(1), 185-200.

Multi-Factor Risk Assessment and Route Optimization for Safe Human Travel

Thilagavathi T[1], Subashini A[2]
Research Scholar, Department of Computer and Information Science, Annamalai University, Annamalai Nagar, Tamil Nadu, India[1]
Assistant Professor, Department of Computer Application, Government Arts College, Chidambaram, Tamil Nadu, India[2]

***Abstract*—In the modern world, frequent travel has become a necessity, with vehicles being the primary mode of transportation. Ensuring human safety while traveling is paramount. To address this, it is essential to adopt a combination of numerous static and dynamic parameters to achieve optimal route design in today's complex transportation systems. This study introduces a methodology titled 'Multi-Factor Risk Assessment and Route Optimization for Safe Human Travel', which consists of three stages: Route Optimization, Risk Factor Analysis, and Data Collection. To assess the safety of various routes, a combination of dynamic and static factors is considered. These include traffic, weather, and road conditions, as well as vehicle-related factors such as type, age, and the surrounding road environment. By analyzing simulated data, the technique identifies potential risks and optimizes travel paths accordingly. For segmented routes, risk factors are calculated using both static and dynamic parameters, ensuring a comprehensive safety assessment. Prioritizing user safety, the system dynamically adjusts routes to offer the most cost-effective and safest travel options. This study lays a robust foundation for intelligent transportation systems, aimed at ensuring safer travel for users across a range of scenarios.**

Keywords*—Multi-factor risk assessment; route optimization; human travel safety; static and dynamic parameters; risk factor analysis

I. Introduction

Travel safety is a key issue in transportation, particularly as the number of vehicles and the complexity of urban environments increase. The focus in traditional route planning is on reducing travel time or distance, but it frequently ignores important safety considerations, leaving travelers exposed to dangers like accidents, injuries, and crime [1]. These shortcomings highlight the necessity for more holistic methods that place safety on par with efficiency when optimizing routes [2].

This paper addresses these challenges by presenting a novel approach that integrates multiple safety parameters for risk assessment in route optimization. As urbanization and population growth continue, the need for safe, reliable transportation systems is increasingly critical. Recent advancements in risk assessment and route optimization, particularly in dynamic road conditions, are essential for improving the safety of drivers and pedestrians alike [3].

The motivation for this study arises from the pressing need to address the limitations of traditional navigation systems, which often neglect crucial safety factors. The proposed approach leverages a combination of static and dynamic parameters to offer a more comprehensive and adaptive framework for route optimization. By incorporating factors such as traffic density, weather conditions, road environments, and vehicle attributes, the system ensures a holistic evaluation of travel risks. This methodology aims to enhance traveler safety by reducing the likelihood of accidents, fostering user confidence, and supporting the development of intelligent transportation systems.

The primary contribution of this study is the development of a multi-factor risk assessment and route optimization model that dynamically evaluates routes based on safety and efficiency. By tailoring recommendations to different demographics, transportation modes, and real-time conditions, this approach ensures inclusivity and adaptability in route planning. Furthermore, the integration of real-time data enhances the system's ability to adjust dynamically to changing conditions, paving the way for safer and more intelligent transportation networks.

This approach moves beyond conventional navigation by incorporating real-time data and multi-factor analysis to prioritize safety and reduce hazards. Traditional systems that focus primarily on travel time and distance have often overlooked important factors influencing safety and fail to account for the ever-changing road environments and the varying needs of travelers. Multi-Factor risk assessment models now address a broad range of considerations, including time of travel, traffic density, vehicle types, demographics, road conditions, lighting, and traffic patterns [4]. This complete approach optimizes routes not only for efficiency but also for the specific safety needs of different individuals and communities, improving overall travel safety.

Multi-Factor models recognize that higher traffic density, particularly during peak hours, can enhance safety by providing more visibility and reducing risks such as theft or harassment [5]. By incorporating time-sensitive routing that considers traffic density, users can opt for routes that may take longer but offer greater safety.

Optimal routes vary significantly for pedestrians, cyclists, motorcyclists, and those using private or rented vehicles. By tailoring recommendations based on the mode of transport, the system ensures that each user's safety is prioritized.

Demographics and traveler population also play a crucial role in multi- Factor risk assessment. Routes are adapted to reflect the age, gender, and travel patterns of users, fostering safer travel for all.

The use of real-time data enables systems to adjust routes based on current weather, road maintenance, and the availability of lighting, offering a dynamic and comprehensive approach to safer travel. By incorporating these elements into the routing process, multi-Factor models provide a comprehensive approach to safe navigation, addressing the full spectrum of risks that travelers may encounter.

This paper outlines the development and application of multi-factor risk assessment and route optimization models. These models represent a significant advancement in ensuring safer travel for all, paving the way for a future where transportation systems are as safe as they are efficient. The paper is structured as follows: Section II presents the literature review, Section III covers the methodology, Section IV provides the implementation, Section V presents the results and discussion, and Section VI provides the conclusion.

II. Literature Review

Safe human route optimization has emerged as a critical area of research due to the growing need for enhancing road safety, crime activities and minimizing accident risks. A wide range of models and methodologies have been developed, incorporating factors such as road conditions, weather, traffic, and human demographics to provide tailored, safer route options. This literature review explores various strategies and models proposed for optimizing safe travel routes, focusing on both static and dynamic risk factors to ensure safer navigation.

Lingamaneni Indraja et al. [6] examined the correlation between accidents, road conditions, and weather, developing a predictive model using machine learning algorithms like Support Vector Machines and Logistic Regression to identify safe, less accident-prone routes. Yash S. Asawa et al. [7] introduced a User-Specific Safe Route Recommendation System that visually represents safe routes on maps using historical crime data. It operates in two tiers: a Decision Network to capture user-specific features and Geospatial Data Analysis to generate personalized safe routes.

Aruna Pavate et al. [8] developed a system using K-means clustering to categorize routes into security levels, helping women avoid high-crime areas. Isha Puthige et al. [9] devised a danger index based on multiple crime factors at specific locations, using clustering algorithms to identify safe paths. Aliasgar Eranpurwala et al. [10] created the "GoWomaniya" app to help women find safe routes in real-time during moments of distress, leveraging mobile technology.

Deepa Bura et al. [11] developed a model using Google Maps to assess the safety of routes, considering risk factors like security and path quality. Roxan Salehab et al. [12] applied supervised machine learning to predict road sign status in Sweden, contributing to transportation safety by maintaining accurate navigation aids. Deepak Kumar Sharma et al. [13] utilized Random Forest algorithms to predict crash risks based on historical accident data, including weather and road conditions.

Juncai Jiang et al. [14] proposed a framework for assessing urban road collapse risks, using SMOTE and Convolutional Neural Networks to predict road integrity. Mukherjee, D et al. [15] combined historical crash data with proactive pedestrian-vehicular risk assessments to identify and rank high-risk intersections in Kolkata, enhancing pedestrian safety.

Lakshmi et al. [16] conducted a systematic review of Safe Route Guidance Systems, focusing on traffic forecasting, congestion avoidance, and traffic signaling. Llopis-Castelló et al. [17] compared the Highway Safety Manual with geometric design consistency to estimate crash occurrences on road segments in North Carolina.

Al-Bdairi et al. [18] investigated injury severity in weather-related crashes, identifying factors like time of day, driver fatigue, and lack of streetlights that increase accident risks. Qiannan Wang et al. [19] explored how population density impacts autonomous vehicle navigation risks, emphasizing the need for risk-aware path planning. Changhong Zhou et al. [20] developed a road disaster risk assessment model using neural networks and a fuzzy comprehensive evaluation, incorporating environmental and geological factors to predict road disasters.

Nishat Tasnim et al. [21] studied how road geometry, traffic volume, and other features influence accident occurrence. Shan Jiang et al. [22] introduced the Safe Route Mapping (SRM) model, combining crash estimates and conflict risks from driver data to predict route safety. Paul Litzinger et al. [23] proposed an algorithm that incorporates real-time weather forecasts into route planning to enhance safety and efficiency.

Nikhitha Pulmamidi et al. [24] proposed a model for identifying safe routes based on user experience, considering factors like road conditions, weather, and accident frequency. Krishnaraj Pawooskar et al. [25] developed a safety score based on features like hospitals, streetlights, and police stations along routes. Helai Huang et al. [26] emphasized the importance of dynamic traffic conditions and stationary road factors in conflict-based travel route safety assessments. The Road Safety Technical Report [27] highlighted the need for tailored safety solutions based on specific road and traffic conditions.

The reviewed studies demonstrate the importance of integrating diverse factors such as road geometry, weather conditions, and user demographics in optimizing safe routes. Collectively, these efforts contribute to a more complete understanding of route safety optimization, paving the way for smarter, more responsive systems that enhance safety, awareness, and efficiency for all road users.

However, most of these studies focus on single factors or use simplistic models that do not account for the complex interactions between different parameters. This study aims to develop a multi-factor risk assessment model that evaluates the safety of travel routes by considering both static and dynamic factors. The model will use the driven data to classify routes based on their risk levels and identify the safest route between a given source and destination.

III. Methodology

The proposed methodology for "Multi-Factor Risk Assessment and Route Optimization for Safe Human Travel" is

designed to address the complexities of modern transportation systems by integrating multiple static and dynamic factors. This approach prioritizes safety, aiming to create a transportation landscape that not only optimizes route efficiency but also enhances the well-being and safety of all users.

The system is divided into three major phases: Data Collection, Risk Factor Analysis, and Route Optimization as shown in Fig. 1. These phases work together find best route based on static and real-time data (dynamic data).

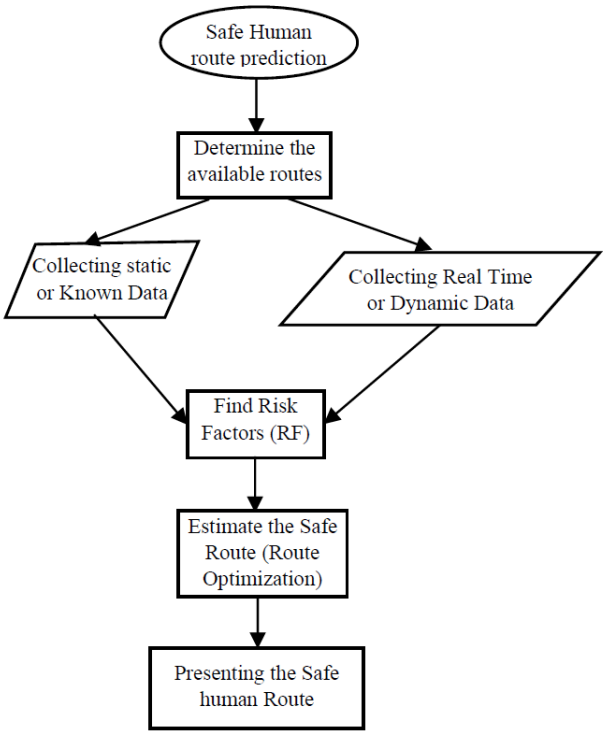


Fig. 1. Phases of route optimization.

A. Data Collection

In the context of Multi-Factor Risk Assessment and Route Optimization for Safe and Efficient Human Travel, the methodology involves a detailed analysis and integration of both static and dynamic parameters as shown in Table I. These parameters are essential for evaluating the safety of various routes and optimizing them to ensure secure travel.

The system accounts for 10 static parameters to ensure route safety. First, the type of vehicle or transport mode is crucial, as different vehicles have distinct requirements for road width, speed limits, and flexibility. Gender-specific concerns are also considered, particularly to avoid areas prone to harassment or crime, especially at certain times of the day. Age is a key factor, influencing mobility and vulnerability; routes safer and more accessible for children, the elderly, and people with mobility challenges are prioritized. For solo travelers, the system suggests safer or more populated routes by factoring in the number of travelers.

TABLE I. LIST OF STATIC AND DYNAMIC PARAMETERS USED

Name of the Parameter	Symbolic Representation
Static Parameters	
Vehicle Type / Transport mode	v
Gender	g
Age	a
Number of Persons travelling	n
Lighting facility	L
Road types	R_t
Public spaces existence	P_s
Road Environment	R_e
Road Complexity	R_x
Availability of CCTV	C
Dynamic Parameters	
Traffic condition	T_c
Weather condition	W_c
Road Conditions	R_c
Time	t

Lighting facilities are critical for night-time safety, so the system prioritizes well-lit routes in the evening and at night. Road type is also considered, as different types offer varying safety levels. Public spaces, such as parks, malls, and police stations, are seen as beneficial, so routes near these areas are preferred. The surrounding environment is evaluated to avoid potentially hazardous zones like forest areas. Road complexity is another factor, with simpler routes being recommended over those with more curves.

Dynamic parameters are also integrated for real-time optimization. Traffic conditions are monitored in real-time to meet the safe condition when mode population density, reducing accident risks and improving travel efficiency. Weather conditions, such as rain, snow, and fog, are tracked, and the system adjusts to avoid dangerous routes during adverse weather. Road conditions, including potholes, construction, and surface quality, are factored in to steer travelers away from hazardous areas. Time of day is another key factor, as poorly lit or high-accident areas are avoided during late hours.

The methodology for multi-factor risk assessment and route optimization begins with data collection. For the data simulation, the available routes between source and destination need to be identified. After the routes are identified, the route may be divided into partitions. A partition refers to a section of the route with a different road type. For example, the entire route section may consist of rural village roads, state highways, or national high ways. Before set the values to static and dynamic parameters, each route is divided into 100-m segments.

The static and dynamic parameter values for each segment are simulated using a randomizer function in Python. To generate random values with the randomizer function, we initialize the static parameter value, such as road type. Based on the road type, the randomizer uses a uniform distribution to set the values for public space existence, road environment, and road complexity for the chosen percentage (minimum and maximum). The dynamic parameters are generated using a normal distribution with the chosen percentage (minimum and maximum) based on the road type and public space existence.

The algorithm for the randomizer function is provided in Algorithm 1:

Algorithm 1: Randomizer Function (generate values)

```
Segment the selected route;
Initialize the road type of each segment;
For all road segments () do
    For parameters (Ps, Re, Rx, C, Tc, Wc, Rc) do
        if parameter_type is "static" then
            Generate a value using a uniform distribution within
            the range [min_value, max_value]
        else if parameter_type is "dynamic" then
            Generate a value using a normal distribution within
            the range [min_value, max_value]
        End
        Return generated value for the parameter
    End
End
```

B. Parameter Value Fixation

We identified 14 key parameters that significantly impact travel safety. Each parameter is symbolically represented and assigned a value between 0 and 1, indicating its influence on the overall risk factor. The value fixations on parameters are given as follows:

1) Vehicle type / transport mode (v): Different types of vehicles have varying levels of stability, speed, and safety features, which influence their risk factor. For example, two-wheelers are generally considered more vulnerable than cars or vans, hence assigned a higher risk value (0.7 for two-wheelers, 0.5 for cars, and 0.3 for vans).

2) Gender (g): Research indicates that gender can impact travel behavior and risk perception. Male travelers are feeling safer and ready to face risk than Female travelers. Hence the value is fixed as 0.9 for female and 0.6 for males. The average gender risk factor is calculated based on the average risk factor of all persons travelling.

3) Age (a): Age influences factors such as reflexes, experience, and risk-facing tendencies. Younger travelers (aged 0-15 years) have a higher risk value (0.9) due to inexperience. Travelers aged 15-30 years are assigned a risk value of 0.5. Those aged 30-45 years are considered the safest, with a lower risk value of 0.2. Travelers aged 46-60 years have a risk value of 0.3, while those over 60 years are considered to have moderate risk, with a value of 0.5. The average age risk factor is calculated based on the number of persons traveling.

4) Number of persons traveling (n): The risk value for traveling decreases as the group size increases, with a risk value of 0.8 for solo travelers, 0.5 for two persons, 0.3 for groups of 3-5, and the lowest risk value of 0.1 for groups larger than five.

5) Lighting facility (L): Adequate lighting reduces the risk of accidents, robberies and other criminal activities. Segments with no artificial lighting are assigned the highest risk value (1), while light-facilitated segments have a value of 0. During the day, the value is set to 0 since there is no need of artificial light. At night, the value is also set to 0 if adequate lighting exists; otherwise, it is set to 1. This parameter is also depending on the public space existence and road types.

6) Road types (Rt): The risk values for different road types decrease with increasing road capacity, with rural roads having a risk value of 0.8, state highways (SH) at 0.6, two-way national highways (NH) at 0.5, four-way NH at 0.4, six-way NH at 0.3, and eight-way NH at 0.2.

7) Public spaces existence (Ps): The presence of public spaces such as parks, shopping areas, villages, and towns impacts the risk value. A value of 1 assigned if no public spaces exist, indicating higher risk, and a value of 0 if public spaces are present, indicating lower risk.

8) Road environment (Re): The risk values for different road environments vary, segments with villages having a risk value of 0.45, towns at 0.4, and metro areas being the safest at 0.2. More hazardous environments include forests segments with a risk value of 0.7, hilly region segments at 0.9, and plain region segments at 0.5.

9) Road complexity (Rx): The risk values for road complexity decrease as the curve angle increases. Segments with curves between 10°-30° have the highest risk value of 0.9, while curves between 30°-50° have a risk of 0.8, and curves from 50°-70° have a risk of 0.7. For more moderate curves, values range from 0.5 for 70°-100°, 0.4 for 100°-140°, 0.3 for 140°-160°, and the lowest risk of 0.1 is assigned to curves between 160°-180° (straight roads).

10)Availability of CCTV (C): The availability of CCTV significantly enhances safety, with segments equipped with cameras having a risk value of 0, indicating lower risk, while segments without CCTV have a higher risk value of 1, reflecting increased safety concerns.

11)Traffic condition (Tc): The traffic conditions make significate effect on the risk factors. Red, indicating a higher presence of people, is the safest with a risk value of 0.3. Orange represents a moderate risk with a value of 0.6, while blue, signifying fewer co-travelers, is the most hazardous with a risk value of 0.8.

12)Weather condition (Wc): Weather conditions significantly affect route safety, with accidents more likely in adverse conditions. Rainy weather has the highest risk value at 0.8, followed by foggy conditions at 0.7. Cloudy weather presents a moderate risk with a value of 0.5, while sunny weather offers the safest conditions with the lowest risk value of 0.3.

13)Road conditions (Rc): Poor road conditions, characterized by ridges and troughs, increase the risk of accidents (value 0.8), whereas plain roads are safer (value 0.2). These values are fixed for each segment on the route.

14)Time (t): Risk values vary throughout the day, with early morning presenting the highest risk at 0.9 due to factors like reduced visibility and increased fatigue. Morning conditions have a risk value of 0.5, while the risk decreases to 0.4 in the afternoon. Evening and midnight have similar risk values of 0.3 and 0.7 respectively, reflecting different factors such as changing light conditions and reduced alertness.

C. Finding Risk Factors

Finding the risk factors for safe human routing involves analysing a combination of static and dynamic parameters to identify potential hazards and vulnerabilities in a given route. The risk factors are identified for the available routes from the source to the destination. The detailed calculation is provided in the implantation section 4.A.

D. Route Optimization

Finally, the safe route is identified using the risk factors calculated for all routes. The safe route measurement and explanation is provided in Section IV(B) This approach ensures that the routing system enhances safety for all users under a variety of conditions.

IV. Implementation

The safety of a travel route is influenced by various factors, which can be broadly categorized into static and dynamic parameters. Static parameters are those that do not change frequently and include factors such as the type of vehicle, the travelers age, and the road environment. Dynamic parameters, on the other hand, are subject to change over time and include traffic conditions, weather, and road conditions.

A. Risk Factor Calculation

For every source and destination pair, multiple routes can typically be identified, each offering a different path between the two points. These routes are referred to as R_j, where $1 \leq j \leq m$, with m representing the total number of possible routes.

To ensure safety and optimize the selection process, it is essential to calculate the risk factor associated with each possible route. As said in Section III(A), each route R_j is divided into smaller, manageable segments of 100 meters, denoted as S_i. Segmenting the route in this way allows for a detailed and accurate analysis of the risk factors associated with each segment of the journey.

The risk factor for each segment, S_i, is determined by analyzing a combination of static and dynamic parameters. The Static Risk Factor (S_{RFi}) for ith segment is calculated as the average value of ten specific static parameters.

$$S_{RF_i} = \frac{v+g+a+n+L+R_t+P_s+R_e+R_x+C}{10} \quad (1)$$

The Dynamic Risk Factor (D_{RFi}) for each segment S_i is calculated by considering four key parameters that reflect the changing conditions such as traffic, weather, road condition and time of travel of the route.

$$D_{RF_i} = \frac{T_c+W_C+R_c+t}{4} \quad (2)$$

Hence, the Risk Factor (RF_i) of the i^{th} segment is determined by averaging both the Static Risk Factor (S_{RFi}) and the Dynamic Risk Factor (D_{RFi}).

$$RF_i = \frac{S_{RF_i}+D_{RF_i}}{2} \quad (3)$$

This approach ensures that the RF_i reflects a complete assessment of the segment's safety, taking into account both the constant, essential risks associated with static parameters and the fluctuating risks introduced by dynamic conditions. By calculating the RF_i for each segment, the overall safety of the route can be accurately evaluated by summing all segments' risk factors as follows:

$$R_j = \frac{\sum_{i=1}^{N} RF_i}{N} \quad (4)$$

The risk factor for the j^{th} route from the source to the destination is denoted as R_j. This factor represents the level of risk associated with that specific route, considering static and dynamic factors. By quantifying R_j, the overall safety of each route can be assessed, which is crucial for optimizing travel and minimizing potential risks during journey.

B. Route Optimization

The safest route (SR) is determined by evaluating the risk factors associated with all identified routes. By analyzing the calculated risk factors, the route with the lowest risk is identified as the safest. This process involves comparing each route's risk factor to ascertain which one presents the least potential for danger, thereby ensuring the most secure travel option.

$$SR = min(R_j) \quad \text{where } 1<j<m \quad (5)$$

The implementation of this approach is designed to identify the safest route by thoroughly evaluating all relevant parameters from the available routes. By integrating both static and dynamic factors, such as vehicle type, road conditions, lighting, real-time traffic, and weather, the system ensures that each route recommendation prioritizes safety. This methodology not only identifies the safest possible routes but also encourages travelers to follow to these recommendations, thereby enhancing overall travel security and reducing potential risks.

V. Results and Discussion

In this section, we present analysis of the multi-factor risk assessment and route optimization methodology applied to various identified routes between source and destination. This section explores the effectiveness of the proposed system in identifying and recommending the safest routes by evaluating the impact of static and dynamic parameters on travel safety.

To implement our proposed methodology, we selected Maragathapuram (near Villupuram), Tamil Nadu, as the source and Parvathipuram, Vadalur, Tamil Nadu, as the destination. Parvathipuram is situated in the Vadalur town area. We considered five distinct routes from Maragathapuram to Parvathipuram, all with similar distances but varying slightly in their specifics. These routes traverse diverse topographies, including rural villages, towns, state highways (SH), and national highways (NH), encompassing both two-way and four-way roads. Additionally, the routes include sections passing through rural town near the destination. The routes were partitioned based on road types, and details are provided in Table II.

TABLE II. POSSIBLE ROUTES AND PARTITIONS FROM SOURCE TO DESTINATION

Sl. No.	Route Number	Partition Type (Road Type)	Partition Size (km)	Number of segments
1	1	Rural Village	3.7	37
2	1	NH38-4 ways	5.3	53
3	1	SH68	17	170
4	1	NH36- 2 ways/ 4-ways	23.5	235
5	1	NH532- 4ways	1	100
6	1	Rural Twon	0.8	80
7	2	Rural Village	4.6	46
8	2	Bye Pass Road - 4 ways	9.7	87
9	2	NH36- 2 ways / 4 ways	38.3	383
10	2	NH532- 4ways	1	100
11	2	Rural Twon	0.8	80
12	3	Rural Village	4.3	43
13	3	NH38-4 ways	3.5	35
14	3	NH38-Town	4.2	42
15	3	NH332-2 ways	5	50
16	3	NH36- 2 ways / 4 ways	41.3	413
17	3	NH532- 4ways	1	100
18	3	Rural Twon	0.8	80
19	4	Rural Village	3.7	37
20	4	NH38-4 ways	10.3	103
21	4	SH9	17.3	173
22	4	NH36- 2 ways/ 4-ways	23.5	235
23	4	NH532- 4ways	1	100
24	4	Rural Twon	0.8	80
25	5	Rural Village	3.7	37
26	5	NH38-4 ways	16.4	164
27	5	SH602	27.9	279
28	5	NH36- 2 ways/ 4-ways	11.4	114
29	5	NH532- 4ways	1	100
30	5	Rural Twon	0.8	80

For the route analysis from Maragathapuram to Parvathipuram, Route 1 includes rural village road, NH38, SH68, NH36, NH532, and a rural town segment. Route 2 features rural village road, a four-lane bypass, NH36, NH532, and a rural town. Route 3 starts with rural village road, NH38, NH38-Town, NH332, NH36, NH532, and ends in a rural town. Route 4 consists of rural village road, NH38, SH9, NH36, NH532, and a rural town segment. Route 5 includes rural village road, NH38, SH602, NH36, NH532, and concludes with a rural town. All five routes start from the same rural village road with little variation due to connect with next partition and end with NH532 and rural town segments of same distance.

C. Risk Factor Analysis

Based on the partition details provided in the Table II and values fixed for parameters in the section 3.B, we have simulated values for all the parameters of all partitions by seriously considering the partitions types. The chosen mode of transport is a car, with four passengers (three men and one woman), and the average age-related risk factor for the group is 0.4. The data was simulated using default values for three parameters: lighting facility was assigned 0 risk due to daytime travel, weather condition was set to sunny, and the travel time was set to afternoon. The remaining parameter values were fixed based on partitions and dependent parameters.

The risk factor is calculated for each 100-meter segments using the Eq. (3) with help of Eq. (1) and Eq. (2). The overall risk factor for the route is calculated using the Eq. (4).

The Fig. 2 shows the risk factors of all segments of Route-1. For Route-1, risk factors across partitions range from a minimum of 0.29375 to 0.34625 and a maximum of 0.40125 to 0.59125. Average risk factors vary between 0.35975 and 0.478885135, with specific averages of 0.478885135, 0.422900943, 0.458838235, 0.432356383, 0.35975, and 0.4253125. This variation reflects inconsistencies in risk levels along the route, particularly in village environments.

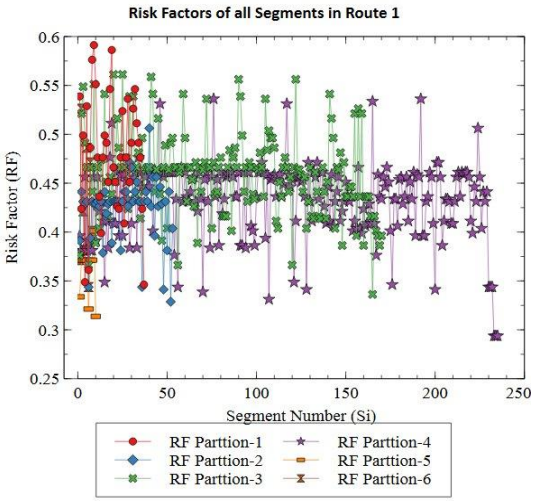


Fig. 2. Risk factors of all segments in route-1.

Fig. 3 presents the risk factors along Route-2. The minimum risk factors for Route-2 range from 0.29375 to 0.34625, while the maximum values vary between 0.40125 and 0.59125. The average risk factors across the five segments are 0.4748, 0.4553, 0.4391, 0.3598, and 0.4253, respectively.

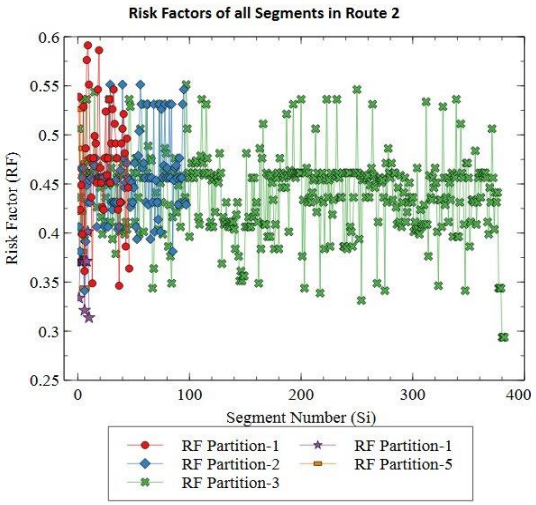


Fig. 3. Risk factors of all segments in route-2.

Route-3 consists of seven partitions and risk factors are calculated. Fig. 4 illustrates the risk factors across all segments of Route-3. The minimum risk factors range from 0.27875 to 0.36125, while the maximum values range from 0.40125 to 0.59125. The average risk factors for the seven segments are 0.4830, 0.4418, 0.3616, 0.4217, 0.4406, 0.3598, and 0.4253, respectively.

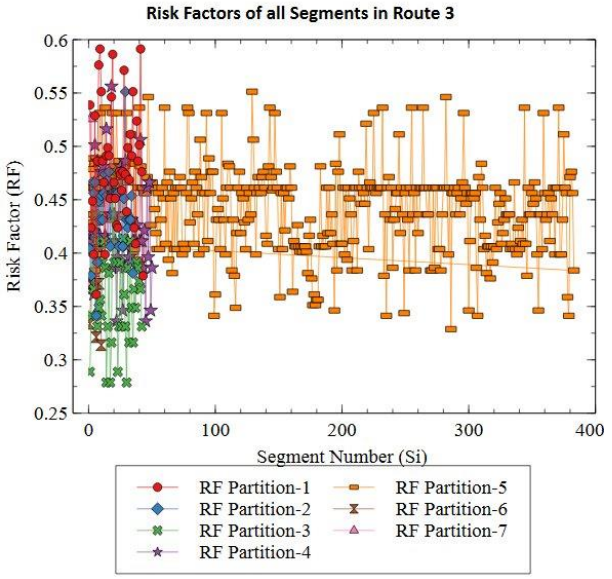


Fig. 4. Risk factors of all segments in route-3.

Route-4 consists of six segments, with the same combinations of road types as discussed in Route-1, but with variations in the distances of state and national highways. It follows a different path compared to Route-1.

Fig. 5 shows the risk factors for all six segments of Route-4, as outlined in Table II. The minimum risk factors range from 0.29375 to 0.34625, while the maximum values range from 0.40125 to 0.59125. The average risk factors for the six segments are 0.4782, 0.4208, 0.4463, 0.4324, 0.3598, and 0.4253, respectively.

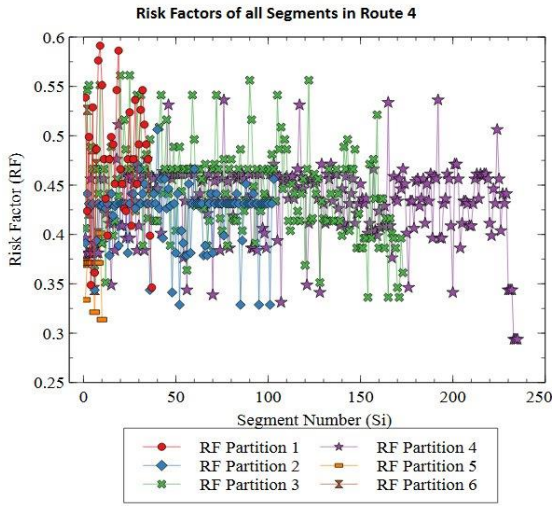


Fig. 5. Risk factors of all segments in route-4.

Similarly, the risk factors for the six segments of Route-5, where the state highway is the major contributing partition, have been calculated. Fig. 6 illustrates the risk factors for all segments of six partitions along Route-5. The minimum risk factors range from 0.29125 to 0.34875, while the maximum values range from 0.33375 to 0.53875. The average risk factors for the six segments are 0.4819, 0.4182, 0.4770, 0.4287, 0.3598, and 0.4253, respectively.

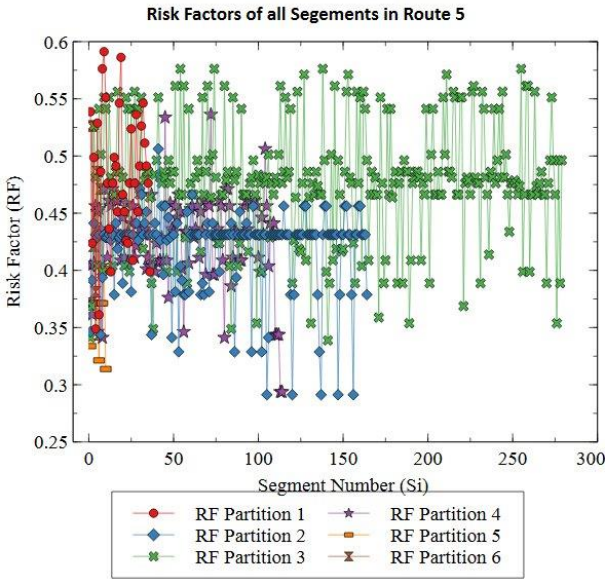


Fig. 6. Risk factors of all segments in route-5.

The risk factors for all partitions across all routes are shown in Fig. 7. The risk factors for the first partition are nearly identical across all routes due to minimal distance variation on the routes. Likewise, the risk factors for the last two partitions are the same, as these partitions remain consistent across all routes.

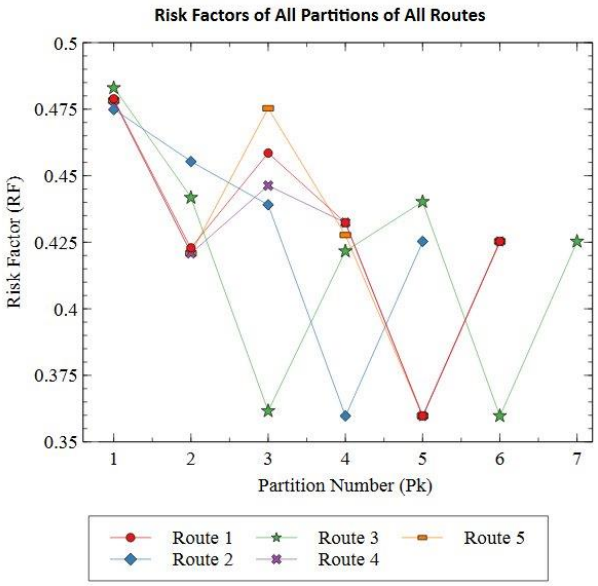


Fig. 7. Risk factors of all partitions in five routes.

The average static, dynamic, and final risk factors for all five routes are shown in Fig. 8. It illustrates that the static risk factor is higher than the dynamic risk factors for all routes except Route 3, which has a larger town area compared to the other routes.

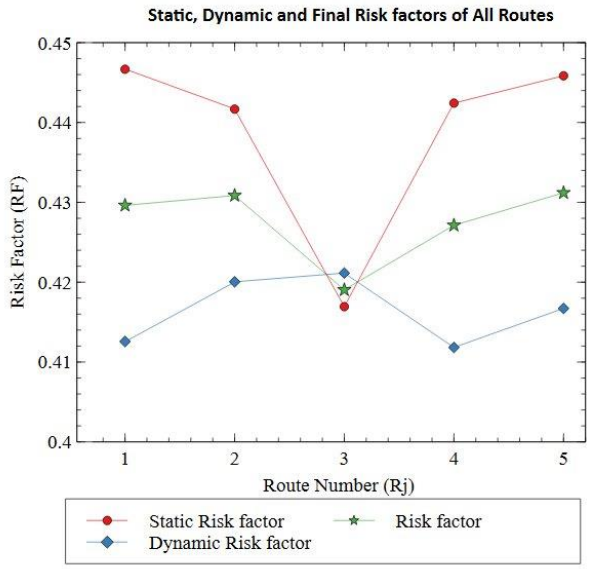


Fig. 8. Static, dynamic and final risk factors of all routes.

D. Safe Route Identification

The safest route is determined using Eq. (5), which calculates the route with the minimum risk factor among the studied routes. In this study, we analyzed five possible routes as given in Table II, each with varying partitions. Fig. 9 presents the risk factor values for all five routes. Route 3 has the lowest risk factor compared to the others.

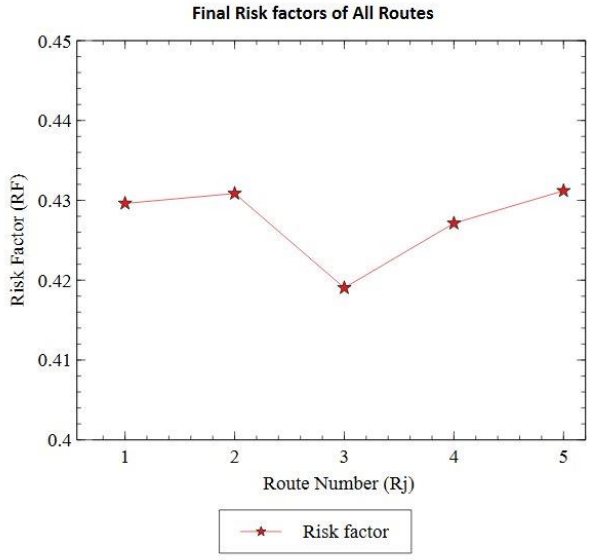


Fig. 9. Risk factors of all routes.

The reduced risk for Route 3 is attributed to several factors. This route passes through more town areas, which typically have better infrastructure and safety measures such as lighting and traffic control. Additionally, Route 3 follows longer stretches of national highways, known for their higher safety standards and better road conditions. Finally, the higher population density along this route also contributes to its lower risk, as densely populated areas have less threatened from the attackers.

The risk factors of five routes are evaluated under varying weather conditions, while maintaining the other parameters constant. Fig. 10 illustrates the impact of different weather conditions on the risk factors across all five routes.

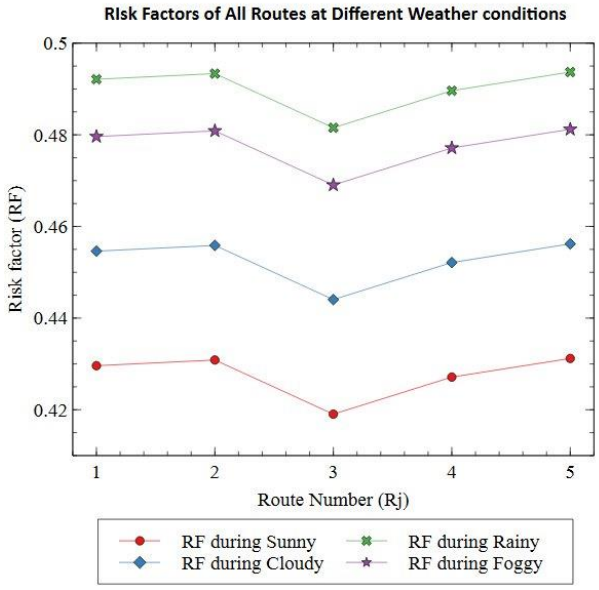


Fig. 10. Risk factors at different weather conditions.

Route 3 consistently offers the lowest risk factor across all weather conditions, as it passes through more densely populated areas.

The time of travel is also taken into account when calculating the risk factors for all five routes. For daytime travel, including morning, afternoon, and evening, the lighting facility value is set to 0, as natural light is sufficient. For night time travel, the lighting facility value is determined based on the presence of public places along the route and the type of route partitions. This adjustment reflects the availability and effectiveness of artificial lighting in reducing risk during night time. Fig. 11 illustrates how travel time influences the overall risk factor calculation across different routes.

The results indicate that Route 3 is the most optimal for daytime travel, yielding the lowest risk factors due to its natural lighting and favorable conditions during daylight hours. Conversely, for nighttime travel, the Route 2 is found to be the safest, offering the lowest risk factors. This is primarily attributed to better lighting infrastructure, the presence of public spaces, and well-defined route partitions that enhance visibility and safety during night hours. These findings highlight the importance of adapting route selection based on the time of travel to minimize risk.

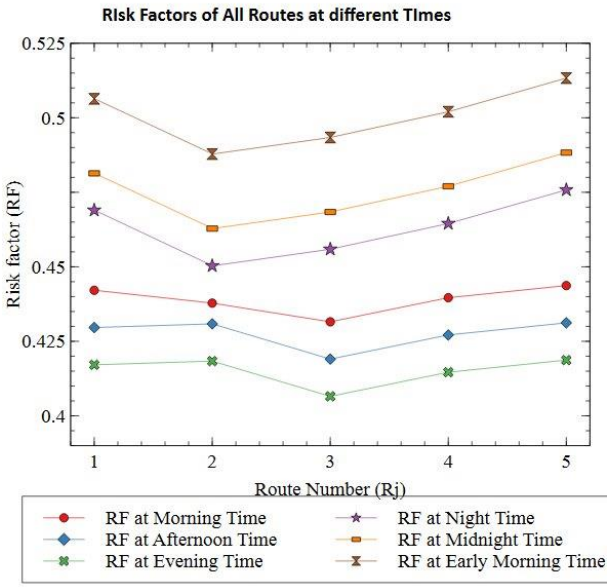


Fig. 11. Risk factors at different travel time.

The results demonstrate the effectiveness of the proposed model in identifying safe travel routes. The inclusion of both static and dynamic parameters ensured a risk assessment, making the model suitable for safe human travelling on the optimal route predicted by the proposed model.

VI. Conclusion

In conclusion, this study presents a multi-factor risk assessment and route optimization methodology aimed at improving travel safety based on the chosen sources and destination places. By incorporating both static and dynamic factors, the system effectively identifies the safest routes based on calculated risk factors. Our analysis reveals that Route 3 is the safest for daytime travel, while Route 2 is optimal for nighttime travel due to better lighting and route partitions. The granular assessment of 100-meter segments along the routes highlights the significant impact of environmental and infrastructural factors on travel safety, including artificial lighting, time of travel, and weather conditions. This adaptable framework, influence widely applicable risk parameters, demonstrates the potential for broader real-world applications in dynamic and changing road networks, ensuring safer route recommendations.

In future work, we aim to enhance the system by integrating real-time data sources, such as live weather updates, traffic congestion reports, and road maintenance data, to provide even more accurate risk assessments. Additionally, we plan to incorporate machine learning techniques to continuously improve the precision of risk predictions based on observed outcomes. By doing so, the system can become more robust and reliable in its route optimization recommendations.

References

[1] Santo, G., Santos, L., Costa, R. L., & Rabadão, C, "Intelligent Transportation Systems Security and Privacy in Information Security and Privacy in Smart Devices: Tools, Methods, and Applications", IGI Global. pp. 122-141, 2023.

[2] Tamagusko, T., Gomes Correia, M., Rita, L., Bostan, T.C., Peliteiro, M., Martins, R., Santos, L. and Ferreira, A., "Data-driven approach for urban micromobility enhancement through safety mapping and intelligent route planning", Smart Cities", Vol 6, Issue 4, pp.2035-2056, 2023.

[3] Parvez, M.S. and Moridpour, S., "Application of smart technologies in safety of vulnerable road users: A review", International Journal of Transportation Science and Technology, 2024, https://doi.org/10.1016/j.ijtst.2024.07.006.

[4] Sadaf, M., Iqbal, Z., Javed, A.R., Saba, I., Krichen, M., Majeed, S. and Raza, A., "Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects", Technologies, Vol.11, Issue 5, p.117, 2023.

[5] Nguyen, L.H., Nguyen, V.L., Hwang, R.H., Kuo, J.J., Chen, Y.W., Huang, C.C. and Pan, P.I., 2024. Towards Secured Smart Grid 2.0: Exploring Security Threats, Protection Models, and Challenges. IEEE Communications Surveys & Tutorials.

[6] L. Indraja and D. D. Suneetha, "Safe Path Prediction Using Machine Learning", International Journal for Research in Applied Science & Engineering Technology, pp. 1771-1773, July 2023.

[7] Y. S. Asawa, S. R. Gupta, V. V and N. J. Jain, "User Specific Safe Route Recommendation System", International Journal of Engineering Research & Technology, vol. 9, no. 10, pp. 574-580, October 2020.

[8] Pavate, A. Chaudhari and R. Bansode, "Envision of Route Safety Direction Using Machine Learning", ACTA SCIENTIFIC MEDICAL SCIENCES, vol. 3, no. 11, pp. 140-145, November 2019.

[9] Puthige, K. Bansal, C. Bindra, M. Kapur, D. Singh, V. K. Mishra, Apeksha Aggarwal, J. Lee, B.-G. Kang, Y. Nam and R. R. Mostafa, "Safest Route Detection via Danger Index Calculation and K-Means Clustering", Computers, Materials & Continua, vol. 69, no. 2, pp. 2761-2777, April 2021.

[10] Eranpurwala, F. Indorewala, N. Mapari and S. Mishra, "Women Safety Application for Safe Route Prediction", International Research Journal of Engineering and Technology, vol. 8, no. 5, pp. 2278-2282, July 2021.

[11] D. Bura, M. Singh and P. Nandal, "Predicting Secure and Safe Route for Women using Google Maps", 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, pp. 103-108, February 2019, doi: 10.1109/COMITCon.2019.8862173.

[12] R. Saleh and H. Fleyeh, "Using Supervised Machine Learning to Predict the Status of Road Signs", Transportation Research Procedia, vol. 62, pp. 221-228, 2022.

[13] D. K. Sharma and P. U. M, "The Traffic Accident Prediction Using Machine Learning", International Research Journal of Modernization in Engineering Technology and Science, vol. 5, no. 7, pp. 2964-2968, July 2023.

[14] J. F. Wang, Y. Wang, W. Jiang, Y. Qiao and W. B. X. Zheng, "An Urban Road Risk Assessment Framework Based on Convolutional Neural Networks", International Journal of Disaster Risk Science, vol. 14, pp. 475-487, June 2023.

[15] Mukherjee, D., & Mitra, S, "Pedestrian safety analysis of urban intersections in Kolkata, India using a combined proactive and reactive approach", Journal of Transportation Safety & Security, Vol.14, no.5, 754–795, September 2020, https://doi.org/10.1080/19439962.2020.1818907.

[16] A. V. Lakshmi and K. S. Joseph, "Travel Safe: A systematic review on Safe Route Guidance System", IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, pp. 1-6, 2022, doi: 10.1109/IATMSI56455.2022.10119408.

[17] Llopis-Castelló, D., Findley, D. J., & García, "A, Comparison of the highway safety manual predictive method with safety performance functions based on geometric design consistency", Journal of Transportation Safety & Security, Vol.13, Issue 12, pp:1365–1386, March 2020, https://doi.org/10.1080/19439962.2020.1738612.

[18] Al-Bdairi, N. S. S., Zubaidi, S. L., Zubaidi, H., & Obaid, I, "Injury severity of single-vehicle weather-related crashes on two-lane highways", Journal of Transportation Safety & Security, pp: 1–21, December 2023, https://doi.org/10.1080/19439962.2023.2293065.

[19] Wang, Q., & Gerdts, M., "Risk-based path planning for autonomous vehicles", Optimization and Control, March 2022, ArXiv. /abs/2203.03681, https://doi.org/10.48550/arXiv.2203.03681

[20] Zhou C, Chen M, Chen J, Chen Y, Chen W, "A Multi-Hazard Risk Assessment Model for a Road Network Based on Neural Networks and Fuzzy Comprehensive Evaluation", Sustainability, Vol. 16, Issue 6, March 2024, https://doi.org/10.3390/su16062429.

[21] Nishat Tasnim, Mohammed Tahmid, Nusrat Jahan, and Sultana Razia Syeda, "Risk Assessment Framework for Selecting the Safer Route for Hazmat Transportation Based on Accident Database and Vulnerability Models", ACS Chemical Health & Safety, Vol 30, Issue 5, pp:302-317, August 2023, DOI: 10.1021/acs.chas.3c00044.

[22] S. Jiang, M. Jafari, M. Kharbeche, M. Jalayer and K. N. Al-Khalifa, "Safe Route Mapping of Roadways Using Multiple Sourced Data", in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 4, pp. 3169-3179, April 2022, doi: 10.1109/TITS.2020.3032643.

[23] Litzinger, Paul & Navratil, Gerhard & Sivertun, Åke & Meier, Daniela, "Using Weather Information to Improve Route Planning", Lecture Notes in Geoinformation and Cartography. January 2012, doi:10.1007/978-3-642-29063-3_11.

[24] Nikhitha Pulmamidi and Rajanikanth Aluvalu and V Uma Maheswari, "Intelligent Travel Route Suggestion System Based on Pattern of Travel and Difficulties", IOP Conference Series: Materials Science and Engineering, vol 1042, no 1, December 2020.

[25] Krishnaraj Pawooskar, Dr Ramakanth Kumar P, "Safest Route Detection Application", International Research Journal of Engineering and Technology (IRJET), Volume: 07 Issue: 05, May 2020, e-ISSN: 2395-0056.

[26] Helai Huang, Yulu Wei, Chunyang Han, Jaeyoung Lee, Suyi Mao, Fan Gao, "Travel route safety estimation based on conflict simulation", Accident Analysis & Prevention, vol 171, June 2022, ISSN 0001-4575, https://doi.org/10.1016/j.aap.2022.106666.

[27] Road Safety Evaluations Based on Human Factors Method - Technical Report, 2019, ISBN: 978-2-84060-561-4.

An Ensemble Machine Learning Model for Predictive Maintenance on Water Injection Pumps in the Oil and Gas Industry

Salama Mohamed Almazrouei[1]*, Fikri Dweiri[2], Ridvan Aydin[3], Abdalla Alnaqbi[4]
Department of Industrial Engineering and Engineering Management-College of Engineering,
University of Sharjah, Sharjah, United Arab Emirates[1, 2, 3]
ADNOC Offshore, Abu Dhabi, United Arab Emirates[4]

***Abstract*—The effective operation of water injection pumps is vital for enhancing oil recovery in the oil and gas industry. To ensure optimal pump performance and prevent unplanned downtime, this study focused on implementing predictive maintenance strategies. We began by identifying five critical operational parameters—Seal Pressure 1, Seal Pressure 2, Vibration Data for the Drive End (VIB DE), Vibration Data for the Non-Drive End (VIB NDE), and Ampere. These parameters were monitored and analyzed to evaluate their impact on pump performance and maintenance needs. To achieve this, we applied three machine learning algorithms: Extreme Gradient Boosting (XGBoost), Light Gradient-Boosting Machine (LGBM), and Random Forest. Each algorithm was independently trained and tested on the dataset corresponding to each operational parameter. We assessed their performance using key accuracy metrics, including R squared, Mean Absolute Error (MAE), and Root Mean Square Error (RMSE). Following this, we developed an Ensemble model, combining the predictive outputs of XGBoost, LGBM, and Random Forest. The Ensemble model was then applied to the same parameters to evaluate its ability to address the limitations observed in standalone models. The results demonstrated that the Ensemble model consistently delivered superior performance, achieving lower RMSE and MAE values and higher R squared coefficients across all parameters. This study culminates in the validation of the Ensemble model as a robust and reliable approach for predictive maintenance. By leveraging the strengths of multiple algorithms, the Ensemble model offers significant improvements in accuracy and reliability, contributing to more effective maintenance systems for the oil and gas industry.**

***Keywords*—Ensemble machine learning models; oil and gas industry; predictive maintenance; water injection pumps**

I. Introduction

The oil and gas sector confronts the critical challenge of substantially reducing operational costs while upholding safety standards [1]. Fortuitously, artificial intelligence (AI) has become instrumental in addressing the challenges faced by the oil and gas industry (OGI), capitalizing on technological advancements and the Big Data revolution to facilitate informed decision making and expedite the transition from issue identification to execution [2]. Encompassing a range of operations spanning exploration to distribution, the OGI functions within a multifaceted environment characterized by extensive infrastructure and high-value assets [3]. Efficient maintenance and reliability management are imperative for ensuring optimal production, safety, and cost-effectiveness in this industry [3]. The adoption of predictive maintenance (PdM) emerges as a pivotal methodology, seamlessly integrating data analysis, machine learning (ML) algorithms, and sensor technologies to collect real-time operational and sensor data [4]. This proactive approach plays a crucial role in early failure identification, thereby mitigating the consequences of unforeseen downtime. A thorough examination of the existing literature reveals numerous successful AI implementations across various domains of petroleum engineering [5]. Within the OGI, a particular emphasis on PdM is evident, particularly concerning Water Injection Pumps (WIPs), which play a fundamental role in maintaining reservoir pressure and optimizing oil recovery [3]. By harnessing advanced technologies like ML and deep learning (DL), PdM for WIPs introduces enhanced strategies for predicting failures early and facilitating real-time condition-based proactive maintenance [6]. In contrast, traditional maintenance approaches often lead to unnecessary actions and disruptive costs, while reactive maintenance poses risks to safety and the environment [7]. PdM tackles these challenges by leveraging cutting-edge technologies and data analytics to continuously monitor the real-time health and performance of equipment. The comprehensive data-driven approach employed by PdM models, drawing on real-time data from sensors, control systems, and historical maintenance records, enables the early detection of potential issues [3,8]. This proactive intervention empowers organizations to anticipate and address impending challenges, effectively minimizing downtime, optimizing maintenance strategies, and improving operational efficiency [9]. The integration of PdM models establishes a proactive maintenance paradigm that fortifies reliability, reduces costs, and prolongs the lifecycle of critical assets [3,4]. The early identification and resolution of potential issues provide operators with the capability to circumvent costly breakdowns, mitigate production losses, and ensure uninterrupted operations. PdM also presents the opportunity for more efficient resource planning and allocation, enabling operators to optimize spare parts inventories and streamline maintenance schedules [2,4,5,10].

Digitalization and the Internet of Things (IoT) generate extensive data, driving the significance of Predictive Maintenance (PdM) in optimizing upstream rotating equipment in the Oil, Gas, and Petrochemical (OGP) industry [11, 12].

Efficient operation of Water Injection Pumps (WIPs) enhances oil recovery and operational success [1–3]. PdM minimizes unplanned downtime and improves pump performance, with Deep Learning (DL) playing a pivotal role in recent studies. Janssens et al. [13] used CNNs for health monitoring via infrared thermal images, showcasing potential in anomaly detection, while Sampaio et al. [14] employed ANNs to predict motor failures, albeit with limited performance analysis. Bekar et al. [15] utilized K-means and PCA for motor PdM, facing challenges related to motor type specificity. Falamarzi et al. [16] applied ANN and SVR to tram track gauge prediction, and Susto et al. [17] proposed a PdM system for epitaxy processes, lacking equipment-specific context.

In developing countries, implementing PdM in the OGP sector encounters barriers such as limited skilled personnel, sensor access, infrastructure constraints, financial limitations, and cultural challenges [18-19]. Initiatives for sustainability and diversification, alongside training and infrastructure investments, aim to address these challenges [19-20]. Despite advancements, there is a research gap in applying AI to predict failures in WIPs, critical for health, safety, and environmental outcomes. This study addresses the gap by leveraging ML models like XGBoost and LGBM to predict WIP failures, focusing on asset loss, regulatory compliance, corporate reputation, and production impacts [3–5].

These algorithms, recognized for their high performance, have not been extensively studied in conjunction with ensemble methods such as Random Forest. The Ensemble model demonstrates unparalleled accuracy and increases the accuracy of predictions. This research is driven by the urgency to provide advanced solutions for PdM in the OGI sector, addressing the complexities of diverse operational parameters. This study specifically addresses the maintenance of water injection pumps, focusing on critical factors such as currents, pressure, and vibrations because these factors are crucial for maintenance but are often under-represented in existing research. This study innovatively integrates multiple algorithms within ensemble models to enhance predictive accuracy and address maintenance challenges in water injection pumps. Unlike previous approaches that often lack specificity in algorithm selection for factors such as currents, pressure, and vibrations, a systematic approach is employed to optimize performance in real-world operational environments. This refinement distinguishes the work by effectively applying ensemble techniques to improve Prognostics and Health Management (PHM) systems, particularly in critical applications such as WIPs. The findings of this study are poised to significantly contribute to the field by presenting a holistic and enhanced approach to predictive modeling in industrial settings. In the upcoming sections, this study delves into PdM through ML. Section II explains the methodology, highlighting the significance of the Ensemble model. Section III presents the results and analysis, while discussion is given in Section IV. Limitation and future work is given in Section V and Section VI respectively. Finally, the paper is concluded in Section VII.

II. METHODOLOGY

Predictive maintenance (PdM) in the OGI industry is critical for optimal production, safety, and cost-effectiveness. This study employs an ensemble of ML models—XGBoost, LGBM, and Random Forest—to enhance predictive accuracy. The unique strengths of each algorithm contribute to a robust framework. The ensemble methodology leverages complementary features, addressing individual weaknesses and mitigating biases. This novel approach aims to outperform standalone models, offering more accurate and reliable results. Fig. 1 illustrates the methodology implemented in our study. The flowchart visually outlines the sequential steps involved: data collection from various sources relevant to WIPs performance, including currents, pressure, and vibrations; preprocessing of the collected data to handle missing values, normalize them, and prepare them for analysis; selection of pertinent features influencing WIPs performance; training of machine learning models, comprising individual algorithms and Ensemble models, using the preprocessed data; evaluation of model performance using metrics such as RMSE to determine accuracy; creation of an Ensemble model by combining outputs from multiple models to enhance predictive accuracy; validation of the Ensemble model using test data to ensure reliability; and deployment of the final model for real-time predictive maintenance of water injection pumps, enabling proactive maintenance scheduling. To model and simulate the water injection network system, the relationships between different components and their respective parameters are established using the given formulae and principles of fluid mechanics. This includes deriving equations for the pump model, the water distributing station model, the well model, the tube element model, the node element model, and the system model, as outlined below. The pump model is represented by the quadratic equation:

$$H = AQ^2 + BQ + C \quad (1)$$

where H is the pump outlet pressure, Q is the pump flow rate, and A, B, and C are co-efficient representing the quadratic, linear, and constant terms, respectively. The water distributing station and well model can be expressed as:

$$P = A\,Q + B \quad (2)$$

where P denotes the pressure at the water distributing station or injection well, Q is the flow rate, and A and B are the linear and constant term coefficients, respectively [21]. The tube element model is described by:

$$qi = ki(hk - hj) \quad (3)$$

$$hf = Pi - Pj \quad (4)$$

where qi is the flow rate through pipeline element i, ki is a variable related to the pipe-line element length, inner diameter, and friction coefficient, hk and hj are the gross heads at the two ends of the pipeline element, and hf is the pressure loss across the pipe sec-tion. The pressure loss in the pipe section is calculated using the Darcy formula:

$$hf = Lv^2/2dg \quad (5)$$

where *hf* is the pressure loss, *L* is the pipe section length, d is the diameter, *v* is the fluid flow velocity, and *g* is the gravitational acceleration. Using these relationships, the system of equations is formulated to describe the behavior of the water injection network. Numerical methods are employed to solve

these equations iteratively, allowing for the simulation of network parameters such as pressure and flow rate at all nodes.

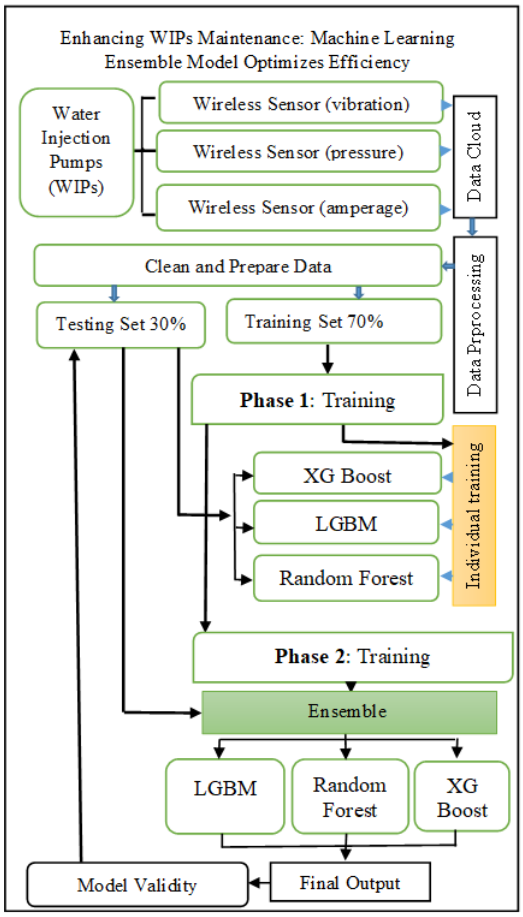


Fig. 1. Methodology flowchart.

A. Ensemble Model Construction

The present study incorporates a diverse ensemble of ML models; namely, X Boost, LGBM, and Random Forest. Each algorithm brings unique strengths, contributing to the overall robustness of the predictive framework. XGBoost's scalability, LGBM's high-performance gradient boosting, and Random Forest's ensemble learning approach individually address distinct aspects of the predictive task. The ensemble methodology aims to leverage the complementary strengths of each algorithm, enhancing predictive accuracy. By fusing the predictive capabilities of XGBoost, LGBM, and Random Forest, the study seeks to capitalize on their collective intelligence, mitigating individual weaknesses. The study asserts that this amalgamation, orchestrated through ensemble techniques, can yield more accurate and reliable results compared to each algorithm operating in isolation. This approach is grounded in the empirical observation that ensemble models often outperform individual algorithms by mitigating biases and reducing overfitting.

B. Data Collection and Preprocessing

The data utilized in this study originates from sensor readings, maintenance records, and operational parameters, collectively offering insights into the pump system's behavior. Sensor data provide real-time insights into operational aspects, including pressure levels, temperatures, and vibrations. Maintenance records offer a historical perspective, detailing interventions over time. Table I presents a succinct overview of the key operational parameters meticulously chosen for the analysis of the Work in Progress WIPs system. Among these parameters are the Ampere, denoting the current employed by the pump; VibDE, representing the vibration in the Drive End bearing; VibNDE denoting the vibration in the Non-Drive End bearing; and 1st Press, and 2nd Press delineating the 1st and 2nd Stage Seal Pressures, respectively.

TABLE I. LIST OF SELECTED RUNNING PARAMETERS FOR WIPS SYSTEM ANALYSIS

Name	Description
1st_Press	1st Stage Seal Press
2nd_Press	2nd Stage Seal Press
VibDE	Vibration in DE bearing
VibNDE	Vibration in NDE bearing
Ampere	The current used by the pump

Evaluating VIB DE and VIB NDE bearings is crucial because they support pump shaft alignment, and their condition directly impacts operational efficiency and reliability [7]. This comprehensive compilation serves as a foundational tool for a nuanced examination, allowing for a detailed assessment of the factors that significantly influence the functionality and performance of the WIPs system.

Preprocessing steps include data cleansing, type conversion, outlier detection, feature selection, correlation analysis, and normalization. Data cleansing addresses inconsistencies and missing values. Type conversion ensures uniformity in calculations. Outlier detection manages outliers that could hinder model training. Feature selection, guided by correlation analysis, reduces model complexity. Normalization and scaling ensure uniform feature scales for effective ML.

C. Data Analysis

An extensive repository of raw data encompassing operational parameters and cumulative operational hours was initially collected. The dataset refinement process involved identifying salient data points that had a high correlation with WIPs. This process aimed to enhance model interpretability and counteract dimensionality augmentation. The selected key operational parameters are Ampere, VibDE, VibNDE, 1st_Press, and 2nd_Press. Feature selection is approached judiciously, ensuring that only the most influential features are considered for each model. The provided code snippet employs the "sweetviz" Python library for exploratory data analysis (EDA), generating comprehensive reports for informed decision making. The analysis involves data cleaning, exclusion of string entries, and construction of a correlation matrix to assess inter-feature relationships. The Correlation Matrix of Feature Influences helps in selecting the pertinent features shown in Fig. 2, contributing to dimensionality re-duction and enhancing model accuracy. This matrix analysis promotes a nuanced understanding of data structure, confounding factors, and noise, ultimately improving the robustness of the research.

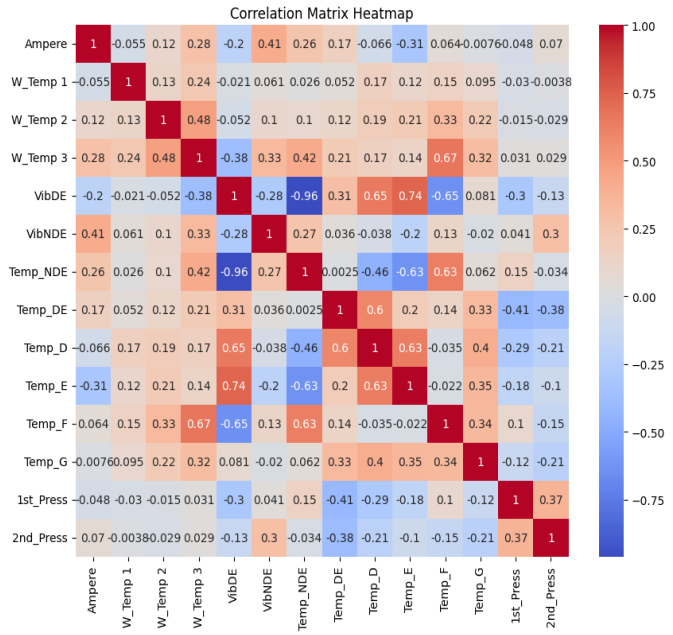


Fig. 2. Correlation matrix of feature influences.

D. Comparative Modeling of Operational Parameters

In this study, an assessment is made of two distinct modeling techniques concerning operational parameters. The Light Gradient Boosting Machine (LGBM), eXtreme Gradient Boosting (XGBoost), and random forest methodologies serve as the primary frameworks for examination [22]. The deliberate selection of multiple modeling techniques enriches the empirical rigor of the research, enabling a comparative analysis of their predictive capabilities and generalization capacities. Rooted in the gradient boosting paradigm, LGBM, XGBoost, and random forest models iteratively enhance accuracy by sequentially fitting weak learners to residuals, capturing intricate data patterns [23]. Chosen for their success in various domains, especially tasks requiring high accuracy and efficiency, these models offer a range of hyperparameter configurations for fine-tuning. By employing two distinct models, the aim is to comprehensively understand their performance variances, strengths, and limitations in capturing the intricate interplay among operational parameters. This deliberate and empirically driven choice enhances the scientific rigor of the research, enriches the depth of analysis, and facilitates a nuanced interpretation of the obtained results.

1) XGboost prediction model: The XGBoost model stands out as a powerful ML algorithm deeply rooted in gradient boosting. Recognized for its versatility and exceptional performance, XGBoost is a valuable asset across various data science and ML domains [24]. Operating as an ensemble of decision trees, XGBoost employs a sequential correction approach to iteratively enhance model performance. This methodology allows it to capture intricate relationships within datasets, while integrated tree pruning controls model complexity for improved computational efficiency [22]. Engineered for optimized speed and efficiency, XGBoost is scalable for large datasets through parallel processing. Its adaptability spans diverse data types, and it excels in both regression and classification tasks [25]. With features such as metric-based feature importance, handling imbalanced datasets, and robust regularization techniques, XGBoost emerges as a versatile and powerful algorithm, known for efficiently tackling complex tasks [26].

2) LightGBM prediction model: The LightGBM model is a high-performance open-source software library designed specifically for gradient boosting. Renowned for its speed, resource efficiency, and scalability, LightGBM finds applications in diverse ML tasks such as classification, regression, and ranking [27]. Unlike some gradient-boosting algorithms, LightGBM employs decision trees as base learners, contributing to its exceptional efficiency. Innovative techniques like Gradient-Based One-Side Sampling (GOSS) and Exclusive Feature Bundling (EFB) further enhance its capabilities for reducing model variance and optimizing feature selection. Notably, LightGBM stands out for its remarkable speed, making it one of the fastest ML libraries capable of efficiently training models on extensive datasets. Its efficiency in memory usage optimization allows it to handle datasets surpassing the memory capacity of alternative libraries [28]. Additionally, LightGBM consistently achieves impressive accuracy, delivering state-of-the-art results across a range of ML tasks, further solidifying its reputation as a powerful and scalable library.

3) Random forest prediction model: Random forest regression, a highly regarded technique in ML, is known for its versatility, robustness, and superior predictive accuracy. This ensemble method combines multiple decision trees, excelling in handling complex nonlinear relationships in diverse prediction tasks [29]. Its acclaim stems from consistently outperforming singular decision trees and other regression models by capturing intricate nonlinear relationships while mitigating overfitting. While recognized for its robustness to outliers and noise, a closer examination is crucial to understand its limits [30]. The algorithm handles high-dimensional data well, but scalability and efficiency are key. Feature importance analysis offers insights, but robustness across datasets is crucial [30]. This analysis aims to provide a nuanced view of random forest regression, emphasizing its strengths and offering alternative scenarios.

III. Results

This section compares XGBoost, LGBM, and Random Forest algorithms in predicting parameters like pressure, vibration, and Ampere values, aiming to assess their real-world effectiveness and reliability.

A. Comparative Analysis of Algorithms

1) XGBoost model for pressure prediction: insights and visual analysis: Tables II and III present a detailed analysis of the XGBoost model's performance metrics for Seal Pressure 1 and Seal Pressure 2, respectively. The XGBoost model for Seal Pressure 1 exhibits commendable metrics, with an RMSE of 5.61, an Mean Absolute Error (MAE) of 2.38, and an R-squared

value of 0.93. These metrics suggest that the model provides accurate predictions, capturing a significant portion of the variance in the data for Seal Pressure 1.

TABLE II. XGBOOST MODEL METRICS FOR SEAL PRESSURE 1

Model	RMSE	MAE	R squared
XGBoost	5.61	2.38	0.93

Table III focuses on Seal Pressure 2, demonstrating the XGBoost model's robust performance with an RMSE of 9.41, an MAE of 4.87, and an R-squared value of 0.91. Despite the slightly higher RMSE and MAE compared to Seal Pressure 1, the model exhibits reasonable accuracy. Interpretation of these metrics should consider specific application needs and tolerance for errors. The R-squared values, nearing 1.0, signify strong correlation, while RMSE and MAE offer insights into prediction errors. Overall, the XGBoost model proves effective in predicting both Seal Pressure 1 and Seal Pressure 2, providing valuable insights for practitioners in pressure prediction scenarios.

TABLE III. XGBOOST MODEL METRICS FOR SEAL PRESSURE 2

Model	RMSE	MAE	R squared
XGBoost	9.41	4.87	0.91

Known for its robustness with complex datasets, the XGBoost algorithm excels in pressure forecasting. This overview explores its application for precise pressure prediction, crucial in diverse sectors. Fig. 3 and Fig. 4 visually compare actual and predicted values, focusing on the initial 25 predictions. Logarithmic scaling enhances clarity, and the limited predictions prevent overcrowding, allowing for a focused evaluation of XGBoost's predictive accuracy.

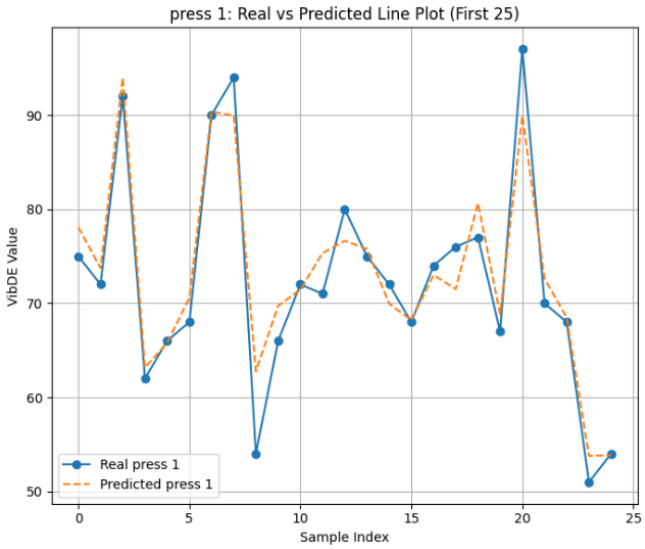


Fig. 3. XGBoost model—line plot analysis of actual vs. predicted pressure 1 (first 25 predictions).

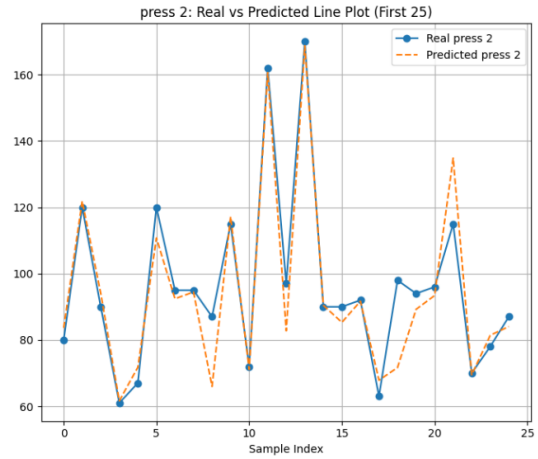


Fig. 4. XGBoost model—focused visualization with limited predictions pressure 2 (first 25 predictions).

2) XGBoost Model for vibration prediction: Insights and visual analysis: Evaluating VIB DE and VIB NDE bearings is crucial for pump system health. In Table IV, focusing on VIB DE, the XGBoost model shows strong performance with an RMSE of 6.32, an MAE of 3.80, and a high R-squared value of 0.99, indicating accurate predictions.

TABLE IV. VIBRATION IN VIB DE—XGBOOST MODEL METRICS

Model	RMSE	MAE	R squared
XGBoost	6.32	3.80	0.99

Table V, evaluating VIB NDE, shows excellence with an RMSE of 3.34, an MAE of 3.80, and an impressive R-squared value of 0.99. These metrics highlight the XGBoost model's proficiency in predicting Non-Drive End-bearing vibration. Comparing Tables IV and V reveals consistent high performance in predicting vibration for both Drive End and Non-Drive End bearings. Strong R-squared values indicate a robust correlation, emphasizing model reliability. Similar MAE values suggest consistent accuracy. Accurate vibration prediction is crucial for identifying potential issues and preventing malfunctions, showcasing the XGBoost model's effectiveness in addressing vibration complexities for overall pump system health and longevity.

TABLE V. VIBRATION IN VIB NDE—XGBOOST MODEL METRICS

Model	RMSE	MAE	R squared
XGBoost	3.34	3.80	0.99

Fig. 5 and Fig. 6 depict the XGBoost model's performance in predicting VIB DE and VIB NDE. Using a line graphs, the visualizations compare the initial 25 predictions with actual values. Applying a logarithmic function enhances scale and normalizes data for a clearer presentation, reducing clutter. The intentional limit of 25 predictions prevents graph overcrowding, ensuring a focused and comprehensive representation.

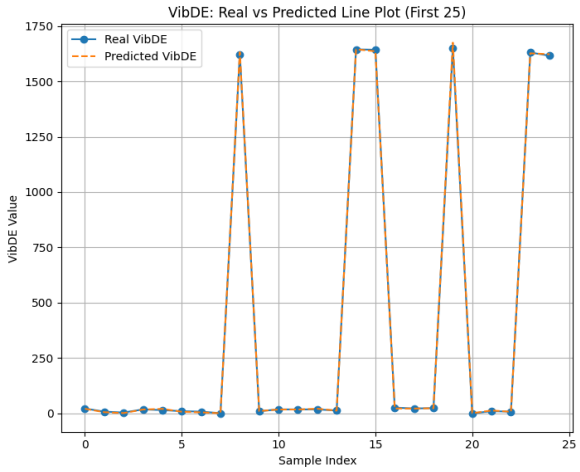


Fig. 5. XGBoost model predictions vs. actual values for VIB DE (line graph).

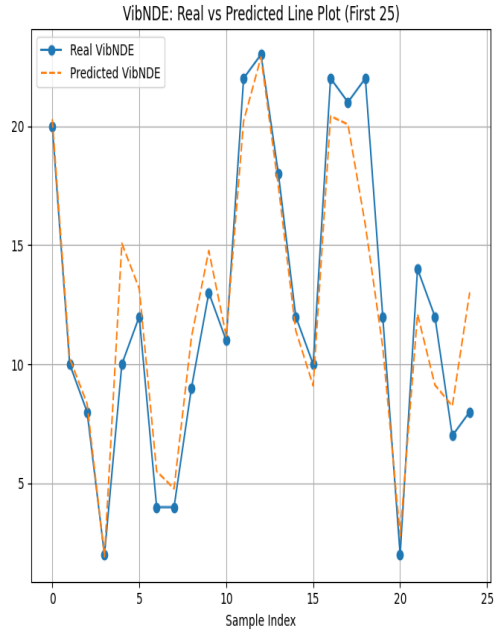


Fig. 6. XGBoost model predictions vs. actual values for VIB NDE (line graph).

3) XGBoost model for AMPERE prediction: insights and visual analysis: Table VI details the predictive performance metrics for the XGBoost model in Ampere measurements forecasting. With an RMSE of 3.28, an MAE of 2.25, and an R-squared value of 0.79, the model shows reasonably accurate predictions for Ampere. While demonstrating proficiency, there is room for improvement, particularly in explaining variance. These metrics serve as benchmarks, guiding potential refinements to enhance precision in future iterations. Insights from Table VI contribute to ongoing efforts to optimize parameters or explore alternative methodologies, crucial for fine-tuning the model and maximizing its effectiveness in real-world applications where accurate Ampere predictions are crucial.

TABLE VI. XGBOOST MODEL METRICS FOR AMPERE PREDICTION

Model	RMSE	MAE	R squared
XGBoost	3.28	2.25	0.79

Fig. 7 visually analyze the XGBoost model's predictive performance, comparing the first 25 predictions with actual values using grouped line plots. The contrast between actual and predicted values highlights the model's accuracy, with line plots depicting continuous performance trends. Applying a logarithmic function enhances clarity and comparability, ensuring better scale and data normalization for a coherent representation. Focusing on the initial 25 predictions prevents visual overcrowding, thereby facilitating a detailed examination of early-phase accuracy.

This approach allows for effective pattern recognition and insights. Overall, these visualizations offer a comprehensive and accessible assessment of the XGBoost model's predictive capabilities, leveraging a combination of graphs and thoughtful data transformations for nuanced understanding and valuable insight.

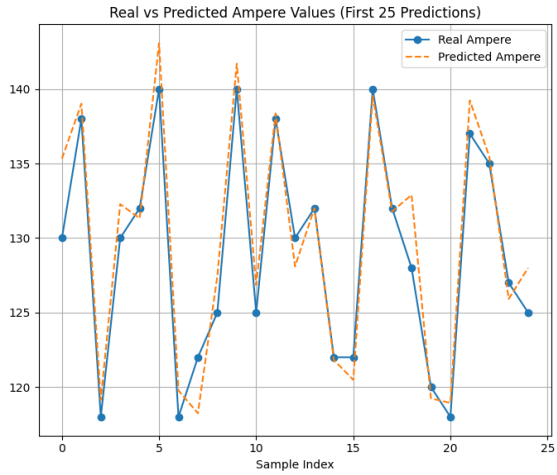


Fig. 7. XGBoost model—line plot analysis of actual vs. predicted values (first 25 predictions).

4) LGBM model for pressure prediction: insights and visual analysis: Examining the outcomes presented in Table VII, it is evident that the LGBM model achieves noteworthy metrics for Seal Pressure 1, with an RMSE of 5.29, an MAE of 2.22, and an R-squared value of 0.94.

TABLE VII. LGBM MODEL METRICS FOR SEAL PRESSURE 1

Model	RMSE	MAE	R squared
LGBM	5.29	2.22	0.94

Moving to Table VIII, the LGBM model's performance for Seal Pressure 2 is notable, featuring an RMSE of 8.98, an MAE of 5.17, and an R-squared value of 0.91. These tabulated results provide a detailed overview of the LGBM model's effectiveness for both Seal Pressure 1 and Seal Pressure 2, facilitating a comprehensive evaluation of its predictive capabilities.

TABLE VIII. LGBM MODEL METRICS FOR SEAL PRESSURE 2

Model	RMSE	MAE	R squared
LGBM	8.98	5.17	0.91

Fig. 8 and Fig. 9 visually showcase the LGBM model's predictive performance in pressure forecasting. Utilizing line plots for a comparative analysis of the initial 25 predictions against actual values, the visualization highlights the LGBM model's effectiveness. Applying a logarithmic function enhances clarity and maintains a normalized scale, ensuring a clearer and less cluttered representation. Focusing on the initial 25 predictions allows for detailed examination of early accuracy, preventing graph overcrowding, and allowing for a interpretable and focused visual representation. These visualizations offer valuable insights into the LGBM model's predictive capabilities, aiding in assessing its performance and reliability in pressure prediction scenarios. The graphical representation facilitates an intuitive understanding of the model's behavior, contributing to a comprehensive evaluation.

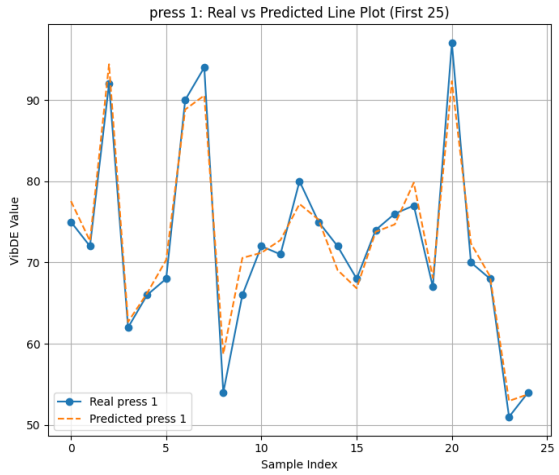


Fig. 8. LGBM Model—Line Plot Analysis of Actual vs. Predicted Pressure (First 25 Predictions).

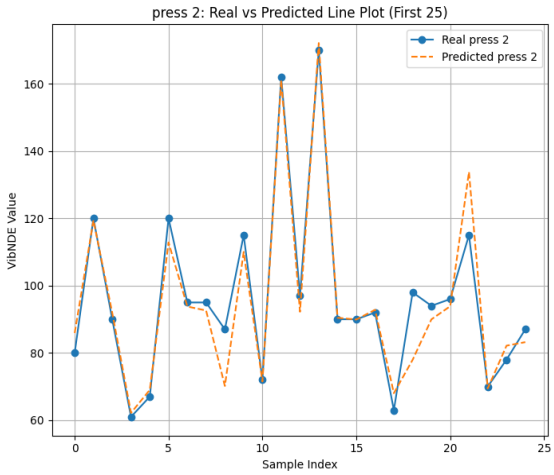


Fig. 9. LGBM Model—Focused Visualization with Limited Predictions (First 25 Predictions).

5) LGBM model for vibration prediction: Insights and visual analysis: The visualizations presented in Fig. 10 depict the performance of the LGBM model in predicting VIB DE and VIB NDE values. The line graphs facilitate a comprehensive comparison of the first 25 predictions with their corresponding actual values. Applying the log function to the values serves the purpose of achieving a better scale and normalization, leading to a clearer and less cluttered visualization. This transformation enhances the interpretability of the data, making it easier to discern patterns and trends in the model's predictions. By limiting the display to the first 25 predictions, the graphs avoid overcrowding, allowing for a focused examination of the model's accuracy in capturing the actual values. This selective approach aids in identifying any discrepancies or areas where the model may exhibit strengths or weaknesses. The discussion of these visualizations should involve a detailed analysis of how well the LGBM model aligns with the actual values, considering factors such as precision, accuracy, and potential areas for improvement. Additionally, any notable patterns or deviations between predicted and actual values should be highlighted and discussed to provide insights into the model's performance and its applicability in predicting VIB DE and VIB NDE.

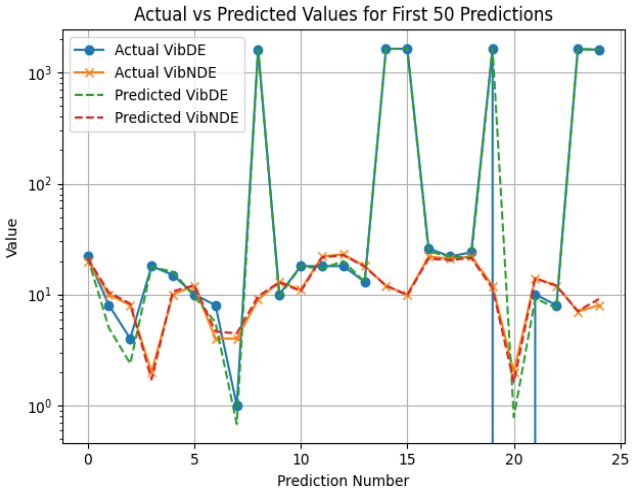


Fig. 10. LGBM Model Predictions vs. Actual Values for VIB NDE.

The LGBM model for VIB DE demonstrates exceptional performance, as indicated by the metrics in Table IX. The Root Mean Squared Error (RMSE) stands impressively low at 45.22, signifying minimal deviation between predicted and actual values. Complementing this, the MAE is commendably low at 6.07, reinforcing the model's accuracy. The high R-squared value of 0.99 emphasizes an excellent fit, showcasing the model's ability to explain the variance in VIB DE.

TABLE IX. PERFORMANCE METRICS FOR VIB DE USING LGBM

Model	RMSE	MAE	R squared
LGBM	45.22	6.07	0.99

Turning to VIB NDE, the LGBM model continues to exhibit strong predictive capabilities, as highlighted in Table X. The RMSE is notably low at 3.46, indicating minimal prediction errors. The MAE, standing at 2.32, further emphasizes the accuracy of the model, with low absolute differences between predicted and actual values. While the R-squared value of 0.84 is slightly lower than in VIB DE, it still signifies a robust model fit and reliable predictions for VIB NDE. The Tables IX and X are collectively underscore the effectiveness of the LGBM model in predicting both VIB DE and VIB NDE.

TABLE X. PERFORMANCE METRICS FOR VIB NDE USING LGBM

Model	RMSE	MAE	R squared
LGBM	3.46	2.32	0.84

6) LGBM model for AmperE prediction: Insights and visual Analysis : Fig. 11 offers a detailed analysis of the LGBM model's Ampere prediction performance using grouped line plots. Comparing the initial 25 predictions with actual values, these visualizations provide insights into the model's accuracy. Line plots offer a continuous overview of the model's performance. Applying a logarithmic function enhances interpretability and comparability, ensuring a clearer and less cluttered visualization. Focusing on the first 25 predictions prevents visual congestion, allowing a detailed examination of early-stage accuracy and facilitating the discernment of performance patterns. The line plots thoughtful data transformations contributes to a nuanced understanding of the LGBM model's predictive performance, facilitating valuable insights from the visualized data.

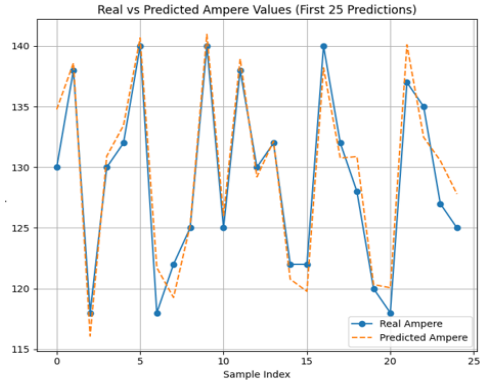


Fig. 11. LGBM Model—Comparison of Actual vs. Predicted Ampere Values (First 25 Predictions).

Table XI succinctly evaluates the LGBM model's performance in predicting Ampere values through the three key metrics—RMSE, MAE, and R-squared. With an RMSE of 3.08 indicating average error magnitude, a low MAE of 2.26 signifying precise predictions, and a high R-squared value of 0.82 showcasing substantial explanatory power, the LGBM model proves effective for Ampere prediction. These metrics affirm the model's reliability and accuracy, positioning it as a valuable tool for forecasting Ampere values across applications. The table provides a concise summary, offering numerical indicators for researchers, practitioners, and decision makers seeking insights into the model's efficacy.

TABLE XI. LGBM MODEL METRICS FOR AMPERE PREDICTION

Model	RMSE	MAE	R squared
LGBM	3.08	2.26	0.82

7) Random forest model for pressure prediction: Insights and visual analysis: Fig. 12 and Fig. 13 visually depict the Random Forest model's predictive performance using line plots, contrasting the initial 25 predictions with actual values. The combination of these visual elements highlights the model's efficacy and provides a comprehensive analysis of its accuracy in predicting the first 25 observations. Applying a logarithmic function enhances clarity and maintains a normalized scale, resulting in a distinct and less cluttered representation. Focusing on the initial 25 predictions offers valuable insights into the model's early predictive behavior, facilitating a detailed examination of accuracy without overcrowding the graphical representation. These visualizations contribute to a nuanced understanding of the Random Forest model's predictive capabilities, offering unique insights through line plots. This visual exploration is crucial for assessing the model's reliability and effectiveness, particularly in scenarios where clarity and precision are paramount.

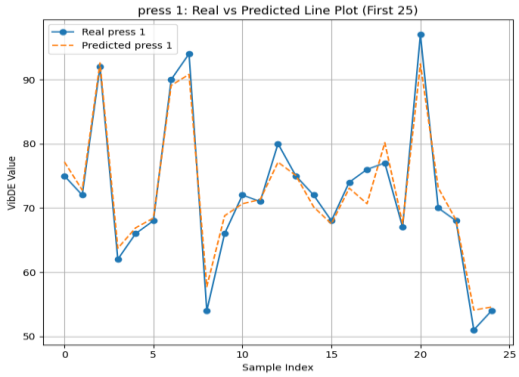


Fig. 12. Random Forest Model—Logarithmic Transformation (First 25 Predictions).

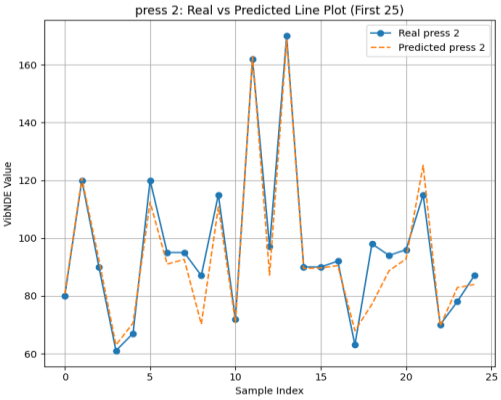


Fig. 13. Random Forest Model—Focused Visualization with Limited Predictions (First 25 Predictions).

In Table XII, the Random Forest model exhibits commendable metrics for Seal Pressure 1, with an RMSE of 4.86, an MAE of 2.01, and an R-squared value of 0.95. These results suggest that the Random Forest model provides accurate predictions, capturing a significant portion of the variance in the data for Seal Pressure 1.

TABLE XII. RANDOM FOREST MODEL METRICS FOR SEAL PRESSURE 1

Model	RMSE	MAE	R squared
Random Forest	4.86	2.01	0.95

Table XIII focuses on Seal Pressure 2, where the Random Forest model demonstrates robust performance with an RMSE of 9.24, an MAE of 4.49, and an R-squared value of 0.91. Despite slightly higher RMSE and MAE values compared to Seal Pressure 1, the model maintains reasonable accuracy. Combined with visualizations, it is evident that the Random Forest model consistently performs well in both seal pressure scenarios. Strong correlation, as indicated by high R-squared values, underscores the model's reliability in predicting seal pressures. The integration of visual and quantitative assessments provides a comprehensive understanding of the Random Forest model's effectiveness.

TABLE XIII. RANDOM FOREST MODEL METRICS FOR SEAL PRESSURE 2

Model	RMSE	MAE	R squared
Random Forest	9.24	4.49	0.91

8) Random forest model for vibration prediction: insights and visual analysis: Fig. 14 and 15 visually analyze the Random Forest model's performance in predicting VIB DE and VIB NDE, employing both bar and line formats to compare the initial 25 predictions with actual values. Applying a log function to the values enhances scaling and normalization, improving visualization clarity. Focusing on the first 25 predictions prevents overcrowding, allowing for a detailed examination of the model's accuracy and nuances in data capture. This approach provides a concise yet meaningful snapshot of the Random Forest model's alignment with actual values, offering valuable insights for further analysis and model refinement.

In Tables XIV and XV, the performance metrics of the Random Forest model in predicting VIB DE and VIB NDE are presented. In Table XIV, the model achieved an RMSE of 9.53, indicating precise predictions with a low average magnitude of errors. The MAE of 3.80 further confirms the model's accuracy, as it represents the average absolute difference between predicted and actual values. The exceptionally high R squared value of 0.99 signifies a remarkable goodness of fit, explaining 99% of the variance in VIB DE.

Turning to Table XV, the Random Forest model showcased a notable RMSE of 3.58 for VIB NDE, indicating accurate predictions with a low average magnitude of errors. The MAE of 2.16 reinforces the model's reliability, showcasing a relatively small average absolute difference from the actual values. The R squared value of 0.83 highlights a strong fit, accounting for 83% of the variance in VIB NDE.

In summary, the Random Forest model demonstrates exceptional predictive accuracy for both VIB DE and VIB NDE. The low RMSE and MAE values, coupled with high R-squared values, underscore the model's effectiveness in capturing and explaining the variance in vibration data. These findings affirm the Random Forest model as a robust tool for vibration prediction in both conditions.

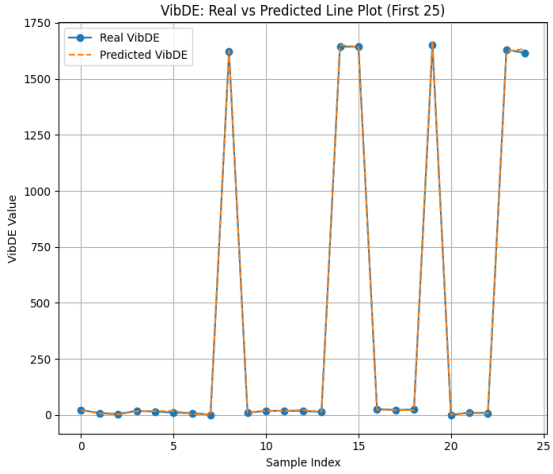


Fig. 14. RandomForest_VIB_DE_Performance_Line.

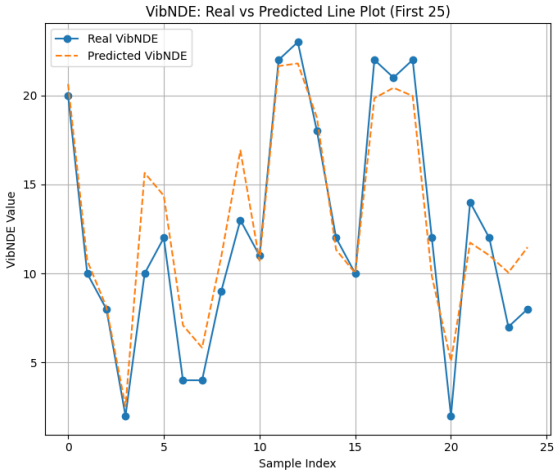


Fig. 15. RandomForest_VIB_NDE_Performance_Line.

TABLE XIV. RANDOM FOREST VIB DE PERFORMANCE

Model	RMSE	MAE	R squared
Random Forest	9.53	3.80	0.99

TABLE XV. RANDOM FOREST VIB NDE PERFORMANCE

Model	RMSE	MAE	R squared
Random Forest	3.58	2.16	0.83

9) Random forest model ampere prediction-insights and visual analysis: The visual representation in Fig. 16 offers a detailed examination of the Random Forest model's efficacy in predicting Ampere values. Utilizing line plots, these visualizations facilitate a comprehensive comparison of the

initial 25 predictions made by the Random Forest model against the actual values. Applying a logarithmic function enhances interpretability and normalization of the data, resulting in a clearer representation of the Random Forest model's predictive accuracy. Focusing on the first 25 predictions prevents visual congestion, allowing a detailed examination of early-stage accuracy and providing valuable insights into the model's predictive behavior for Ampere values.

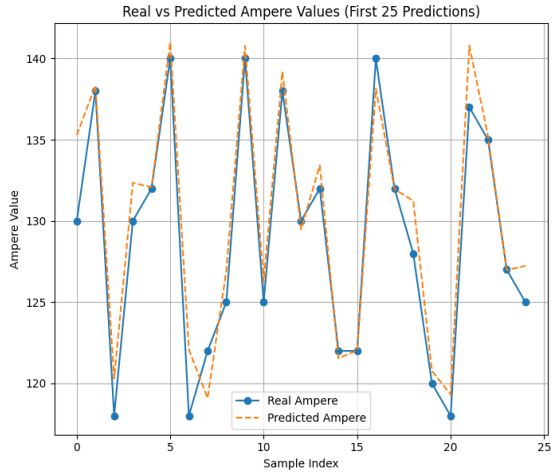


Fig. 16. Random Forest Model - Line Plot Analysis of Actual vs. Predicted Ampere Values (First 25 Predictions).

The performance metrics for Ampere prediction using the Random Forest model, as presented in Table 16, showcase its commendable accuracy. With a low RMSE of 2.96 and a close match between predicted and actual values indicated by an MAE of 2.10, the model demonstrates robust predictive capabilities. The high R-squared value of 0.83 further emphasizes its ability to explain a substantial proportion of the variance in Ampere measurements. In summary, these metrics affirm the Random Forest model's effectiveness in delivering accurate Ampere predictions, underscoring its potential for reliable forecasting in relevant applications.

TABLE XVI. RANDOM FOREST MODEL METRICS FOR AMPERE PREDICTION

Model	RMSE	MAE	R squared
Random Forest	2.96	2.10	0.83

B. Ensemble Approach for Maintenance Prediction

Ensembling XGBoost, LightGBM, and Random Forest models in maintenance prediction, as shown in Fig. 17, combines their predictive outputs to boost accuracy and robustness. This approach capitalizes on the unique strengths of each model—XGBoost's efficiency, LightGBM's speed, and Random Forest's robustness. By fusing these models, the ensemble leverages their collective intelligence, mitigating individual weaknesses. The visual in Fig. 17 illustrates how this collaboration forms a cohesive and reliable maintenance prediction framework, enhancing resilience to uncertainties and improving overall effectiveness in complex scenarios.

To improve predictive outcomes, an ensembling approach combines three models—XGBoost, LGBM, and Random Forest. Ensemble learning—leveraging the strengths of multiple models, mitigating risks of overfitting and underfitting, and enhancing predictive accuracy [17]. It addresses common ML challenges, making models more robust and stable. Ensemble learning excels in capturing complex data relationships, proving effective in scenarios where a single model may struggle. In the voting mechanism, soft voting is preferred for its regression nature. Soft voting, averaging predicted probabilities, offers a nuanced approach over hard voting, which is particularly beneficial when models exhibit varying confidence levels. The advantages of soft voting include enhanced predictive performance and flexibility, making it suitable for imbalanced datasets. In conclusion, strategic ensembling—especially through soft voting—stands as a simple yet effective method for improving ML model performance, particularly in scenarios with varying confidence levels.

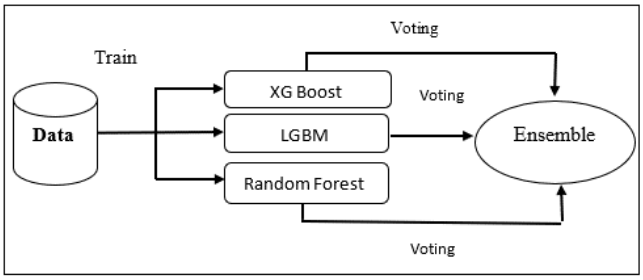


Fig. 17. Ensemble of XGBoost, LightGBM, and Random Forest Models for Maintenance Prediction.

1) Results and analysis of ensemble model prediction for seal pressure: The results from the evaluation of the pump's seal pressure models, presented in Tables XVII and XVIII, demonstrate the performance of XGBoost, LGBM, Random Forest, and the ensemble approach. For Seal Pressure 1 (Table XVII), the standalone models perform well: XGBoost (RMSE: 5.61, MAE: 2.38, R-squared: 0.93); LGBM (RMSE: 5.29, MAE: 2.22, R-squared: 0.94); and Random Forest (RMSE: 4.86, MAE: 2.01, R-squared: 0.95). The Ensemble model significantly outperforms these, with RMSE: 1.94, MAE: 0.92, and R-squared: 0.99. Similarly, for Seal Pressure 2 (Table XVII), the standalone models show strong performance: XGBoost (RMSE: 9.41, MAE: 4.87, R-squared: 0.91); LGBM (RMSE: 8.98, MAE: 5.17, R-squared: 0.91); and Random Forest (RMSE: 9.24, MAE: 4.49, R-squared: 0.91). Again, the Ensemble model achieves superior results, with RMSE: 2.94, MAE: 1.74, and R-squared: 0.99. These findings underscore the Ensemble model's enhanced predictive capabilities for both Seal Pressure 1 and Seal Pressure 2. The marked improvement in RMSE, MAE, and R-squared values indicates that the ensemble approach effectively combines the strengths of XGBoost, LGBM, and Random Forest, leading to higher accuracy and reduced prediction errors.

TABLE XVII. INDIVIDUAL AND ENSEMBLE MODEL METRICS FOR SEAL PRESSURE 1

Model	RMSE	MAE	R squared
XGBoost	5.61	2.38	0.93
LGBM	5.29	2.22	0.94
Random Forest	4.86	2.01	0.95
Ensemble	1.94	0.92	0.99

Table XVIII provides an insightful comparison of metrics for Seal Pressure 2. The standalone models (XGBoost, LGBM, Random Forest) exhibit respectable performance, while the Ensemble model consistently outshines them across all metrics. This emphasizes the Ensemble model's effectiveness in enhancing accuracy and reducing errors in predicting Seal Pressure 2.

TABLE XVIII. INDIVIDUAL AND ENSEMBLE MODEL METRICS FOR SEAL PRESSURE 2

Model	RMSE	MAE	R squared
XGBoost	9.41	4.87	0.91
LGBM	8.98	5.17	0.91
Random Forest	9.24	4.49	0.91
Ensemble	2.94	1.74	0.99

From Tables XVII and XVIII, it is evident that, for both Seal Pressures 1 and 2, the error rate is notably higher when employing stand-alone models compared to the Ensemble model. Utilizing three distinct error metrics—root mean squared, mean average precision, and error squared—we consistently observe that the Ensemble model outperforms each of the stand-alone models. This observation underscores the potential of combining multiple models into an ensemble, demonstrating its efficacy in achieving heightened accuracy and minimizing prediction errors across diverse evaluation metrics. Fig. 18 offers a visual representation of the Ensemble model's performance in predicting Seal Pressure 1, employing line plots to compare the initial 25 predictions with their actual values. The visual presentation underscores the effectiveness of the Ensemble model through line plots, providing a comprehensive analysis of its accuracy in predicting the first 25 observations of Seal Pressure 1. The application of a logarithmic function to the values serves the dual purpose of enhancing the visualization's clarity and maintaining a normalized scale. This transformation results in a more distinct and less cluttered representation of the model's performance. Focusing on the initial 25 predictions ensures a detailed examination of the Ensemble model's accuracy during the initial phase, contributing to a nuanced understanding of its predictive behavior. This approach also helps to prevent overcrowding in the graphs, ensuring that the visual representation remains interpretable and focused. These visualizations, in conjunction with quantitative metrics, contribute to a comprehensive evaluation of the Ensemble model's reliability and effectiveness in predicting Seal Pressure 1. The integration of visual and quantitative assessments enhances the overall understanding of the model's predictive capabilities and aids in decision making for real-world applications.

Fig. 19 explores the Ensemble model's performance in predicting Seal Pressure 2, comparing the initial 25 predictions with actual values using line plots. The visual representation highlights the model's accuracy, providing a comprehensive analysis of its performance. Applying a logarithmic function enhances clarity and maintains a normalized scale, resulting in a clearer and more distinct representation. Focusing on the initial 25 predictions allows for a detailed examination of the model's accuracy during the early phase, contributing to a nuanced understanding of its predictive behavior. This approach ensures interpretability by preventing graph overcrowding. The visualizations, complemented by quantitative metrics, offer a thorough evaluation of the Ensemble model's reliability and effectiveness in predicting Seal Pressure 2, enhancing the overall understanding of its predictive capabilities for real-world applications.

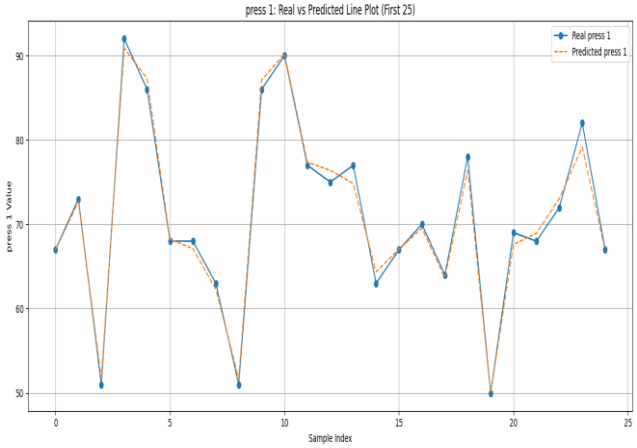


Fig. 18. Ensemble Model—Line Plot Analysis of Actual vs. Predicted Seal Pressure 1 (First 25 Predictions).

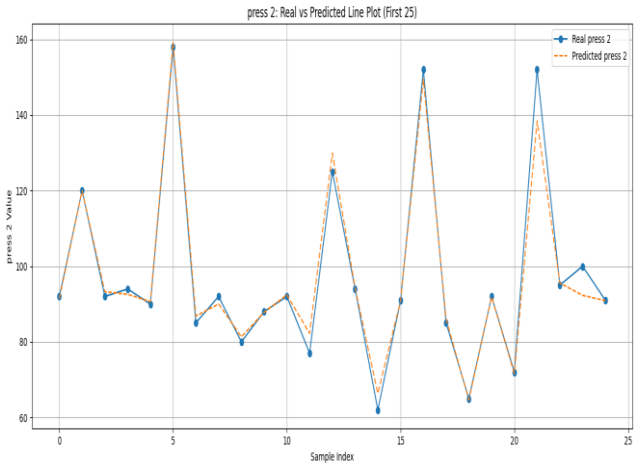


Fig. 19. Ensemble Model—Line Plot Analysis of Actual vs. Predicted Seal Pressure 2.

The examination of both the tables and graph reveals a noticeable elevation in error metrics for individual models. However, a compelling contrast emerges when these models are amalgamated, resulting in a substantial reduction in error, as evidenced by the graphical representations. This improvement is distinctly illustrated by the diminished variance between the

actual and predicted lines in the line graph. A comparative analysis of the line graphs for the Ensemble model's underscores the significant enhancement achieved by combining individual models, resulting in a more accurate and reliable predictive outcome.

2) Results and analysis of ensemble model prediction for vibration prediction: The evaluation of the Vibration Diagnoses Equipment (VIB DE) and Vibration Non-Diagnoses Equipment (VIB NDE) models provides valuable insights into their predictive performance for bearing vibrations using RMSE, MAE, and R-squared metrics. In Table XIX, the VIB DE models show high RMSE values, indicating substantial prediction errors, with the LGBM model having an exceptionally high RMSE of 45.22. However, the Ensemble model reduces the RMSE to 8.60, demonstrating the effectiveness of combining the models. The decline in MAE and consistently high R-squared values further emphasize the Ensemble model's superior ability to reduce prediction errors and improve accuracy.

TABLE XIX. INDIVIDUAL AND ENSEMBLE MODEL METRICS FOR VIB DE MODEL METRICS

Model	RMSE	MAE	R squared
XGBoost	6.32	3.80	0.99
LGBM	45.22	6.07	0.99
Random Forest	9.53	3.80	0.99
Ensemble	8.60	1.42	0.99

In Table XX, individual models such as LGBM and Random Forest show notable RMSE values for VIB NDE evaluation. The Ensemble model significantly enhances accuracy with lower RMSE and MAE and higher R-squared values. Interestingly, XGBoost slightly outperforms the Ensemble for VIB DE, indicating algorithmic influence. Graphical and tabular presentations consistently illustrate the Ensemble model's superior performance in error metrics, emphasizing its effectiveness in predicting and managing vibration issues in critical system maintenance.

TABLE XX. INDIVIDUAL AND ENSEMBLE MODEL METRICS FOR VIB NDE MODEL METRICS

Model	RMSE	MAE	R squared
XGBoost	3.34	3.80	0.99
LGBM	3.46	2.32	0.84
Random Forest	3.58	2.16	0.83
Ensemble	1.17	0.75	0.98

Fig. 20 showcases the ensemble of XGBoost, LightGBM, and Random Forest models, leveraging their strengths for accurate and robust maintenance predictions. By integrating diverse perspectives, the ensemble enhances resilience to uncertainties, offering a comprehensive solution for complex operational scenarios. This collaborative approach mitigates individual weaknesses, leading to improved performance compared to standalone models and enhancing the effectiveness of maintenance prediction systems.

Examining the table and graphs reveals notable error metrics for individual models, indicating relatively high errors. However, a significant improvement is evident when these models are integrated into an ensemble. The comparison of actual and predicted lines in the line graph vividly illustrates this enhancement. The Ensemble model, depicted in the graphs, showcases a considerable reduction in error compared to individual models.

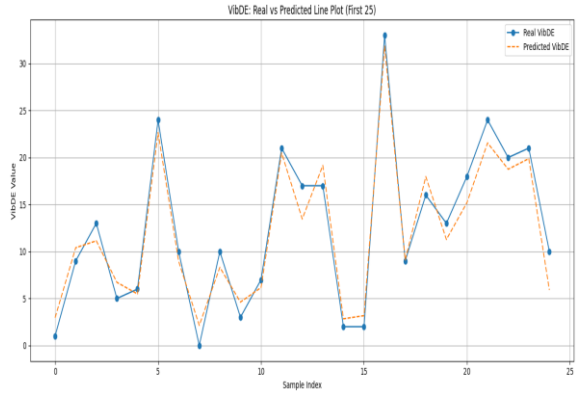


Fig. 1. Ensemble Model's Performance for VIB NDE (Line Graphs).

3) Results and analysis of ensemble model prediction for ampere prediction: When evaluating power consumption, Ampere readings serve as a crucial parameter, with higher readings indicative of increased power consumption. In scenarios where direct current measurements are unavailable, employing ML models becomes a viable option for prediction. In this context, three distinct models—XGBoost, LGBM, and Random Forest—were implemented to forecast Ampere readings. Subsequently, these models were amalgamated into an Ensemble model to harness their collective predictive capabilities. The performance metrics, including RMSE, mean average error (MAE), and R-squared values, were employed to assess the accuracy of each model and the Ensemble model's. The results are presented in Table XXI.

TABLE XXI. AMPERE PREDICTION MODEL PERFORMANCE METRICS

Model	RMSE	MAE	R squared
XGBoost	3.28	2.25	0.79
LGBM	3.08	2.26	0.82
Random Forest	2.96	2.10	0.83
Ensemble	1.69	0.94	0.95

Analysis of the table indicates a substantial decrease in error rates when utilizing the Ensemble model as opposed to individual models. Employing three distinct error metrics consistently demonstrates the superior performance of the Ensemble model, affirming its effectiveness in achieving heightened accuracy and minimizing prediction errors. This underscores the value of combining diverse models to enhance predictive capabilities. The visual representation above showcases the performance of the Ensemble model for the Ampere prediction. Utilizing line graph in Fig. 21, the graph allows a comparison of the first 25 predictions with their actual

values. To enhance clarity and minimize clutter, a logarithmic function has been applied to the values, resulting in a more normalized and visually accessible presentation. The decision to focus on 25 predictions ensures a concise and uncluttered depiction, facilitating a clear understanding of the Ensemble model's effectiveness in predicting Ampere values.

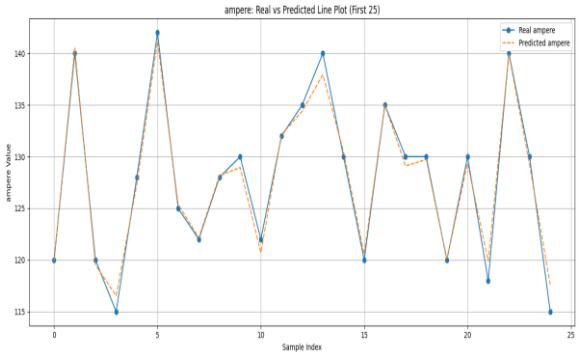


Fig. 2. Line Graph for Ampere Ensemble Model Performance.

Fig. 21 illustrates the performance of the Ensemble model for the Ampere prediction. These visualizations showcase a comparison between the first 25 predictions and their actual values, employing both bar and line graphs. To enhance clarity and maintain a cleaner display, a logarithmic function has been applied to the values, ensuring a more balanced scale. The limited focus on 25 predictions prevents graph overcrowding, facilitating a more straightforward interpretation of the results.

IV. Discussion

This study presents a novel approach to predictive maintenance (PdM) in the oil and gas industry by utilizing an ensemble of three machine learning algorithms—XGBoost, Light Gradient-Boosting Machine (LGBM), and Random Forest. The ensemble model consistently outperformed individual models, demonstrating superior accuracy and reliability across all operational parameters (Seal Pressure 1, Seal Pressure 2, VIB DE, VIB NDE, and Ampere). Notably, the Ensemble model showed lower Root Mean Square Error (RMSE) and Mean Absolute Error (MAE) values and higher R-squared coefficients, indicating better performance in predicting the health of water injection pumps (WIPs). This finding aligns with research conducted by Zhang et al. [1], where combining multiple machine learning models improved prediction accuracy in industrial applications. The novelty of this study lies in the hybridization of these models to predict diverse operational parameters, which is an improvement over the standalone approaches often used in previous research. For example, Janssens et al. [2] applied Convolutional Neural Networks (CNNs) to detect anomalies using infrared thermal images, but the study was limited in its ability to handle different operational variables. Similarly, Sampaio et al. [3] explored Artificial Neural Networks (ANNs) for motor failure prediction but did not consider the comprehensive evaluation of various predictive models. The Ensemble model, in contrast, demonstrates a broader applicability by leveraging the strengths of multiple algorithms, thus mitigating the individual limitations of each method and achieving more robust and reliable predictions. Furthermore, the results of this study highlight the importance of addressing operational parameters beyond vibration data, such as seal pressure and amperage, which are often overlooked in predictive maintenance studies. This is in contrast to previous studies that focused primarily on vibration data for fault detection and failure prediction [4], [5]. By including additional operational parameters, this research provides a more holistic approach to predictive maintenance, which could lead to more effective early detection of potential failures in WIPs, ultimately reducing unplanned downtime and improving operational efficiency. The ensemble approach presented in this study also reflects a growing trend in the literature toward integrating multiple machine learning techniques to enhance the accuracy of PdM models. This is consistent with the findings of Kim et al. [6], who demonstrated that ensemble methods, when applied to predictive maintenance in industrial equipment, resulted in significant improvements in both prediction accuracy and reliability. The success of the ensemble model in this study suggests that further refinement and adaptation of this methodology could be applied to other critical equipment within the oil and gas industry, as well as other industrial sectors facing similar challenges with unplanned downtime. In sum, the findings of this study contribute to the growing body of research on predictive maintenance by offering an innovative methodology for improving the accuracy of failure predictions in water injection pumps. The ensemble model's superior performance, when compared to individual models, underscores the potential for more accurate and reliable predictive systems in industrial applications. The results also pave the way for further exploration of hybrid machine learning models in PdM, particularly in industries with complex operational environments, such as oil and gas.

V. Limitations

The Ensemble model, comprising XGBoost, LGBM, and Random Forest, demonstrates commendable predictive accuracy across diverse operational parameters. However, it is imperative to acknowledge certain limitations inherent in the approach. First, the efficacy of the Ensemble model is highly contingent on the quality of the input data. Instances of data inconsistencies, inaccuracies, or a lack of representativeness concerning diverse operating conditions can potentially compromise the performance. Moreover, the representativity of the training set plays a pivotal role. The Ensemble model relies on a training dataset that effectively captures the various operating scenarios of the pump system. Notably, the study focused on predicting pressure, vibration, and amperage for temperature, while considering other features that could contribute to PdM in WIPs within the OGI. These limitations underscore the importance of meticulous data quality assurance, comprehensive representation in training datasets, and ongoing refinement of hyperparameter configurations for the reliable and robust application of the Ensemble model in PdM scenarios.

VI. Future Research Direction

The Ensemble model, comprising XGBoost, LGBM, and Random Forest, consistently demonstrates notable predictive accuracy for various operational parameters in WIPs. However, the model's performance is contingent on high-quality input data and a representative training set. Notably, the sensitivity to hyperparameter configurations requires ongoing optimization

efforts. Future research directions could explore advanced ensemble techniques beyond the current models and dynamic hyperparameter tuning mechanisms for autonomous adaptation. Investigating the impact of external factors, transitioning to real-time predictions, enhancing explainability, scalability testing, and integrating the model into existing maintenance systems are promising avenues. Seeking feedback from industry practitioners is vital for refining the model's real-world applicability.

VII. Conclusions

In conclusion, this study demonstrates the effectiveness of combining multiple machine learning algorithms—XGBoost, LGBM, and Random Forest—into an Ensemble model for predictive maintenance of water injection pumps. The Ensemble model consistently outperforms individual algorithms, showcasing superior accuracy through lower RMSE and MAE values, as well as higher R-squared coefficients. By integrating the strengths of these algorithms, the Ensemble model mitigates the limitations of standalone models, offering a more robust and reliable predictive maintenance tool. The results underscore the potential for improving operational efficiency and reducing unplanned downtime in the oil and gas industry. This research not only advances predictive modeling techniques but also highlights the significant implications for enhancing maintenance strategies in industrial applications, ensuring better asset management and cost-effectiveness in critical systems.

References

[1] Gupta, D.; Shah, M. A comprehensive study on artificial intelligence in oil and gas sector. Environ. Sci. Pollut. Res. 2022, 29, 50984–50997.

[2] Trevathan, M.M.T. The Evolution, Not Revolution, of Digital Integration in Oil and Gas. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2020

[3] Almazrouei, S.; Dweiri, F.; Aydin, R.; Alnaqbi, A. A review on the advancements and challenges of artificial intelligence based models for predictive maintenance of water injection pumps in the oil and gas industry. SN Appl. Sci. 2023, 5, 391.

[4] Chen, C.; Fu, H.; Zheng, Y.; Tao, F.; Liu, Y. The advance of digital twin for predictive maintenance: The role and function of machine learning. J. Manuf. Syst. 2023, 71, 581–594.

[5] Ngu, K.M.; Philip, N.; Sahlan, S. Proactive and predictive maintenance strategies and application for instrumentation & control in oil & gas industry. Int. J. Integr. Eng. 2019, 11, 119–130.

[6] Manchadi, O., Ben-Bouazza, F.E., & Jioudi, B. Predictive Maintenance in healthcare system: A Survey. IEEE Access 2023, 11, 61313–61330

[7] Omri, F.; Choura, O.; Taieb, L.H.; Elaoud, S. Prediction of Bearing Fault Effect on the Hydraulic Performances of a Centrifugal Water Pump. J. Vib. Eng. Technol. 2022, 10, 1905–1915.

[8] Xiang, C.; Li, B. Research on ship intelligent manufacturing data monitoring and quality control system based on industrial Internet of Things. Int. J. Adv. Manuf. Technol. 2020, 107, 983–992.

[9] Hornyák, O. The Role of Condition-Based Maintenance in Minimizing Operational Costs. Prod. Syst. Inf. Eng. 2023, 11, 43–53.

[10] Aissani, N.; Beldjilali, B.; Trentesaux, D. Dynamic scheduling of maintenance tasks in the petroleum industry: A reinforcement approach. Eng. Appl. Artif. Intell. 2009, 22, 1089–1103.

[11] Compare, M.; Baraldi, P.; Zio, E. Challenges to IoT-enabled predictive maintenance for industry 4.0. IEEE Internet Things J. 2019, 7, 4585–4597.

[12] Saputelli, L.; Palacios, C.; Bravo, C. Case Studies Involving Machine Learning for Predictive Maintenance in Oil and Gas Production Operations. In Machine Learning Applications in Subsurface Energy Resource Management. CRC Press: Boca Raton, FL, USA, 2022; pp. 313–336.

[13] Janssens, O.; Van de Walle, R.; Loccufier, M.; Van Hoecke, S. Deep learning for infrared thermal image based machine health monitoring. IEEE/ASME Trans. Mechatron. 2017, 23, 151–159.

[14] Scalabrini Sampaio, G.; Vallim Filho, A.R.d.A.; Santos da Silva, L.; Augusto da Silva, L. Prediction of motor failure time using an artificial neural network. Sensors 2019, 19, 4342.

[15] Bekar, E.T.; Nyqvist, P.; Skoogh, A. An intelligent approach for data pre-processing and analysis in predictive maintenance with an industrial case study. Adv. Mech. Eng. 2020, 12, 1687814020919207.

[16] Otchere, D.A.; Ganat, T.O.A.; Gholami, R.; Lawal, M. A novel custom ensemble learning model for an improved reservoir permeability and water saturation prediction. J. Nat. Gas Sci. Eng. 2021, 91, 103962.

[17] Susto, G.A.; McLoone, S.; Pagano, D.; Schirru, A.; Pampuri, S.; Beghi, A. Prediction of integral type failures in semiconductor manufacturing through classification methods. In Proceedings of the 2013 IEEE 18th Conference on Emerging Technologies & Factory Automation (ETFA), Cagliari, Italy, 10–13 September 2013; pp. 1–4.

[18] Praveenkumar, T.; Saimurugan, M.; Krishnakumar, P.; Ramachandran, K.I. Fault diagnosis of automobile gearbox based on machine learning techniques. Procedia Eng. 2014, 97, 2092–2098.

[19] Kumar, A.; Shankar, R.; Thakur, L.S. A big data driven sustainable manufacturing framework for condition-based maintenance prediction. J. Comput. Sci. 2018, 27, 428–439. https://doi.org/10.1016/j.jocs.2017.06.006.

[20] Kolokas, N.; Vafeiadis, T.; Ioannidis, D.; Tzovaras, D. Forecasting faults of industrial equipment using machine learning classifiers. In Proceedings of the 2018 Innovations in Intelligent Systems and Applications (INISTA), Thessaloniki, Greece, 3–5 July 2018; pp. 1–6.

[21] Liu, L.; Liu, W. Calculation method of water injection forward modeling and inversion process in oilfield water injection network. AIP Conf. Proc. 2018, 1955, 040065.

[22] Aziz, N.; Abdullah, M.H.A.; Osman, N.A.; Musa, M.N.; Akhir, E.A.P. Predictive Analytics for Oil and Gas Asset Maintenance Using XGBoost Algorithm. In The International Conference on Emerging Technologies and Intelligent Systems; Springer International Publishing: Cham, Switzerland, 2022; pp. 108–117.

[23] Shehadeh, A.; Alshboul, O.; Al Mamlook, R.E.; Hamedat, O. Machine learning models for predicting the residual value of heavy construction equipment: An evaluation of modified decision tree, LightGBM, and XGBoost regression. Autom. Constr. 2021, 129, 103827.

[24] Udo, W.; Muhammad, Y. Data-driven predictive maintenance of wind turbine based on SCADA data. IEEE Access 2021, 9, 162370–162388.

[25] Salim, K.; Hebri, R.S.A.; Besma, S. Classification predictive maintenance using XGboost with genetic algorithm. Rev. Intell. Artif. 2022, 36, 833.

[26] Hu, Z.; Chan, C.W. In-situ bioremediation for petroleum contamination: A fuzzy rule-based model predictive control system. Eng. Appl. Artif. Intell. 2015, 38, 70–78.

[27] Hosseinzadeh, A.; Chen, F.F.; Shahin, M.; Bouzary, H. A predictive maintenance approach in manufacturing systems via AI-based early failure detection. Manuf. Lett. 2023, 35, 1179–1186.

[28] Wang, M.; Shen, K.; Tai, C.; Zhang, Q.; Yang, Z.; Guo, C. Research on fault diagnosis system for belt conveyor based on internet of things and the LightGBM model. PLoS ONE 2023, 18, e0277352.

[29] Kizito, R.; Scruggs, P.; Li, X.; Kress, R.; Devinney, M.; Berg, T. The Application of Random Forest to Predictive Maintenance. In Proceedings of the 2018 IIE Annual Conference, Orlando, FL, USA, 19–22 May 2018; pp. 354–359; Institute of Industrial and Systems Engineers (IISE): Peachtree Corners, GA, USA, 2018.

[30] Chazhoor, A.; Mounika, Y.; Sarobin, M.V.R.; Sanjana, M.V.; Yasashvini, R. Predictive maintenance using machine learning based classification models. IOP Conf. Ser. Mater. Sci. Eng. 2020, 954, 012001.

Performance Evaluation of the AuRa Consensus Algorithm for Digital Certificate Processes on the Ethereum Blockchain

Robiah Arifin[1]*, Wan Aezwani Wan Abu Bakar[2]*, Mustafa Man[3], Evizal Abdul Kadir[4]
Department of Big Data, Infostructure and Network Management Centre, Universiti Sultan Zainal Abidin, 21030 Kuala Nerus, Terengganu, Malaysia[1]
Faculty of Informatics and Computing-Universiti Sultan Zainal Abidin, 22200 Besut Campus, Besut, Terengganu, Malaysia[2]
Faculty of Computer Science and Mathematics-Universiti Malaysia Terengganu, 21030 Kuala Nerus, Terengganu, Malaysia[3]
Universitas Islam Riau, Jl. Kaharuddin Nasution 113, Pekanbaru 28284, Riau, Indonesia[4]

Abstract*—The blockchain serves as a distributed database where data is stored across different servers and networks. It encompasses various types, with Bitcoin, Ethereum, and Hyperledger being notable examples. To safeguard the security of data transactions on the blockchain, it relies on a consensus algorithm. This algorithm facilitates agreement among nodes within the network. There are multiple types of consensus algorithms, each possessing unique specialties and characteristics. This paper drives into the examination of specific Authority Round, here claimed as AuRa_ori consensus algorithm. The AuRa_ori is a specific type of PoA consensus mechanism used primarily in private or permission blockchain networks. It works by having a set of trusted validators take turns in a round-robin fashion to produce new blocks. It is supported by Parity and Ethereum Clients. AuRa_ori assumes that all the authority nodes are synchronised and honest on every transaction process. In AuRa_ori, every transaction process will execute the four phases i.e., assigning of a new leader, proposing a block, commencing agreement and finally, the phase of committing. However, there exist some discrepancies in some of the phases. In response to the scenario, this paper presents a thorough discussion on the vulnerabilities adhered in AuRa phases in transaction execution by focusing on the first phase of assigning a new leader and the third phase, namely the agreement. The vulnerabilities are subjected to the risk of impacting the performance of Transaction Speed Per Second (TPS), Transaction Throughput (TGS), Percentage Decrease (PD) of TPS and Percentage Increase (PI) of TGS. The new improved method, named AuRa_v1 is parallel presented to overcome the vulnerabilities of AuRa_ori at the selected phases. It aims to increase the TPS and to calculate the PD in transaction process using the Ethereum private blockchain systems. The implementation used three set of data scroll certificate. The result showed that the AuRa_v1 able to decrease the TPS almost 30% based on difference number set of data.

Keywords*—Blockchain; Ethereum; consensus algorithm; smart contract; AuRa_ori; AuRa_v1

I. Introduction

The section drives the important components within the scope of the paper discussion on the AuRa_ori algorithm starting from the introduction of the blockchain technology, the platform that offers the technology, to what component and algorithm that determines the efficiencies of the blockchain technology. The efficiency determinants of the blockchain relies on the robustness of the consensus algorithm, wherein the discussion on the AuRa_ori is initiated. The consensus algorithms are crucial in further bolstering security within blockchain transactions by orchestrating an agreement among nodes. This ensures that the throughput remains consistent, uniform, and valid across the network.

Blockchain, as a decentralised distributed database, serves as a platform for storing transactional data and information. It represents a departure from traditional methods, transitioning data management from a single centralised location to a decentralised setup across various servers or networks [1]. This decentralised data storage comprises a series of interconnected records known as blocks [2].

Data is dispersed among different nodes across diverse servers within the blockchain network. Often referred to as a peer-to-peer (P2P) network, blockchain operates through nodes communicating directly with each other [3]. Utilising cryptographic techniques and hash functions, blockchain ensures the security and integrity of digital data stored within its system [4].

While blockchain encompasses several types, Bitcoin, Ethereum, and Hyperledger stand out as the most popular and widely used variants [5], [6]. These platforms have been developed over the years with a focus on encouraging businesses to integrate blockchain into their operations [7]. Despite their similarities, each blockchain platform possesses unique characteristics. Ethereum, conceptualized by Vitalik Buterin in 2013 [8], emerged as a response to the limitations of Bitcoin [9]. Crowdfunding in 2014 facilitated the advancement of Ethereum's technologies, leading to its live network launch in 2015 [10].

Ethereum implements distributed data storage, enabling users to deploy their applications and operate their blockchain instances [11]. Notably, Ethereum offers the capability to store data with an unlimited block size [12]. Specifically, the AuRa_ori consensus algorithm is used in voting domain and focusing on the electronic voting application. The researcher was comparing the AuRa_ori and Geth based on certain criteria such as time, consistency, and scalability. This application runs

the test net environment including remix IDE, Ethereum test net and web3.

Additionally, the efficiency of blockchain is reinforced by the consensus algorithm, which facilitates an agreement process among nodes dispersed across various servers and networks. This algorithm ensures the maintenance of consistency and decentralisation among nodes within the blockchain system [4], [13],[14]. The consensus mechanism necessitates four essential elements in transactions, as outlined in Table I.

TABLE I. Element of consensus algorithm

Element	Description
Termination	The successful transaction process dependence on the content of block that proposed
Agreement	The acceptance block needed to assign by the honest authorities
Validity	The block should be accepted if nodes that received is valid and same with the proposed block
Integrity	Only the honest node should be acceptance their transaction

There are numerous types of consensus algorithms that are able to support the security of data transaction in blockchain environment. However, this paper provides the detailed exposure of the consensus algorithms in conjunction to the strengths and the weaknesses in AuRa_ori used in Ethereum and reveals and proposes the improvement mechanism as a means of solution on the weaknesses.

There are numerous types of consensus algorithms that are able to support the security of data transaction in blockchain environment. However, this paper aim discussed the detail AuRa_ori including it procedure to transact data into the blockchain. We also provide the detailed exposure of the consensus algorithms in conjunction to the strengths and the weaknesses in AuRa_ori used in Ethereum environment.

Prior to the weakness of AuRa, the analysis of the effect of AuRa weakness in term of transaction speed was executed. The weakness is able to expose the risk including the cloning attack and malicious leader. Then the improvement mechanism as a means of solving weaknesses were proposed and revealed.

II. AURA_ORI CONSENSUS ALGORITHM

AuRa_ori, short for Authority Round, was initially proposed for the Parity client, which utilises Rust as its programming language [15]. This consensus relies on the assumption of honest authorities and synchronous network communication among nodes. If any issues such failed to assign a new leader or leader failed to produce the signature the process must be repeat at beginning. This impact the throughput and transaction process. Additionally, AuRa_ori consists of four key steps including assigned a new leader, proposed block, agreement and commit transaction into the blockchain. This consensus mechanism has been implemented by various platforms including Laava, VecHain Thor, xDai DPOS network, Microsoft Azure (for deployment only), and Kovan Testnet [16].

AuRa_ori has gained widespread adoption in blockchain applications, with nearly 4,000 projects implementing this consensus algorithm [17]. For example, AuRa_ori was implemented in health domain focused on health record sharing. The researcher proposed new methods to improve the time in block transaction process of AuRa_ori [18]. The AuRa_ori is well implemented to support the Copyright System in [19]. This effort drives the implementation of AuRa_ori and performs the analysis of its transaction throughput. It also concerns about the network synchronisation.

A. Assigning a New Leader

Initially, a leader is assigned, with each authority taking turns using the Round Robin Algorithm [20]. The leader assignment process involves calculating the difference value t_d) between the current timestamp t and the last timestamp at the genesis t_g as shown in Eq. (1).

$$t_d = t - t_g \tag{1}$$

Where t_d is a difference values of t and t_g . While$t$ is a current timestamp and t_g is the last time stamp at the genesis. After getting the values of t_d, next is to assign the leader among the authorities based on Eq. (2).

$$i = \frac{t_d}{D} \, mod n \tag{2}$$

In the formula, i represents the node tasked with assigning a leader, while D stands for the Step Duration specified in the genesis file. The n denotes the number of nodes configured in the blockchain environment. Following the assignment of the leader based on this formula, the subsequent step involves the leader proposing a block.

B. Propose Block

The block that proposed by a leader based on set of values, there are data v on t_p , number of proposed blocks n and signature of authorities account on leader v_s. Every proposed block process must include the set value $\{v, n, v_s\}$. Based on set values the other authorities will apply the voting process.

C. Agreement

After finding the leader and proposing the block $\{v, n, v_s\}$, the next step is agreement among the nodes. The block that was proposed agreed or not by the authorities depends on data on proposed block v, numbering of proposed block n and the authorities account on leader is different v_s. After getting the agreement result from the authorities, The data will transfer to block transaction queue that declare as t_q. Then after the authorities 'members complete their agreement process, the next step is the voting process based on Eq. (3).

$$2f + 1 \leq n \tag{3}$$

Where f is a faulty node, n is a number of nodes. In that case the number of faulty nodes at least must be less or the same as the number of nodes 50%.

D. Commit

Subsequently, the leader puts forward a block, comprising a leader signature key, current timestamp, and block data. Following the proposal of the block, the process proceeds to the

voting and acceptance phase. If the agreement achieves more than 50%, the next is the commit process. Thet_q will be inserted into the blockchain, and the value of t_q and $t_p$will be deleted from the transaction process. Fig. 1 shows the patterns of AuRa in committing the transaction data.

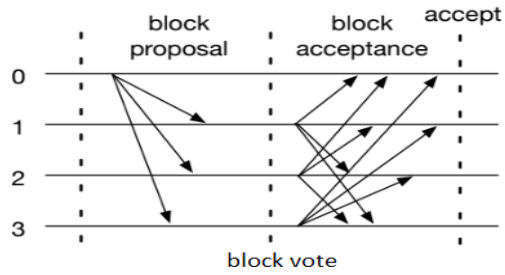


Fig. 1. Pattern of aura transaction process.

According to Fig. 1, the AuRa_ori process is bifurcated into two primary stages: block proposal and block acceptance. Once the leader is designated, the leader initiates the block proposal phase by proposing a block. Subsequently, the block acceptance phase commences, during which the members of the authority vote on the block proposed by the leader to determine if it should be committed.

III. AURA_ORI RELATED WORKS AND DRAWBACKS

The implementation of AuRa_ori can be widely seen in various domains of applications. It is considered as a stable algorithm and able to support the transaction process into the blockchain. However, the AuRa_ori is vulnerable to the exposure of attacks if the issues persist in all over the transaction process.

A. Challenges Faces in AuRa

The AuRa_ori has been widely embraced to enhance the speed of blockchain transactions. Previous research has delved into various aspects of AuRa_ori. For instance, [21] examined partitioning tolerance in AuRa_ori. The author investigates strategies for preventing partitioning tolerance in AuRa_ori. The AuRa_ori is capable of detecting only the absence status of authorities.

However, it cannot discern whether missing authorities are inactive or located in a different partition, as it lacks the ability to identify network partitioning. Lack of ability to identify availability authorities 'impact to transaction speed and throughput. It needed extra time if authorities are detected not available a long transaction process because AuRa_ori needed to assign a new leader and get the signature key from a new leader to assign data into the blockchain. Extra time was risk to any attack.

Additionally, the study in [22] conducted research on transaction speeds using the Geth and Parity clients. Both Geth and Parity support by PoA, with Geth focusing on Clique and Parity on AuRa_ori. On average, the Parity client exhibited a 91% faster transaction speed compared to Geth. The experiment based on transaction data from 1000 to 5000. The comparison is conducted on a private test net, considering factors such as CPU, RAM, and the number of nodes. The performance analysis criteria included the time, consistency and scalability. However, it does not consider the security and safety criteria in this analysis.

Furthermore, the study in [23] discussed a comparison between Geth and Parity in terms of transaction speed and performance level. Their analysis cantered on the consumption of CPU and RAM resources by the two Ethereum clients. However, this research did not specify the type of consensus utilised, and details regarding CPU, RAM, and server type were not provided. As previously noted, AuRa_ori operates under the assumption that nodes remain synchronised, which impacts both availability and consistency. According to prior research by [24], which focused on comparing AuRa_ori, Clique, and PBFT in terms of availability, consistency, and partition tolerance, the synchronisation requirement of AuRa poses a risk, especially when deployed over a wide area. This algorithm relies heavily on accurate timestamps for both genesis and proposed blocks.

Regarding transaction speed, [25] explored the performance of AuRa_ori in comparison to PoW. The research discussed how AuRa surpasses PoW in transaction speed due to its lower computing power requirements and higher throughput. Moreover, AuRa_ori offers the enhancement in security compared to PoW, as it incorporates an additional layer of security and operates with two levels of acceptance: the proposed block and the subsequent voting process but the voting process exploit the security issue if it needed extra time to complete the task.

B. Reviews on the Challenges that AuRa_ori Faced

The widespread implementation of AuRa_ori has sparked interest among researchers to scrutinise its intricacies. Previous studies have identified several drawbacks associated with AuRa_ori, particularly in the initial step of leader assignment and the subsequent voting agreement phase.

Assigning a new leader for each transaction process poses a challenge within AuRa_ori. To accomplish this, AuRa_ori employs a Round Robin schedule. However, if authority members are unavailable, the process of reassigning a new leader becomes necessary, resulting in decreased throughput, affecting transaction speed and time execution [19]. Because AuRa needs to assign a new leader and it increases time to complete the transaction. Then it needs to create a new fork to allow a queued transaction in proposing a new block.

Process to assign a new leader causing risk to attack including AuRa_ori assumes each node is synchronised, but sometimes unexpected network delays happen. To overcome this situation AuRa_ori allowed the authorities to postpone the validation process and cause the block to be delayed. This exploited loophole to assigned the malicious leader when the previous transaction not completed because time delay to complete the transaction.

Furthermore, complications arise if the assigned leader fails to create a signature or becomes corrupted, leading to decreased throughput and failed transactions [26]. To mitigate these issues, the concept of a dummy signature has been proposed. If authority members accept the dummy signature, it is converted

into a real signature then the transaction process is able to continue. The challenge is how to verify the dummy signature is accurate. Because this research did not explain how the dummy signature creates and verify.

Additionally, changes in assigned authorities can occur at any time, any changes requiring agreement from other authorities. Normally the changes occur if the nodes not available because of network or configuration issues. Assigning new authorities process introduces delays until the new authorities are accepted, impacting the security, performance, and transaction speed of AuRa_ori.

The election of a leader for each transaction process exposes the algorithm to potential attacks [27] because the leader needed to create the signature. The signature was used in proposed block, voting committing transactions. If the leader failed to sign a signature the new leader must assign and it impacts the execution time, throughput, transaction speed and epoch time. Additionally, the validation process among authorities before committing transactions to the blockchain requires extra time to achieve agreement, affecting throughput and potentially leading to forks.

A delayed verification can also leave AuRa_ori vulnerable to cloning attacks (CA) [28]. This occurs due to the creation of forks during delayed verification, allowing for the replication of identities using the same private and public keys. Delay verification occur if the leader failed to sign the signature or the signature not valid. Then it needed to assign new leader and new signature, then impact the execution time and potential the attacks.

To address these challenges, this paper proposes the implementation of a heartbeat-based approach to thwart cloning attacks. This involves signing and sending the heartbeats to other authorities, who then accept proposed blocks based on the heartbeat signature.

IV. Proposed Methodology

Based on previous studies, AuRa_ori is tightly bound with the transaction speed issues. These issues because of the procedure in AuRa_ori needed to assign a new leader for every transaction process and needed the verify phase before the transaction was able to commit into the blockchain. This research proposed a new algorithm called AuRa_v1 to overcome these issues.

The new proposed algorithm named AuRa_v1 consists of 4 steps including preassigned new leader, transaction pending, proposed block and voting. Numbering steps are the same with the AuRa_ori, but it's needless to assign a new leader for every transaction process. Each step in AuRa_v1 is enhanced from the AuRa_ori.

A. Predefine Leader

Predefining a leader is a process to assign a new leader as oppose to AuRa_ori where it requires the assignment of a new leader at every transaction process. In contradiction, AuRa_v1 assigns a new leader only on condition the leader that was assigned is not available, or the signature key by the previous leader is not valid. Fig. 2 highlights the detail of predefined leader procedure.

Algorithm 1

```
[1]  While true do
[2]      t_d ← TIMESTAMPDIFF(second, t - t_g)
[3]      l ← ((t_d/D) mod n)
[4]     sk ← generate by l
[5]     Transaction_Pending(sk, l, n)
[6]  End Process
```

Fig. 2. AuRa_v1 predefined leader algorithm.

The new leader assignment in Fig. 2 will be made available if and only if either the occurrence of the 2 conditions i.e., 1) the previous assigned leader is not available, or 2) the signature key owned by the previous assigned leader is not valid. Line 2 aims to get the difference value between current timestamp and genesis timestamp. The difference value based on Eq. (4).

$$t_d = t - t_g \tag{4}$$

Where value of t_d is a difference value of current timestamp t and genesis time, t_g. However, this research proposes the difference value was converted into a second based on timestamp format using the function $TIMESTAMPDIFF(second)$. We propose converting into second because it is able to improve the transaction speed. Then the value of t_d was used to choose the new leader as line 3 based on Eq. (5),

$$l = \frac{t_d}{D} mod n \tag{5}$$

Where l is new leader that was assigned and D is the value of step duration, D value can be any number in minutes or second, normally value of D setup by developer including 5 until 10 seconds. Then n is a number of authorities that register in blockchain setup.

A. Voting and Commit Transactions

Voting and commit process is the last process before the transaction is stored into the blockchain. This process there is no need to collect the agreement from the available authorities. It just counts the number of available authorities. Fig. 3 illustrates the voting and commit procedure.

Algorithm 2

```
[1]  voting(b_p, sk, l, n)
[2]  nt ← datetime.now()
[3]  If((nt - t) <= D) then
[4]    ca ← count(aa)
[5]    if ca >= 1 ∧ ca <= n) then
[6]       Commit
[7]    else
[8]       Failed
[9]  else
[10]    Failed
[11] If (l ≙ l) then
[12]    transaction_pending(sk, l)
[13] else
[14]    pre_assigned_leader()
[15] End
```

Fig. 3. Algorithm of voting and commit procedure.

In Fig. 3 at line 2 to 3, ntrefer to new current timestamp. This procedure needed to capture the new current timestamp. Then the new timestamp minus t and the value must be less or the same with step duration value D. Line 4 to 6, it counts the authorities available, if authorities available more than 1, and numbers of available authorities less or the same with the number of authorities the transaction process is able to commit into the blockchain. Lastly line 7 until 14, refer to failure completed the prerequisite, the procedure back to transaction pending or pre assigned leader process.

V. IMPLEMENTATION

This studies aims to analyst the performance of AuRa_ori and AuRa_v1. The analysis based on result of digital certificate process. The certificate process implemented into two version including AuRa_ori and AuRa_v1. To support the implementation of AuRa_ori and AuRa_v1, the installation and configuration of AuRa_v1 and AuRa_ori was executed. The installation and configuration of AuRa_ori based on standard AuRa_ori. Fig. 4 portrays the installation and configuration of the AuRa_ori.

However the installation and configuration of AuRa_v1 based on proposed algorithm of AuRa_v1. Then the node file was created for both of AuRa_ori and AuRa_v1. The number of nodes file based on the number of node that is created on AuRa_ori and AuRa_v1 engine. Fig. 5 depicts part of nodes file.

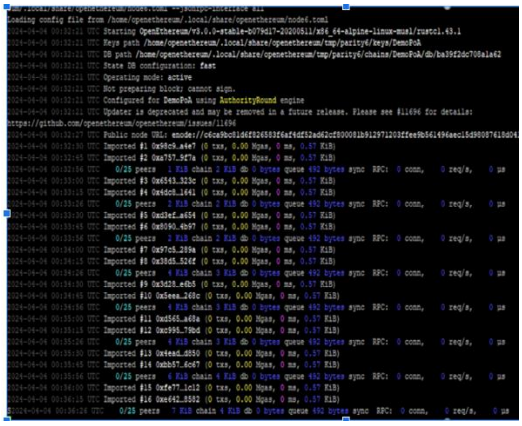


Fig. 4. The installation and configuration of aura engine.

Code1: xxx.toml

```
[1] [parity]
[2] chain = "chain directory"
[3] base_path = "aura engine directory"
[4] [network]
[5] port = 30301
[6] [rpc]
[7] port = 8541
[8] apis=["web3","eth","net","personal","parity","parity_set",
[9] "traces", "rpc", "parity_accounts"]
[10][websockets]
[11]port = 8451
[12][ipc]
[13]disable = true
```

Fig. 5. Code of parity engine configuration

Based on Fig. 5, the file $xxx.toml$ used the parity engine (line 1) and read the chain file (line2). Line 4 and 5 mention the port network that is used is 3301. Line 6 and 7 mention the Remote Procedure Call(RPC) port that used 8541. Line 8 and 9 are about dependencies that implement and line 10 - 11 is about the web sockets port used is 8451.

Besides that, this study also require created the smart contract file. Smart contract is a special element in Ethereum, it consists of the business logic for executing the command of user requirement. After the completed the smart contract, the next step is to migrate the smart contract with the both AuRa_v1 and AuRa_ori engine. The migration process used the truffle framework. The truffle engine is needed for installation and configuration as denoted in Fig. 6 while the three sets of scroll datasets are characterised as in Table II.

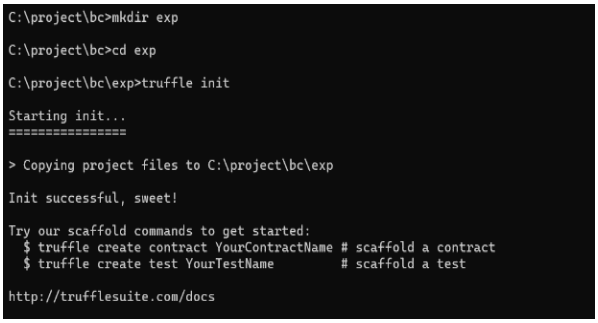


Fig. 6. The truffle framework installation.

TABLE II. SET OF DATA

Set of Data	Number of Data	Size per Data	Type of Data
Set 1	1021	32.8KB - 33.01KB	Scroll
Set 2	2435	32.2KB - 33.11KB	Scroll
Set 3	3422	32.5KB - 33.07KB	Scroll

Referring to Table II, Set 1 includes 1021 data, set 2, 2435 data and set 3 with 3422 data. These data consist information of scroll student including name, program and final cumulative grade. These 3 sets of data are being executed in transaction process on both AuRa_ori and AuRa_v1.

Additionally, the research has also developed the frontend interface to generate the digital certificate. The interface connected with both AuRa_ori, and AuRa_v1 through the Application Programmers Interface (API) and backend code as depicted at Fig. 7.

The front-end consists of a few modules including the dashboard, create certificate and verification. These function able to access regarding the user access level. Fig. 8, Fig. 9 and Fig. 10 show the development interfaces done during experimentation. Regarding Fig. 8, the interface that is developed consists of a few modules including the create certificate and verified certificate. Then Fig. 9, is an interface to create the digital certificate. Lastly at Fig. 10, is an interface to process the digital certificate.

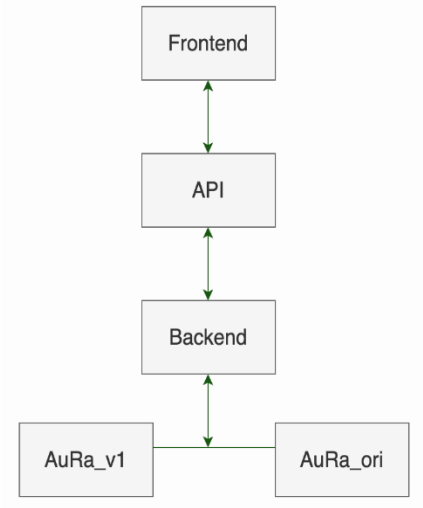


Fig. 7. The framework of digital certificate process.

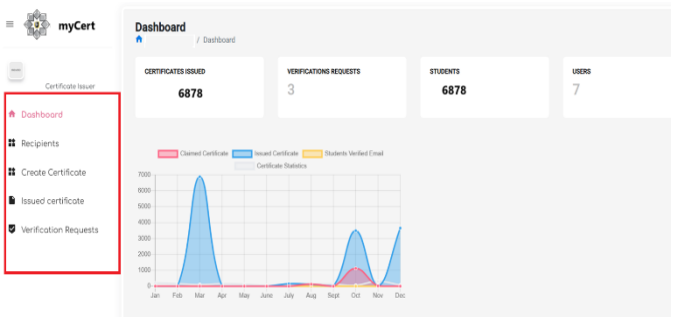


Fig. 8. The dashboard and main interface.

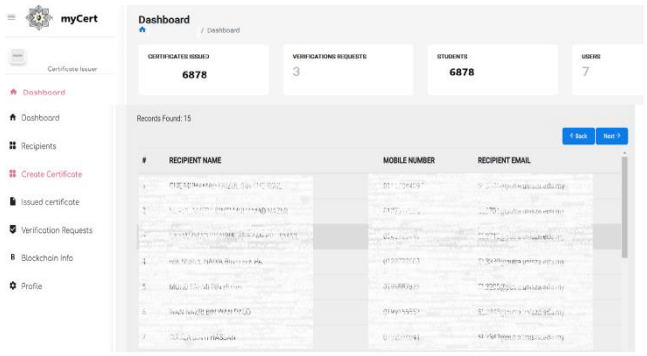


Fig. 9. The digital certificate generate interface.

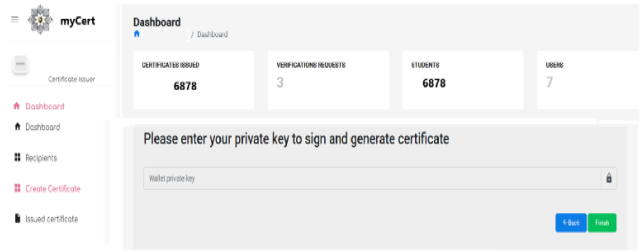


Fig. 10. The digital certificate generate process.

VI. Result and Discussion

According these implementation, the TPS result were captured to analysis the performance of AuRa_v1 and AuRa_ori.

A. TPS Result of AuRa_ori

This result based on implementation the AuRa_ori used three set of data. Regarding Fig. 11, the TPS result of set data 1 is 0.059. Set data 2 the TPS result is 0.032 and set data 3 is 0.069. According the TPS result, set data 2 more rapidly compared set data1 and set data 3. Set data 3 very slow compared set data 1 and set data 3.

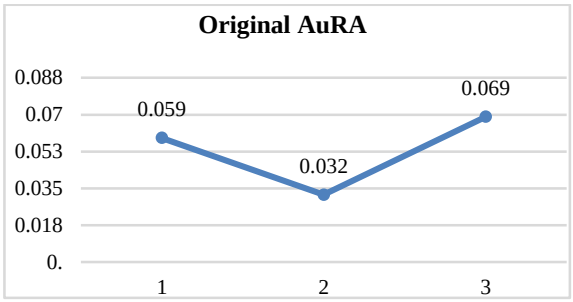


Fig. 11. TPS result of AuRa_ori.

B. TPS Result of AuRa_v1

This outcome based on execution the AuRa_v1 used three set of data. Fig. 12 depicted the result of TPS that executed the AuRa_v1. The result of Set data 1 is 0.041, set data 2 is 0.029 and set data 3 is 0.036. These TPS result showed that the set data 2 is faster and set data 3 is slow compare three set of data.

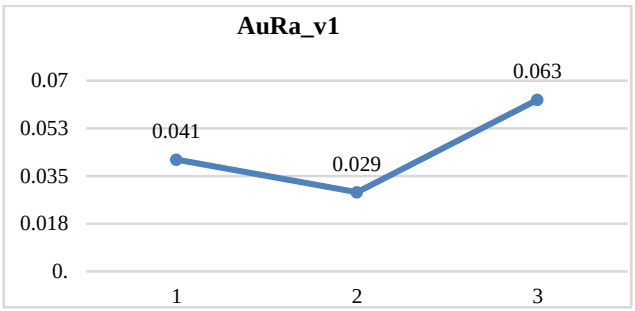


Fig. 12. TPS result based on aura_v1.

C. TPS AuRa_ori Versus AuRa_v1

This section aims to compare the result between the AuRa_ori and AuRa_v1. Regarding Fig. 13 depicted that the result of AuRa_ori (orange line) at set data 1 is 0.059, set data 2 is 0.032 and set data 3 is 0.069. Then TPS result of AuRa_v1 (blue line) , set data 1 is 0.041, set data 2 is 0.029 and set data 3 is 0.063.

According these result, set data 1, AuRa_v1 is able decrease the transaction process compared AuRa_ori. Then set data 2 and set data3 also showed that AuRa_v1 prove decrease the TPS result compared AuRa_ori.

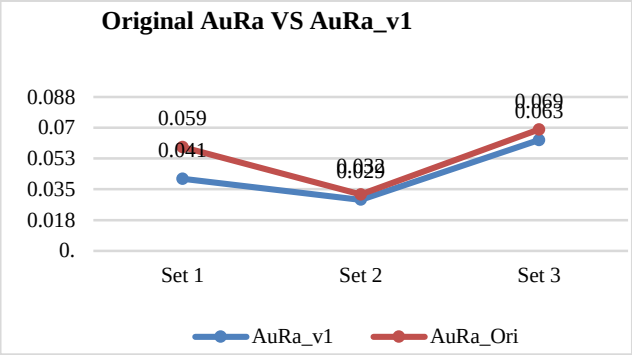


Fig. 13. Comparison TPS result between AuRa_ori and aura_v1.

D. Percentage Decrease of TPS

This research aims to decrease the transaction speed process into the blockchain using the AuRa_v1. Regarding the TPS result, the percentage Decrease PD measured to obtain the PD based on AuRa_v1. The measurement of $PD$the based on Eq. (6),

$$PD = \left(\frac{(i_v - f_v)}{i_v}\right) * 100 \quad (6)$$

In Eq. (6), PD refer to Percentage Decrease, then i_v is interval value for AuRa_ori value and f_v is the final value for AuRa_v1 value. The PD result was measured and described in Table III.

TABLE III. THE PERCENTAGE DECREASE OF TPS

Data	Result
Set Data: 1	30%
Set Data: 2	9.375%
Set Data: 3	8.69%

The results show that the implementation of AuRa_v1 able to decrease the TPS result. Set data 1, able to decrease the TPS result by 30%, set data 2 by 9.375 % while set data 3 with 8.69%.

VII. CONCLUSION

The optimal consensus algorithm hinges on the shortest transaction execution time within the blockchain. Previous research discussed earlier indicates that both assigning a new leader and voting during the transaction process impact the transaction speed and throughput of AuRa_ori and AuRa_v1. The heightened transaction speed presents risks such as decreased throughput, cloning attacks, and the possibility of assigning a malicious leader.

Nearly all previous studies underscore the limitations of the AuRa_ori consensus algorithm regarding performance of TPS, attributed to the necessity of assigning a new leader for every transaction process. This results in a reduction in transaction throughput. Additionally, the increased TPS of AuRa_ori is influenced by the requirement for a voting phase before transactions can be committed to the blockchain. The future plan is restructured prior to results obtained that aims to measure the TGS and TPS use the same set of data. The compare the result between AuRa_ori and AuRa_v1. Also calculate the PD and PI.

ACKNOWLEDGMENT

We express sincere gratitude to the Center of Research and Innovation Management (CREIM) at UniSZA for their invaluable financial support towards the publication. Our heartfelt appreciation also goes to all team members from UniSZA, including Pn. Robiah Arifin, the PhD candidate for the technical configuration of the project, and Dr. Wan Aezwani Wan Abu Bakar as her supervisor for the conceptual and technical proofread writing, as well as the UMT member, Assoc Prof. Ts. Dr. Mustafa Man for the network linkages and the reviewer's suggestions. Also, we are grateful for the international contributions and collaboration provided by Dr. Evizal Abdul Kadir, a research fellow from Universitas Islam Riau, Indonesia.

REFERENCES

[1] Dabbagh, M., Kakavand, M., Tahir, M., & Amphawan, A. (2020, September). Performance analysis of blockchain platforms: Empirical evaluation of hyperledger fabric and ethereum. In 2020 IEEE 2nd International conference on artificial intelligence in engineering and technology (IICAIET) (pp. 1-6). IEEE.

[2] Rajeswari, T. R., Shareef, S. K., Khan, S., Venkatesh, N., Ali, A., & Devi, V. S. M. (2021, July). Generating and validating certificates using blockchain. In 2021 6th international conference on communication and electronics systems (ICCES) (pp. 1048-1052). IEEE.

[3] Kim, H., Jang, J., Park, S., & Lee, H. N. (2021). Error-correction code proof-of-work on Ethereum. IEEE Access, 9, 135942-135952.

[4] Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials, 22(2), 1432-1465.

[5] Nguyen, B. M., Dao, T. C., & Do, B. L. (2020). Towards a blockchain-based certificate authentication system in Vietnam. PeerJ Computer Science, 6, e266.

[6] Saleh, O.S., Ghazali, O., & Rana, M.E. (2020). BLOCKCHAIN BASED FRAMEWORK FOR EDUCATIONAL CERTIFICATES VERIFICATION.

[7] Yadav, A. S., Singh, N., & Kushwaha, D. S. (2023). Evolution of Blockchain and consensus mechanisms & its real-world applications. Multimedia Tools and Applications, 82(22), 34363-34408.. Evolution of Blockchain and consensus mechanisms & its real-world applications. Multimedia Tools and Applications, 82(22), 34363-34408.

[8] V. Buterin, "Ethereum white paper: a next generation smart contract & decentralized application platform," 2013, available at: http://www.theblockchain.com/docs/Ethereum_white_papera_next_generation_smart_contract_and_decentralized_application_platf orm-vitalik-buterin.pdf.

[9] Vujičić, D., Jagodić, D., & Ranđić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In 2018 17th international symposium infoteh-jahorina (infoteh) (pp. 1-6). IEEE.

[10] Guo, H. and Yu, X., 2022. A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), p.100067.

[11] A. Welligton dos Santos Abreu, E. F. Coutinho and C. Ilane Moreira Bezerra, "Performance Evaluation of Data Transactions in Blockchain," in IEEE Latin America Transactions, vol. 20, no. 3, pp. 409-416, March 2022, doi: 10.1109/TLA.2022.9667139.

[12] Fan, C., Ghaemi, S., Khazaei, H., & Musilek, P. (2020). Performance evaluation of blockchain systems: A systematic survey. *IEEE Access*, *8*, 126927-126950.

[13] B. Lashkari and P. Musilek. A comprehensive review of blockchain consensus mechanisms. IEEE Access, 9:43620–43652, 2021.

[14] M. M. Islam, M. M. Merlec and H. P. In.(2022). A Comparative Analysis of Proof-of-Authority Consensus Algorithms: Aura vs Clique. IEEE International Conference on Services Computing (SCC), Barcelona, Spain, 2022, pp. 327-332, doi: 10.1109/SCC55611.2022.00054.

[15] De Angelis, S. (2018). Assessing security and performances of consensus algorithms for permissioned blockchains. arXiv preprint arXiv:1805.03490.

[16] Zhang, X., Wang, Q., Li, R., & Wang, Q. (2022, May). Frontrunning block attack in poa clique: A case study. In 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-3). IEEE.

[17] Zhang, Xinrui & Li, Rujia & Wang, Qin & Wang, Qi & Duan, Sisi. (2023). Time-manipulation Attack: Breaking Fairness against Proof of Authority Aura. 2076-2086. 10.1145/3543507.3583252.

[18] Hashim, F., Shuaib, K., & Sallabi, F. (2021, December). Performance Evaluation of Blockchain Consensus Algorithms for Electronic Health Record Sharing. In 2021 Global Congress on Electrical Engineering (GC-ElecEng) (pp. 136-143). IEEE.

[19] Islam, M. M., & In, H. P. (2023). Decentralized Global Copyright System Based on Consortium Blockchain with Proof of Authority. IEEE Access.

[20] M. M. Islam, M. M. Merlec and H. P. In.(2022). A Comparative Analysis of Proof-of-Authority Consensus Algorithms: Aura vs Clique. IEEE International Conference on Services Computing (SCC), Barcelona, Spain, 2022, pp. 327-332, doi: 10.1109/SCC55611.2022.00054.

[21] Kuperberg, M. (2020, August). Towards an analysis of network partitioning prevention for distributed ledgers and blockchains. In 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) (pp. 94-99). IEEE.

[22] Dhulavvagol, P. M., Bhajantri, V. H., & Totad, S. G. (2020). Blockchain ethereum clients performance analysis considering E-voting application. Procedia Computer Science, 167, 2506-2515.

[23] Rouhani, S., & Deters, R. (2017, November). Performance analysis of ethereum transactions in private blockchain. In 2017 8th IEEE international conference on software engineering and service science (ICSESS) (pp. 70-74). IEEE.

[24] De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. In CEUR workshop proceedings (Vol. 2058). CEUR-WS.

[25] Seri, P. R. (2021). Blockchain Based e-Voting. Southern Illinois University at Carbondale.

[26] Shi, E. (2019, June). Analysis of deterministic longest-chain protocols. In 2019 IEEE 32nd Computer Security Foundations Symposium (CSF) (pp. 122-12213). IEEE.

[27] De Angelis, S., Lombardi, F., Zanfino, G., Aniello, L., & Sassone, V. (2023). Security and dependability analysis of blockchain systems in partially synchronous networks with Byzantine faults. International Journal of Parallel, Emergent and Distributed Systems, 1-21.

[28] Hu, Y., Tian, G., Jiang, A., Liu, S., Wei, J., Wang, J., & Tan, S. (2023). A practical heartbeat-based defense scheme against cloning attacks in PoA blockchain. Computer Standards & Interfaces, 83, 103656.

Enhancing Multiple-Attribute Decision-Making with Interval-Valued Neutrosophic Sets: Diverse Applications in Evaluating English Teaching Quality

Lijuan Zhao[1]*, Shuo Du[2]
Shijiazhuang University of Applied Technology, Shijiazhuang, 050081, Hebei, China[1, 2]

***Abstract*—The evaluation of college English teaching quality is a key method for systematically analyzing and providing feedback on the teaching process and outcomes. It aims to comprehensively assess the effectiveness of teaching, student learning outcomes, and the appropriateness of the course design. The evaluation typically covers aspects such as teaching methods, classroom atmosphere, student engagement, use of teaching resources, and learning achievements. By collecting data from student feedback, teaching supervision, and exam results, the evaluation helps to improve teaching strategies, enhance students' English proficiency, and ultimately achieve continuous optimization and improvement of teaching quality. The teaching quality evaluation of college English is viewed as the multiple-attribute decision-making (MADM). In this paper, some Aczel-Alsina operators are produced under interval-valued neutrosophic sets (IVNSs). Then, interval-valued neutrosophic number (IVNN) Aczel-Alsina weighted averaging (IVNNAAWA) operator is employed to cope with MADM problem. Finally, the numerical decision example for teaching quality evaluation of college English is employed to illustrate the produced method.**

Keywords*—Multiple-attribute decision-making; interval-valued neutrosophic sets (IVNSs); Aczel-Alsina operations; teaching quality evaluation

I. Introduction

Evaluation of college English teaching quality is an essential tool for systematically analyzing and assessing the teaching process and outcomes. Its aim is to enhance teaching quality through a scientifically sound evaluation system, meeting students' learning needs and the societal demands for English proficiency. The evaluation typically covers various aspects, including teaching methods, curriculum design, utilization of teaching resources, student learning outcomes, and classroom participation. Diverse evaluation methods, such as student feedback, classroom observation, and test performance analysis, are widely employed to ensure comprehensiveness and objectivity. Through continuous quality evaluation, universities can optimize teaching strategies, improve course design, and promote the development of students' comprehensive English skills, laying a foundation for cultivating internationally competitive talents in line with contemporary demands. Starting in 2013, Lu and Huang [1] explored the construction of English teaching quality evaluation systems and the applicability of cultivating students' comprehensive English abilities. They suggested reforming the existing college English teaching evaluation methods by referencing the Canadian language benchmarks to comprehensively enhance teaching quality and students' comprehensive English proficiency. In the same year, Ma and Li [2] attempted to construct a multidimensional ecological evaluation system under network environments, based on constructivism and educational ecology theories, to promote the ecologicalization and quality improvement of college English teaching. In 2015, Wu and Tang [3] analyzed the current state of classroom teaching quality evaluation systems in universities, identifying existing problems and designing various evaluation forms to enhance the scientific and rational nature of evaluations. Yu [4] proposed a diversified evaluation model, combining modern quality management theory, constructivism, and multiple intelligences theory, emphasizing the use of various methods for comprehensive teaching quality evaluation to improve college English course quality. In 2016, Yuan [5] analyzed teaching evaluation strategies for subsequent college English courses, highlighting the need for differentiated strategies in evaluation subjects, content, and methods to enhance teaching quality across language culture, skills, and language application courses. In 2017, Deng [6] studied the application of participatory teaching models in college English, proposing related teaching quality evaluation methods. The study emphasized that participatory teaching methods should focus not only on students' exam scores but also on their practical application abilities. In 2018, Yang [7] developed a teaching quality evaluation index system for flipped classrooms in vocational college English, emphasizing the importance of developmental and process evaluations. The evaluation indices were refined through expert consultation and surveys to align with the characteristics of flipped classroom teaching. In 2019, Li [8] explored strategies for constructing college English teaching quality evaluation systems under the applied talent training system, proposing the establishment of a scientific and reasonable evaluation system to improve English teaching quality and meet the societal demand for applied talents. In 2020, Xu [9] discussed the application of stratified teaching methods in college English, analyzing its role in reducing student learning differences, enhancing learning interest, and ensuring classroom teaching quality, while proposing specific application strategies. In 2021, Yang and Li [10] constructed a classroom teaching quality evaluation model based on set pair analysis in the context of the digital era to meet the requirements of "golden course" construction. The study emphasized the importance of integrating modern information technology with college English courses. In 2022, Zhang [11] studied college English teaching quality evaluation through value speculation guidance, constructing an evaluation model

*Corresponding author.

based on the SERVQUAL model. This aimed to identify gaps and deficiencies in teaching by comparing students' "expectations" and "actual perceptions," and proposed improvement measures. In 2023, Gong and Peng [12] proposed a college English teaching quality evaluation model based on ISSA-DRNN, utilizing an improved deep recurrent neural network and optimized sparrow search algorithm to enhance the model's evaluation performance and precision. In 2024, Zhang [13] constructed an English teaching quality evaluation system based on the CIPP model, proposing a comprehensive framework that includes context, input, process, and product evaluations. This provided a scientific and operational evaluation standard for college English teaching.

Multi-Attribute Decision Making (MADM) is a decision-making method used to address selection problems involving multiple evaluation criteria [14-17]. This type of decision-making approach is widely applied in fields such as management science, engineering, and economics, aiding decision-makers in making rational choices in complex situations [18-21]. In multi-attribute decision making, the decision problem typically involves multiple competing attributes or criteria, which may have different levels of importance [22-25]. Therefore, decision-makers need to weight each attribute to reflect its relative importance. Common weighting methods include expert scoring, Analytic Hierarchy Process (AHP), and entropy method. The basic steps of multi-attribute decision making include: first, clarifying the decision objectives and available alternatives; second, determining the evaluation attributes and assigning weights to them [26-29]; then, collecting and organizing data on the performance of each alternative across different attributes[30-33]; next, applying appropriate decision-making methods (such as TOPSIS, VIKOR, ELECTRE) to comprehensively evaluate the alternatives; finally, selecting the optimal alternative or ranking the alternatives based on the evaluation results. The advantage of this method is that it systematically considers multiple factors, making the decision process more comprehensive and objective. However, the reliability of the decision results largely depends on the accuracy of the attribute weights and the completeness of the data [34-38]. Therefore, decision-makers need to carefully assess the rationality of each step and the accuracy of the data when using multi-attribute decision-making methods. The problems of teaching quality evaluation of college English is MADM [39-45]. Aczél and Alsina [46] structured some new operations named as Aczel-Alsina t-norm and t-conorm operations. Yong et al.[29] and Ashraf et al. [47] structured the Aczel-Alsina decision operations to SVNNs and produced the Aczel-Alsina fused operators of SVNNs for MADM. The main aim of this defined paper is to expand the Aczel-Alsina operations [46] to cope with MADM under IVNSs. The main study motivations are listed: (1) the Aczel-Alsina operations are extended to IVNSs; (2) some Aczel-Alsina aggregating operators are produced under IVNSs; (3) the IVNNAAWA method is designed for MADM; (4) a case study about translation quality decision evaluation of college English is given to show the IVNNAAWA method; (5) some comparative models are used to proof the IVNNAAWA method. The remainder sections of this paper are set out. Section II lists the IVNSs. In Section III, the some Aczel-Alsina aggregating operators are produced under IVNSs. In Section IV, the IVNNAAWA operator is built for MADM. In Section V, a case study for translation quality decision evaluation of college English is listed and some comparative decision methods are done. The defined decision study ends in Section VI.

II. PRELIMINARIES

Wang et al. [48] produced the IVNSs

Definition 1 [49]. The IVNSs A in X is:

$$\tilde{A}=\left\{\left(x,TT_{\tilde{A}}(x),II_{\tilde{A}}(x),FF_{\tilde{A}}(x)\right)\middle|x\in X\right\} \quad (1)$$

with truth-membership $TT_{\tilde{A}}(x)$, indeterminacy-membership $II_{\tilde{A}}(x)$ and falsity-membership $FF_{\tilde{A}}(x)$, $TT_{\tilde{A}}(x),II_{\tilde{A}}(x),FF_{\tilde{A}}(x)\in[0,1]$, $0\le \sup TT_{\tilde{A}}(x)+\sup II_{\tilde{A}}(x)+\sup FF_{\tilde{A}}(x)\le 3$.

The IVNN is expressed as $\tilde{A}=\left(TT_{\tilde{A}},II_{\tilde{A}},FF_{\tilde{A}}\right)=\left(\left[TL_{\tilde{A}},TR_{\tilde{A}}\right],\left[IL_{\tilde{A}},IR_{\tilde{A}}\right],\left[FL_{\tilde{A}},FR_{\tilde{A}}\right]\right)$, where $TT_{\tilde{A}}\subseteq[0,1],II_{\tilde{A}}\subseteq[0,1],FF_{\tilde{A}}\subseteq[0,1]$, $0\le TR_{\tilde{A}}+IR_{\tilde{A}}+FR_{\tilde{A}}\le 3$.

Definition 2[50]. Let $\tilde{A}=\left(\left[TL_{\tilde{A}},TR_{\tilde{A}}\right],\left[IL_{\tilde{A}},IR_{\tilde{A}}\right],\left[FL_{\tilde{A}},FR_{\tilde{A}}\right]\right)$, the score value is expressed:

$$SV\left(\tilde{A}\right)=\frac{\left(2+TL_{\tilde{A}}-IL_{\tilde{A}}-FL_{\tilde{A}}\right)+\left(2+TR_{\tilde{A}}-IR_{\tilde{A}}-FR_{\tilde{A}}\right)}{6},\quad SV\left(\tilde{A}\right)\in[0,1]. \quad (2)$$

Definition 3[50]. Let $\tilde{A}=\left(\left[TL_{\tilde{A}},TR_{\tilde{A}}\right],\left[IL_{\tilde{A}},IR_{\tilde{A}}\right],\left[FL_{\tilde{A}},FR_{\tilde{A}}\right]\right)$, the accuracy value is expressed:

$$AV\left(\tilde{A}\right)=\frac{\left(TL_{\tilde{A}}+TR_{\tilde{A}}\right)-\left(FL_{\tilde{A}}+FR_{\tilde{A}}\right)}{2},\ AV\left(\tilde{A}\right)\in[-1,1]. \quad (3)$$

Huang et al. [50] expressed the order relation for IVNNs.

Definition 4[50]. Let $\tilde{A}=\left(\left[TL_{\tilde{A}},TR_{\tilde{A}}\right],\left[IL_{\tilde{A}},IR_{\tilde{A}}\right],\left[FL_{\tilde{A}},FR_{\tilde{A}}\right]\right)$ and $\tilde{B}=\left(\left[TL_{\tilde{B}},TR_{\tilde{B}}\right],\left[IL_{\tilde{B}},IR_{\tilde{B}}\right],\left[FL_{\tilde{B}},FR_{\tilde{B}}\right]\right)$, let

$$SV\left(\tilde{A}\right)=\frac{\left(2+TL_{\tilde{A}}-IL_{\tilde{A}}-FL_{\tilde{A}}\right)+\left(2+TR_{\tilde{A}}-IR_{\tilde{A}}-FR_{\tilde{A}}\right)}{6}$$

and

$$SV\left(\tilde{B}\right)=\frac{\left(2+TL_{\tilde{B}}-IL_{\tilde{B}}-FL_{\tilde{B}}\right)+\left(2+TR_{\tilde{B}}-IR_{\tilde{B}}-FR_{\tilde{B}}\right)}{6}$$

, and let $AV\left(\tilde{A}\right)=\frac{\left(TL_{\tilde{A}}+TR_{\tilde{A}}\right)-\left(FL_{\tilde{A}}+FR_{\tilde{A}}\right)}{2}$ and $AV\left(\tilde{B}\right)=\frac{\left(TL_{\tilde{B}}+TR_{\tilde{B}}\right)-\left(FL_{\tilde{B}}+FR_{\tilde{B}}\right)}{2}$, then if $SV\left(\tilde{A}\right)<SV\left(\tilde{B}\right)$, we have $\tilde{A}<\tilde{B}$; if $SV\left(\tilde{A}\right)=SV\left(\tilde{B}\right)$, (1)if $HV\left(\tilde{A}\right)=HV\left(\tilde{B}\right)$, we have $\tilde{A}=\tilde{B}$; (2) if $HV\left(\tilde{A}\right)<HV\left(\tilde{B}\right)$, we have $\tilde{A}<\tilde{B}$.

Aczél and Alsina [46] structured some new operations named as Aczel-Alsina t-norm and t-conorm operations, which have true advantage of changeability through adjusting a decision parameter. Yong et al.[29] and Ashraf et al. [47] structured the Aczel-Alsina operations to SVNNs. Similarly, the Aczel-Alsina decision operations for IVNNs are produced.

Definition 5. Let $\tilde{A}=\left(\left[TL_{\tilde{A}},TR_{\tilde{A}}\right],\left[IL_{\tilde{A}},IR_{\tilde{A}}\right],\left[FL_{\tilde{A}},FR_{\tilde{A}}\right]\right)$ and $\tilde{B}=\left(\left[TL_{\tilde{B}},TR_{\tilde{B}}\right],\left[IL_{\tilde{B}},IR_{\tilde{B}}\right],\left[FL_{\tilde{B}},FR_{\tilde{B}}\right]\right)$, $\phi\geq 1$, $\lambda>0$, the Aczel-Alsina operations for IVNNs are produced:

$$\tilde{A}\oplus\tilde{B}=\left(\begin{array}{l}\left[1-e^{-\left(\left(-\ln\left(1-TL_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(1-TL_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}},1-e^{-\left(\left(-\ln\left(1-TR_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(1-TR_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(\left(-\ln\left(IL_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(IL_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}},\ e^{-\left(\left(-\ln\left(IR_{\tilde{A}}\right)\right)^{\theta}+\left(-\ln\left(IR_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(\left(-\ln\left(FL_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(FL_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}},\ e^{-\left(\left(-\ln\left(FR_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(FR_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}}\right]\end{array}\right)$$

$$\tilde{A}\otimes\tilde{B}=\left(\begin{array}{l}\left[e^{-\left(\left(-\ln\left(TL_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(TL_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(\left(-\ln\left(TR_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(TR_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[1-e^{-\left(\left(-\ln\left(1-IL_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(1-IL_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}},1-e^{-\left(\left(-\ln\left(1-IR_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(1-IR_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[1-e^{-\left(\left(-\ln\left(1-FL_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(1-FL_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}},1-e^{-\left(\left(-\ln\left(1-FR_{\tilde{A}}\right)\right)^{\phi}+\left(-\ln\left(1-FR_{\tilde{B}}\right)\right)^{\phi}\right)^{1/\phi}}\right]\end{array}\right)$$

$$\lambda A=\left(\begin{array}{l}\left[1-e^{-\left(\lambda\left(-\ln\left(1-TL_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}},1-e^{-\left(\lambda\left(-\ln\left(1-TR_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(\lambda\left(-\ln\left(IL_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(\lambda\left(-\ln\left(IR_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(\lambda\left(-\ln\left(FL_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(\lambda\left(-\ln\left(FR_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}}\right]\end{array}\right)$$

$$(A)^{\lambda}=\left(\begin{array}{c}\left[e^{-\left(\lambda\left(-\ln\left(TL_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(\lambda\left(-\ln\left(TR_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[1-e^{-\left(\lambda\left(-\ln\left(1-IL_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}},1-e^{-\left(\lambda\left(-\ln\left(1-IR_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[1-e^{-\left(\lambda\left(-\ln\left(1-FL_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}},1-e^{-\left(\lambda\left(-\ln\left(1-FR_{\tilde{A}}\right)\right)^{\phi}\right)^{1/\phi}}\right]\end{array}\right)$$

III. Some Aczel-Alsina Weighted Averaging Operators with NNs

In this section, Some Aczel-Alsina aggregating operators with IVNNs are produced.

The IVNN Aczel-Alsina weighted averaging (IVNNAAWA) is defined.

Definition 7. Let $SA_i=\left(\left[TL_i,TR_i\right],\left[IL_i,IR_i\right],\left[FL_i,FR_i\right]\right)$ the IVNNs with their weight $sw_i=(sw_1,sw_2,\ldots,sw_n)^T$, $\sum_{i=1}^{n}sw_i=1$, $\phi\geq 1$. If

$$\text{IVNNAAWA}_{sw}\left(SA_1,SA_2,\cdots,SA_n\right)=\overset{n}{\underset{i=1}{\oplus}}sw_iSA_i \tag{4}$$

The Theorem 1 is obtained.

Theorem 1. Let $SA_i=\left(\left[TL_i,TR_i\right],\left[IL_i,IR_i\right],\left[FL_i,FR_i\right]\right)$ the IVNNs with their weight $sw_i=(sw_1,sw_2,\ldots,sw_n)^T$, $\sum_{i=1}^{n}zw_i=1$, $\phi\geq 1$. If

$$\text{IVNNAAWA}_{sw}\left(SA_1,SA_2,\cdots,SA_n\right)=\overset{n}{\underset{i=1}{\oplus}}sw_iSA_i$$

$$=\left(\begin{array}{c}\left[1-e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(1-TL_j\right)\right)^{\phi}\right)^{1/\phi}},1-e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(1-TR_j\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(IL_j\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(IR_j\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(FL_j\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(FR_j\right)\right)^{\phi}\right)^{1/\phi}}\right]\end{array}\right) \tag{5}$$

Proof:

(a) Let $i=2$, then

$$\text{IVNNAAWA}_{sw}\left(SA_1,SA_2\right)=sw_1SA_1\oplus sw_2SA_2$$

$$\left(\begin{array}{c}\left[1-e^{-\left(sw_1\left(-\ln\left(1-TL_1\right)\right)^{\phi}\right)^{1/\phi}},1-e^{-\left(sw_1\left(-\ln\left(1-TR_1\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(sw_1\left(-\ln\left(IL_1\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(sw_1\left(-\ln\left(IR_1\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(sw_1\left(-\ln\left(FL_1\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(sw_1\left(-\ln\left(FR_1\right)\right)^{\phi}\right)^{1/\phi}}\right]\end{array}\right)\oplus$$

(b)
$$\left(\begin{array}{c}\left[1-e^{-\left(sw_2\left(-\ln\left(1-TL_2\right)\right)^{\phi}\right)^{1/\phi}},1-e^{-\left(sw_2\left(-\ln\left(1-TR_2\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(sw_2\left(-\ln\left(IL_2\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(sw_2\left(-\ln\left(IR_2\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(sw_2\left(-\ln\left(FL_2\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(sw_2\left(-\ln\left(FR_2\right)\right)^{\phi}\right)^{1/\phi}}\right]\end{array}\right)$$

$$=\left(\begin{array}{c}\left[1-e^{-\left(\sum_{i=1}^{2}sw_i\left(-\ln\left(1-TL_j\right)\right)^{\phi}\right)^{1/\phi}},1-e^{-\left(\sum_{i=1}^{2}sw_i\left(-\ln\left(1-TR_j\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(\sum_{i=1}^{2}sw_i\left(-\ln\left(IL_j\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(\sum_{i=1}^{2}sw_i\left(-\ln\left(IR_j\right)\right)^{\phi}\right)^{1/\phi}}\right],\\ \left[e^{-\left(\sum_{i=1}^{2}sw_i\left(-\ln\left(FL_j\right)\right)^{\phi}\right)^{1/\phi}},e^{-\left(\sum_{i=1}^{2}sw_i\left(-\ln\left(FR_j\right)\right)^{\phi}\right)^{1/\phi}}\right]\end{array}\right)$$

(c) If Eq. (10) holds for $i=k$, then

$$\mathrm{IVNNAAWA}_{sw}\left(SA_1, SA_2, \cdots, SA_k\right) = \bigoplus_{i=1}^{k} sw_i SA_i$$

$$= \left(\begin{bmatrix} 1-e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(1-TL_j\right)\right)^{\phi}\right)^{1/\phi}}, 1-e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(1-TR_j\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \begin{bmatrix} e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(IL_j\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(IR_j\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \begin{bmatrix} e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(FL_j\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(FR_j\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix} \right)$$

(d) Set $i = k+1$. From Definition 5, we have

$$\mathrm{IVNNAAWA}_{sw}\left(SA_1, SA_2, \cdots, SA_{k+1}\right) = \bigoplus_{i=1}^{k} sw_i SA_i \oplus sw_{k+1} SA_{k+1}$$

$$= \left(\begin{bmatrix} 1-e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(1-TL_j\right)\right)^{\phi}\right)^{1/\phi}}, 1-e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(1-TR_j\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \begin{bmatrix} e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(IL_j\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(IR_j\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \begin{bmatrix} e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(FL_j\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{k} sw_i\left(-\ln\left(FR_j\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix} \right) \oplus$$

$$\left(\begin{bmatrix} 1-e^{-\left(sw_{k+1}\left(-\ln\left(1-TL_{k+1}\right)\right)^{\phi}\right)^{1/\phi}}, 1-e^{-\left(sw_{k+1}\left(-\ln\left(1-TR_{k+1}\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \begin{bmatrix} e^{-\left(sw_{k+1}\left(-\ln\left(IL_{k+1}\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(sw_{k+1}\left(-\ln\left(IR_{k+1}\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \begin{bmatrix} e^{-\left(sw_{k+1}\left(-\ln\left(FL_{k+1}\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(sw_{k+1}\left(-\ln\left(FR_{k+1}\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix} \right)$$

$$= \left(\begin{bmatrix} 1-e^{-\left(\sum_{i=1}^{k+1} sw_i\left(-\ln\left(1-TL_j\right)\right)^{\phi}\right)^{1/\phi}}, 1-e^{-\left(\sum_{i=1}^{k+1} sw_i\left(-\ln\left(1-TR_j\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \begin{bmatrix} e^{-\left(\sum_{i=1}^{k+1} sw_i\left(-\ln\left(IL_j\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{k+1} sw_i\left(-\ln\left(IR_j\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \begin{bmatrix} e^{-\left(\sum_{i=1}^{k+1} sw_i\left(-\ln\left(FL_j\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{k+1} sw_i\left(-\ln\left(FR_j\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix} \right)$$

From the above (a), (b), and (c), it can be seen that Eq. (5) holds for any i.

The IVNNAAWA has good properties.

Property 1. (idempotency). If $SA_i = SA = \left(\left[TL, TR\right], \left[IL, IR\right], \left[FL, FR\right]\right)$

$$\mathrm{IVNNAAWA}_{sw}\left(SA_1, SA_2, \cdots, SA_n\right) = SA \tag{6}$$

Property2. (Monotonicity). Let $SA_i = \left(\left[TL_{A_i}, TR_{A_i}\right], \left[IL_{A_i}, IR_{A_i}\right], \left[FL_{A_i}, FR_{A_i}\right]\right)$, $SB_i = \left(\left[TL_{B_i}, TR_{B_i}\right], \left[IL_{B_i}, IR_{B_i}\right], \left[FL_{B_i}, FR_{B_i}\right]\right)$. If $TL_{A_i} \le TL_{B_i}, IL_{A_i} \ge IL_{B_i}, FL_{A_i} \ge FL_{B_i}$,

$TR_{A_i} \le TR_{B_i}, IR_{A_i} \ge IR_{B_i}, FR_{A_i} \ge FR_{B_i}$ holds for all i, then

$$\mathrm{IVNNAAWA}_{sw}\left(SA_1, SA_2, \cdots, SA_n\right) \le \mathrm{IVNNAAWA}_{sw}\left(SB_1, SB_2, \cdots, SB_n\right) \tag{7}$$

Property 3 (Boundedness). Let $SA_i = \left(\left[TL_{A_i}, TR_{A_i}\right], \left[IL_{A_i}, IR_{A_i}\right], \left[FL_{A_i}, FR_{A_i}\right]\right)$. If

$$ZA^{+} = \left(\begin{bmatrix} \max_i(TL_i), \max_i(TR_i) \end{bmatrix}, \begin{bmatrix} \min_i(IL_i), \min_i(IR_i) \end{bmatrix}, \begin{bmatrix} \min_i(FL_i), \min_i(FR_i) \end{bmatrix} \right),$$

$$ZA^{+} = \left(\begin{bmatrix} \min_i(TL_i), \min_i(TR_i) \end{bmatrix}, \begin{bmatrix} \max_i(IL_i), \max_i(IR_i) \end{bmatrix}, \begin{bmatrix} \max_i(FL_i), \max_i(FR_i) \end{bmatrix} \right)$$

then

$$ZA^{-} \le \mathrm{IVNNAAWA}_{sw}\left(SA_1, SA_2, \cdots, SA_n\right) \le ZA^{+} \tag{8}$$

Then, the IVNN Aczel-Alsina OWA (IVNNAAOWA) is expressed.

Definition 8. Let $SA_i = \left(\left[TL_i, TR_i\right], \left[IL_i, IR_i\right], \left[FL_i, FR_i\right]\right) (i = 1, 2, \ldots, n)$ be IVNNs, $\theta \geq 1$. If:

$$\text{IVNNAAOWA}_{sw}\left(SA_1, SA_2, \cdots, SA_n\right) = \bigoplus_{i=1}^{n} sw_{\sigma(i)} SA_{\sigma(i)}$$

$$= \left(\begin{bmatrix} 1 - e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(1 - TL_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}}, 1 - e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(1 - TR_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(IL_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(IR_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(FL_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(FR_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix} \right) \quad (9)$$

where $\left(\sigma(1), \sigma(2), \cdots, \sigma(n)\right)$ is permutation of $(1, 2, \cdots, n)$, such that $SA_{\sigma(j-1)} \geq SA_{\sigma(j)}$ for all $j = 2, \cdots, n$, and $zw = \left(zw_1, zw_2, \cdots, zw_n\right)^T$ is weight of IVNNAAOWA operator, and $0 \leq zw_j \leq 1$, $\sum_{j=1}^{n} zw_j = 1$.

The IVNNAAOWA has three properties.

Property 4. (idempotency). If $SA_i = SA = \left(\left[TL, TR\right], \left[IL, IR\right], \left[FL, FR\right]\right)$

$$\text{IVNNAAOWA}_{zw}\left(SA_1, SA_2, \cdots, SA_n\right) = SA \quad (10)$$

Property 5. (Monotonicity). Let $SA_i = \left(\left[TL_{A_i}, TR_{A_i}\right], \left[IL_{A_i}, IR_{A_i}\right], \left[FL_{A_i}, FR_{A_i}\right]\right)$, $SB_i = \left(\left[TL_{B_i}, TR_{B_i}\right], \left[IL_{B_i}, IR_{B_i}\right], \left[FL_{B_i}, FR_{B_i}\right]\right)$. If $TL_{A_i} \leq TL_{B_i}, IL_{A_i} \geq IL_{B_i}, FL_{A_i} \geq FL_{B_i}$, $TR_{A_i} \leq TR_{B_i}, IR_{A_i} \geq IR_{B_i}, FR_{A_i} \geq FR_{B_i}$ holds for all i, then

$$\text{IVNNAAOWA}_{zw}\left(SA_1, SA_2, \cdots, SA_n\right) \leq \text{IVNNAAOWA}_{zw}\left(SB_1, SB_2, \cdots, SB_n\right) \quad (11)$$

Property 6 (Boundedness). Let $SA_i = \left(\left[TL_{A_i}, TR_{A_i}\right], \left[IL_{A_i}, IR_{A_i}\right], \left[FL_{A_i}, FR_{A_i}\right]\right)$. If $ZA^+ = \left(\left[\max_i(TL_i), \max_i(TR_i)\right], \left[\min_i(IL_i), \min_i(IR_i)\right], \left[\min_i(FL_i), \min_i(FR_i)\right]\right)$, $ZA^+ = \left(\left[\min_i(TL_i), \min_i(TR_i)\right], \left[\max_i(IL_i), \max_i(IR_i)\right], \left[\max_i(FL_i), \max_i(FR_i)\right]\right)$ then

$$ZA^- \leq \text{IVNNAAOWA}_{zw}\left(SA_1, SA_2, \cdots, SA_n\right) \leq ZA^+ \quad (12)$$

From the Definitions 7 and 8, it's shown that IVNNAAWA and IVNNAAOWA operators weigh the IVNNs and the ordered positions of the IVNNs, respectively. An IVNN Aczel-Alsina hybrid average (IVNNAAHA) operator is produced to include the characteristics of IVNNAAWA and IVNNAAOWA operators together.

Definition 9. Let $SA_i = \left(\left[TL_i, TR_i\right], \left[IL_i, IR_i\right], \left[FL_i, FR_i\right]\right) (i = 1, 2, \ldots, n)$ be the IVNNs. An IVNNAAHA operator is produced:

$$\text{IVNNAAHA}_{zw,sw}\left(SA_1, SA_2, \cdots, SA_n\right) = \bigoplus_{i=1}^{n} \left(zw_i SSA_{\sigma(i)}\right)$$

$$= \left(\begin{bmatrix} 1 - e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(1 - STL_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}}, 1 - e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(1 - STR_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(SIL_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(SIR_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(SFL_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{n} zw_i \left(-\ln\left(SFR_{\sigma(i)}\right)\right)^{\phi}\right)^{1/\phi}} \end{bmatrix} \right) \quad (13)$$

which $zw = \left(zw_1, zw_2, \cdots, zw_n\right)^T$ is the associated weight, with $0 \leq zw_i \leq 1$, $\sum_{i=1}^{n} zw_i = 1$, $SSA_{\sigma(i)}$ is the i-th largest value of the IVNNs $SSA_i\left(SSA_i = \left(nsw_i\right) SA_i\right) = \left(\left[STL_i, STR_i\right], \left[SIL_i, SIR_i\right], \left[SFL_i, SFR_i\right]\right)$, $sw = \left(sw_1, sw_2, \cdots, sw_n\right)$ is the weight of IVNNs $SA_i \left(i = 1, 2, \cdots, n\right)$, with $sw_j \in \left[0, 1\right]$, $\sum_{i=1}^{n} sw_i = 1$, and n is the balancing coefficient.

If $zw = \left(1/n, 1/n, \cdots, 1/n\right)^T$, IVNNAAHA reduces to the IVNNAAWA; and if $sw = \left(1/n, 1/n, \cdots, 1/n\right)$, the IVNNAAHA reduces to IVNNAAOWA.

IV. Method for MADM Based on the IVNNAAWA

The IVNNAAWA is used to build for MADM. Let $CS = \left\{CS_1, CS_2, \cdots, CS_m\right\}$ be alternatives, and attributes

set $GG=\{GG_1,GG_2,\cdots,GG_n\}$ with weight $sw=\{sw_1,sw_2,\cdots,sw_n\}$, where $sw_j\in[0,1],\sum_{j=1}^{n}sw_j=1$. Suppose that values are assessed with IVNNs $QQ=(qq_{ij})_{m\times n}=\left(\left[TL_{ij},TR_{ij}\right],\left[IL_{ij},IR_{ij}\right],\left[FL_{ij},FR_{ij}\right]\right)_{m\times n}$.

Then, method for MADM is built based on the IVNNAAWA. The given steps are produced.

Step 1. Build the IVNN matrix $QQ=(qq_{ij})_{m\times n}=\left(\left[TL_{ij},TR_{ij}\right],\left[IL_{ij},IR_{ij}\right],\left[FL_{ij},FR_{ij}\right]\right)_{m\times n}$.

$$QQ=\left[qq_{ij}\right]_{m\times n}=\begin{bmatrix} qq_{11} & qq_{12} & \cdots & qq_{1n} \\ qq_{21} & qq_{22} & \cdots & qq_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ qq_{m1} & qq_{m2} & \cdots & qq_{mn} \end{bmatrix} \tag{14}$$

Step 2. Normalize $QQ=(qq_{ij})_{m\times n}$ to $NQ=\left[nq_{ij}\right]_{m\times n}$.

$$\begin{aligned} nq_{ij}&=\left(\left[NTL_{ij},NTR_{ij}\right],\left[NIL_{ij},NIR_{ij}\right],\left[NFL_{ij},NFR_{ij}\right]\right)\\ &=\begin{cases}\left(\left[TL_{ij}^{k},TR_{ij}^{k}\right],\left[IL_{ij}^{k},IR_{ij}^{k}\right],\left[FL_{ij}^{k},FR_{ij}^{k}\right]\right), & GG_j \text{ is a benefit criterion}\\ \left(\left[FL_{ij}^{k},FR_{ij}^{k}\right],\left[IL_{ij}^{k},IR_{ij}^{k}\right],\left[TL_{ij}^{k},TR_{ij}^{k}\right]\right), & GG_j \text{ is a cost criterion}\end{cases}\end{aligned} \tag{15}$$

Step 3. According to $NQ=\left[nq_{ij}\right]_{m\times n}$, the overall IVNNs $nq_i\,(i=1,2,\cdots,m)$ are produced through IVNNAAWA operator:

$$\begin{aligned} nq_i&=\text{IVNNAAWA}_{sw}(nq_{i1},nq_{i2},\cdots,nq_{in})\\ &=\bigoplus_{i=1}^{n}sw_i nq_{ij}\\ &=\left(\left[NTL_i,NTR_i\right],\left[NIL_i,NIR_i\right],\left[NFL_i,NFR_i\right]\right)\\ &=\left(\begin{bmatrix}1-e^{-\left(\sum_{j=1}^{n}sw_i\left(-\ln\left(1-NTL_{ij}\right)\right)^{\phi}\right)^{1/\phi}}, 1-e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(1-NTR_{ij}\right)\right)^{\phi}\right)^{1/\phi}}\end{bmatrix},\right.\\ &\quad\begin{bmatrix}e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(NIL_{ij}\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(NIR_{ij}\right)\right)^{\phi}\right)^{1/\phi}}\end{bmatrix},\\ &\quad\left.\begin{bmatrix}e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(NFL_{ij}\right)\right)^{\phi}\right)^{1/\phi}}, e^{-\left(\sum_{i=1}^{n}sw_i\left(-\ln\left(NFR_{ij}\right)\right)^{\phi}\right)^{1/\phi}}\end{bmatrix}\right)\end{aligned} \tag{16}$$

Step 4. Obtain the $SV(nq_i),AV(nq_i)(i=1,2,\cdots,m)$.

$$\begin{aligned} SV(nq_i)&=\frac{\begin{pmatrix}\left(2+NTL_i-NIL_i-NFL_i\right)\\ +\left(2+NTR_i-NIR_i-NFR_i\right)\end{pmatrix}}{6}\\ AV\left(\left(nq_i\right)\right)&=\frac{\left(NTL_i+NTR_i\right)-\left(NFL_i+NFR_i\right)}{2}\end{aligned} \tag{17}$$

Step 5. Rank the $CS_i\,(i=1,2,\cdots,m)$ through $SV(nq_i),AV(nq_i)$.

Step 6. End.

V. Numerical Example and Comparative Analysis

A. Numerical Example

The evaluation of college English teaching quality is an essential aspect of higher education management. It aims to provide a comprehensive analysis and feedback on various aspects of English teaching to ensure the improvement of teaching effectiveness and the enhancement of students' English proficiency. Teaching quality evaluation not only measures the teaching level of instructors but also serves as a critical monitoring tool for assessing student learningoutcomes and the appropriateness of course design. Through this evaluation system, universities can identify the strengths and weaknesses in teaching, continuously improving the content and methods to ensure the achievement of teaching goals. The core aspects of teaching quality evaluation generally include the following: First is the teacher's attitude and teaching ability. This covers the teacher's preparation, teaching methods, attention to students, and the organization and presentation of course content. An excellent English teacher should not only have solid language knowledge but also be able to effectively stimulate students' interest in learning and flexibly use various teaching methods to meet the needs of students at different levels. Second is student participation and learning outcomes. This part of the evaluation assesses student performance in class, completion of assignments, exam results, and other indicators of learning achievement. Student engagement directly affects their learning outcomes, so classroom interaction, task completion, and similar factors are key evaluation criteria. The third aspect is the design of course content and the use of teaching resources. Whether the course content meets the actual needs of students, whether teaching resources are diverse and abundant, and whether modern

teaching methods are employed are all crucial factors influencing teaching quality. Through well-designed courses, students not only acquire language knowledge but also develop cross-cultural communication skills and critical thinking. There are various methods for evaluating teaching quality, including student evaluations, peer reviews, expert observations, and supervision by teaching administrators. Student evaluations are a key component of the evaluation system, providing direct feedback on students' learning experiences and satisfaction with the course. Peer reviews and expert observations offer a more objective assessment of the teacher's capabilities from a professional perspective. By collecting data from multiple sources, the evaluation of college English teaching quality provides constructive feedback to teachers, helping them continuously improve their teaching strategies. Additionally, this evaluation system assists university administrators in gaining a better understanding of the current teaching situation, optimizing resource allocation, and ultimately achieving continuous improvement in English teaching quality. The teaching quality evaluation of college English is looked as MADM. Five possible foreign colleges $CS_i\left(i=1,2,3,4,5\right)$ are assessed with four attributes: ①GG_1 is **Student Learning Outcomes**: This is a key effectiveness indicator, assessed through students' exam scores, language proficiency tests, classroom performance, and the ability to use English in extracurricular activities. High-quality teaching should significantly improve students' English skills. ②GG_2 is **Teaching Costs**: As the sole cost indicator, this involves the input of human, material, and financial resources. It includes teacher salaries, the purchase and maintenance of teaching equipment, textbook expenses, and related training costs. Effective cost management can ensure high teaching quality while achieving efficient resource utilization. ③GG_3 is **Student Satisfaction**: This effectiveness indicator is gathered through surveys, interviews, and other methods to obtain feedback on course content, teaching methods, teacher proficiency, and the learning environment. High satisfaction generally reflects the effectiveness of teaching and student approval. ④GG_4 is **Enhancement of Employability**: This measures students' employment status after graduation, including employment rates, starting salaries, and the ability to use English in the workplace. This indicator reflects the extent to which English teaching supports students' career development and is an important measure of teaching quality. GG_2 is the cost. The IVNNAAWA is built for teaching quality evaluation of college English.

Step 1. Build the $QQ=\left(qq_{ij}\right)_{5\times4}$ in Table I.

TABLE I. IVNN INFORMATION

	GG_1	GG_2
CS_1	([0.42, 0.53], [0.21, 0.32], [0.26, 0.37])	([0.63, 0.74], [0.18, 0.29], [0.22, 0.33])
CS_2	([0.43, 0.54], [0.32, 0.43], [0.23, 0.34])	([0.64, 0.75], [0.23, 0.34], [0.13, 0.24])
CS_3	([0.62, 0.73], [0.26, 0.37], [0.13, 0.24])	([0.48, 0.59], [0.38, 0.49], [0.14, 0.25])
CS_4	([0.58, 0.69], [0.13, 0.24], [0.28, 0.39])	([0.52, 0.63], [0.28, 0.39], [0.17, 0.28])
CS_5	([0.64, 0.75], [0.11, 0.22], [0.22, 0.33])	([0.57, 0.68], [0.24, 0.35], [0.14, 0.25])
	GG_3	GG_4
CS_1	([0.54, 0.65], [0.27, 0.38], [0.16, 0.27])	([0.57, 0.68], [0.12, 0.23], [0.28, 0.39])
CS_2	([0.55, 0.66], [0.14, 0.25], [0.27, 0.38])	([0.53, 0.64], [0.22, 0.33], [0.21, 0.32])
CS_3	([0.73, 0.84], [0.13, 0.24], [0.17, 0.28])	([0.68, 0.79], [0.18, 0.29], [0.12, 0.23])
CS_4	([0.63, 0.74], [0.22, 0.33], [0.13, 0.24])	([0.73, 0.84], [0.12, 0.23], [0.11, 0.22])
CS_5	([0.48, 0.59], [0.32, 0.43], [0.22, 0.33])	([0.62, 0.73], [0.18, 0.29], [0.18, 0.29])

Step 2. Normalize $QQ=\left[qq_{ij}\right]_{5\times4}$ to $NQ=\left[nq_{ij}\right]_{5\times4}$ (see Table II).

TABLE II. THE NORMALIZED IVNN MATRIX

	GG_1	GG_2
CS_1	([0.42, 0.53], [0.21, 0.32], [0.26, 0.37])	([0.22, 0.33], [0.18, 0.29], [0.63, 0.74])
CS_2	([0.43, 0.54], [0.32, 0.43], [0.23, 0.34])	([0.13, 0.24], [0.23, 0.34], [0.64, 0.75])
CS_3	([0.62, 0.73], [0.26, 0.37], [0.13, 0.24])	([0.14, 0.25], [0.38, 0.49], [0.48, 0.59])
CS_4	([0.58, 0.69], [0.13, 0.24], [0.28, 0.39])	([0.17, 0.28], [0.28, 0.39], [0.52, 0.63])

CS_5	([0.64, 0.75], [0.11, 0.22], [0.22, 0.33])	([0.14, 0.25], [0.24, 0.35], [0.57, 0.68])
	GG_3	GG_4
CS_1	([0.54, 0.65], [0.27, 0.38], [0.16, 0.27])	([0.57, 0.68], [0.12, 0.23], [0.28, 0.39])
CS_2	([0.55, 0.66], [0.14, 0.25], [0.27, 0.38])	([0.53, 0.64], [0.22, 0.33], [0.21, 0.32])
CS_3	([0.73, 0.84], [0.13, 0.24], [0.17, 0.28])	([0.68, 0.79], [0.18, 0.29], [0.12, 0.23])
CS_4	([0.63, 0.74], [0.22, 0.33], [0.13, 0.24])	([0.73, 0.84], [0.12, 0.23], [0.11, 0.22])
CS_5	([0.48, 0.59], [0.32, 0.43], [0.22, 0.33])	([0.62, 0.73], [0.18, 0.29], [0.18, 0.29])

Step 3. The subjective weights are obtained through AHP technique (Table III).

TABLE III. THE SUBJECTIVE WEIGHTS

	GG_1	GG_2	GG_3	GG_4
weight	0.2746	0.1832	0.3105	0.2317

Step 4. Obtain the $nq_i\left(i=1,2,\cdots,5\right)$ by utilizing IVNNAAWA operator (Table IV).

TABLE IV. THE $nq_i\left(i=1,2,\cdots,5\right)$ ($\theta=2$)

Alternatives	$nq_i\left(i=1,2,\cdots,5\right)$
CS_1	([0.1023, 0.2134], [0.0456, 0.1567], [0.2789, 0.3890])
CS_2	([0.2145, 0.3256], [0.0678, 0.1789], [0.1901, 0.3012])
CS_3	([0.3267, 0.4378], [0.0890, 0.2001], [0.1456, 0.2567])
CS_4	([0.1345, 0.2456], [0.0123, 0.1234], [0.3678, 0.4789])
CS_5	([0.2467, 0.3578], [0.0345, 0.1456], [0.2890, 0.4001])

Step 5. Obtain the $SV\left(nq_i\right)\left(i=1,2,\cdots,5\right)$ (Table V).

TABLE V. THE $SV\left(nq_i\right)\left(i=1,2,\cdots,5\right)$

Alternatives	$SV\left(nq_i\right)\left(i=1,2,\cdots,5\right)$	Order
CS_1	0.5143	5
CS_2	0.6509	1
CS_3	0.5427	4
CS_4	0.5540	3
CS_5	0.5672	2

Step 6. From Table V, the order is: $XP_2 > XP_5 > XP_4 > XP_3 > XP_1$, and the best choice is XP_2.

B. Comparative Analysis

The IVNNAAWA is compared with IVNNWA & IVNNWG [51]. For IVNWA, the calculating values is: $EV\left(CS_1\right)=0.2897, EV\left(CS_2\right)=0.6658$, $EV\left(CS_3\right)=0.2179,$

$EV(CS_4) = 0.5576,\ EV(CS_5) = 0.4776$. Thus, the order is $CS_2 > CS_4 > CS_5 > CS_1 > CS_3$ .For IVNWG, the calculating values is: $EV(CS_1) = 0.2799, EV(CS_2) = 0.6476, EV(CS_3) = 0.2549,$ $EV(CS_4) = 0.5287,\ \ EV(CS_5) = 0.4769$. So the order is $CS_2 > CS_4 > CS_5 > CS_1 > CS_3$.

Then, IVNNAAWA is compared with IVNN-CODAS[52], the assessment values is: $SVNNAV(CS_1) = -0.2465, SVNNAV(CS_2) = 0.3778,$ $SVNNAV(CS_3) = -0.3239,\ \ SVNNAV(CS_4) = 0.2558,$ $SVNNAV(CS_5) = 0.1379$. Thus, the order is $CS_2 > CS_4 > CS_5 > CS_1 > CS_3$.

TABLE VI. THE COMPARATIVE ANALYSIS

Models	order
IVNNWA [51]	$CS_2 > CS_4 > CS_5 > CS_1 > CS_3$
IVNNWG [51]	$CS_2 > CS_4 > CS_5 > CS_1 > CS_3$
IVNN-CODAS[52]	$CS_2 > CS_4 > CS_5 > CS_1 > CS_3$
IVNNAAWA	$CS_2 > CS_4 > CS_5 > CS_1 > CS_3$

From Table VI, it is evident that the three models under consideration all identify the same optimal choice, albeit in a slightly different sequence. This consistency underscores the rationality and effectiveness of the IVNNAAWA method. Each of the five models discussed has distinct advantages, but the IVNNAAWA stands out for several reasons. One of its most notable strengths is the ability to determine the most favorable alternative by appropriately setting parameter values within the IVNNAAWA operators. This feature offers decision-makers a novel and flexible approach to addressing IVNN-MADM challenges. By incorporating a parameter, the IVNNAAWA method allows for a straightforward representation of fuzzy information, enhancing the transparency of the information aggregation process compared to some existing techniques. This transparency is crucial for decision-makers who need to understand and trust the aggregation process. In contrast, existing aggregation operators, as referenced in prior studies, often lack this level of flexibility in data aggregation. Consequently, the proposed aggregation operator is more advanced and reliable when it comes to decision-making involving IVNN data. The flexibility of the IVNNAAWA method not only simplifies the representation of complex fuzzy information but also enhances the decision-making process by making it more adaptable to various scenarios. This adaptability is particularly beneficial in situations where decision-makers face uncertainty and need to rely on robust methods to guide their choices. The ability to adjust parameters to suit specific needs means that decision-makers can tailor the aggregation process to better fit the unique aspects of their decision-making environment. In summary, the IVNNAAWA aggregation operator provides a significant improvement over existing methods by offering a more flexible and transparent approach to handling IVNN data. Its ability to adapt to different decision-making contexts makes it a valuable tool for decision-makers seeking reliable and sophisticated solutions to complex problems. This innovation in aggregation techniques marks a noteworthy advancement in the field of multi-attribute decision making, ensuring that decision-makers have access to the best possible tools for their needs.

VI. CONCLUSION

The quality evaluation of university English teaching is a comprehensive process that involves multiple dimensions. Firstly, student learning outcomes are a key indicator, assessed through exam scores, language proficiency tests, and classroom performance to evaluate improvements in students' English skills. Secondly, teaching costs are an important factor, including teacher salaries, teaching equipment, and textbook expenses. Effective cost management aids in the efficient utilization of resources. Additionally, student satisfaction is gathered through surveys and interviews, reflecting students' approval of course content, teaching methods, and teacher proficiency. Lastly, the enhancement of employability measures students' ability to use English in the workplace after graduation, including employment rates and starting salaries. These indicators collectively form a comprehensive evaluation of the quality of university English teaching, helping educational institutions continuously optimize teaching strategies and improve teaching effectiveness. The teaching quality evaluation of college English is regarded as the MADM. This paper introduces several Aczel-Alsina operators within the framework of IVNSs. Subsequently, the interval-valued neutrosophic number (IVNN) Aczel-Alsina weighted averaging (IVNNAAWA) operator is utilized to address multi-attribute decision-making (MADM) problems. To demonstrate the effectiveness of the proposed method, a numerical example is provided, focusing on the evaluation of college English teaching quality. This example illustrates how the IVNNAAWA operator can be applied to assess and improve decision-making processes in educational settings. By leveraging the unique characteristics of IVNSs, the method offers a nuanced approach to handling uncertainty and imprecision in decision-making, making it particularly suitable for complex evaluation tasks such as assessing teaching quality. The proposed approach not

only enhances the flexibility of decision-making but also provides a framework for integrating various attributes into a cohesive evaluation model. This contributes to more informed and reliable decision outcomes, ultimately aiding educational institutions in optimizing their teaching strategies and improving overall educational effectiveness.

REFERENCES

[1] C. Lu, J. Huang, Exploration of Constructing an English Teaching Quality Evaluation System and Cultivating Students' Comprehensive English Abilities, Economic Research Guide, (2013) 320-322.

[2] X. Ma, J. Li, Construction of a Multidimensional Ecological Evaluation System in a Network Environment—A Case Study of College English Listening and Speaking Courses, Journal of Jixi University, 13 (2013) 73-75.

[3] Q. Wu, X. Tang, Analysis and Research on College English Classroom Teaching Quality Evaluation System, China Educational Technology & Equipment, (2015) 62-65.

[4] M. Yu, Feasibility Analysis of Improving College English Course Teaching Quality through Diversified Evaluation Models, Journal of Chifeng University (Philosophy and Social Science Edition), 36 (2015) 248-249.

[5] C. Yuan, Analysis of Teaching Evaluation Strategies for Subsequent College English Courses, Journal of Language and Literature (Foreign Language Education and Teaching), (2016) 111-112.

[6] L. Deng, Research on Teaching Quality Evaluation of Participatory Teaching Model in College English, Bohai Economic Outlook, (2017) 150.

[7] B. Yang, Construction of a Teaching Quality Evaluation Index System for Flipped Classrooms in Vocational College English, Journal of Hunan University of Science and Technology, 39 (2018) 114-116.

[8] J. Li, Research on Constructing College English Teaching Quality Evaluation System under the Applied Talent Training System, China Multimedia and Network Teaching Journal (First Half), (2019) 67-68.

[9] J. Xu, Discussion on the Application of Stratified Teaching Methods in College English, Contemporary Research and Teaching, (2020) 115.

[10] S. Yang, R. Li, Construction of a Classroom Teaching Quality Evaluation Model in the Digital Era, Journal of Xi'an International Studies University, 29 (2021) 78-81.

[11] Y. Zhang, Research on College English Teaching Quality Evaluation Guided by Value Speculation, Journal of Anhui University of Technology (Social Science Edition), 39 (2022) 36-40.

[12] C. Gong, R. Peng, English Teaching Quality Evaluation Model Based on ISSA-DRNN, Journal of Chongqing Electric Power College, 28 (2023) 39-43.

[13] J. Zhang, Construction of an English Teaching Quality Evaluation System Based on the CIPP Model, Journal of Taiyuan Urban Vocational College, (2024) 93-96.

[14] B.Q. Yin, S.J. Ouyang, Y.L. Hou, J.Z. Ma, Modified TODIM-TOPSIS technique for type-2 neutrosophic number multiple-attribute decision-making and applications to innovation and entrepreneurship education evaluation in vocational colleges, Journal of Intelligent & Fuzzy Systems, 46 (2024) 5957-5973.

[15] H.L. Wang, L.Q. Feng, M. Deveci, K. Ullah, H. Garg, A novel CODAS approach based on Heronian Minkowski distance operator for T-spherical fuzzy multiple attribute group decision-making, Expert Systems with Applications, 244 (2024) 16.

[16] R. Verma, E. Alvarez-Miranda, Multiple-attribute group decision-making approach using power aggregation operators with CRITIC-WASPAS method under 2-dimensional linguistic intuitionistic fuzzy framework, Applied Soft Computing, 157 (2024) 33.

[17] T. Senapati, An Aczel-Alsina aggregation-based outranking method for multiple attribute decision-making using single-valued neutrosophic numbers, Complex & Intelligent Systems, 10 (2024) 1185-1199.

[18] M. Jamil, F. Afzal, A. Maqbool, S. Abdullah, A. Akgül, A. Bariq, Multiple attribute group decision making approach for selection of robot under induced bipolar neutrosophic aggregation operators, Complex & Intelligent Systems, 10 (2024) 2765-2779.

[19] T. Cui, P.X. Sun, X. Liu, Research on effectiveness evaluation of corporate culture construction based on the neutrosophic cubic number multiple attribute decision making, Journal of Intelligent & Fuzzy Systems, 46 (2024) 2219-2231.

[20] H.L. Wang, T. Mahmood, K. Ullah, Improved CoCoSo Method Based on Frank Softmax Aggregation Operators for T-Spherical Fuzzy Multiple Attribute Group Decision-Making, International Journal of Fuzzy Systems, 25 (2023) 1275-1310.

[21] T. Senapati, G.Y. Chen, R. Mesiar, R.R. Yager, Intuitionistic fuzzy geometric aggregation operators in the framework of Aczel-Alsina triangular norms and their application to multiple attribute decision making, Expert Systems with Applications, 212 (2023) 15.

[22] H.Y. Zhang, G.W. Wei, Location selection of electric vehicles charging stations by using the spherical fuzzy CPT-CoCoSo and D-CRITIC method, Computational & Applied Mathematics, 42 (2023) 35.

[23] H. Zhang, H. Wang, G. Wei, Spherical fuzzy TODIM method for MAGDM integrating cumulative prospect theory and CRITIC method and its application to commercial insurance selection, Artificial Intelligence Review, 56 (2023) 10275-10296.

[24] Z. Wang, Q. Cai, G. Wei, Modified TODIM method based on cumulative prospect theory with Type-2 neutrosophic number for green supplier selection, Engineering Applications of Artificial Intelligence, 126 (2023) 106843.

[25] H. Sun, Z. Yang, Q. Cai, G.W. Wei, Z.W. Mo, An extended Exp-TODIM method for multiple attribute decision making based on the Z-Wasserstein distance, Expert Systems with Applications, 214 (2023) 14.

[26] B.W. Zhu, Y.H. Xiao, W.Q. Zheng, L. Xiong, X.Y. He, J.Y. Zheng, Y.C. Chuang, A Hybrid Multiple-Attribute Decision-Making Model for Evaluating the Esthetic Expression of Environmental Design Schemes, Sage Open, 12 (2022) 20.

[27] M.W. Zhao, G.W. Wei, Y.F. Guo, X.D. Chen, CPT-TODIM METHOD FOR INTERVAL-VALUED BIPOLAR FUZZY MULTIPLE ATTRIBUTE GROUP DECISION MAKING AND APPLICATION TO INDUSTRIAL CONTROL SECURITY SERVICE PROVIDER SELECTION (vol 27, pg 1186, 2021), Technological and Economic Development of Economy, 28 (2022) 581-582.

[28] H.D. Zhang, T.B. Nan, Y.P. He, q-Rung orthopair fuzzy N-soft aggregation operators and corresponding applications to multiple-attribute group decision making, Soft Computing, 26 (2022) 6087-6099.

[29] R. Yong, J. Ye, S.G. Du, A.Q. Zhu, Y.Y. Zhang, Aczel-Alsina Weighted Aggregation Operators of Simplified Neutrosophic Numbers and Its Application in Multiple Attribute Decision Making, Cmes-Computer Modeling in Engineering & Sciences, 132 (2022) 569-584.

[30] S.H. Gurmani, H.Y. Chen, Y.H. Bai, An extended MABAC method for multiple-attribute group decision making under probabilistic T-spherical hesitant fuzzy environment, Kybernetes, 52 (2023) 4041-4060.

[31] C.X. Guo, Y.Y. Wang, S. Yuan, Z.Y. Li, A Novel Hybrid Multiple Attribute Decision Making Framework for Enterprise Green Marketing Performance Management Evaluation Based on the Triangular Fuzzy Neutrosophic Sets, Ieee Access, 11 (2023) 142676-142688.

[32] M. Feng, H.J. Guan, Some Novel Maclaurin Symmetric Mean Operators for q-Rung Picture Fuzzy Numbers and Their Application to Multiple Attribute Group Decision Making, Ieee Access, 11 (2023) 50710-50743.

[33] Y. Deng, W.X. Zhang, An ExpTODIM-GRA based multiple attribute group decision-making method for development level evaluation of digital inclusive finance under intuitionistic fuzzy circumstances, Journal of Intelligent & Fuzzy Systems, 45 (2023) 10661-10673.

[34] M. Palanikumar, K. Arulmozhi, C. Jana, M. Pal, Multiple-attribute decision-making spherical vague normal operators and their applications for the selection of farmers, Expert Systems, 40 (2023) 26.

[35] A. Noori, H. Bonakdari, A.H. Salimi, L. Pourkarimi, J.M. Samakosh, A novel Multiple Attribute Decision-making approach for assessing the effectiveness of advertising to a target audience on drinking water consumers? behavior considering age and education level, Habitat Int., 133 (2023) 9.

[36] T. Mahmood, U.U. Rehman, Z. Ali, Analysis and applications of Aczel-Alsina aggregation operators based on bipolar complex fuzzy information

in multiple attribute decision making, Information Sciences, 619 (2023) 817-833.

[37] N.N. Liao, H. Gao, R. Lin, G.W. Wei, X.D. Chen, An extended EDAS approach based on cumulative prospect theory for multiple attributes group decision making with probabilistic hesitant fuzzy information, Artificial Intelligence Review, 56 (2023) 2971-3003.

[38] A. Jaglan, G. Sadera, P. Singh, B.P. Singh, G. Goel, Probiotic potential of gluten degrading Bacillus tequilensis AJG23 isolated from Indian traditional cereal-fermented foods as determined by Multiple Attribute Decision-Making analysis, Food Res. Int., 174 (2023) 10.

[39] C.H. Hsu, B.C. Jiang, Fuzzy multiple attribute decision making using a simplified centroid-based arithmetic process, International Journal of Industrial Engineering-Theory Applications and Practice, 6 (1999) 61-71.

[40] Z.S. Xu, A note on linguistic hybrid arithmetic averaging operator in multiple attribute group decision making with linguistic information, Group Decision and Negotiation, 15 (2006) 593-604.

[41] G.L. Tang, X.Y. Zhao, Z.Y. Zhao, J.J. Yu, L. Guo, Y.H. Wang, Simulation-based Fuzzy Multiple Attribute Decision Making framework for an optimal apron layout for aRoll-on/Roll-off/Passenger terminal considering passenger service quality, Simulation-Transactions of the Society for Modeling and Simulation International, 97 (2021) 451-471.

[42] R. Verma, On intuitionistic fuzzy order-alpha divergence and entropy measures with MABAC method for multiple attribute group decision-making, Journal of Intelligent & Fuzzy Systems, 40 (2021) 1191-1217.

[43] L. Wang, Y.L. Bao, Multiple-Attribute Decision-Making Method Based on Normalized Geometric Aggregation Operators of Single-Valued Neutrosophic Hesitant Fuzzy Information, Complexity, 2021 (2021) 15.

[44] M.T. Yan, J. Wang, Y.R. Dai, H.H. Han, A method of multiple-attribute group decision making problem for 2-dimension uncertain linguistic variables based on cloud model, Optimization and Engineering, 22 (2021) 2403-2427.

[45] M.W. Zhao, G.W. Wei, X.D. Chen, Y. Wei, Intuitionistic fuzzy MABAC method based on cumulative prospect theory for multiple attribute group decision making, International Journal of Intelligent Systems, 36 (2021) 6337-6359.

[46] J. Aczél, C. Alsina, Characterizations of some classes of quasilinear functions with applications to triangular norms and to synthesizing judgements, Aequationes Mathematicae, 25 (1982) 313-315.

[47] S. Ashraf, S. Ahmad, M. Naeem, M. Riaz, M.A. Alam, Z. Stevic, Novel EDAS Methodology Based on Single-Valued Neutrosophic Aczel-Alsina Aggregation Information and Their Application in Complex Decision-Making, Complexity, 2022 (2022) 1-18.

[48] H. Wang, F. Smarandache, Y.Q. Zhang, R. Sunderraman, Interval Neutrosophic Sets and Logic: Theory and Applications in Computing, Hexis: Phoenix, AZ, USA, (2005).

[49] H. Wang, F. Smarandache, Y.Q. Zhang, R. Sunderraman, Single valued neutrosophic sets, Multispace Multistruct, (2010) 410-413.

[50] Y.H. Huang, G.W. Wei, C. Wei, VIKOR Method for Interval Neutrosophic Multiple Attribute Group Decision-Making, Information, 8 (2017) 144.

[51] H.Y. Zhang, J.Q. Wang, X.H. Chen, Interval Neutrosophic Sets and Their Application in Multicriteria Decision Making Problems, Scientific World Journal, 2014 (2014) 645953.

[52] E. Bolturk, A. Karasan, Prioritization of Investment Alternatives for a Hospital by Using Neutrosophic CODAS Method, Journal of Multiple-Valued Logic and Soft Computing, 33 (2019) 381-396.

A Smoke Source Location Method Based on Deep Learning Smoke Segmentation

Yuanpan ZHENG*, Zeyuan HUANG, Hui WANG, Binbin CHEN, Chao WANG, Yu ZHANG
School of Computer Science and Technology
Zhengzhou University of Light Industry, Zhengzhou 450000, Henan, China

***Abstract*—The generation of smoke is an early warning sign of a fire, and fast, accurate detection of smoke sources is crucial for fire prevention. However, due to the strong diffusivity of smoke, its morphology is easily influenced by environmental factors, and in complex real-world scenarios, smoke sources are often obscured. Current methods lack precision, generalization ability, and robustness in complex environments. With the advancement of deep learning-based smoke segmentation technology, new approaches to smoke source localization have emerged. Smoke segmentation, driven by deep learning models, can accurately capture the morphological characteristics of smoke. This paper proposes a precise and robust smoke source localization method based on deep learning-enabled smoke segmentation. We first conducted experimental evaluations of commonly used deep learning segmentation models and selected the best-performing model as input. Based on the segmentation results, we analyzed the diffusion characteristics and transmittance of smoke, constructed a concentration model, and used it to accurately locate the smoke source. Experimental results demonstrate that, compared with existing methods, this approach maintains high localization accuracy in multi-target smoke scenarios and complex environments, with superior generalization ability and robustness.**

***Keywords*—Smoke segmentation; smoke source detection; deep learning; instance segmentation; mathematical modeling**

I. INTRODUCTION

Disaster monitoring and prevention is a broad research area directly related to the safety of people's lives and property. The key to fire monitoring and prevention lies in early detection and timely response. In the field of computer vision, early fire detection and prevention essentially focuses on the detection and warning of fire smoke, as smoke is a significant indicator of fire occurrence. Research shows that during the early stages of a fire, the combustion intensity is weak, the temperature and radiant heat of the fire scene are low, and flames are not produced when the temperature of combustible materials has not yet reached the ignition point. Usually, smoke is generated on the surface of combustible materials at this stage [1]. Therefore, the appearance of smoke is a precursor to fire outbreaks [2].

Accurately locating the source of fire smoke is crucial in fire monitoring and prevention. Pinpointing the smoke source helps rapidly identify the location of a fire, providing key information for emergency response, reducing response time, and improving firefighting efficiency. Additionally, smoke source localization helps understand the fire's development and spread direction, which supports the formulation of evacuation routes and protective measures to minimize casualties and property losses. Furthermore, accurately determining the smoke source can prevent false alarms caused by similar phenomena, thereby enhancing the reliability and effectiveness of fire warning systems. Thus, smoke source localization is not only a critical technology for early fire warning but also an essential part of ensuring fire response and disaster mitigation capabilities.

With the continuous development of related technologies in the field of computer vision, methods for detecting smoke using visual sensors have gradually matured. However, due to smoke strong diffusion and the multiple reflections and occlusions it experiences in everyday environments, accurately determining the smoke source remains a challenge. In recent years, significant progress has been made in deep learning-based smoke segmentation methods. Smoke segmentation technology can visually reflect the spatial distribution of smoke, making it easier to analyze its diffusion and indirectly infer the smoke source location, providing new insights for smoke source localization.

This paper proposes a precise smoke's source localization method that combines instance segmentation and mathematical modeling. First, the smoke area was extracted from the background using segmentation techniques. Then, mathematical modeling was applied to the smoke region to extract pixel coordinates and grayscale values, and the smoke diffusion characteristics and direction were derived by curve fitting. Based on this, a smoke concentration model is constructed using the dark channel algorithm to locate the area with the highest concentration, thereby estimating the exact position of the smoke source. The main contributions of this paper are as follows:

1) We constructed a fire smoke segmentation dataset with multi-scale, complex scenes and varying attributes.

2) We proposed a smoke source detection method. By analyzing the smoke segmentation results, we established a diffusion model and transmittance model based on smoke contours and static characteristics, combined these two models to construct a smoke concentration model, and inferred the smoke source location using the concentration model.

3) We analyzed several instance segmentation models, including the U-Net series [4, 15], DeepLab series [7-10], and others like FCN [3], SegNet [5], and PSPNet [6], for fire smoke segmentation tasks. After evaluating their performance and accuracy, we selected the optimal model to support smoke source detection.

The structure of this paper is as follows: Section II introduces related work on fire smoke source localization and smoke

segmentation; Section III describes the algorithm proposed for locating fire smoke sources; Section IV presents a comparative analysis of several commonly used smoke segmentation models, selects the most suitable model for fire smoke segmentation, and tests the proposed smoke source localization scheme; Section V concludes the paper and discusses future research directions.

II. Related Work

A. Smoke Segmentation

Research in recent years has shown that scholars are more inclined to use deep learning methods to segment smoke, but most of the methods rely on existing semantic segmentation networks. Researchers achieve smoke segmentation by improving the semantic segmentation model with better performance, Wang et al. [13] improved the Deeplab V3 network model by embedding channel attention and deformable pyramid in the model, and feature refinement of the input image to improve the model segmentation accuracy, although the enhancement is not obvious, it provides a direction for the model improvement. Liu et al. [14] improved the Deeplab v3+ network model by improving ASPP structure through heterogeneous sensory wild fusion and incorporating a channel attention module. Salman Khan et al. [11] added an improved multi-scale separable convolutional encoder and decoder to the Deeplab v3+ model, along with a per-pixel classifier to improve the model. Taoyang Wang et al. [12] improved on Unet++ by introducing a convolutional attention module CBAM in the original coding layer making the network adaptively selectable and feature-enhanced to be able to focus more on smoke targets.

In addition to improving the model, some scholars have also implemented smoke segmentation by designing new model structures. Yuan et al. [16] designed a W-Net network model to segment smoke, which uses asymmetric encoders and decoders stacked in multiple layers, and segments the smoke region through the use of smoke density estimation. Yuming Li et al. [17] proposed a two-path smoke semantic segmentation network, although the architecture is different from conventional segmentation models, the core idea is still using pyramid pooling and channel attention. After proving that the attention mechanism can effectively improve the accuracy of the model, Yuan et al. [18] proposed a cross-scale hybrid attention network, a kind of fusion of 3D attention, multi-scale channel attention, and hybrid cross-enhancement, which is experimentally proved to have a certain degree of smoke segmentation ability.

B. Smoke Source Localization

Research on smoke source localization is relatively limited, especially regarding automated or intelligent methods for locating smoke sources. Traditionally, smoke source localization has relied on conventional visual monitoring and manual intervention techniques [19]. While these methods have been used in practical applications, their efficiency and accuracy largely depend on experience. In recent years, with the rapid development of computer vision technology, some image processing and machine learning methods have been applied in fire monitoring systems, but specialized techniques for smoke source localization remain relatively scarce.

Most existing smoke source localization methods are based on the physical properties of smoke diffusion, sensor data fusion, and multi-angle visual information. Cao et al. [20] proposed a feature foreground network that models the complex variation patterns of smoke features, enhancing smoke recognition capabilities. By using feature extraction and separation techniques, and integrating environmental conditions such as temperature and wind speed provided by sensors, they effectively separated smoke foreground from complex backgrounds, enabling smoke source prediction in dynamic environments. Zhou et al. [21] developed a vision-based localization method that analyzes the dynamic diffusion patterns of smoke captured by cameras using the U-Net algorithm to estimate the smoke source. However, the high cost of sensors and their susceptibility to environmental conditions, along with the highly random nature of smoke diffusion in the air [22], limit the widespread application of these methods in complex environments.

III. Methods

Smoke detection and segmentation can roughly determine the overall area where the smoke is located, but due to the diffusive nature of smoke, accurately pinpointing the smoke source is often difficult. Therefore, when predicting the smoke source, it is necessary to incorporate data related to smoke morphology, color, transmittance, and its diffusion characteristics into the calculations to model the smoke region. By constructing a fitted curve, we can solve for the pixel diffusion rate and the diffusion direction within the smoke region. Additionally, we apply the dark channel algorithm [23] to process the image, reducing the impact of light sources on the smoke and analyzing the grayscale values presented by the smoke. This allows us to build a smoke transmittance model. Finally, by combining the diffusion rate model and the transmittance model, we construct a smoke concentration model, identifying the point of highest smoke concentration. Using the diffusion direction, we can then predict the precise area of the smoke source. The flowchart for smoke source localization is shown in Fig. 1.

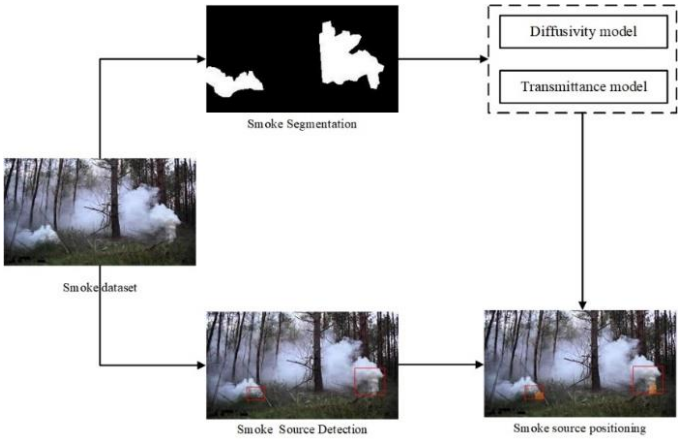


Fig. 1. Smoke source localization flowchart.

A. Smoke Information Extraction

First, the grayscale value of each pixel in the smoke region is obtained, as the grayscale value can reflect the foreground

degree of the current smoke region. The foreground degree can be inferred from the relative thickness of the smoke, indirectly reflecting the transmittance of the smoke. Before converting the image to grayscale, the dark channel algorithm is applied to reduce the impact of bright fog on the smoke region, ensuring that the grayscale values more accurately reflect the smoke's foreground intensity. Then, by traversing the coordinates of all smoke pixels, a set of coordinate points for the smoke region is constructed, allowing for binarization of the smoke region.

B. Diffusivity and Transmittance Modeling

The diffusion direction of smoke generally spreads from bottom to top and from inside to outside. In terms of computer vision, the construction of the diffusion model is primarily based on the contour information of the smoke. The transmittance model is constructed based on the grayscale values of the smoke processed using the dark channel algorithm. First, a cubic polynomial regression curve is constructed based on the coordinate data from the set of coordinate points, and the coefficients are solved using the least squares method. Next, after constructing the fitted curve, the data from the set of coordinate points is grouped into segments of 10 pixels each, and the average variance between the pixel points in each group and the fitted curve is calculated. The size of the average variance is considered the value of the diffusion rate, with lighter colors having smaller diffusion rates and darker colors having larger diffusion rates. Additionally, the sets of points with the largest and smallest diffusion rates are obtained, and the direction from the area with the smallest diffusion rate to the area with the largest diffusion rate is regarded as the direction of smoke diffusion.

$$Y = AX^3 + BX^2 + CX + D \tag{1}$$

The transmittance model is based on the grayscale value of each pixel. After processing the image using the dark channel algorithm, part of the bright fog effect can be eliminated, allowing the transmittance of the smoke to be judged based on the grayscale values. Regions with larger grayscale values indicate that they are closer to the foreground, meaning the smoke is denser and the transmittance is relatively low. Conversely, regions with smaller grayscale values are closer to the background, where the smoke is less dense than in the foreground, resulting in higher transmittance. In the field of computer vision, the image model is defined as follows:

$$I(x) = J(x)t(x) + A(1-t(x)) \tag{2}$$

where, I represents the image with haze, J represents the image without haze, t represents the transmittance, and A represents the global atmospheric light.

The formula for the dark channel algorithm is as follows:

$$J_{dark}(x) = \min_{y\in\Omega(x)}\left(\min_{c\in(r,g,b)} J_c(y)\right) \to 0 \tag{3}$$

where J_{dark} represents the dark channel, Ω(x) represents a square region centered at x, and Jc represents the image processed through the dark channel in the c-channel.

$$t(x) = 1 - \min_{y\in\Omega(x)}\left(\min_{c\in(r,g,b)} \frac{I_c(y)}{A_c}\right) \tag{4}$$

The diffusivity model and the transmittance model are illustrated in Fig. 2.

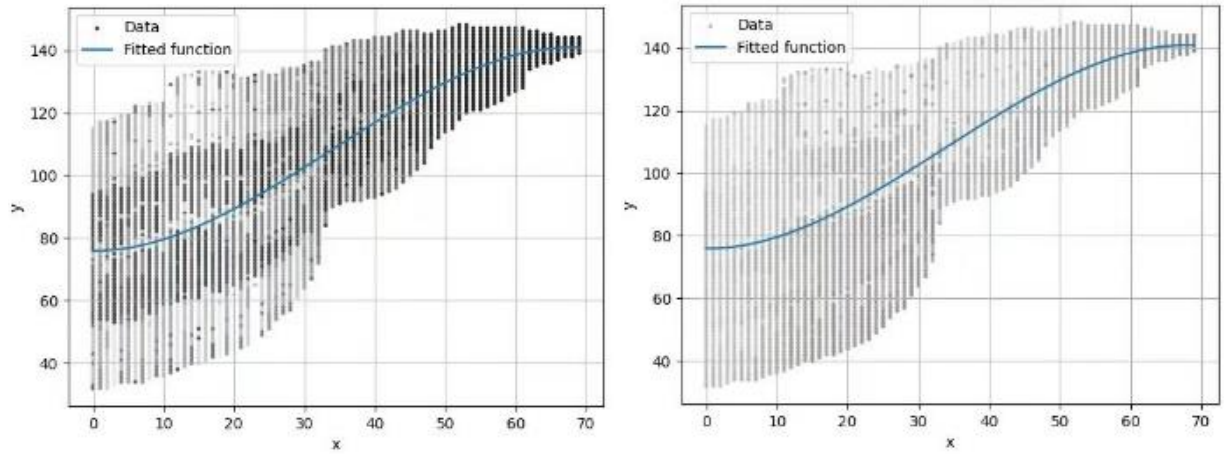
C. Smoke Concentration Modeling

The smoke concentration model is based on the diffusivity and transmittance models, where the diffusivity and transmittance values are added at different ratios to form the concentration value. After modeling the concentration, extreme concentration areas are marked, with red indicating areas of highest smoke concentration and blue indicating areas of lowest smoke concentration.

The smoke concentration can be expressed as:

$$N = yK + (1-y)(1-T) \tag{5}$$

where N represents the concentration value, K represents the diffusivity value, T represents the transmittance, and y represents the ratio.



Diffusivity model. Transmittance model.

Fig. 2. Diffusivity and transmittance model.

In addition to single-target smoke, there is also multi-target smoke. The multi-target smoke concentration model is constructed by dividing the smoke based on enclosed regions, where the smoke in each enclosed region is modeled separately as a concentration. After completing the smoke model construction, a set of pixels with the highest smoke concentration is obtained. The highest concentration area is tangential to the fitted curve, and the area formed by the extension of the tangent line and the extension line in the opposite direction of diffusion is used as the predicted smoke source area. The size of the predicted smoke source region is set to the size of the outer bounding box of the area with the highest concentration.

The predicted smoke source region is illustrated in Fig. 3. To further enhance the effectiveness of smoke source localization, we also selected the YOLOv8n [24] smoke source region detection model as a supplementary method to assist in limiting the location of the smoke source. Fig. 4 illustrates the schematic diagram of the smoke source localization method.

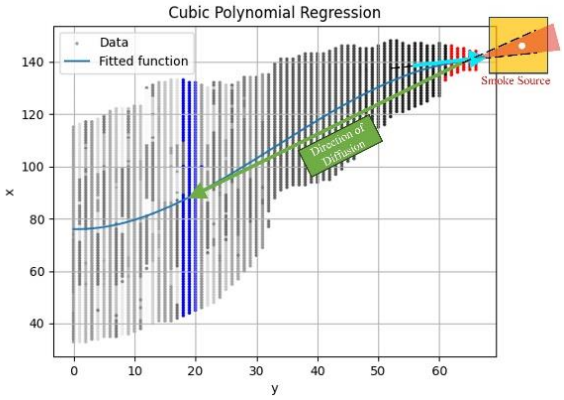


Fig. 3. Smoke source prediction area.

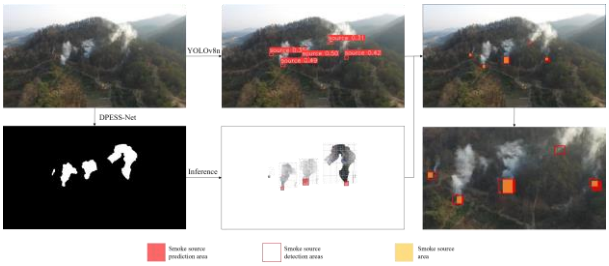


Fig. 4. Schematic diagram of smoke source localization method.

IV. Experimental Results

A. Segmentation Model Selection

In this section, our goal is to select a segmentation model that strikes a balance between segmentation accuracy and speed, meeting the needs of smoke source localization. Specifically, the model must maintain high accuracy while maximizing segmentation speed to ensure the timeliness of smoke source localization. Fig. 5 shows the proposed model testing flowchart.

Building on previous work, we have selected the nine most representative and high-performing segmentation models from commonly used models. These models were tested and evaluated on a self-constructed smoke segmentation dataset to ensure that the selected model possesses good adaptability and stability in practical applications.

1) Dataset and Evaluation Metrics: Next, we will introduce the dataset and evaluation metrics used to analyze the strengths and weaknesses of the segmentation models. The experimental dataset was selected from publicly available sources that could serve as valid samples. For video files, we used frame segmentation to divide the entire video data frame by frame and sampled up to 20 frames at intervals to avoid having overly similar samples. Additionally, we used real fire videos and images from scenarios such as urban areas, forests, and grasslands, selecting relevant fire smoke footage for frame-by-frame segmentation and interval sampling.

Furthermore, we simulated fire smoke generation in open areas, using video tools placed at different locations relative to the smoke source to record the smoke formation. These recordings were then segmented frame by frame, and interval samples were collected to capture fire smoke samples of various scales. Lower-resolution samples were also included to address extreme conditions. In total, the dataset collected 1,511 valid data points, including samples with multiple scales and targets, samples with complex backgrounds, and those exhibiting complex static attributes such as color, concentration, shape, texture, and expansion.

We used image processing software to manually annotate each collected sample. Since this study focuses on the detailed edges of smoke, most of the annotations were made at the pixel level. However, to minimize issues such as overfitting, generalization errors, and information loss, the edges of the labels were appropriately smoothed. We also applied symmetric processing to all samples and their corresponding labels on the left and right sides, and increased the size of the training set through data augmentation to address the challenges of sample refinement.

After these processes, our effective dataset contained 3,022 fire smoke sample images and 3,022 corresponding label annotations. To verify the validity of our custom fire smoke segmentation dataset, we randomly selected 1,000 samples and their labels to conduct comparative experiments using a basic semantic segmentation model on the training set. From the model's training results, our custom fire smoke segmentation dataset generally yielded better training outcomes compared to publicly available fire smoke segmentation datasets. Part of the dataset is shown in Fig. 6.

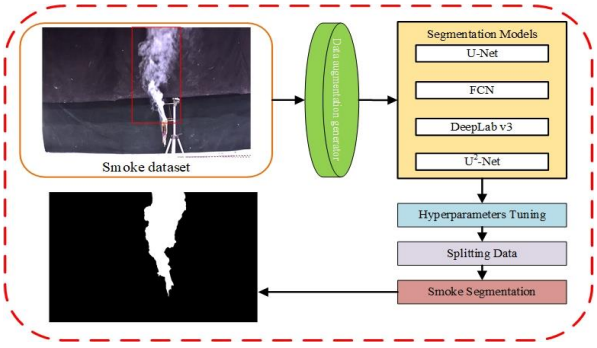


Fig. 5. Model testing flowchart.

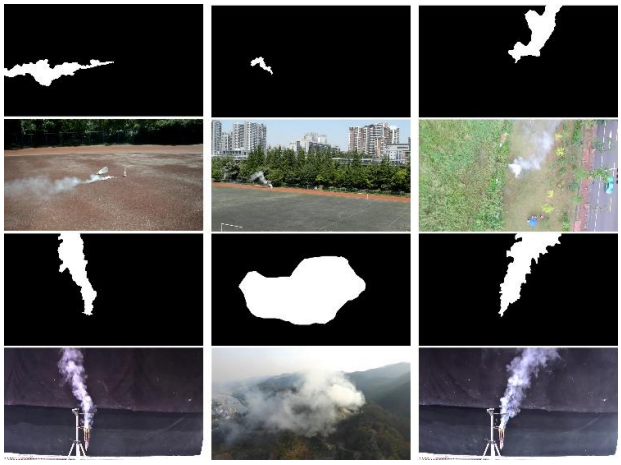


Fig. 6. Partial dataset.

2) Experimental Environment and Evaluation Metrics

The hardware environment used for the experiments in this paper is shown in Table I.

TABLE I. EXPERIMENTAL ENVIRONMENT

CPU	AMD EPYC 7773X @ 3.50GHz
GPU	GeForce RTX 4090
RAM	80G
Operating System	Ubuntu 20.04
Programming Language	Python 3.8
Deep Learning Framework	Pytorch 2.0.0
GPU Acceleration Library	Cuda 11.8

For the smoke segmentation model, we primarily focus on its segmentation accuracy and speed. Therefore, we selected mIoU, mPA, MaxF1, and FPS as the evaluation metrics for the segmentation model.

*a)*mIoU measures the overlap between the predicted segmentation and the ground truth. It is the average IoU for each class. The calculation formulas are shown in Eq. (6) and Eq. (7).

$$IoU = \frac{TP}{TP + FP + FN} \tag{6}$$

$$mIoU = \frac{1}{N}\sum_{i=1}^{N}\frac{TP_i}{TP_i + FP_i + FN_i} \tag{7}$$

where N represents the number of classes, and i represents the total number of categories.

*b)*mPA measures the pixel classification accuracy for each class, averaging the pixel accuracy for each category. The calculation formula is shown in Eq. (8).

$$mPA = \frac{1}{N}\sum_{i=1}^{N}\frac{TP_i}{TP_i + FN_i} \tag{8}$$

F1 Score is the harmonic mean of precision and recall, balancing both metrics. MaxF1 is the maximum F1 score obtained during multi-threshold testing. The formulas are shown in Eq. (9) and Eq. (10).

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{9}$$

$$MaxF1 = \max\left(F1\right) \tag{10}$$

The formulas for Precision and Recall are provided in Eq. (11) and Eq. (12).

$$Precision = \frac{TP}{TP + FP} \tag{11}$$

$$Recall = \frac{TP}{TP + FN} \tag{12}$$

FPS measures the processing speed of the model, indicating how many image frames the model can process per second. It is used to evaluate the real-time performance of the model.

3) Experimental Results and Analysis: We trained and tested several models, including U-Net, FCN, SegNet, PSPNet, DeepLab V3+, U2-Net, U2-Net+, DPESS-Net+ (64 channels), and DPESS-Net, using our custom fire smoke segmentation dataset. The final test results are shown in Table II, and the mIoU training process is illustrated in Fig. 7. The experimental data in Table II indicate that DPESS-Net performed the best overall, achieving mIoU scores of 91.09% under AVG20 and 91.18% under TOP1, an mPA of 96.96%, and a MaxF1 score of 94.37%. However, its FPS was 15.60, placing it in the medium range for processing speed.

TABLE II. THE PERFORMANCE OF THE MODEL IN COMPARATIVE EXPERIMENTS AND BOLD FONT INDICATES BEST GRADE.

Model	mIoU (%)		mPA (%)	MaxF1 (%)	FPS
	AVG²⁰	*TOP¹*			
U-Net	86.07	87.70	96.09	93.46	26.39
FCN	84.59	85.97	95.31	91.95	**27.37**
SegNet	85.47	86.45	95.70	92.48	21.22
PSPNet	84.23	85.16	95.20	91.61	17.54
DeepLab V3+	85.50	87.31	95.28	92.29	11.50
U^2-Net	86.83	87.80	96.01	93.01	13.37
U^2-Net+	85.98	86.68	95.90	92.67	12.91
DPESS-Net+	89.08	89.73	96.75	93.45	9.34
DPESS-Net (Ours)	**91.09**	**91.18**	**96.96**	**94.37**	15.60

Fig. 7. The results of mIoU of the models in the comparative experiment.

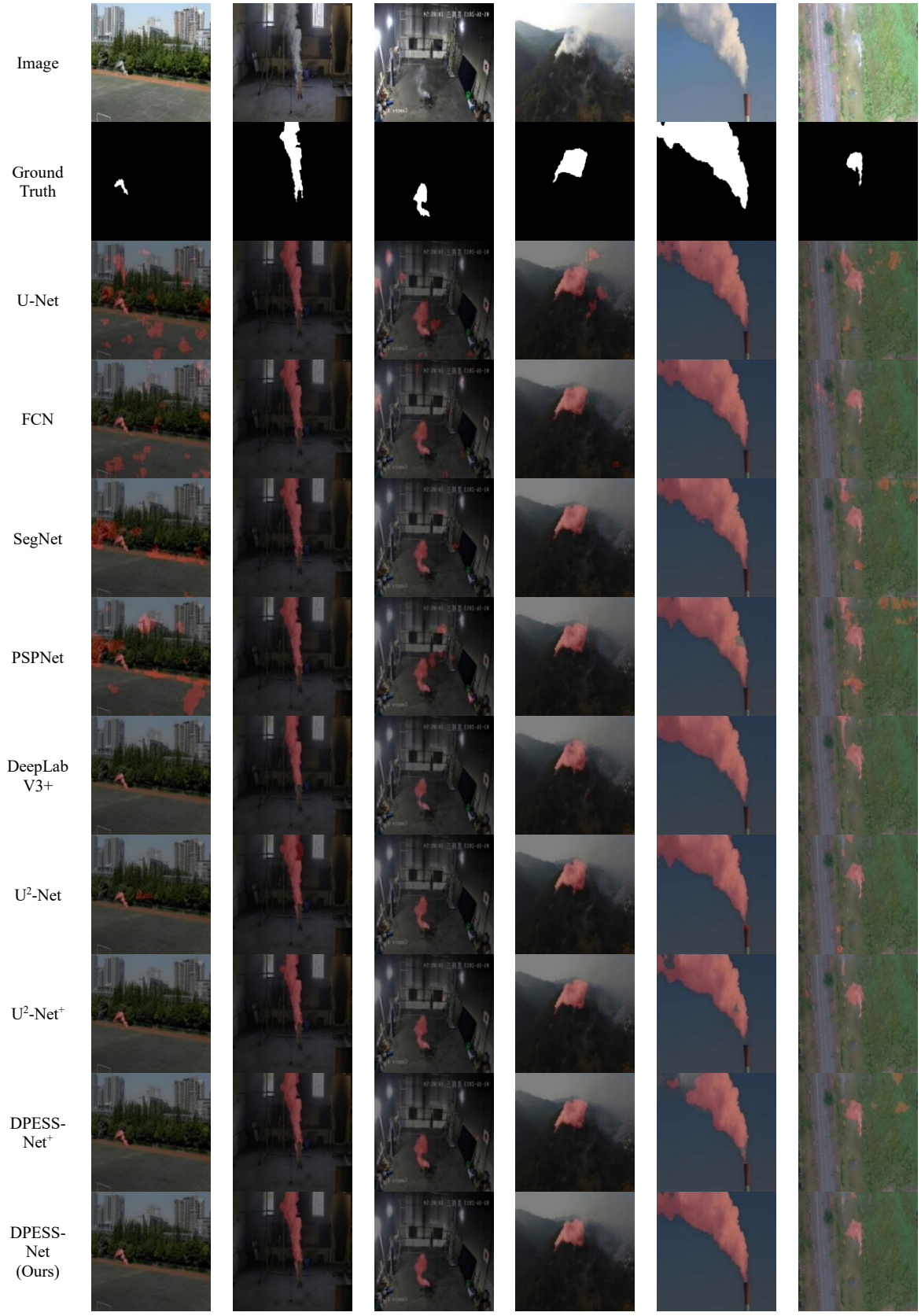


Fig. 8. Comparison of segmentation performance between our proposed method and the other eight models.

DPESS-Net's ability to achieve these results is largely attributed to its dual-channel encoder design, which enables effective information exchange between the channels. The fusion of multi-scale body features and edge-enhanced features further improves the model's ability to capture smoke targets, resulting in higher segmentation accuracy while focusing on both smoke mass and edge details.

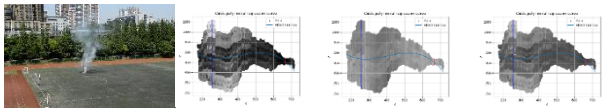
As observed in the training process shown in Fig. 7, U-Net maintains a moderate level of performance, while U2-Net slightly outperforms U-Net. FCN, PSPNet, and SegNet exhibit relatively lower segmentation accuracy but higher FPS because their architectures are relatively simple, allowing for faster segmentation speeds. DeepLab V3+, due to its more complex architecture, remains stable with relatively slower segmentation speed. DPESS-Net+, a version of DPESS-Net with the number of channels reduced to 64, decreases the parameter count and model size, improving efficiency at the cost of slightly lower accuracy.

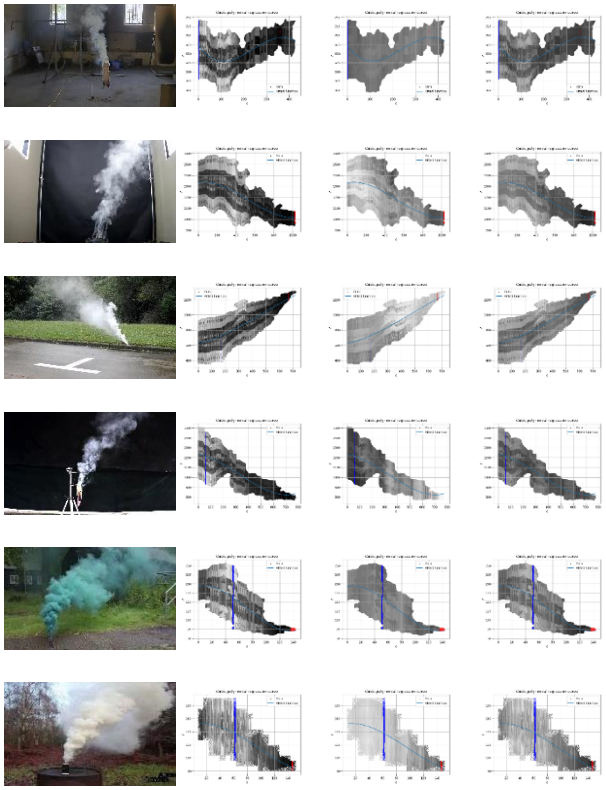
To more intuitively display the segmentation accuracy and performance of the models, we present the segmentation results of each model in Fig. 8. From the comparison images, it can be seen that in scenarios with complex backgrounds and small smoke bodies, most segmentation models experience errors and fail to segment the smoke completely. In scenarios with relatively simple backgrounds and clear main subjects, most models are able to segment the main body of the smoke; however, the details along the edges are not segmented as clearly.

In many scenes, DPESS-Net outperforms the other models, showing minimal segmentation errors. It achieves complete smoke body segmentation with clear edge details, meeting the segmentation accuracy requirements for smoke semantic segmentation as discussed in this paper. Therefore, DPESS-Net is selected as the smoke segmentation solution for the smoke source localization method.

B. *Experimental Results of Smoke Source Localization*

During the modeling process of the concentration model, it was found that the concentration modeling for single-target smoke is relatively stable and can accurately find the area with the highest concentration. However, in case of multi-target smoke, the results of the smoke segmentation model often show multiple smoke targets, which may be connected if the distance between the smoke targets is too small, and this has led to leakage detection in the concentration model when inferring the smoke source area. For this situation, we output the prediction results of YOLOv8n smoke region detection at the same time to maximize the accuracy of the algorithm. The results of the concentration model construction and the results of the smoke source localization algorithm are shown in Fig. 9 and Fig. 10.





Images Diffusivity Transmittance Concentration

Fig. 9. Model building results.

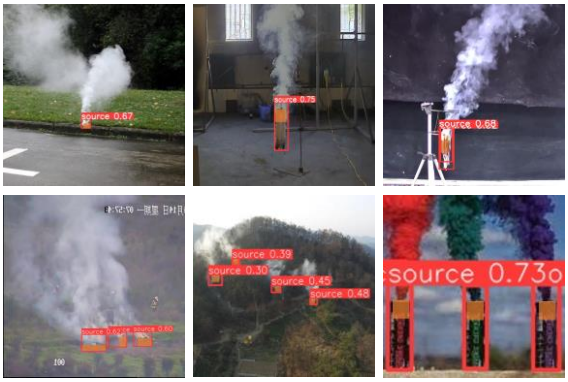


Fig. 10. Smoke source localization results.

V. Conclusions

This paper presents a smoke source localization method based on smoke segmentation, aimed at improving the precision of smoke source localization. Firstly, the paper compares and analyzes various mainstream smoke segmentation models, evaluating their performance in practical applications, and ultimately selects the most suitable segmentation model as the core algorithm. This model effectively extracts the morphological and concentration distribution characteristics of smoke, which are then used for reverse inference of the smoke diffusion process. Combined with a smoke source detection algorithm, the paper achieves high-precision localization of the smoke source. The core of this method lies in utilizing the results of smoke segmentation to correlate the dynamic diffusion

process of smoke with the source point, thereby enabling accurate trace-back localization.

From a practical perspective, this method has significant potential in enhancing early fire detection systems and industrial safety monitoring by providing accurate smoke source localization in complex environments. However, the proposed method still relies heavily on high-quality segmentation results, and its performance in extremely noisy or occluded scenarios requires further investigation. Additionally, the computational cost of the current algorithm may pose challenges for large-scale or real-time applications, which calls for future optimizations.

Future research will focus on two key areas of optimization: first, further improving the processing speed of the segmentation model to meet real-time application requirements; and second, enhancing localization accuracy in multi-target scenarios to ensure efficient and precise smoke source identification in complex environments. Additionally, efforts will be made to simplify the algorithmic process of source localization to reduce computational complexity and improve the system's applicability.

Looking ahead, integrating this method with other data sources, such as thermal imaging or environmental sensors, could further enhance its robustness and adaptability. The continued advancement of AI and IoT technologies also holds promise for creating more intelligent and efficient smoke detection systems. By addressing these challenges and leveraging these opportunities, the proposed method can serve as a foundation for more reliable and effective safety warning systems in the future.

DATA AVAILABILITY

Data used for this article were collected by the research team and will be given to other researchers upon request.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

ACKNOWLEDGMENT

This study was supported by the Key Scientific Research Project Plan for Higher Education Institutions of Henan Province, China（No.25A520033)

REFERENCES

[1] M. A. Finney, "The wildland fire system and challenges for engineering," Fire Safety Journal, vol. 120, p. 103085, 2021.

[2] S. Chaturvedi, P. Khanna, and A. Ojha, "Comparative Analysis of Traditional and Deep Learning Techniques for Industrial and Wildfire Smoke Segmentation," in 2021 Sixth International Conference on Image Information Processing (ICIIP), 2021, vol. 6, pp. 326-331.

[3] J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks for semantic segmentation," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2015, pp. 3431-3440.

[4] O. Ronneberger, P. Fischer, and T. Brox, "U-net: Convolutional networks for biomedical image segmentation," in Medical image computing and computer-assisted intervention–MICCAI 2015: 18th international conference, Munich, Germany, October 5-9, 2015, proceedings, part III 18, 2015, pp. 234-241: Springer.

[5] V. Badrinarayanan, A. Kendall, and R. Cipolla, "Segnet: A deep convolutional encoder-decoder architecture for image segmentation," vol. 39, no. 12, pp. 2481-2495, 2017.

[6] H. Zhao, J. Shi, X. Qi, X. Wang, and J. Jia, "Pyramid scene parsing network," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2017, pp. 2881-2890.

[7] L. C. Chen, G. Papandreou, and I. Kokkinos, "Semantic image segmentation with deep convolutional nets and fully connected crfs," in International conference on learning representations, 2015.

[8] L.C. Chen, G. Papandreou, and I. Kokkinos, "Deeplab: Semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected crfs," vol. 40, no. 4, pp. 834-848, 2017.

[9] L.C. Chen, G. Papandreou, and Schroff F, "Rethinking atrous convolution for semantic image segmentation," arXiv preprint arXiv:1706.05587, 2017.

[10] L.C. Chen, Y. Zhu, G. Papandreou, F. Schroff, and H. Adam, "Encoder-decoder with atrous separable convolution for semantic image segmentation," in Proceedings of the European conference on computer vision (ECCV), 2018, pp. 801-818.

[11] S. Khan et al., "Deepsmoke: Deep learning model for smoke detection and segmentation in outdoor environments," Expert Systems with Applications, vol. 182, p. 115125, 2021.

[12] T. Wang et al., "AOSVSSNet: Attention-guided optical satellite video smoke segmentation network," IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 15, pp. 8552-8566, 2022.

[13] Z. Y. Wang, Y. T. Su, Y. Y. Liu, and W. Zhang, "An improved smoke segmentation algorithm for DeeplabV3 network," Journal of Xidian University, vol. 46, no. 6, pp. 52-59, 2019.

[14] Z. Liu, C. Xie, J. Li, and Y. Sang, "Smoke area segmentation and recognition algorithm based on improved Deeplabv3+," System Engineering and Electronic Technology, vol. 43, no.2, pp. 328-335, 2021.

[15] Z. Zhou, M. M. Rahman Siddiquee, N. Tajbakhsh, and J. Liang, "Unet++: A nested u-net architecture for medical image segmentation," in Deep Learning in Medical Image Analysis and Multimodal Learning for Clinical Decision Support: 4th International Workshop, DLMIA 2018, and 8th International Workshop, ML-CDS 2018, Held in Conjunction with MICCAI 2018, Granada, Spain, September 20, 2018, Proceedings 4, 2018, pp. 3-11.

[16] F. Yuan, L. Zhang, X. Xia, Q. Huang and X. Li, "A Wave-Shaped Deep Neural Network for Smoke Density Estimation," in IEEE Transactions on Image Processing, vol. 29, pp. 2301-2313, 2019.

[17] Y. Li, W. Zhang, Y. Liu, and X. Shao, "A lightweight network for real-time smoke semantic segmentation based on dual paths," Neurocomputing, vol. 501, pp. 258-269, 2022.

[18] F. Yuan, Y. Shi, L. Zhang, and Y. Fang, "A cross-scale mixed attention network for smoke segmentation," Digital Signal Processing, vol. 134, p. 103924, 2023.

[19] M. Park, J. Bak, and S. Park, "Advanced wildfire detection using generative adversarial network-based augmented datasets and weakly supervised object localization," International Journal of Applied Earth Observation and Geoinformation, vol. 114, p. 103052, 2022.

[20] Y. Cao, Q. Tang, X. Wu, and X. Lu, "EFFNet: Enhanced feature foreground network for video smoke source prediction and detection," IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no. 4, pp. 1820-1833, 2021.

[21] H. Zhou, H. Cong, Y. Wang, and Z. Dou, "A computer-vision-based deep learning model of smoke diffusion," Process Safety and Environmental Protection, vol. 187, pp. 721-735, 2024.

[22] C.Y. Xu, B.T. Zha, J.Q. Bao, H. Zhang, and H.X. Li, "Analysis of temporal and spatial distribution characteristics of ammonium chloride smoke particles in confined spaces," Defence Technology, vol. 18, no. 7, pp. 1269-1280, 2022.

[23] X. Zhuang, F Tan, Z Li, L Li, " Image Defogging Algorithm Based On Dark Channel Priorand Optimized Auto-Color," Computer Applications and Software, vol. 38, no. 7, pp. 190-195, 2021.

[24] A. C. G. Jocher, and J. Qiu, “YOLO by Ultralytics.” https://github.com/ultralytics/ ultralytics, 2023. Accessed: February 30, 2023.

Detecting GPS Spoofing Attacks Using Corrected Low-Cost INS Data with an LSTM Network

Mohammed AFTATAH, Khalid ZEBBARA
IMISR Laboratory, FSA Ait Melloul, Ibn Zohr University, Agadir, Morocco

***Abstract*—With the emergence of new technologies ranging from smart cities to the Internet of Things (IoT), many objects rely on satellite-based navigation systems, such as GPS, to accomplish their tasks securely. However, GPS receivers are exposed to various unintentional and intentional attacks, threatening the availability and reliability of the delivered information. GPS spoofing is considered as one of the most dangerous attacks, where attackers transmit intense signals on the same frequency to disrupt the GPS receiver, leading to erroneous position calculations. Detection methods for GPS spoofing are crucial to ensure secure navigation. This paper proposes a method for GPS spoofing detection that utilizes artificial intelligence algorithms in combination with raw data from an inertial navigation system (INS). Since INS sensors are prone to accumulating errors over time, these inaccuracies are corrected via a Long Short-Term Memory (LSTM) algorithm. The corrected accelerations and angular rates are then compared to the accelerations and angular rates estimated from the GPS data to detect GPS spoofing signals. This comparison uses the modified M-of-N method, demonstrating its effectiveness by a detection rate reaching 80% of the spoofing zones.**

***Keywords*—Secure navigation; GPS spoofing; inertial systems; LSTM; M-of-N method; anti-spoofing techniques**

I. Introduction

In the era of recent technologies such as smart cities and IoT, Global Navigation Satellite Systems (GNSS), including GPS, play a pivotal role in delivering navigation information, time, and location, which are essential for the security of systems relying on such information [1]. GPS is a constellation of satellites orbiting the Earth at approximately 20,200 kilometers of altitude. These satellites continuously transmit signals to the Earth's surface, which are received by GPS receivers to determine precise locations and time information.

However, this reliance on radio signals introduces a significant vulnerability: the susceptibility to interference and malicious attacks. One of the most concerning types of attacks is GPS spoofing. This attack broadcasts false GPS signals that deceive the receiver into calculating incorrect position or time. This exploitation poses a serious threat to the integrity and security of GPS-based systems, especially in safety-critical applications such as autonomous vehicles, aviation, and drones.

In response to this growing threat, there is an urgent need to develop robust detection methods to secure GNSS from spoofing attacks. This work proposes a novel method that integrates inertial data with an LSTM network to detect the GPS spoofing attack and ensure secure navigation for GPS-dependent systems.

The structure of the rest of this paper is as follows: The introduction of the study, the review of related work, the research gaps, and the discussion of associated challenges are detailed in Section I. Section II outlines our approach to simulate the IMU sensors, followed by the mechanization process to derive navigation data. Section III focuses on GPS vulnerabilities, particularly spoofing attacks, which are examined in detail. Section IV presents our proposed approach to recognize GPS spoofing attacks using the LSTM algorithm, INS raw data, and the M-of-N method. Section V demonstrates the performance of our approach in a simulated transport scenario. Section VI concludes the paper, while Section VII explores future directions for this research.

A. Existing Work

During the last decade, diverse works have been published in the literature dealing with the problems of detecting, identifying, and mitigating intentional and unintentional attacks on satellite-based systems such as GPS. Intentional attacks include both jamming and spoofing attacks [2] [3] [4] [5]. For example, the authors of study [6] developed a covert spoofing algorithm for UAVs using a GPS/INS-integrated navigation system. The method involves estimating the UAV's current state using external sensors and calculating a spoofing control input to guide the UAV toward a deceptive trajectory while making it appear as if it is following its original reference trajectory. The proposed algorithm was validated through simulations, demonstrating that the UAV can be covertly spoofed by making its estimated position remain near the reference trajectory, while its actual path deviates towards the deceptive target state. The results showed effective trajectory manipulation with minimal disruption to the UAV's original path. To overcome these issues, numerous research studies were developed employing various techniques of machine learning, including Artificial Neural Networks (ANN) and Support Vector Machine (SVM), to evaluate their effectiveness in identifying spoofed signals [7].

The authors of study [8] developed an approach based on machine learning called PERDET for detecting GPS spoofing attacks in unmanned aerial vehicles (UAVs). This method utilizes perception data collected from real flight experiments, including both normal and attacked scenarios, to enhance the detection capabilities against GPS spoofing. The authors performed feature analysis based on the principles of position and attitude estimation, selecting relevant sensor data types to improve the accuracy of their detection model. They concluded that PERDET outperformed in terms of effectiveness compared to various machine learning algorithms after applying them to their dataset.

In study [9], the authors developed a method for detecting GNSS signal spoofing based on supervised machine learning. The technique used includes SVM and Principal Component Analysis (PCA) for identifying manipulated GNSS signals. The SVM model achieved high performance in the experiments, with over 98% accuracy. However, the paper notes a potential challenge with model complexity, which may result in longer computation times.

Sun et al. [10] developed a method for GPS spoofing detection, specifically designed for small UAVs, based on deep learning techniques. They proposed a model combining a PCA, a Convolutional Neural Network (CNN), and an LSTM to enhance the detection accuracy. The approach was validated using a dataset acquired from UAV flights with normal and spoofed GPS signals, achieving an accuracy of 99.49%. In contrast, the primary gap identified in this paper is the challenge of adapting the model to real-world environments.

In 2020, Kwon and Shim [11] exploited Attitude and Heading Reference System (AHRS) accelerometers to develop a direct GPS spoofing detection method. This method involves a comparison between the acceleration estimated from the GPS receiver and the acceleration generated by the accelerometers to detect potential spoofing. The results indicated that both decision variables showed strong detection capabilities under different spoofing scenarios. However, the gap identified in this paper lies in the sensitivity of the decision variables to changes in moving acceleration.

In study [12], the authors developed a GPS spoofing detection method using a tightly coupled Receiver Autonomous Integrity Monitoring (RAIM) with INS integration. The method monitors discrepancies between GPS and inertial measurements, using residual-based RAIM techniques. This approach utilizes an integrated GPS/INS architecture with a tightly coupled Kalman filter to improve sensitivity to spoofing attacks. The results demonstrated that the RAIM monitor effectively detected short-duration spoofing attacks.

Shafique et al. [13] used two machine-learning techniques, SVM and K-fold analysis, for GPS spoofing detection. Various machine-learning algorithms were tested, and SVM with a polynomial kernel achieved the best results. Multiple metrics were utilized to evaluate the proposed, including accuracy, precision, recall, and F1-score, achieving an overall accuracy of 99%. However, the gap identified is that the method's performance may degrade with noisy data and might not be robust against highly sophisticated spoofing attacks.

The authors of study [14] designed a method, for detecting GPS spoofing attacks on Unmanned Aerial Systems (UAS), based on supervised machine learning. The proposed approach leverages an ANN model to classify GPS signals as genuine or spoofed using extracted features such as pseudo-range, Doppler shift, signal-to-noise ratio (SNR), and satellite vehicle number (SVN). The results showed that the ANN model with two hidden layers provided high detection accuracy, achieving up to 98.3% accuracy and a probability of detection of 99.2% with a low probability of false alarms. However, a primary gap identified in the study is that the model's performance is highly dependent on the quality of the collected GPS data.

B. Research Gaps and Challenges

Despite the increasing use of low-cost INS in navigation applications, these sensors suffer from high error rates and limited accuracy, making them unreliable in scenarios involving GPS spoofing or jamming. Current methods to address these issues heavily depend on high-grade INS, which are expensive and not feasible for large-scale adoption. This highlights a significant gap in the availability of robust, low-cost solutions that can maintain high accuracy. Additionally, many approaches lack adaptability to real-time changes in error characteristics, particularly during GPS spoofing or jamming events, making them less effective in dynamic environments.

To address these challenges, our research focuses on developing a methodology for enhancing the quality of low-cost INS data by employing LSTM networks, using tactical-grade INS as a reference. The developed simulation platform in MATLAB enables researchers to build and validate their solutions based on our sensor modeling approach. This platform can simulate various scenarios without the need for complex infrastructure or expensive real-world setups involving GPS receivers and sensors mounted on vehicles. This flexibility makes it easier to test multiple configurations and spoofing scenarios efficiently. Successfully addressing these challenges will provide a practical and accessible platform for reliable navigation in GPS-compromised environments.

II. Inertial Navigation Simulation and Mechanization

A. INS Simulation

In this study, a real INS was not used; instead, a simulated one was employed, with errors affecting its sensors taken into consideration. This section presents the simulation of the six sensors of the Inertial Measurement Unit (IMU). Typically, a real INS is mounted on a mobile platform during a trajectory, measuring accelerations and angular rates [15]. However, in this case, we assume the availability of the real trajectory coordinates and proceed to simulate the behavior of the sensors accordingly. This allows us to replicate how the IMU would function in a real-world scenario, accounting for sensor errors without using an actual INS.

To model INS sensors, two main frames are used to represent the sensor outputs, the navigation frame and the body frame [16]. The body frame represents local coordinates relative to the vehicle [17], while the navigation frame aligns with the Earth's coordinate system [18]. Table I explains the differences between these frames, including their axes, alternative names, and reference centers.

TABLE I. Differences Between the ENU Frame and the Body Frame

Characteristic	Body frame	Navigation frame
Axes	X(Longitudinal), Y (Lateral), and Z (Vertical)	East (E), North (N), and Up (U)
Alternative name	Local frame, vehicle frame, or b-frame	ENU frame or n-frame
Reference Center	Center of the vehicle or mobile object	Earth's surface

The equations that model the outputs of the three orthogonal accelerometers and the three orthogonal gyroscopes in the navigation frame can be expressed using the following equations (1) (2) (3) [19].

$$\begin{bmatrix}\varphi\\ \theta\\ \psi\end{bmatrix} = \begin{bmatrix} \dfrac{\partial\left(\arctan\dfrac{\partial N/\partial t}{\partial E/\partial t}\right)}{\partial t} \\ \dfrac{\partial\left(\arctan\dfrac{\partial U/\partial t}{\partial E/\partial t}\right)}{\partial t} \\ \dfrac{\partial\left(\arctan\dfrac{\partial U/\partial t}{\partial N/\partial t}\right)}{\partial t} \end{bmatrix}^{n} \tag{1}$$

$$\begin{bmatrix}p\\ q\\ r\end{bmatrix}^{b} = \left(\begin{bmatrix} 1 & \dfrac{\sin\varphi\sin\theta}{\cos\theta} & \dfrac{\cos\varphi\sin\theta}{\cos\theta} \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \dfrac{\sin\varphi}{\cos\theta} & \dfrac{\cos\varphi}{\cos\theta} \end{bmatrix} * \begin{bmatrix}\dot{\varphi}\\ \dot{\theta}\\ \dot{\psi}\end{bmatrix}\right)^{-1} \tag{2}$$

$$\begin{bmatrix}f_E\\ f_N\\ f_U\end{bmatrix}^{b} = \frac{\partial}{\partial t}\left(C_n^b \begin{bmatrix}\dfrac{\partial E}{\partial t}\\ \dfrac{\partial N}{\partial t}\\ \dfrac{\partial U}{\partial t}\end{bmatrix}^{n}\right) - C_n^b\begin{bmatrix}0\\0\\g\end{bmatrix} + \begin{bmatrix}0 & -r & q\\ r & 0 & -p\\ -q & p & 0\end{bmatrix} * C_n^b \begin{bmatrix}\dfrac{\partial E}{\partial t}\\ \dfrac{\partial N}{\partial t}\\ \dfrac{\partial U}{\partial t}\end{bmatrix}^{n} \tag{3}$$

The components of Eq. (1), (2), and (3) are detailed in Table II.

TABLE II. DESCRIPTION OF EQUATION COMPONENTS FOR IMU MODELING

Equation component	Description/Meaning
[φ, θ, ψ]	Euler angles
[E, N, U]	3D position in the ENU frame
t	Time
[p, q, r]	Angular velocity
$\left[\dot{\varphi}, \dot{\theta}, \dot{\psi}\right]$	Time derivative of the Euler angles
$\left[f_E, f_N, f_U\right]$	3D linear acceleration
C_n^b	Transformation matrix from n-frame to b-frame

B. INS Mechanization

Once the sensors are simulated, their outputs can be generated using any predefined trajectory. The simulated sensor outputs include specific forces and angular rates. These outputs are processed through the mechanization equations to compute position, velocity, and orientation of the mobile. The mechanization equations integrate the sensor data over time, allowing for the continuous update of the navigation solution. These equations are given by Eq. (4) [20] [21] [22].

$$\begin{pmatrix}\dot{r}^n\\ \dot{v}^n\\ \dot{C}_b^n\end{pmatrix} = \begin{pmatrix} D^{-1}v^n \\ C_b^n f^b - (2\Omega_{ie}^n + \Omega_{en}^n)v^n + g^n \\ C_b^n(\Omega_{ib}^b - \Omega_{in}^b)\end{pmatrix} \tag{4}$$

Where,

r^n presents the position components in terms of latitude, longitude, and height;

v^n is the velocity;

C_n^b is a 3x3 conversion matrix from the ENU frame to the body frame;

f^b are the raw accelerations in the body frame;

g^n is the gravity.

The specific forces are integrated twice to derive the position in the body frame. Following this, the angular rates play a crucial role in calculating the transformation matrix, which is used to convert the values from the b-frame to the ENU frame. This transformation is key to ensuring that the navigation information, such as position and velocity, is expressed correctly relative to the Earth or the navigation frame. The process of INS mechanization is detailed in Fig. 1, illustrating the steps involved in converting raw IMU data into usable navigation data.

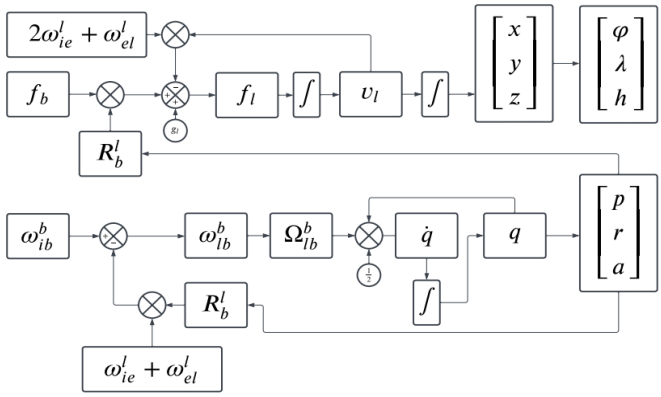


Fig. 1. Illustration of the INS mechanization process [23] [24].

III. GPS SPOOFING

Radiofrequency technologies are widely used to offer mobility and cost-effectiveness for numerous applications. GPS, one of the most in-demand navigation systems, relies on electromagnetic waves for positioning and navigation. However, this reliance on electromagnetic signals makes GPS

highly vulnerable to various attacks. These vulnerabilities can be categorized into intentional and unintentional threats. Unintentional threats may arise from environmental interference or signal obstruction. The primary unintentional attacks targeting GPS systems are illustrated in Fig. 2, highlighting the risks associated with GPS's reliance on radio frequencies.

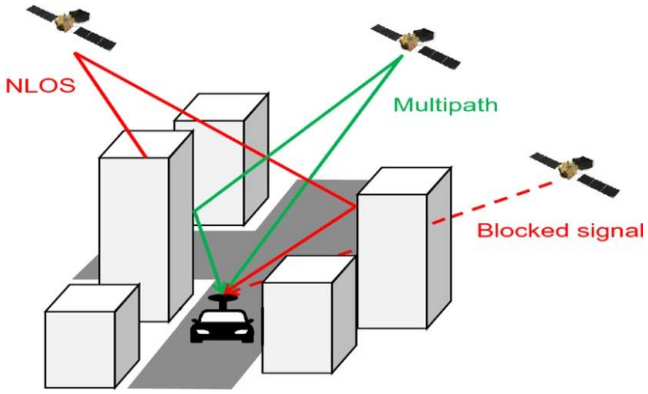


Fig. 2. Primary unintentional attacks targeting GPS [25].

Intentional attacks, often realized by hackers, include jamming and spoofing. Spoofing involves a powerful illegitimate signal transmitted at the same frequency as the legitimate GPS signal, with the intent to disrupt the receiver's ability to calculate the accurate location. The attacker can trick the GPS receiver into accepting false location data, leading to errors in navigation and positioning or reporting incorrect coordinates. The principle behind this spoofing attack is depicted in Fig. 3.

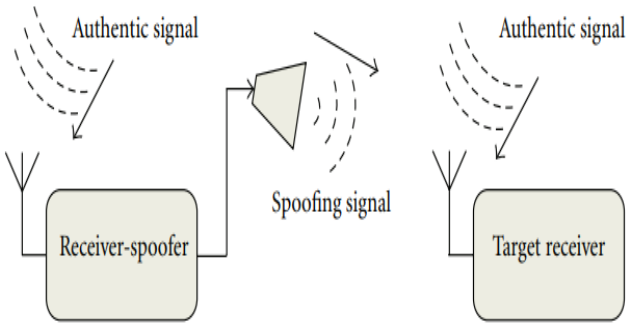


Fig. 3. The principle of the GPS spoofing attack [26].

In a legitimate GPS operation, the pseudo-range is the calculated distance between the receiver and the satellite, based on the time it takes for the satellite signal to reach the receiver. The legitimate pseudo-range to satellite *i* can be represented as Eq. (5).

$$\rho_i = c.(t_r - t_s^i) \tag{5}$$

Where ρ_i is the true pseudo-range to satellite i, c is the light's speed, t_r is the time of signal reception, and t_s^i is the time of signal transmission from the satellite i.

When a spoofing signal is introduced, the receiver detects a false signal that leads to an altered pseudo-range $\rho_i^{'}$ given by Eq. (6).

$$\rho_i^{'} = c.(t_r - t_s^{'i}) \tag{6}$$

Where $t_s^{'i}$ is the fake time of transmission introduced by the spoofer. This new pseudo-range $\rho_i^{'}$ deviates from the true pseudo-range ρ_i, causing the receiver to calculate an incorrect position. The difference between the true and spoofed pseudo-ranges, $\Delta\rho_i$, can be expressed as Eq. (7).

$$\Delta\rho_i = \rho_i^{'} - \rho_i = c.(t_s^i - t_s^{'i}) \tag{7}$$

IV. LSTM AND M-OF-N METHOD

A. LSTM Model

LSTM is a deep learning network belonging to the Recurrent Neural Networks (RNNs) family. It is particularly preferred when dealing with sequential data, such as INS measurements, effectively capturing long-term dependencies in time-series data, unlike traditional neural networks or deep neural networks. Fig. 4 illustrates the main structure of a basic LSTM unit. As shown in the following figure, this unit consists of three gates: the input gate, the forget gate, and the output gate.

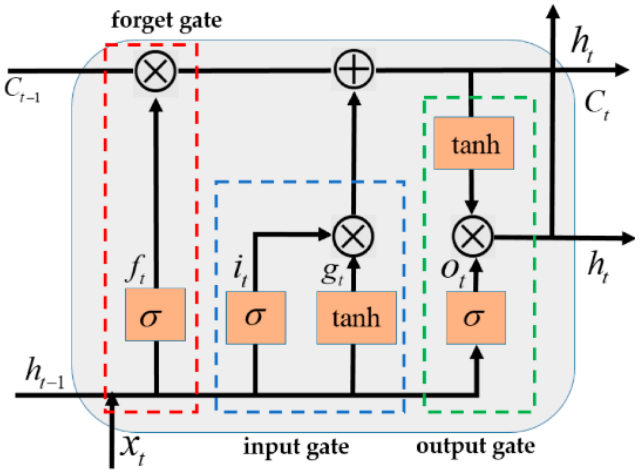


Fig. 4. Structure of a basic LSTM unit with input, forget, and output gates [27].

The input gate controls the information entering the cell state, the forget gate determines which information should be discarded from the memory, and the output gate decides which information is sent to the output. Eq. (8) (9) (10) (11) (12) give the LSTM-specific formulas [27] [28].

$$f_t = \sigma.(x_t W_{xf} + h_{t-1} W_{hf} + b_f) \tag{8}$$

$$i_t = \sigma.(x_t W_{xi} + h_{t-1} W_{hi} + b_i) \tag{9}$$

$$o_t = \sigma.(x_t W_{xo} + h_{t-1} W_{ho} + b_o) \tag{10}$$

$$c_t = f_t.c_{t-1} + i_t.g_t \quad (11)$$

$$h_t = o_t.\tanh c_t \quad (12)$$

B. M-of-N Method

In this study, we employ a modified M-of-N method to enhance the detection of GPS spoofing through the fusion of INS and GPS data. This approach compares sensor measurements from both systems and evaluates whether at least *M-of-N* measurements remain within an acceptable threshold. Deviations beyond this threshold are flagged as potential GPS spoofing events. Unlike traditional methods, the modified M-of-N approach incorporates tolerance for minor deviations arising from sensor noise and environmental factors, which are common in real-world scenarios. This method is based on calculating key statistical metrics such as the residual error E_k, the standard deviation σ_k, and a predefined confidence threshold C. These metrics help in determining whether the discrepancies between GPS and INS measurements are significant enough to be classified as spoofing or normal deviations due to noise. The equations used in this approach are as follows (13) (14).

$$E_k = \left| GPS_k - INS_k \right| \quad (13)$$

$$\left(\sigma_k\right)^2 = \frac{1}{n}\sum_{i=1}^{n}\left(E_i - \mu\right)^2 \quad (14)$$

Where E_k is the absolute difference between the GPS estimated measurement at the time step k and the corresponding INS measurement, σ_k is the standard deviation of the residual errors over a window of size N, and μ is the mean of the residual errors in that window. Furthermore, the threshold is expressed as Eq. (15).

$$Th = C \cdot \sigma_k \quad (15)$$

This threshold helps to distinguish between normal measurement deviations and significant anomalies caused by GPS spoofing. If the residual error E_k exceeds this threshold, a potential spoofing event is flagged.

In this study, we fix $C = 3$ to balance between sensitivity and false alarm rate. In a Gaussian distribution, a threshold of 3σ encompasses 99.73% of all normal data, meaning that only 0.27% of residual errors are expected to exceed this threshold due to noise. This makes the system sensitive to significant deviations while minimizing false alarms. Using a lower value, such as $C = 2$, would increase the sensitivity but also result in a higher false alarm rate, as 4.55% of the data would exceed the threshold, potentially flagging benign deviations as spoofing. Conversely, a higher value, such as $C = 4$, would further reduce the false alarm rate but could make the system less sensitive, missing smaller but meaningful anomalies. Therefore, $C = 3$ is chosen as an optimal value to provide reliable detection while minimizing false positives. The calculated values of E_k and Th are then used to detect the presence of anomalies in the GPS data. The flowchart of the detection process using the modified M-of-N technique is detailed in Fig. 5.

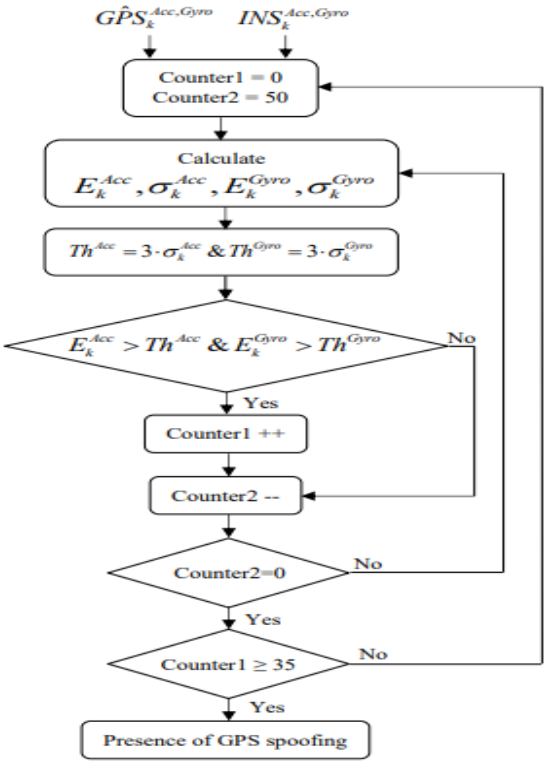


Fig. 5. Flowchart diagram of GPS spoofing detection using modified M-of-N technique.

To reduce false alarms in GPS spoofing detection, a reasonable value for N is 50, meaning spoofing is checked over every window of 50 points. This ensures that approximately 60 regions are covered in the trajectory. The value of M determines the sensitivity of the spoofing detection algorithm. To avoid high sensitivity to false positives due to noise, M is set at 35, around 70-80% of N. This ensures that the method requires a majority of the measurements in each window to exceed the threshold to flag an anomaly, providing a balance between sensitivity and robustness against noise.

V. Proposed Approach

Our proposed method relies on three key factors: corrected raw INS data, a supervised LSTM algorithm, and the modified M-of-N method. First, we model two categories of INS, tactical and low-cost, using the model described in Section I with adjustment of the appropriate characteristics for each category. The data from the tactical-grade INS are used with the LSTM algorithm to correct the raw data from the low-cost INS. Next, the simulated GPS data are employed to estimate accelerations and angular rates. The difference between the corrected low-cost INS data and the GPS-estimated values is then computed. Finally, the M-of-N method is applied to detect GPS spoofing by setting a threshold to identify discrepancies between the two data sources.

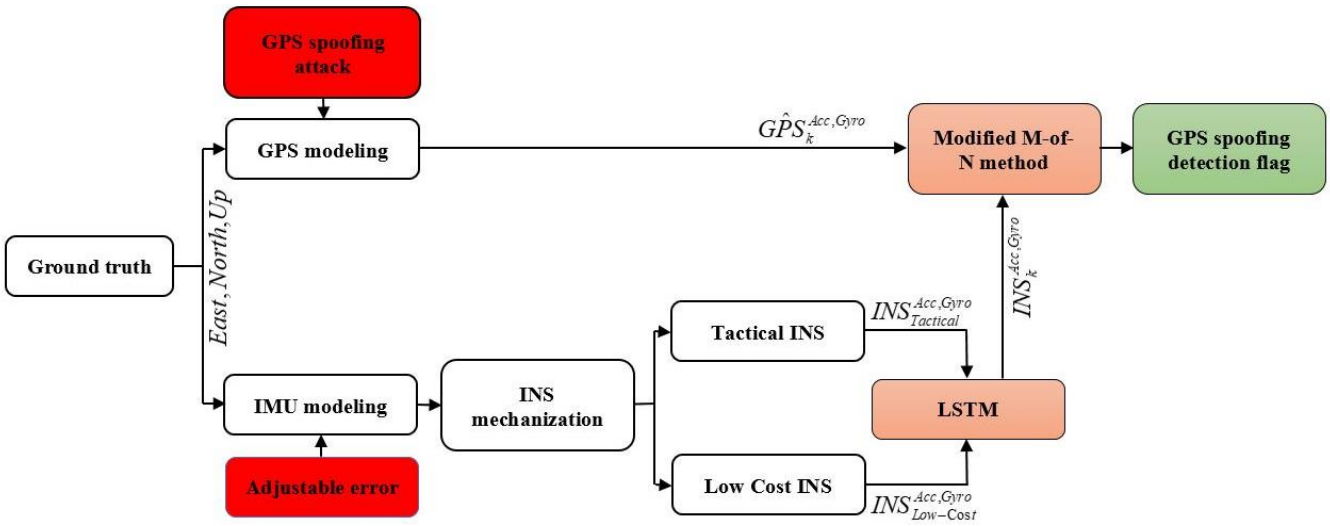


Fig. 6. The proposed approach.

The proposed method is highlighted in Fig. 6, showing the process steps from the initial INS sensor modeling to the final stage of GPS spoofing detection using the modified M-of-N method. The process begins with modeling the tactical and low-cost INS systems, followed by applying the LSTM algorithm for data correction. The simulated GPS data is then integrated to estimate motion parameters, which are compared to the corrected INS data. Discrepancies between these two sources are assessed using the modified M-of-N method, allowing for precise identification of GPS spoofing events.

Algorithm 1 provides a step-by-step description of the developed approach to detect GPS spoofing attacks using corrected inertial data.

Algorithm 1: GPS spoofing detection using corrected INS and modified M-of-N method

Initialization :
- Set Counetr1=0;
- Set Counetr2=50;
- Parameters : M=50, N=35, C=3;

Computation:
While (new data is available) do
  For (each point k of the trajectory) do
  Compute residual errors E_k^{Acc} and E_k^{Gyro}
  Calculate detection thresholds Th^{Acc} and Th^{Gyro}
    If ($E_k^{Acc} > Th^{Acc}$ & $E_k^{Gyro} > Th^{Gyro}$) then
      Increment counter1
    Else
      If (counter2) then
        Decrease counter2
      Else
        Move to the next trajectory point k+1
    If (Counter1≥35) then
      Confirm the presence of GPS spoofing
    Else
      Reinitialize Counter1=0 and reset Counter2=50
  End
  End

VI. Simulation and Results

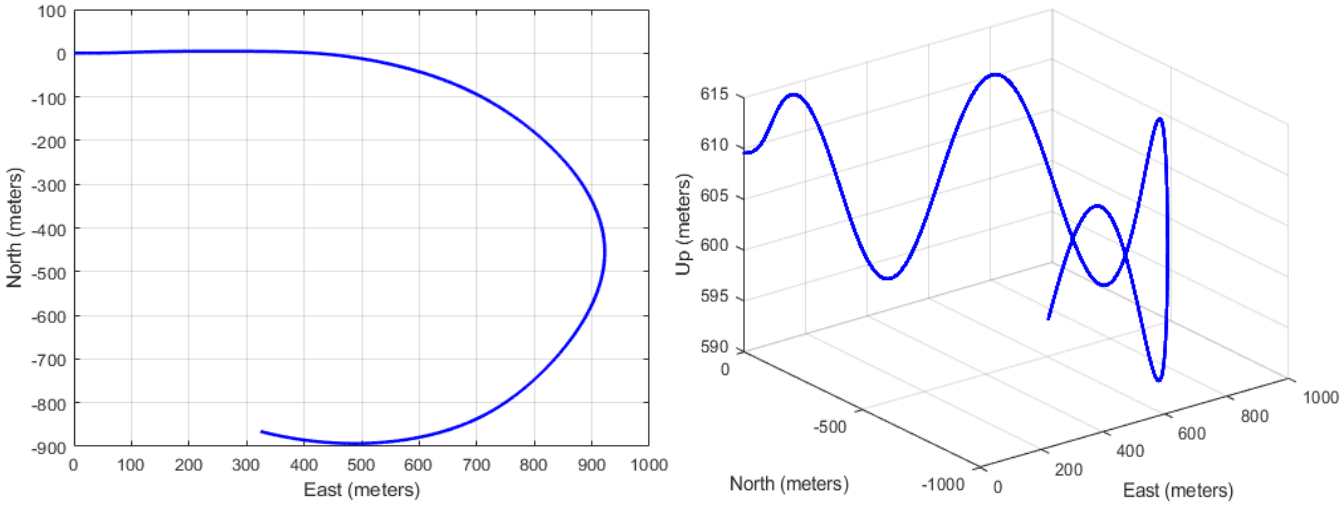
A. Simulation Platform

The experience was conducted using the MATLAB environment. The simulation begins by generating a reference trajectory with a total duration of 50 minutes. This ground truth trajectory incorporates both straight paths and complex curves, along with changes in the vertical (Up) direction, to emulate a realistic urban transportation scenario, as depicted in Fig. 7. These variations aim to reflect the dynamic conditions often encountered in such environments, providing a more accurate representation for evaluating the system's performance in challenging navigation contexts. Additionally, ten spoofing attacks were carried out on the GPS signal at separate intervals along the trajectory.

B. LSTM Correction of Low-Cost INS Data

The key characteristics of the two grades of INS include the levels of bias, scale factor, and noise, which directly affect both the accelerometers and gyroscopes. In this paper, the values were selected based on the specifications of existing and commercially available INS. The main characteristics of each grade of INS are summarized in Table III, highlighting the differences in performance and precision between the low-cost and tactical models.

Using the characteristics of each INS grade and based on the INS modeling equations presented in Section I, we modeled the six sensors composing both the low-cost and tactical INS grades. The result of this modeling process was the simulated outputs of the sensors in terms of specific forces and angular rates. Fig. 8 and Fig. 9 illustrate the comparison between the reference values, the estimated measurements from the low-cost INS sensors, and the estimated measurements from the tactical INS sensors. This comparison highlights the performance differences between the two grades, with the tactical INS showing improved accuracy and lower error margins compared to the low-cost INS.

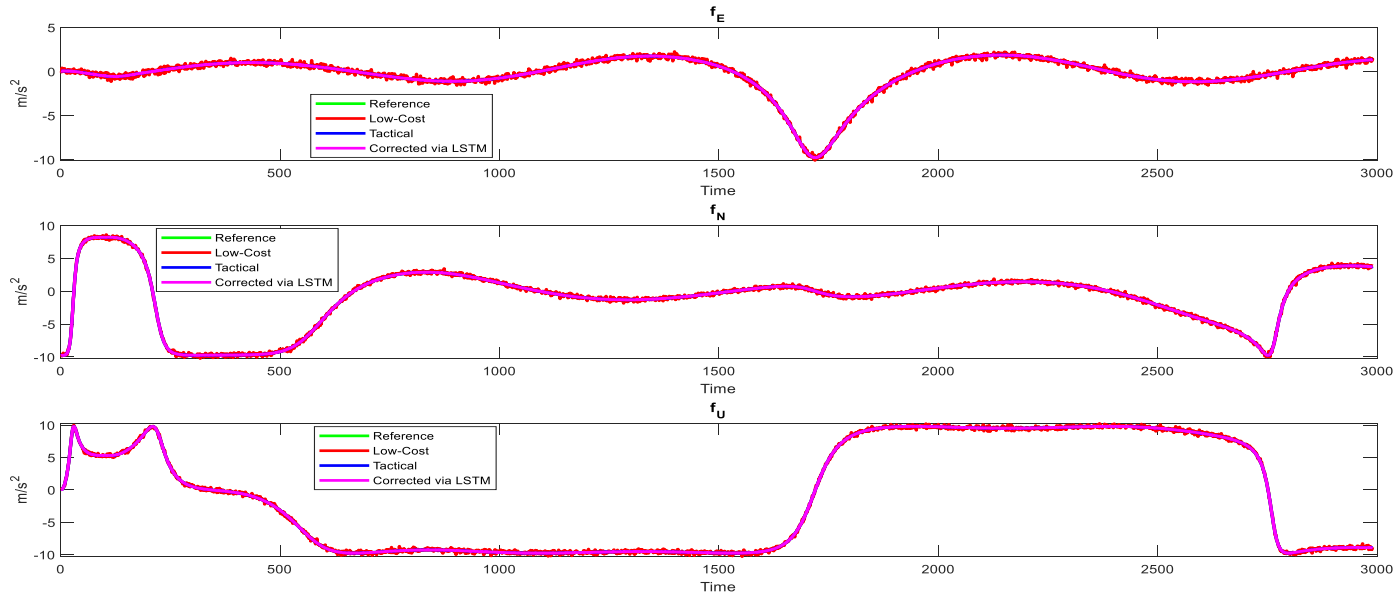


(a) (b)

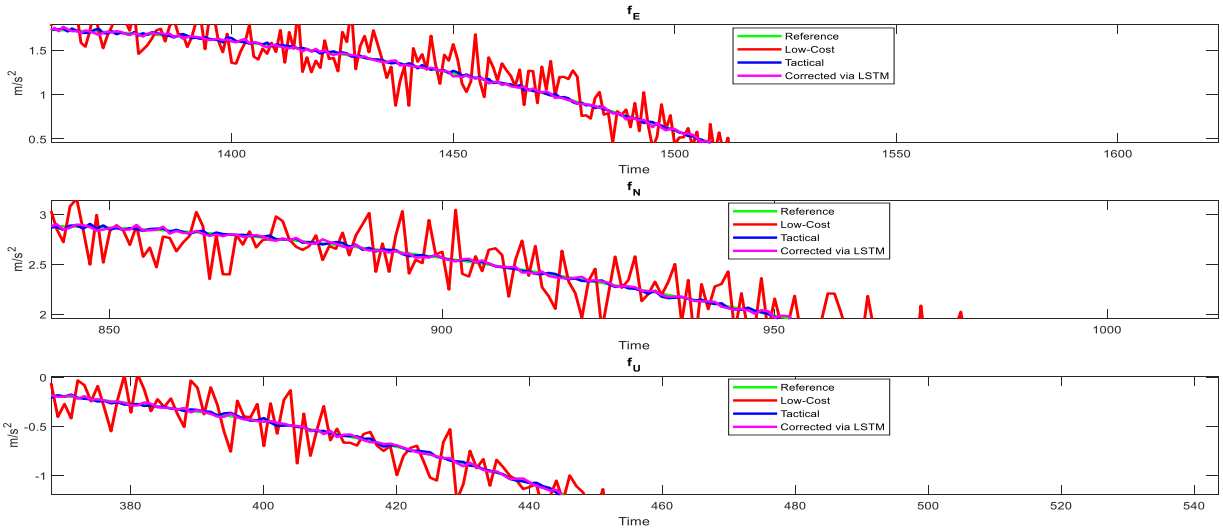
Fig. 7. Reference trajectory for urban transportation simulation: 2D overview (a) and 3D overview (b).

TABLE III. KEY CHARACTERISTICS OF LOW-COST AND TACTICAL INS MODELS [29] [30]

Key characteristics	**INS grade**	
	Low Cost	***Tactical***
Gyroscopes		
Noise	0.1°/s/√Hz	0.01°/s/√Hz
Bias	<±1.5 deg/s	<±0.0055 deg/s
Scale factor	<2%	<0.15%
Accelerometers		
Noise	500 µg/√Hz	50 µg/√Hz
Bias	1 mg	0.1 mg
Scale factor	<1%	<0.4%
Range	±6 g	±10 g

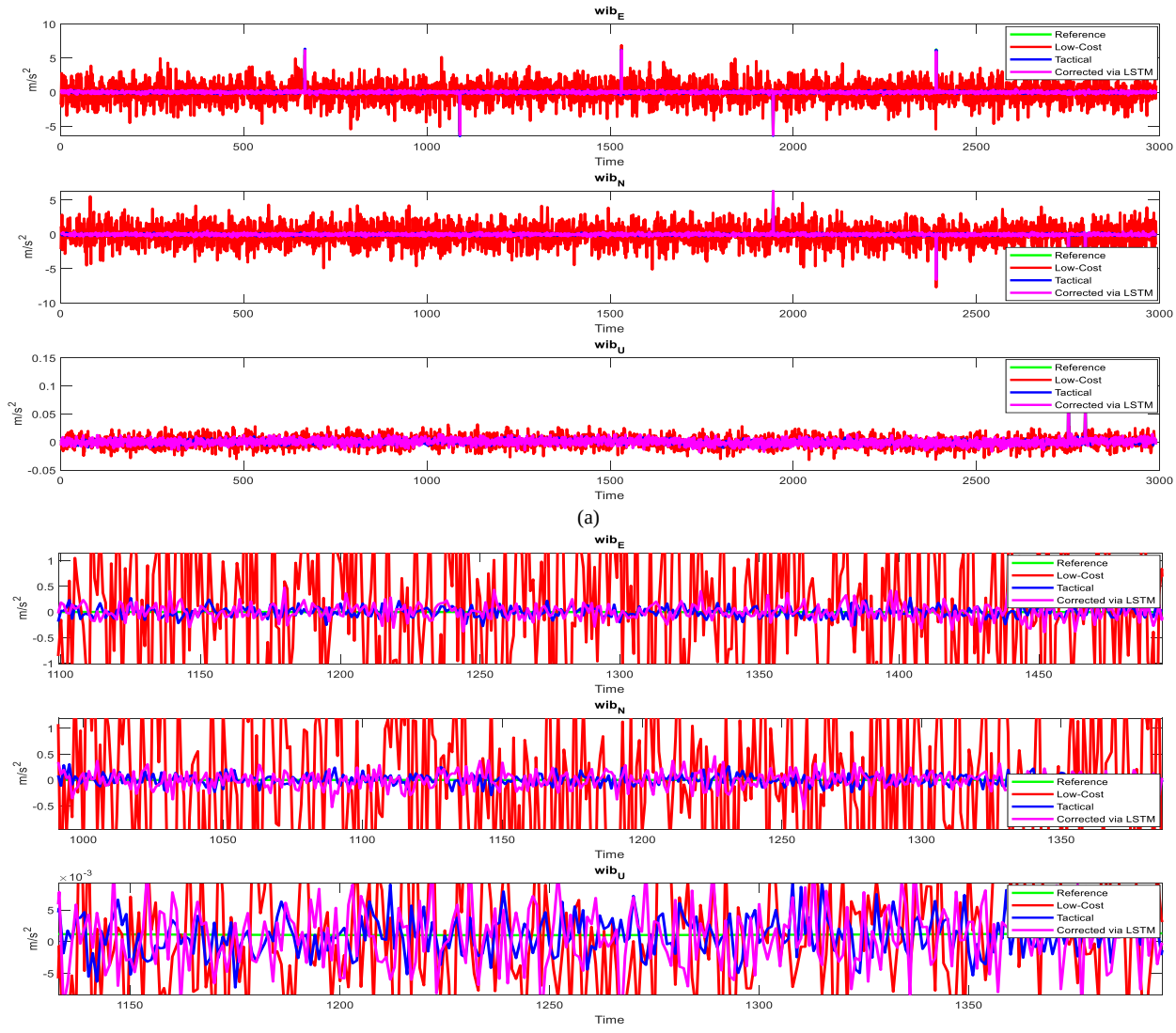


(a)



(b)

Fig. 8. Comparison of accelerometer outputs from reference, Low-Cost INS, tactical INS, and corrected data: (a) Full view and (b) Zoomed-in view.



(a)

(b)

Fig. 9. Comparison of gyroscope outputs from reference, Low-Cost INS, tactical INS, and corrected data: (a) Full view and (b) Zoomed-In view.

The Root Mean Square Error (RMSE) is the metric used to highlight the deviation from the reference for the low-cost INS, the tactical INS, and the corrected data. Table IV presents the calculated metric in the three directions (E, N, and U) for each grade. The equation of this metric is given in Eq. (16) [31].

$$RMSE^2 = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \quad (16)$$

Where y_i = Actual value, $\hat{y}_i$ = Estimated value, and n = Number of observations.

TABLE IV. RMSE FOR LOW-COST INS, TACTICAL INS, AND CORRECTED DATA IN EAST, NORTH, AND UP DIRECTIONS

Direction	RMSE					
	Low-Cost INS		*Tactical INS*		*Corrected data*	
	Accelo	*Gyro*	*Accelo*	*Gyro*	*Accelo*	*Gyro*
E (East)	1.97	1.48	0.11	0.10	0.18	0.15
N (North)	2.03	1.52	0.97	0.12	1.04	0.19
U (Up)	2.94	2.13	1.12	0.83	1.68	1.12
Total RMSE	2.36	1.74	0.86	0.49	1.15	0.66

The results show a significant reduction in RMSE values when comparing the low-cost INS to the corrected data via LSTM. The low-cost INS determines higher errors in all directions, with a total RMSE of 2.36 m/s² for accelerometers and 1.74 rad/s for gyroscopes. Due to its higher precision, the tactical INS achieves a notable decrease in RMSE, particularly in the East and North directions, resulting in a total RMSE of 0.86 m/s² for accelerometers and 0.49 rad/s for gyroscopes. The corrected data, representing the application of the LSTM algorithm for error mitigation, shows improved performance over the low-cost INS, with a total RMSE of 1.15 m/s² for accelerometers and 0.66 rad/s for gyroscopes, indicating successful error reduction.

C. GPS Spoofing Detection via M-of-N Method

To test our detection method, we have introduced ten zones of GPS spoofing along the trajectory, each lasting 60 points. Using the corrected accelerations and angular rates with estimated values from GPS, we applied the modified M-of-N method to detect GPS spoofing. As depicted in Fig. 10, the method detected eight of the 10 zones. This indicates good performance in detecting GPS spoofing, achieving a detection percentage of 80%. However, two zones were not detected due to the spoofing signal's similarity to the true GPS data or to the duration of spoofing in these zones, set to 60 points, was insufficient for the method to accumulate the required number of consecutive detections, leading to missed detections. These limitations suggest the need for refining the detection thresholds or increasing sensitivity in specific regions to improve overall performance.

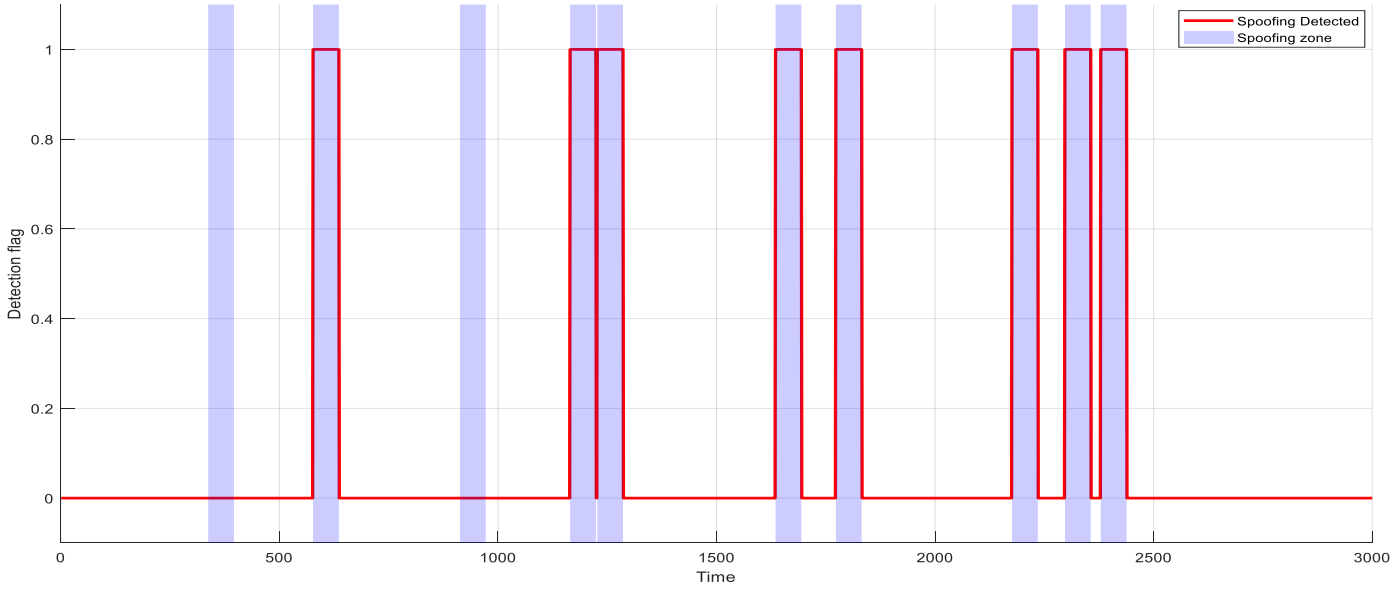


Fig. 10. Detection of GPS spoofing zones along the trajectory.

VII. CONCLUSION

This paper presents a GPS spoofing detection technique that integrates artificial intelligence algorithms with data from INS. By exploiting an LSTM algorithm to correct inherent INS errors, the proposed approach significantly improves the accuracy of the INS measurements, as evidenced by the reduction in the RMSE values. The corrected accelerations and angular rates are used in combination with the modified M-of-N method to detect spoofing by comparing INS outputs with GPS-estimated values. Experimental results demonstrate that the approach successfully detected 80% of the introduced spoofing zones. However, some zones were not detected, likely due to similarities between the spoofed and true GPS signals or the limited duration of the spoofing events, which did not provide enough consecutive detections for confirmation. These findings highlight the potential of the proposed technique but also indicate areas for further refinement, such as optimizing detection thresholds and improving sensitivity in specific segments of the trajectory to achieve reliable spoofing detection in diverse scenarios.

VIII. Future Work

Although the modified M-of-N method demonstrated promising results in detecting GPS spoofing attacks, it revealed certain limitations. One of the main challenges is its sensitivity to transient anomalies, which can lead to false positives in the detection process. To address these limitations, our future work will explore the robustness of both the K-consecutive alarm method and the modified Tong method. We will then compare the performances of these three approaches to identify the most effective solution for GPS spoofing detection.

References

[1] Phudinan Singkhamfu, Parinya Suwansrikham, "An Experiment for Outdoor GPS Localization Enhancement using Kalman Filter with Multiantenna Consumer-Grade Sensors," International Journal of Advanced Computer Science and Applications, Vol. 12, No. 4, 2021.

[2] Cuntz, M., Konovaltsev, A., Dreher, A., Meurer, M, "Jamming and Spoofing in GPS/GNSS Based Applications and Services – Threats and Countermeasures, " In: Aschenbruck, N., Martini, P., Meier, M., Tölle, J. (eds) Future Security. Future Security 2012. Communications in Computer and Information Science, vol 318. Springer, Berlin, Heidelberg, 2012, https://doi.org/10.1007/978-3-642-33161-9_29

[3] Warner, Jon S., and Roger G. Johnston, "GPS spoofing countermeasures," Homeland Security Journal 25.2 (2003): 19-27.

[4] Khan SZ, Mohsin M, Iqbal W, "On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions, " PeerJ Computer Science 7:e507, https://doi.org/10.7717/peerj-cs.507

[5] Aftatah, M., Zebbara, K. (2024), "A Comprehensive Survey on Secure Navigation for Intelligent Systems: Artificial Intelligence Approaches to GPS Jamming and Spoofing Detection," In: Mejdoub, Y., Elamri, A. (eds) Proceeding of the International Conference on Connected Objects and Artificial Intelligence (COCIA2024). COCIA 2024. Lecture Notes in Networks and Systems, vol 1123. Springer, Cham. https://doi.org/10.1007/978-3-031-70411-6_17

[6] Guo, Y., Wu, M., Tang, K., Tie, J., & Li, X, "Covert Spoofing Algorithm of UAV Based on GPS/INS-Integrated Navigation, " IEEE Transactions on Vehicular Technology, 68(7), 2019, 6557-6564, https://doi.org/10.1109/TVT.2019.2914477

[7] Talaei Khoei, T.; Ismail, S.; Shamaileh, K.A.; Devabhaktuni, V.K.; Kaabouch, N, "Impact of Dataset and Model Parameters on Machine Learning Performance for the Detection of GPS Spoofing Attacks on Unmanned Aerial Vehicles, " Appl. Sci, 2023, 13, 383.

[8] Wei, X.; Wang, Y.; Sun, C, "PERDET: Machine-Learning-Based UAV GPS Spoofing Detection Using Perception Data," Remote Sens. 2022, 14, 4925. https://doi.org/10.3390/rs14194925

[9] Semanjski, S., Semanjski, I., De Wilde, W., & Muls, A, "Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-World Meaconing and Spoofing Data—Part I, " Sensors, 20(4), 1171, 2020, https://doi.org/10.3390/s20041171

[10] Sun, Y., Yu, M., Wang, L., Li, T., & Dong, M, "A Deep-Learning-Based GPS Signal Spoofing Detection Method for Small UAVs, " Drones, 7, 370, 2023.

[11] Kwon, K.-C., & Shim, D.-S, "Performance Analysis of Direct GPS Spoofing Detection Method with AHRS/Accelerometer, " Sensors, 20(4), 954, 2020.

[12] Khanafseh, S., Roshan, N., Langel, S., Chan, F.-C., Joerger, M., & Pervan, B, "GPS Spoofing Detection using RAIM with INS Coupling, " Sensors, 20(4), 1171, 2020.

[13] Shafique, A., Mehmood, A., & Elhadef, M, "Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models, " IEEE Access, 3089847, 2021, https://doi.org/10.1109/ACCESS.2021.3089847

[14] Manesh, M. R., Kenney, J., Hu, W. C., Devabhaktuni, V. K., & Kaabouch, N, "Detection of GPS Spoofing Attacks on Unmanned Aerial Systems, " IEEE Transactions on Vehicular Technology, 68(7), 6557-6564, 2020.

[15] Franček, Petar, Kristian Jambrošić, Marko Horvat, and Vedran Planinec, "The Performance of Inertial Measurement Unit Sensors on Various Hardware Platforms for Binaural Head-Tracking Applications," Sensors 23, no. 2: 872, 2023, https://doi.org/10.3390/s23020872

[16] Liu, Jianfeng & Pu, Jiexin & Sun, Lifan & He, Zishu., "An Approach to Robust INS/UWB Integrated Positioning for Autonomous Indoor Mobile Robots, " Sensors. 19. 950, 2019, https://doi.org/10.3390/s19040950

[17] Oliveros, Juan Carlos, and Hashem Ashrafiuon, "Multi-Vehicle Navigation Using Cooperative Localization," Electronics 12, no. 24: 4945, 2023, https://doi.org/10.3390/electronics12244945

[18] Negru, Sorin Andrei, Patrick Geragersian, Ivan Petrunin, and Weisi Guo, "Resilient Multi-Sensor UAV Navigation with a Hybrid Federated Fusion Architecture," Sensors 24, no. 3: 981, 2024, https://doi.org/10.3390/s24030981

[19] AFTATAH M, ZEBBARA K, "Modeling Low-cost Inertial Navigation Systems and Their Errors, " International Journal of Computer Networks & Communications (IJCNC), Vol.16, No.6, November 2024.

[20] Krystian Borodacz, Cezary Szczepański, "Impact of Motion-Dependent Errors on the Accuracy of an Unaided Strapdown Inertial Navigation System, " Sensors, Volume 23, Issue 7, 2023, Article 3528.

[21] Boguspayev, N., Akhmedov, D., Raskaliyev, A., Kim, A., Sukhenko, A, "A Comprehensive Review of GNSS/INS Integration Techniques for Land and Air Vehicle Applications, " Appl Sci, 2023;13:4819.

[22] Mahdi, AE, Azouz, A, Abdalla, AE, Abosekeen, A, "A Machine Learning Approach for an Improved Inertial Navigation System Solution, " Sensors, 2022;22:1687.

[23] Yabo Wang, Ruihan Jiao, Tingxiao Wei, Zhaoxing Guo, Yueyang Ben, "A Method for Predicting Inertial Navigation System Positioning Errors Using a Back Propagation Neural Network Based on a Particle Swarm Optimization Algorithm, " Sensors, Volume 24, Issue 12, 2024, Article 3722.

[24] Saleh S, Bader Q, Karaim M, Elhabiby M, Noureldin A, "Integrated 5G mmWave Positioning in Deep Urban Environments: Advantages and Challenges, " In Proceedings of the 2023 IEEE Global Communications Conference (GLOBECOM). IEEE, 2023. p. 195-200.

[25] AFTATAH M, ZEBBARA K, "Robust ConvNet-Kalman Filter Integration for Mitigating GPS Jamming and Spoofing Attacks Basing on Inertial Navigation System Data," Data and Metadata [Internet]. 2024 Jan. 1 [cited 2024 Sep. 28];3:.405. https://doi.org/10.56294/dm2024.405

[26] Jafarnia-Jahromi A, Broumandan A, Nielsen J, Lachapelle G, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques, "International Journal of Navigation and Observation, 2012, https://doi.org/10.1155/2012/127072

[27] Liu, Fuchao, Hailin Zhao, and Wenjue Chen, "A Hybrid Algorithm of LSTM and Factor Graph for Improving Combined GNSS/INS Positioning Accuracy during GNSS Interruptions," Sensors 24, no. 17: 5605, 2024, https://doi.org/10.3390/s24175605

[28] Cao, Yu, Hongyang Bai, Kerui Jin, and Guanyu Zou, "An GNSS/INS Integrated Navigation Algorithm Based on PSO-LSTM in Satellite Rejection," Electronics 12, no. 13: 2905, 2023, https://doi.org/10.3390/electronics12132905

[29] Zhang, Chunxi, Xianmu Li, Shuang Gao, Tie Lin, and Lu Wang, "Performance Analysis of Global Navigation Satellite System Signal Acquisition Aided by Different Grade Inertial Navigation System under Highly Dynamic Conditions," Sensors 17, no. 5: 980, 2017, https://doi.org/10.3390/s17050980

[30] Aboutaleb, Ahmed, Amr S. El-Wakeel, Haidy Elghamrawy, and Aboelmagd Noureldin, "LiDAR/RISS/GNSS Dynamic Integration for Land Vehicle Robust Positioning in Challenging GNSS Environments," Remote Sensing 12, no. 14: 2323, 2020, https://doi.org/10.3390s/rs12142323

[31] AFTATAH M, ZEBBARA K, "Evaluating the impact of convolutional neural network layer depth on the enhancement of inertial navigation system solutions, " International Journal of Computer Networks & Communications (IJCNC), Vol.16, No.5, September 2024, DOI: 10.5121/ijcnc.2024.16504

Time Distributed MobileNetV2 with Auto-CLAHE for Eye Region Drowsiness Detection in Low Light Conditions

Farrikh Alzami*, Muhammad Naufal, Harun Al Azies, Sri Winarno, Moch Arief Soeleman
Faculty of Computer Science, Universitas Dian Nuswantoro, Indonesia

***Abstract*—Driver drowsiness is a critical factor in road safety, contributing significantly to traffic accidents. This study proposes an innovative approach integrating Auto-CLAHE with Time Distributed MobileNetV2 to enhance drowsiness detection accuracy. This study leveraged the ULg Multimodality Drowsiness Database (DROZY) for facial expression analysis, focusing on the eye region. This study methodology involved segmenting videos into 10-second intervals, extracting 20 images per segment, and applying the Haar Cascade method for eye region detection. The Auto-CLAHE technique was developed to dynamically adjust contrast enhancement parameters based on image characteristics. The analysis yielded promising results. Integrating Auto-CLAHE with Time Distributed MobileNetV2 achieved a classification accuracy of 93.62%, outperforming traditional methods including Greyscale (92.55%), AHE (92.91%), and CLAHE (91.13%). Notably, a precision of 93.71% in detecting drowsiness, with a recall of 93.62% and an F1 score of 93.59% were obtained. Statistical analysis using ANOVA and Tukey HSD tests confirmed the significance of present study results. The key innovation of this study is the implementation of Auto-CLAHE, which significantly improves image contrast adaptation. This approach surpasses AHE and basic CLAHE in drowsiness detection performance, demonstrating remarkable robustness across diverse lighting conditions and facial expressions.**

***Keywords*—Driver drowsiness detection; Auto-CLAHE; time distributed; MobileNetV2; eye region analysis**

I. Introduction

Traffic accidents impose significant societal costs, both in human lives and economic costs [1]. Road accidents claimed over a million lives globally, with drowsy driving contributing to a significant portion of these tragedies [2], [3], [4]. The economic impact is equally staggering, encompassing medical expenses, property damage, and lost productivity [5], [6], [7]. Consequently, road safety has become a critical priority for governments and communities worldwide.

Driver drowsiness poses a particular challenge to road safety. A driver's attention wavers as fatigue sets in and reaction times slow dramatically. This impairment can mean the difference between avoiding a hazard and a catastrophic collision in a split second. Interestingly, research by Cai et al. (2021) suggests that drivers often underestimate their level of drowsiness, further compounding the risk [5].

Despite advancements in vehicle safety technologies, the challenge of detecting driver drowsiness in real time remains a pressing concern. Existing systems often struggle with varying lighting conditions, individual facial differences, and the subtle onset of fatigue symptoms [8], [9]. The present study addresses these limitations by proposing a novel integration of Auto-CLAHE (Contrast Limited Adaptive Histogram Equalization) with Time Distributed MobileNetV2.

The approach uses Auto-CLAHE (Contrast Limited Adaptive Histogram Equalization) to enhance image contrast in videos by dynamically automatically adjusting the contrast limits based on the specific characteristics of each image [10], [11], focusing on the eye area, which is a primary indicator of driver drowsiness and is more robust against ethnic variations and less susceptible to facial recognition biases compared to other facial features. Auto-CLAHE was chosen for its advantages in overcoming the limitations of Adaptive Histogram Equalization (AHE) [12] and Contrast Limited Adaptive Histogram Equalization (CLAHE) [13]. AHE enhances image contrast by dividing the image into several small regions and applying histogram equalization to each region [14], [15]. However, AHE often produces excessive noise enhancement, especially in low-contrast areas, which can obscure essential image details [16]. CLAHE addresses this issue by incorporating contrast-limiting mechanisms that prevent excessive noise amplification and maintain better image detail [17], [18]. The drawback of using CLAHE is that it is highly dependent on parameter settings, such as block size and clip limit. A block size of 2 can be advantageous in specific applications requiring great detail but may not be suitable for all scenarios due to potential noise amplification and computational demands [19]. Thus, developers and researchers should choose parameters based on the specific requirements of the application and the characteristics of the images they are processing [20]. Nevertheless, the Auto-CLAHE approach tailors contrast enhancement to the unique properties of each image, such as variations in lighting conditions or image quality.

The MobileNetV2 model was chosen for this research due to its outstanding efficiency in handling image data while maintaining a small model size and high processing speed [21], [22]. MobileNetV2 is designed explicitly with depth-wise separable convolutions, which reduce the number of parameters and computational costs compared to traditional convolutional neural networks [23]; this makes MobileNetV2 highly suitable for real-time applications where processing speed and resource constraints are critical, such as vehicle drowsiness detection systems [24], [25].

The Time Distributed layer is a concept in deep learning that allows models to process sequences of data by applying the same layer or set of layers to each time step independently. This approach is particularly useful in tasks involving temporal data, such as reducing computational cost on video processing [26], and enhancing the model's ability to reason over time-varying data for time-series analysis [27].

This innovative approach enhances image contrast adaptively and provides a computationally efficient solution suitable for real-time applications. By leveraging Auto-CLAHE's ability to optimize image quality across diverse conditions and MobileNetV2's lightweight architecture, we aim to push the boundaries of drowsiness detection accuracy and practicality.

The present study research objectives are threefold: 1) Develop a more accurate drowsiness detection system that adapts to varying lighting and individual facial characteristics; 2) Evaluate the system's performance across diverse conditions, including different times of day and driver demographics.; 3) Consider computational efficiency and real-time processing capabilities to assess the potential for practical vehicle implementation.

To achieve these goals, The ULg Multimodality Drowsiness Database (DROZY) [28] are utilized, a comprehensive dataset of facial expressions under various states of alertness. This present study methodology involved careful video segmentation, strategic image extraction, and the application of advanced image processing techniques.

The remainder of this paper is structured as follows: Section II provides a related work in drowsiness detection. Section III details materials and methods, including the innovative integration of Auto-CLAHE and Time Distributed MobileNetV2. Section IV presents results and Section V offers a thorough discussion of their implications. Finally, Section VI concludes the paper, summarizing key findings and suggesting directions for future research.

Through this study, we aim to contribute to the ongoing efforts to make roads safer, offering a more reliable and efficient approach to drowsiness detection that could save countless lives.

II. Related Work

Driver drowsiness detection has seen significant advancements in recent years, with researchers exploring various approaches to enhance road safety. This section critically overviews critical studies, highlighting their contributions and limitations.

A. Neural Network Approaches

Pattarapongsin et al. (2020) utilized Deep Neural Networks (DNN) for early drowsiness detection. Their method, which incorporated Eye Aspect Ratio (EAR), Mouth Aspect Ratio (MAR), and driver pose estimation, showed promising results in real-time performance [29]. However, their approach faced challenges in adapting to diverse lighting conditions.

Other researchers, such as Jasim (2022), introduced an innovative combination of Artificial Neural Networks (ANN) and the Gray Wolf Optimizer (GWO) algorithm. Testing on the National Tsing Hua University dataset obtained impressive accuracy rates: 91.18% for drowsiness classification and 97.06% for early detection [30]. While groundbreaking, this method's computational intensity posed challenges for real-time implementation in-vehicle systems.

The present study research addresses these limitations by integrating Auto-CLAHE with Time Distributed MobileNetV2, offering improved adaptability to diverse lighting conditions while maintaining computational efficiency.

B. Advanced Video Analysis Techniques

Shen et al. (2020) took a different approach, developing a two-stream network with 3D attention mechanisms. By extracting temporal information from driver videos, they achieved 94.46% accuracy on the NTHU-DDD dataset [19]. This method significantly outperformed previous techniques relying solely on static features, though it required substantial computational resources.

Addressing the crucial issue of nighttime driving, Valsan (2021) created a system specifically for low-light conditions. Their use of facial landmarks to detect subtle changes in expressions proved accurate and reliable in real-time trials, marking a significant step forward in nighttime accident prevention [9]. Even though Valsan's approach is better, it suffers from face recognition features due to ethnicity and low-quality light conditions.

The present study approach builds upon these advancements by focusing on the eye region and utilizing Auto-CLAHE, potentially offering more robust performance in low-light conditions without the need for extensive computational resources.

C. Image Enhancement in Drowsiness Detection

Recent studies have explored image enhancement techniques to improve drowsiness detection, particularly in challenging lighting conditions. Yakno et al. (2021) combined Contrast Limited Adaptive Histogram Equalization (CLAHE) using clip limit 5.0 with Fuzzy Adaptive Gamma (FAG) to enhance hand vein image visualization [31], a technique that could potentially be adapted for facial feature detection.

In a related application, Chen et al. (2023) successfully integrated the YOLO model with CLAHE for nighttime road sign detection, achieving a Mean Average Precision (MAP) of 86.40% [32]. This approach demonstrates the potential of CLAHE in improving image quality for computer vision tasks in low-light environments. The probable reason the MAP from Chen’s results is not higher is the inability of CLAHE in the clip limit value.

The present study extends this concept by introducing Auto-CLAHE, which dynamically adjusts contrast enhancement parameters, potentially offering superior adaptability across various lighting conditions in real-time drowsiness detection scenarios.

D. Algorithmic Innovations

Pandey (2021) developed a novel algorithmic approach focusing on open-eye analysis. By utilizing temporal features

of the eyes and head movement, they achieved 94.2% accuracy in detecting driver drowsiness [33]. This method significantly improved early recognition compared to previous techniques.

Further, Bakhet (2020) proposed a framework based on an improved Histogram of Oriented Gradients (HOG) feature set. Their experimental results showed a detection accuracy of 85.62%, offering a competitive alternative in drowsiness detection [34].

While these algorithms show promise, present study research combines advanced image processing with efficient deep learning models, potentially offering a more comprehensive solution that balances accuracy and real-time performance.

E. Real-Time Approaches

Sharan et al. (2021) introduced two algorithms for real-time drowsiness detection: Multi-Contrast Convolutional Neural Networks (MC-CNN) and Single-Shot Multibox Detector (SSD). These algorithms cleverly utilize various image contrasts to enhance prediction accuracy, showing potential for application in other contexts such as customer satisfaction detection [35].

In a comprehensive approach, Sharanabasappa (2022) proposed a fully automated method focusing on driver fatigue. Using the Kanade-Lucas-Tomasi-Viola-Jones (KLT-ViolaJones) algorithm for face detection and the Light Weighted Dense Convolution Network (Li-DenseNet), they achieved remarkable results: 98.44% accuracy, 91.5% sensitivity, and 92.3% specificity on the NTHU-DDD dataset [36].

This present study work builds on these real-time approaches by incorporating Auto-CLAHE and Time Distributed MobileNetV2, aiming to enhance both the quality of input images and the efficiency of the detection model for practical in-vehicle implementation.

F. Time Distributed Layer

Time Distributed Layer is one of a clever trick in the deep learning toolbox. It's like having a smart assembly line for handling data that comes in sequences. Instead of trying to process everything at once, this layer tackles each piece of data one at a time, but with the same set of instructions. This approach really shines when dealing with information that unfolds over time, like a video or a string of numbers that change as time passes. For instance, when working with video, it can apply the same analysis to each frame while keeping track of the overall sequence. It's a bit like having a diligent virtual assistant that examines each part of data consistently, but still keeps an eye on how things are changing over time [26], [27].

Hu et al. (2020) utilized Time Distributed Layer with CNN for video semantic segmentation. The method leverages the temporal continuity in videos by distributing sub-networks across sequential frames, allowing lightweight computations for feature extraction. [26]. This method face challenges in robustly propagating pixel-level information over time due to motion between frames. This can lead to misalignment and decreased accuracy.

Overall, while these studies have significantly advanced the field of drowsiness detection, challenges remain in developing a highly accurate and computationally efficient system for real-time use in vehicles. This present study research aims to address these gaps by integrating Auto-CLAHE with Time Distributed MobileNetV2, offering a novel approach that balances accuracy with practical implementation. Moreover, we chose the eye region method because it is more reliable than the facial landmark method. Facial landmarks tend to be oriented towards facial features, which can introduce bias across different ethnicities. Through this innovative combination of techniques, present study research strives to push the boundaries of drowsiness detection accuracy and practicality in real-world driving conditions.

III. MATERIALS AND METHODS

The present study implements an innovative approach to enhance image contrast for driver drowsiness detection by integrating Auto-CLAHE and Time Distributed MobileNetV2. The present study Auto-CLAHE automatically adjusts image contrast, addressing noise issues and improving image quality under various lighting conditions.

The image processing workflow, illustrated in Fig. 1, outlines the systematic procedures involved in this research.

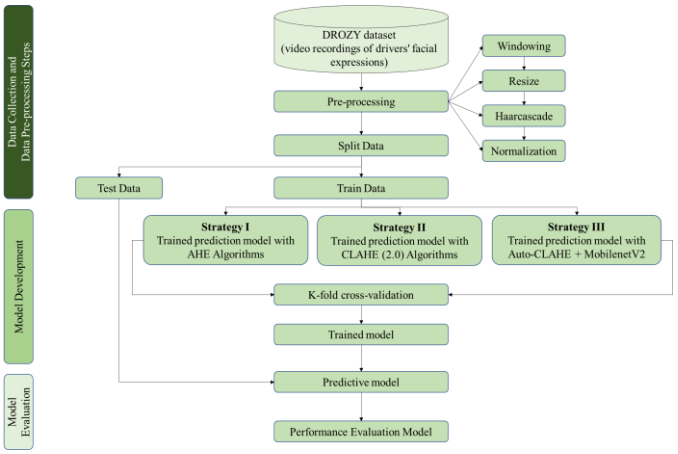


Fig. 1. Workflow of image processing for driver drowsiness detection.

The explanation of Fig. 1 is described in the following subsection. It details the methodology, covering data collection, preprocessing, and model development.

A. Data Collection

The ULg Multimodality Drowsiness Database (DROZY) [28] were utilized, a comprehensive dataset for facial expression analysis in the context of drowsiness detection [37] The dataset comprises: 36 videos (14 non-drowsy, 22 drowsy conditions); Duration: approximately 10 minutes each; Resolution: 512x424 pixels; Format: mp4; Frame rate: 15-30 fps.

Here, the DROZY dataset is unbalanced and relatively small. These videos are selected to provide a diverse and accurate representation of drivers' facial expressions when they experience drowsiness, enabling the detection model to capture

various expressions that indicate different levels of fatigue effectively.

B. Preprocessing

The preprocessing pipeline involves several key steps:

1) Video segmentation: Videos are divided into 10-second segments, capturing critical details within the typical timeframe of microsleeps [38], [39].

2) Image extraction: 20 images were extracted (two per second) from each segment to effectively represent driver facial expressions.

3) Image resizing: Original images were resized from 512x424 to 96x96 pixels, balancing detail preservation with computational efficiency [40].

4) Normalization: Pixel values were normalized with values 255 resulted in 0-1 range, enhancing model performance [41].

5) Eye region detection: The Haar Cascade method were employed with the following parameters:

a) Scale factor: 1.3 to 1.1

b) minNeighbors: 4 to 1

c) minSize: (10, 10)

The justification for selecting these parameters is as follows:

- The choice of 10-second segments and 20 images per segment was based on previous research indicating that microsleeps often occur within this timeframe [42]. This sampling rate balances capturing critical details and managing computational load. The resizing to 96x96 pixels was determined through empirical testing to optimize the trade-off between image detail preservation and processing efficiency.
- The Haar Cascade method was employed to detect the eye region, a critical indicator of drowsiness [43], [44], [45]. Here, we adopt the Haar cascade method from Santana et al. [46]. Several parameters were utilized, such as scaleFactor, used for control image resizing during detection to capture objects at various scales; minNeighbors, which determines the number of neighbors that need to detect an object in the surrounding area to be considered valid; minSize specifies the minimum size of objects to be detected and used to avoid false detection of small, irrelevant objects. These parameters were fine-tuned through iterative testing to optimize detection accuracy across various facial orientations and lighting conditions.

From preprocessing steps, 1882 frames were obtained from Haar Cascade, 809 of which were non-drowsy and 1073 of which were drowsy. Then, split data as 70% for training, 15% for validation, and 15% for testing. Fig. 2 represent visualization of the Haar Cascade Method on Image Data. Auto-CLAHE results on image quality is par with original image.

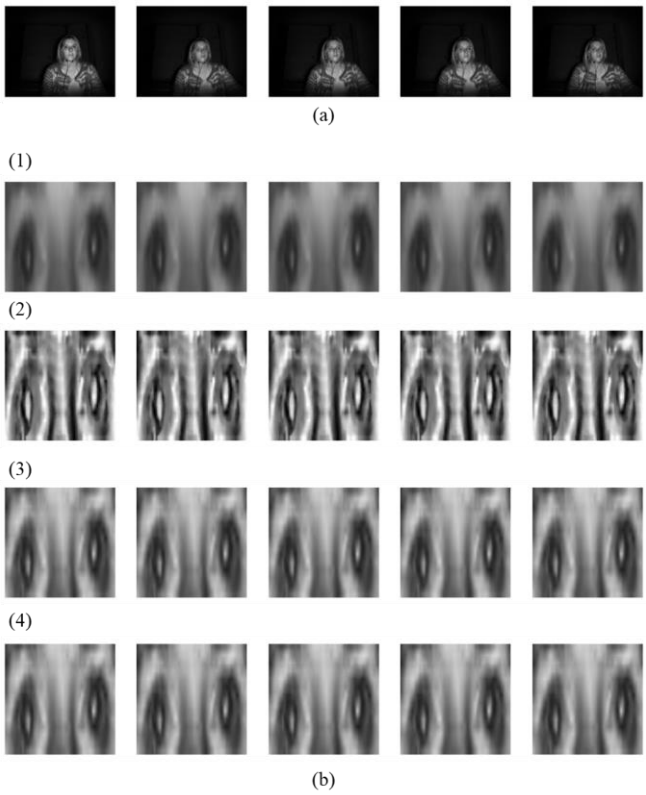


Fig. 2. Visualization of the haar cascade method on image data: (a) Original Image; (b) Results after applying different image processing techniques: (b.1) Greyscale; (b.2) AHE; (b.3) CLAHE; (b.4) Auto-CLAHE.

C. Model Development

The model development strategy revolves around the MobileNetV2 architecture, chosen for its optimal balance between complexity and inference speed [47] due to it employing depth-wise separable convolutions to reduce the number of parameters and speed up inference without significantly compromising accuracy [48], which is crucial for deployment in resource-constrained environments such as vehicle systems.

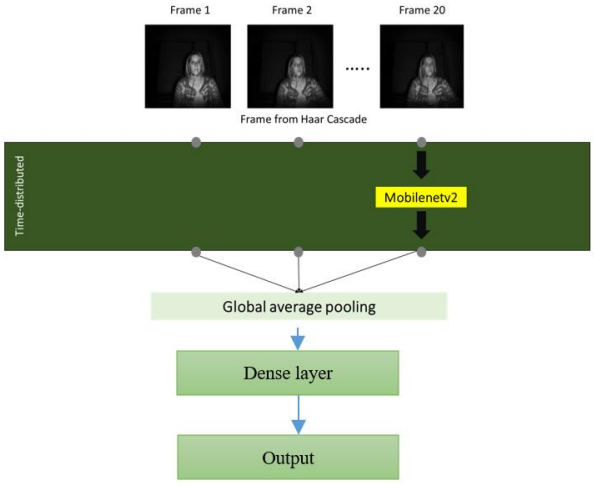


Fig. 3. The proposed architecture.

For the Fig. 3 explanation, three main strategies were explored:

1) AHE Algorithms with MobileNetV2.
2) CLAHE (2.0) Algorithms with MobileNetV2.
3) Auto-CLAHE with MobileNetV2.

For each strategy, MobileNetV2 are configured with:

1) Time Distributed layer processes sequential data, applying the same layer to each time step and maintaining the output in sequence form.

a) Let $X = \{X_1, X_2, \dots, X_T\}$ be the input sequence, where each $X_t \in \mathbb{R}^{H\times W\times C}$ is a frame at time step t. Here T = number of video frames; H, W = Height and width of each frame; C = Number of channels (3 RGB channels).

b) $f(\cdot)$ be the transformation function of the convolutional layer.

Using time Distributed layer, the same transformation $f(\cdot)$ is applied independently to every time step t:

$$Y_t = f(X_t), \forall_t = 1,2, \dots, T \quad (1)$$

Thus, the output for the entire sequence becomes:

$$Y = \{Y_1, Y_2, \dots, Y_T\}, Y_t \in \mathbb{R}^{H'\times W'\times C'} \quad (2)$$

Where H' and W' are the height and width after convolutional transformation.

Computational complexity Per frame: O(H×W×C) and computational complexity Total sequence: O(T×H×W×C).

2) Fine tuning MobileNetV2. Here, the layers were freeze from the beginning until before the last three layers on MobileNetV2. The reason is that DROZY dataset is different from the image weight. The mathematics of MobileNetV2 which core of the efficient model can described as follows:

a) Depth-wise Convolution:

$$DW(i,j,k) = \sum_m \sum_n K(m,n,k) \times X(i+m, j+n, k) \quad (3)$$

Where DW represents the result of a depthwise convolution, which is performed independently on each channel of the input feature map, K is the convolution kernel applied to a single channel k, X is input feature map, (i,j) are spatial coordinates, k is channel index.

In depthwise convolution, each channel is processed independently, and There is no interaction between different channels, which drastically reduces computational complexity compared to standard convolution.

b) Point-wise Convolution:

$$PW(i,j,n) = \sum_k DW(i,j,k) \times P(k,n) \quad (4)$$

Where: PW represents the result of a pointwise convolution, which uses 1×1 kernels to combine information across channels, P is 1×1 convolution kernel, n is output channel index.

The pointwise convolution enables cross-channel interactions, which is essential for generating meaningful features after the depthwise convolution.

c) Total Operations:

In standard convolution, we can see the equation as follows:

$$standard\ conv = H \times W \times C_{in} \times C_{out} \times K \times K \quad (5)$$

Where H and W: Height and width of the input feature map; C_{in}: Number of input channels; C_{out}: Number of output channels; K×K: Size of the convolution kernel. Thus, Standard convolution performs K×K operations for every input-output channel pair, leading to high computational cost.

$$MNetV2 = DWC + PWC \quad (6)$$

Subject to

$$\text{DWC} = (H \times W \times C_{in} \times K \times K) \quad (7)$$

$$PWC = (H \times W \times C_{in} \times C_{out}) \quad (8)$$

Where Depthwise Convolution (DWC) Computes spatial features independently for each channel, and Pointwise Convolution (PWC) Combines features across channels using 1×1 convolutions.

This separation between spatial and cross-channel processing reduces computational complexity significantly compared to standard convolution.

$$reduction\ factor = \left(\frac{1}{C_{out}} + \frac{1}{K^2}\right) \quad (9)$$

Where C_{out}: Number of output channels; and K^2: Kernel size squared (e.g., for a 3×3 kernel, K^2=9).

The reduction factor measures the efficiency of depthwise separable convolution compared to standard convolution. It represents the ratio of MobileNetV2's computational cost to the cost of standard convolution.

MobileNetV2 is efficient due to replaces the computationally expensive standard convolution ($H\times W\times C_{in}\times C_{out}\times K\times K$) with DWC and PWC as C_{out} or K increases, the reduction factor decreases, meaning the efficiency of MobileNetV2 improves.

Finally, the architecture can be described as follows:

TABLE I. PROPOSED MOBILENETV2 ARCHITECTURE

Layer (type)	Output Shape	Param #
TimeDistributed MobileNetV2	(None, 20, 3, 3, 1280)	2257984
GlobalAveragePooling3D	(None, 1280)	0
Dense (relu + l1 regularizer)	(None, 8)	10248
Dense 1 (sigmoid)	(None, 1)	9
Total params: 2,268,241 Trainable params: 422,417 Non-trainable params: 1,845,824		

From Table I, this model leverages MobileNetV2 wrapped in a Time Distributed layer to extract features from sequential inputs, followed by 3D global average pooling to reduce dimensionality. It includes a dense layer with ReLU activation and L1 regularization to capture non-linear patterns and a final dense layer with sigmoid activation for binary classification. With 2,268,241 total parameters, only 422,417 are trainable, indicating transfer learning is used by freezing most of MobileNetV2's layers to improve efficiency and prevent overfitting.

3) Adam optimizer is used for training, with a learning rate 0.0001 to enhance the model's performance [49]. The Adam optimizer can be defined as Eq. (8) and Eq. (10):

$$\theta_{t+1} = \theta_t - \eta * m_t \quad (10)$$

where

$$m_t = \beta m_{t-1} + (1-\beta)\left[\frac{\delta L}{\delta \theta_t}\right] \quad (11)$$

Here, θ_{t+1} = weights at time t+1; θ_t= weights at time t; η = learning rate at time t; m_t = aggregate of gradients at time t [current], β = Moving average parameter; m_{t-1}= aggregate of gradients at time t-1; δL = derivative of Loss Function; and $\delta\theta_t$= derivative of weights at time t. The Adam optimizer was selected for its adaptive learning rate capabilities, which help in faster convergence, especially in noisy gradients. A grid search optimization process determined the learning rate of 0.0001, balancing convergence speed and model stability.

4) Batch size 32 is chosen to balance training speed and accuracy.

5) Training epochs: 25 epochs to achieve optimal convergence.

6) Global average pooling before the output layer with Eq. (12) is as follows:

$$GAP(X) = \frac{1}{(W*H)} * \sum_{i=1}^{W}\sum_{j=1}^{H} x_{ij} \quad (12)$$

Where $GAP(X)$ = represents the Global Average Pooling applied to the feature map; W = The width of the image or feature map; H = The height of the image or feature map; x_{ij} = The pixel value at position i, j in the feature map.

7) L1 regularizer on the final layer [50], [51], [52], penalizing huge weights [53] to prevent overfitting. The L1 equation [see Eq. (11)] can be seen as follows:

$$L_1(W) = \lambda * \sum|w_i| \quad (13)$$

where λ = regularization parameter; w_i = kernelweight.

The L1 regularizer was applied to mitigate overfitting, particularly given the relatively small dataset size. This choice encouraged sparsity in the model parameters, effectively reducing model complexity and improving generalization to unseen data.

8) ReLu is used because it is computationally efficient. It requires only simple thresholding at zero, which reduces the time needed for calculations compared to more complex activation functions like sigmoid or tanh. ReLu itself is capable of avoiding overfitting.

9) A binary cross-entropy loss function is selected, suitable for binary classification tasks like drowsiness detection [54]. The sigmoid activation function for the final dense layer is applied to create a dense layer with one value. Sigmoid is good since it produces values between 0 and 1, which is helpful for probability. It also helps the model learn effectively during training. The formula for the sigmoid activation function is in Eq. (14).

$$\sigma(x) = \frac{1}{1+e^{-x}} \quad (14)$$

10) Where σ is the sigmoid(x), the output value will always be between 0 and 1. Here, x represents the input value, and e^{-x} denotes the exponential function of $-x$. This allows the model to retain features learned during initial training while retraining the last three layers to adapt specifically to drowsiness detection.

This configuration enables MobileNetV2 to detect drowsiness with high accuracy and computational efficiency, making it practical for real-world applications.

a) Strategy I: AHE Algorithms with MobileNetV2

AHE is applied to enhance local image contrast, making subtle facial expressions more noticeable, crucial for detecting early signs of drowsiness. The processed images are then fed into MobileNetV2, a lightweight and efficient model. The model is trained using the Adam optimizer over 25 epochs, with binary cross-entropy as the loss function and a batch size of 32. To prevent overfitting, an L1 regularizer is applied to the final layer, and the initial layers are frozen during fine-tuning, allowing only the last three layers to be trained. This strategy ensures the model can effectively use learned features while adapting specifically to drowsiness detection.

Here, AHE works by dividing the image into small tiles (usually 8x8 pixels), computing the histogram of each tile, and then using this local histogram to redistribute the lightness values of the image. The equation for AHE can be represented as follows:

For a pixel at position (x, y) in the image, the transformed intensity g(x, y) is given by:

$$g(x,y) = floor\left(\left(cdf\big(f(x,y)\big) - cdf_{min}\right) * \frac{L-1}{(M*N) - cdf_{min}}\right) \quad (15)$$

Where:

- f(x,y) is the input image
- cdf(f(x,y)) is the cumulative distribution function of the pixel intensities in the local region around (x,y)
- cdf_{min} is the minimum non-zero value of the cdf
- M*N is the number of pixels in the local region
- L is the number of possible intensity values (usually 256 for 8-bit images)

The CDF for each local region is calculated as:

$$cdf(i) = \sum_{j=0}^{i} p(j) \quad (16)$$

Where p(j) is the probability of intensity j occurring in the local region.

b) Strategy II: CLAHE (2.0) Algorithms with MobileNetV2.

CLAHE improves image quality by minimizing local contrast and preventing over-amplification and noise. These enhancements make CLAHE a more effective and preferable type of picture contrast enhancement than AHE, especially in photos with noise, high dynamic range, and complex textures. This approach is especially beneficial in fluctuating or inadequate lighting circumstances, resulting in crisper photos with more defined details. The photos improved with CLAHE with a clip limit size of 2.0 are then processed by MobileNetV2, which is set up similarly to Strategy I. The contrast improvement is guided by Eq. (17).

$$\beta = \frac{M}{N}\left(1 + \frac{\alpha}{100}(S_{max} - 1)\right) \quad (17)$$

Here, M denotes the region size area, N is the grayscale value (typically 256), α is the clip factor that adjusts the histogram limit boundary, and S_{max} is the maximum possible pixel value after applying CLAHE. As indicated by Equation 10, the controlled contrast enhancement provided by CLAHE, with a clip limit of 2.0, is expected to significantly enhance the model's accuracy in detecting drowsiness by producing more precise, more detailed images.

c) Strategy III: Auto-CLAHE implementation with MobileNetV2.

Auto-CLAHE is implemented to address variable lighting conditions, using the following formula for clip limit calculation in Eq. (18):

$$\alpha = \left(\frac{k}{\bar{x}}\right) \quad (18)$$

Where α represents the clip limit value, k is the normalization constant (k=10), $\bar{x}$ represents the average intensity of all pixel values.

The choice of k=10 is based on the following mathematical considerations:

1) For grayscale images where $\bar{x} \in [0,255]$:

a) When $\bar{x}$ approaches minimum (very dark images): α increases, providing stronger enhancement

b) When $\bar{x}$ approaches maximum (bright images): α decreases, providing subtle enhancement

2) This produces a clip limit that automatically adjusts based on image brightness:

a) $\lim(\bar{x}\to 0)\ \alpha = \infty$ (maximum enhancement for dark images)

b) $\lim(\bar{x}\to 255)\ \alpha = k/255$ (minimal enhancement for bright images)

Thus, Auto-CLAHE can be write as Eq. (19):

$$\beta = \frac{M}{N}\left(1 + \frac{(\alpha)}{100}(S_{max} - 1)\right) \quad (19)$$

Where:

- M is the region size.
- N is the number of grayscale levels (typically 256).
- Smax is the maximum pixel value.

The algorithm's complexity is O(M×N) where M×N is the image dimensions. As summary, here, the number 10 was chosen because, based on the results of CLAHE with a commonly used clip limit of 2.0, it produces a histogram that deviates significantly from the original image. Therefore, ten is used as a constant to ensure the clip limit value falls within the range of 0 to 1. This approach is expected to enhance contrast while preserving the original image's quality. The Present study approach provides greater adaptability to different image conditions, which is crucial for real-time applications like drowsiness detection due to its simplicity. MobileNetV2 then processes the optimized images with the same configuration as the previous strategies. This method aims to improve detection accuracy by ensuring the images are optimally enhanced, allowing the model to adapt more effectively to various real-world conditions and deliver more accurate and efficient drowsiness detection results. The final model architecture and hyperparameters were determined through extensive experimentation and cross-validation. A systematic grid search approach were employed to optimize critical parameters, ensuring the best possible performance on the specific task of drowsiness detection.

D. Evaluation Metrics

The present study model were evaluated using several key metrics:

- Accuracy, which measures how well the model classifies the entire dataset of driver facial recordings, provides a fundamental measure of its overall effectiveness [55].
- Precision able to evaluate the model's ability to make correct optimistic predictions related to drowsiness while minimizing errors. Inaccurate predictions can have severe consequences, such as failing to detect a drowsy driver in time, potentially leading to accidents [56], [57].
- Recall (Sensitivity) measures the model's ability to identify all actual cases of drowsiness. High recall is critical in this context as it ensures the model can detect as many drowsiness scenarios as possible, enabling timely intervention to prevent accidents.
- F1 Score balances precision and recall, providing a more comprehensive evaluation of the model's performance by addressing the trade-off between these two metrics [57].

- A confusion matrix is an essential instrument in machine learning and data analysis employed to assess the efficacy of classification models. This table contrasts the anticipated class labels with the actual class labels for a certain set of test data. The matrix is advantageous in binary and multi-class classification tasks, offering insights into the nature of errors committed by the model, including false positives and false negatives [57].

These metrics were chosen to comprehensively evaluate the model's performance, particularly considering the safety-critical nature of drowsiness detection.

E. Statistical Analysis

To validate the differences between image processing algorithms, we conducted:

- ANOVA (Analysis of Variance) is a statistical method used to determine if there are significant differences among the means of three or more groups [58]. It calculates an F-value, which compares the variance between groups to the variance within groups, and a p-value to assess the statistical significance of these differences [59].
- Tukey HSD (Honestly Significant Difference) post-hoc tests [60]. Tukey HSD compares all possible pairs of groups to identify which pairs have significant differences, helping to pinpoint exactly where the differences lie among the image processing techniques [61], [62].

These tests helped determine the statistical significance of performance differences among the various techniques. Through this methodology, the present study aim to develop a robust, efficient, and accurate drowsiness detection system that can adapt to real-world driving conditions.

IV. RESULTS

The present study developed a drowsiness detection model using four different image processing techniques: Greyscale, AHE, CLAHE with a parameter of 2.0, and Auto-CLAHE. These techniques were applied to the training data to improve the quality of input images before the model processed them, aiming to enhance the accuracy of detecting drowsiness in drivers. The results of applying the enhancement technique can be observed in Fig. 4.

The graph in Fig. 4, presents a comparison of histograms resulting from different image enhancement techniques. The Auto-CLAHE histogram (blue) shows minimal deviation from the original grayscale histogram (black), indicating that this method preserves the overall intensity distribution of the original image while still enhancing contrast. In contrast, the AHE histogram (green) exhibits a more uniform distribution across all pixel values, which may lead to over-enhancement and loss of natural image characteristics. The CLAHE histogram (yellow) shows a middle ground, with some contrast enhancement but less extreme than AHE. The CLAHE histogram also tells us that CLAHE failed to preserve the original image's quality.

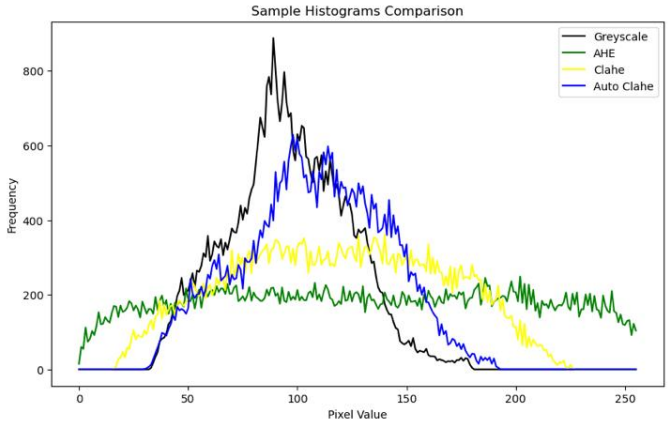


Fig. 4. Sample histogram comparison of enhancement.

This comparison suggests that Auto-CLAHE provides a balanced approach to image enhancement, potentially preserving critical facial features for drowsiness detection while improving image quality. We evaluated each image processing technique's performance using five-fold cross-validation during model training. This K-Fold method divides the dataset into five subsets, iteratively using four for training and one for testing. Consequently, each data point serves in training and testing capacities, ensuring a robust evaluation. [63]. The accuracy results obtained from each fold are presented in Table II.

TABLE II. ACCURACY RESULTS OF DIFFERENT IMAGE PROCESSING TECHNIQUES IN DROWSINESS DETECTION MODEL TRAINING

Fold	Greyscale	AHE	CLAHE (2.0)	AUTO CLAHE
1	0.9129	0.8523	0.9280	**0.9356**
2	0.8674	0.8712	0.9431	**0.9470**
3	0.9354	0.9430	0.9429	**0.9468**
4	0.8897	0.9049	0.9581	**0.9658**
5	0.9049	0.9468	0.9505	**0.9430**
Standard deviation	0.0235	0.0351	0.0109	0.0099
Average	0.9021	0.9036	0.9445	**0.9476**

In this training data, the Greyscale technique converts color images to black-and-white, reducing data dimensions but achieving an average accuracy of 0.9021 with a standard deviation of 0.0235. The AHE technique enhances local contrast in images, with an average accuracy of 0.9036 and a standard deviation of 0.0351, showing slightly better performance than Greyscale but with more significant variability. The CLAHE technique with a parameter of 2.0, which limits excessive contrast to reduce noise, demonstrated excellent performance with an average accuracy of 0.9445 and a low standard deviation of 0.0109, indicating more consistent results. Meanwhile, Auto-CLAHE, which automatically adjusts image processing parameters for each image, achieved the highest average accuracy of 0.9476 and the lowest standard deviation of 0.0099, showing superior accuracy and stability in detecting drowsiness. From these results, it can be concluded that Auto-CLAHE is the most effective image processing

method for drowsiness detection in drivers, providing the highest accuracy and stability across all tested folds.

After training the drowsiness detection model using four different image processing techniques, the training results were further reinforced by analyzing the loss and accuracy metrics, as depicted in the graphs below. The training and validation losses for each technique are depicted in Fig. 5.

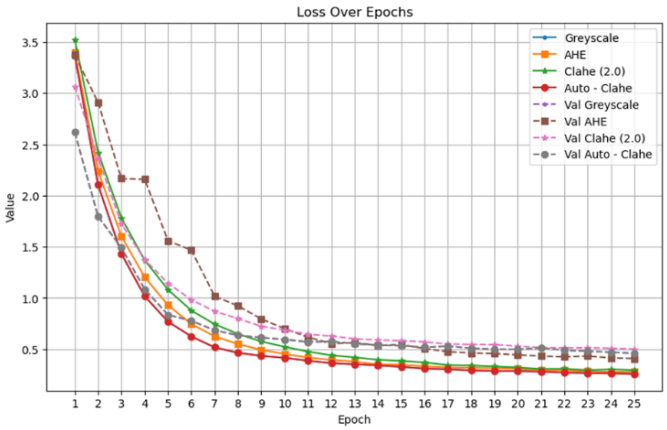


Fig. 5. Training and validation loss for different image processing techniques.

In Fig. 5, Greyscale showed a gradual decrease in loss throughout the training, although its loss remained higher than the other techniques. Validation loss followed a similar pattern, consistently higher than the other methods. AHE demonstrated a more pronounced reduction in loss compared to Greyscale, with validation loss also decreasing steadily over the epochs. CLAHE exhibited a stable decline in loss, but its validation loss was higher than that of AHE and Auto-CLAHE. Auto-CLAHE, however, displayed the most substantial reduction in loss and validation loss, with both metrics remaining low throughout the epochs. This indicates that Auto-CLAHE learned effectively and showed strong generalization capabilities.

The trends in accuracy and validation accuracy are illustrated in Fig. 6. In terms of accuracy, Greyscale exhibited a slow increase throughout the training phase, with lower accuracy values compared to the other methods. Its validation accuracy also increased more slowly and remained lower. AHE showed a faster improvement in accuracy and validation accuracy compared to Greyscale, although it did not reach the levels achieved by Auto-CLAHE. CLAHE demonstrated a steady rise in accuracy, with validation accuracy relatively high but still needs to be higher than Auto-CLAHE. Auto-CLAHE achieved the most significant gains in accuracy and validation accuracy, with the highest values observed at the final epochs. This highlights its superior performance in both the training and validation phases.

Here, the Anova and Tukey HSD results for loss were calculated. From Table III. The ANOVA results for loss revealed a highly significant difference among the techniques, with an F-value of 1.43 x 10^{31} and a p-value of 0.000. This indicates that the variations in loss are statistically significant.

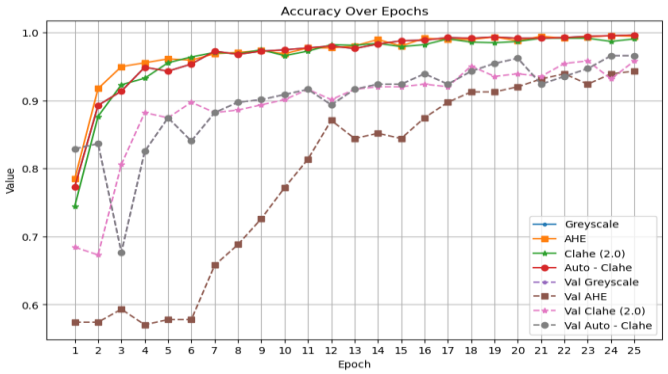


Fig. 6. Training and validation accuracy for different image processing techniques.

TABLE III. ANOVA AND TUKEY HSD RESULTS FOR LOSS

Source	Sum of Squares	Degrees of Freedom	F-Statistics	P-Value
Anova	7.94 x 10^{-1}	3	1.43 x 10^{31}	0.000*
Tukey HSD Post-Hoc	Group1	Group2	Mean Difference	p-adjusted
	AHE	Auto-Clahe	-0.0184	0.000*
	AHE	Clahe (2.0)	0.0174	0.000*
	AHE	Greyscale	0.5132	0.000*
	Auto-Clahe	Clahe (2.0)	0.0358	0.000*
	Auto-Clahe	Greyscale	0.5316	0.000*
	Clahe (2.0)	Greyscale	0.4958	0.000*

*) Significant at $\alpha = 0.05$

As shown in Table III, the Tukey HSD test results demonstrate that Auto-CLAHE significantly outperformed all other techniques. Specifically, Auto-CLAHE showed a substantial mean loss difference of -0.0184 compared to AHE, 0.0358 compared to CLAHE, and 0.5316 compared to Greyscale, with all comparisons being statistically significant (p-values of 0.000). Also, CLAHE exhibited a significant advantage over Greyscale, with a mean difference of 0.4958. These results highlight that Auto-CLAHE consistently provides the lowest loss, making it the most effective image-processing method among those tested.

To further validate the differences between the image processing algorithms in terms of accuracy, ANOVA and Tukey HSD posthoc tests were conducted and presented in Table IV.

TABLE IV. ANOVA AND TUKEY HSD RESULTS FOR ACCURACY

Source	Sum of Squares	Degrees of Freedom	F-Statistics	P-Value
Anova	4.345 x 10-2	3	4.579 x 1028	0.000
Tukey HSD Post-Hoc	Group1	Group2	Mean Difference	p-adjusted
	AHE	Auto-Clahe	0.0019	0.000
	AHE	Clahe (2.0)	-0.0038	0.000
	AHE	Greyscale	-0.1209	0.000
	Auto-Clahe	Clahe (2.0)	-0.0057	0.000
	Auto-Clahe	Greyscale	-0.1228	0.000
	Clahe (2.0)	Greyscale	-0.1171	0.000

*) Significant at $\alpha = 0.05$

As seen in Table IV. The ANOVA results for accuracy indicated a highly significant difference among the techniques, with an F-value of 4.579 x 10^{28} and a p-value of 0.000. This demonstrates that the variations in accuracy are statistically significant.

The Tukey HSD test results in Table IV reveal that Auto-CLAHE outperformed AHE, CLAHE, and Greyscale regarding accuracy, with mean differences and p-values of 0.000, indicating statistical significance at $\alpha = 0.05$. Specifically, Auto-CLAHE showed a mean accuracy difference of 0.0019 compared to AHE, -0.0057 compared to CLAHE, and -0.1228 compared to Greyscale. Additionally, CLAHE demonstrated a significant advantage over Greyscale, with a mean accuracy difference of -0.1171. These results confirm that Auto-CLAHE provides the highest accuracy among the image processing methods evaluated.

TABLE V. PERFORMANCE METRICS OF IMAGE PROCESSING TECHNIQUES IN DROWSINESS DETECTION MODEL TESTING

Method	Accuracy	Precision	Recall	F1 Score
Greyscale	0.9255	0.9274	0.9255	0.9250
AHE [64]	0.9291	0.9299	0.9291	0.9287
CLAHE (2.0) [65]	0.9113	0.9130	0.9113	0.9116
Auto-CLAHE	**0.9362**	**0.9371**	**0.9362**	**0.9359**

From Table V, the testing results revealed that the Greyscale technique achieved a solid accuracy of 0.9255 but fell short in precision and recall compared to the other methods. The AHE technique demonstrated an accuracy of 0.9291 and a precision of 0.9299, indicating its effectiveness in enhancing image quality and improving the model's drowsiness detection capability. On the other hand, CLAHE with a parameter of 2.0 yielded an accuracy of 0.9113, which was lower than other techniques, possibly due to less optimal parameter settings for some image conditions. The subsequent model testing phase evaluated each image processing technique, Greyscale, AHE, CLAHE, and Auto-CLAHE, using a weighted average approach. Auto-CLAHE emerged as the top-performing technique, achieving the highest accuracy of 0.9362, with precision, recall, and F1 scores closely aligned at 0.9371, 0.9362, and 0.9359, respectively. This indicates that Auto-CLAHE with Time Distributed MobileNetV2 excelled during training and provided the most consistent and accurate results during testing, confirming its effectiveness as the most reliable image-processing method for detecting drowsiness. Overall, the testing results demonstrate that Auto-CLAHE Time Distributed MobileNetV2 is the most effective image processing technique for the drowsiness detection model, delivering superior performance across all evaluated metrics and proving to be the most accurate and dependable method for detecting drowsiness in drivers.

After selecting Auto-CLAHE as the optimal model, its prediction accuracy was further assessed using the confusion matrix shown in Fig. 7. This matrix provides a detailed breakdown of the model's performance in classifying drivers as drowsy or not drowsy [66]. The confusion matrix (Fig. 7) indicates that the Auto-CLAHE model correctly identified 156 drowsy drivers (True Positives) and 108 non-drowsy drivers (True Negatives) out of a total of 282 tests. However, the model incorrectly classified 5 non-drowsy drivers as drowsy (False Positives) and failed to detect 13 drowsy drivers (False Negatives).

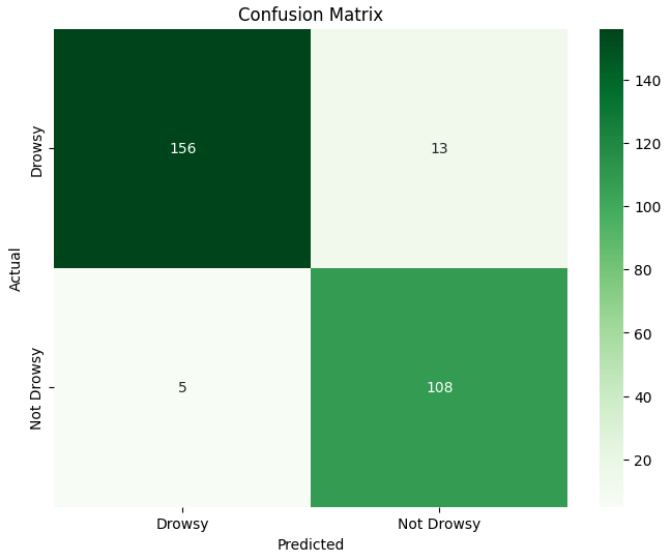


Fig. 7. Confusion matrix for auto-CLAHE model.

V. DISCUSSIONS

The superior performance of Auto-CLAHE can be attributed to its adaptive contrast enhancement capabilities. The histogram comparison (Fig. 4) reveals that Auto-CLAHE maintains optimal image characteristics while avoiding the over-enhancement issues observed in traditional AHE implementations. This balance proves particularly crucial in low-light conditions, where maintaining feature distinction without introducing artificial artifacts becomes essential for accurate drowsiness detection.

The ANOVA results ($F = 1.43 \times 10^{31}$, $p < 0.001$) demonstrate the substantial impact of processing method selection on system performance. The Tukey HSD findings highlight Auto-CLAHE's significant advantages over conventional methods, with the mean difference of 0.5316 versus Greyscale indicating a substantial practical improvement in detection capability. This statistical evidence supports the theoretical advantages of dynamic parameter adaptation in image enhancement. The confusion matrix results reveal important patterns in system behavior. The presence of 13 false negatives compared to 5 false positives suggests a slight conservative bias in drowsiness detection. This characteristic proves advantageous in practical applications, as false alarms (false positives) typically cause more user dissatisfaction than missed detections. The overall accuracy of 0.9362 indicates robust performance suitable for real-world deployment. The computational efficiency of the system, particularly through MobileNetV2 integration, addresses key deployment challenges. The processing speed meets real-time requirements while maintaining high accuracy. However, implementation in vehicle systems requires consideration of hardware constraints and environmental variability. Thus, several limitations warrant consideration: 1) Performance

variation under extreme lighting conditions; 2) Processing requirements for high-resolution video streams; 3) Need for broader demographic validation.

VI. CONCLUSION

The present sdtudy research into driver drowsiness detection using the Auto-CLAHE with integrated Time Distributed MobileNetV2 model has yielded promising results with significant implications for road safety. The key findings of the present study are as follows:

- Performance Excellence: The Auto-CLAHE model accurately distinguished between drowsy and non-drowsy drivers. With an overall accuracy of 93.6%, the present Study approach represents a substantial advancement in drowsiness detection technology.
- Precision and Recall Balance: Present Study model detected drowsiness with a high precision of 96.9% and a strong recall rate of 92.3%. This balance is crucial for real-world applications, minimizing false alarms and missed detections.
- Robustness Across Conditions: The Auto-CLAHE approach showed remarkable adaptability to various lighting conditions and facial expressions, addressing a common challenge in existing systems.
- Computational Efficiency: By leveraging MobileNetV2's architecture, Present Study method maintains high accuracy while being computationally efficient, making it suitable for real-time processing in-vehicle environments.
- Statistical Validation: ANOVA and Tukey HSD tests confirmed the statistical significance of Auto-CLAHE's performance improvements over other techniques, underscoring the validity of present Study approach.

These results underscore the potential of Present Study system to significantly enhance driver drowsiness warning systems, contributing to improved road safety. The high precision in drowsiness detection and a low false-positive rate suggest that Present Study system could be implemented in vehicles with minimal risk of unnecessary interruptions to alert drivers. However, we acknowledge certain limitations in the present study. The dataset, while comprehensive, was relatively small and may only partially represent some possible driving scenarios. Future research should focus on validating these results with larger, more diverse datasets that include a more comprehensive range of driving conditions and driver demographics. Looking ahead, here are several suggestions for future work:

- Real-world Testing: Implementing and evaluating the system in actual driving conditions to assess its performance and user acceptance.
- Integration with Other Systems: Exploring how Present Study drowsiness detection system can be integrated with other vehicle safety features for a more comprehensive driver monitoring solution.
- Personalization: Investigating the potential for adapting the system to individual drivers' characteristics and patterns over time.
- Multimodal Approach: To further improve detection accuracy, the present Study could combine visual-based system with other physiological signals (e.g., EEG, heart rate variability). These approaches can help each other to improve drowsiness detection, especially in night time condition.
- Intervention Strategies: Develop and test effective alert mechanisms and intervention strategies once drowsiness is detected.

In conclusion, Present Study research demonstrates that integrating Auto-CLAHE with Time Distributed MobileNetV2 offers a promising approach to driver drowsiness detection. We have taken a significant step towards more reliable and implementable drowsiness detection systems by addressing critical challenges in image processing and computational efficiency. As vehicle safety continues to evolve, techniques like this present Study have the potential to play a crucial role in reducing fatigue-related accidents and saving lives on roads worldwide.

ACKNOWLEDGMENT

This work was supported by the Kemdikbud Research Grant on Penelitian Fundamental - Reguler with grant number 108/E5/PG.02.00.PL/2024.

REFERENCES

[1] A. I. Qureshi et al., “Mandated societal lockdown and road traffic accidents,” Accident Analysis & Prevention, vol. 146, p. 105747, Oct. 2020, doi: 10.1016/j.aap.2020.105747.

[2] C. Chantith, C. K. Permpoonwiwat, and B. Hamaide, “Measure of productivity loss due to road traffic accidents in Thailand,” IATSS Research, vol. 45, no. 1, pp. 131–136, Apr. 2021, doi: 10.1016/j.iatssr.2020.07.001.

[3] M. Elsebaei, O. Elnawawy, A. A. E. Othman, and M. Badawy, “Causes and impacts of site accidents in the Egyptian construction industry,” International Journal of Construction Management, vol. 22, no. 14, pp. 2659–2670, Oct. 2022, doi: 10.1080/15623599.2020.1819523.

[4] D. Osei-Asibey, J. Ayarkwa, A. Acheampong, E. Adinyira, and P. Amoah, “Impacts of accidents and hazards on the Ghanaian construction industry,” International Journal of Construction Management, vol. 23, no. 4, pp. 708–717, Mar. 2023, doi: 10.1080/15623599.2021.1920161.

[5] A. W. T. Cai, J. E. Manousakis, T. Y. T. Lo, J. A. Horne, M. E. Howard, and C. Anderson, “I think I’m sleepy, therefore I am – Awareness of sleepiness while driving: A systematic review,” Sleep Medicine Reviews, vol. 60, p. 101533, Dec. 2021, doi: 10.1016/j.smrv.2021.101533.

[6] S. Soares, S. Ferreira, and A. Couto, “Drowsiness and distraction while driving: A study based on smartphone app data,” Journal of Safety Research, vol. 72, pp. 279–285, Feb. 2020, doi: 10.1016/j.jsr.2019.12.024.

[7] C. Fan, S. Huang, S. Lin, D. Xu, Y. Peng, and S. Yi, “Types, Risk Factors, Consequences, and Detection Methods of Train Driver Fatigue and Distraction,” Computational Intelligence and Neuroscience, vol. 2022, pp. 1–10, Mar. 2022, doi: 10.1155/2022/8328077.

[8] Y. Albadawi, M. Takruri, and M. Awad, “A Review of Recent Developments in Driver Drowsiness Detection Systems,” Sensors, vol. 22, no. 5, p. 2069, Mar. 2022, doi: 10.3390/s22052069.

[9] V. Valsan A, P. P. Mathai, and I. Babu, “Monitoring Driver’s Drowsiness Status at Night Based on Computer Vision,” in 2021

International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India: IEEE, Feb. 2021, pp. 989–993. doi: 10.1109/ICCCIS51004.2021.9397180.

[10] J. Dong et al., "Property and microstructure of Ni50.3Ti29.7Hf20 high-temperature shape memory alloys with different aging conditions," Acta Materialia, vol. 265, p. 119642, Feb. 2024, doi: 10.1016/j.actamat.2023.119642.

[11] A. L. Wang, M. H. Hansen, Y.-C. Lai, J. Dong, and K. Y. Xie, "Improving orientation mapping by enhancing the diffraction signal using Auto-CLAHE in precession electron diffraction data," Microstructures, vol. 3, no. 4, Oct. 2023, doi: 10.20517/microstructures.2023.27.

[12] V. Stimper, S. Bauer, R. Ernstorfer, B. Scholkopf, and R. P. Xian, "Multidimensional Contrast Limited Adaptive Histogram Equalization," IEEE Access, vol. 7, pp. 165437–165447, 2019, doi: 10.1109/ACCESS.2019.2952899.

[13] H. Singh et al., "Multi-exposure microscopic image fusion-based detail enhancement algorithm," Ultramicroscopy, vol. 236, p. 113499, Jun. 2022, doi: 10.1016/j.ultramic.2022.113499.

[14] U. K. Acharya and S. Kumar, "Genetic algorithm based adaptive histogram equalization (GAAHE) technique for medical image enhancement," Optik, vol. 230, p. 166273, Mar. 2021, doi: 10.1016/j.ijleo.2021.166273.

[15] S. H. Majeed and N. A. M. Isa, "Adaptive Entropy Index Histogram Equalization for Poor Contrast Images," IEEE Access, vol. 9, pp. 6402–6437, 2021, doi: 10.1109/ACCESS.2020.3048148.

[16] Y. Qi et al., "A Comprehensive Overview of Image Enhancement Techniques," Arch Computat Methods Eng, vol. 29, no. 1, pp. 583–607, Jan. 2022, doi: 10.1007/s11831-021-09587-6.

[17] C. A. C. De Vasconcelos Filho, P. C. Cortez, and V. H. C. De Albuquerque, "IQAEvolNet: a novel unsupervised evolutionary image enhancement algorithm on chest X-ray scans," Res. Biomed. Eng., Jul. 2024, doi: 10.1007/s42600-024-00366-3.

[18] Madhavi V. Vijaya and L. S. Kumari, "Enrichment of Retinal Fundus Images using EN-CLAHE and Auto-CLAHE Methods," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 3, pp. 1213–1221, Mar. 2024.

[19] Q. Shen, S. Zhao, R. Zhang, and B. Zhang, "Robust Two-Stream Multi-Features Network for Driver Drowsiness Detection," in Proceedings of the 2020 2nd International Conference on Robotics, Intelligent Control and Artificial Intelligence, Shanghai China: ACM, Oct. 2020, pp. 271–277. doi: 10.1145/3438872.3439093.

[20] Y. Chang, C. Jung, P. Ke, H. Song, and J. Hwang, "Automatic Contrast-Limited Adaptive Histogram Equalization With Dual Gamma Correction," IEEE Access, vol. 6, pp. 11782–11792, 2018, doi: 10.1109/ACCESS.2018.2797872.

[21] M. Akay et al., "Deep Learning Classification of Systemic Sclerosis Skin Using the MobileNetV2 Model," IEEE Open J. Eng. Med. Biol., vol. 2, pp. 104–110, 2021, doi: 10.1109/OJEMB.2021.3066097.

[22] R. Indraswari, R. Rokhana, and W. Herulambang, "Melanoma image classification based on MobileNetV2 network," Procedia Computer Science, vol. 197, pp. 198–207, Jan. 2022, doi: 10.1016/j.procs.2021.12.132.

[23] H. Z. Ilmadina, M. Naufal, and D. S. Wibowo, "Drowsiness Detection Based on Yawning Using Modified Pre-trained Model MobileNetV2 and ResNet50," matrik, vol. 22, no. 3, pp. 419–430, Jun. 2023, doi: 10.30812/matrik.v22i3.2785.

[24] K. Kapoor, R. Pamula, and S. V. Murthy, "Real-Time Driver Distraction Detection System Using Convolutional Neural Networks," in Proceedings of ICETIT 2019, vol. 605, P. K. Singh, B. K. Panigrahi, N. K. Suryadevara, S. K. Sharma, and A. P. Singh, Eds., in Lecture Notes in Electrical Engineering, vol. 605. , Cham: Springer International Publishing, 2020, pp. 280–291. doi: 10.1007/978-3-030-30577-2_24.

[25] S. Pahariya, P. Vats, and S. Suchitra, "Driver Drowsiness Detection using MobileNetV2 with Transfer Learning Approach," in 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), Chennai, India: IEEE, Apr. 2024, pp. 1–6. doi: 10.1109/ADICS58448.2024.10533606.

[26] P. Hu, F. Caba, O. Wang, Z. Lin, S. Sclaroff, and F. Perazzi, "Temporally Distributed Networks for Fast Video Semantic Segmentation," in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, USA: IEEE, Jun. 2020, pp. 8815–8824. doi: 10.1109/CVPR42600.2020.00884.

[27] K. Liu, F. Zhao, G. Xu, X. Wang, and H. Jin, "Temporal Knowledge Graph Reasoning via Time-Distributed Representation Learning," in 2022 IEEE International Conference on Data Mining (ICDM), Orlando, FL, USA: IEEE, Nov. 2022, pp. 279–288. doi: 10.1109/ICDM54844.2022.00038.

[28] Q. Massoz, T. Langohr, C. Francois, and J. G. Verly, "The ULg multimodality drowsiness database (called DROZY) and examples of use," in 2016 IEEE Winter Conference on Applications of Computer Vision (WACV), Lake Placid, NY, USA: IEEE, Mar. 2016, pp. 1–7. doi: 10.1109/WACV.2016.7477715.

[29] P. Pattarapongsin, B. Neupane, J. Vorawan, H. Sutthikulsombat, and T. Horanont, "Real-time Drowsiness and Distraction Detection using Computer Vision and Deep Learning," in Proceedings of the 11th International Conference on Advances in Information Technology, Bangkok Thailand: ACM, Jul. 2020, pp. 1–6. doi: 10.1145/3406601.3406638.

[30] S. S. Jasim, A. K. Abdul Hassan, and S. Turner, "Driver Drowsiness Detection Using Gray Wolf Optimizer Based on Face and Eye Tracking," ARO, vol. 10, no. 1, pp. 49–56, May 2022, doi: 10.14500/aro.10928.

[31] M. Yakno, J. Mohamad-Saleh, and M. Z. Ibrahim, "Dorsal Hand Vein Image Enhancement Using Fusion of CLAHE and Fuzzy Adaptive Gamma," Sensors, vol. 21, no. 19, p. 6445, Sep. 2021, doi: 10.3390/s21196445.

[32] R.-C. Chen, C. Dewi, Y.-C. Zhuang, and J.-K. Chen, "Contrast Limited Adaptive Histogram Equalization for Recognizing Road Marking at Night Based on Yolo Models," IEEE Access, vol. 11, pp. 92926–92942, 2023, doi: 10.1109/ACCESS.2023.3309410.

[33] N. N. Pandey and N. B. Muppalaneni, "A novel algorithmic approach of open eye analysis for drowsiness detection," Int. j. inf. tecnol., vol. 13, no. 6, pp. 2199–2208, Dec. 2021, doi: 10.1007/s41870-021-00811-x.

[34] S. Bakheet and A. Al-Hamadi, "A Framework for Instantaneous Driver Drowsiness Detection Based on Improved HOG Features and Naïve Bayesian Classification," Brain Sciences, vol. 11, no. 2, p. 240, Feb. 2021, doi: 10.3390/brainsci11020240.

[35] S. Sharan, R. Reddy, and P. Reddy, "Multi-level Drowsiness Detection using Multi-Contrast Convolutional Neural Networks and Single Shot Detector," in 2021 International Conference on Intelligent Technologies (CONIT), Hubli, India: IEEE, Jun. 2021, pp. 1–6. doi: 10.1109/CONIT51480.2021.9498568.

[36] Sharanabasappa and S. Nandyal, "Driver Drowsiness Estimation Based on Hybrid Feature Extraction and Light weighted Dense Convolutional Network," in 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India: IEEE, Apr. 2022, pp. 1–6. doi: 10.1109/ICDCECE53908.2022.9792965.

[37] L. Zhao et al., "Data-driven learning fatigue detection system: A multimodal fusion approach of ECG (electrocardiogram) and video signals," Measurement, vol. 201, p. 111648, Sep. 2022, doi: 10.1016/j.measurement.2022.111648.

[38] Z. Feng et al., "Perfecting and extending the near-infrared imaging window," Light Sci Appl, vol. 10, no. 1, p. 197, Sep. 2021, doi: 10.1038/s41377-021-00628-0.

[39] M. Salvi, U. R. Acharya, F. Molinari, and K. M. Meiburger, "The impact of pre- and post-image processing techniques on deep learning frameworks: A comprehensive review for digital pathology image analysis," Computers in Biology and Medicine, vol. 128, p. 104129, Jan. 2021, doi: 10.1016/j.compbiomed.2020.104129.

[40] S. Saponara and A. Elhanashi, "Impact of Image Resizing on Deep Learning Detectors for Training Time and Model Performance," in Applications in Electronics Pervading Industry, Environment and Society, vol. 866, S. Saponara and A. De Gloria, Eds., in Lecture Notes in Electrical Engineering, vol. 866. , Cham: Springer International Publishing, 2022, pp. 10–17. doi: 10.1007/978-3-030-95498-7_2.

[41] L. Huang, J. Qin, Y. Zhou, F. Zhu, L. Liu, and L. Shao, "Normalization Techniques in Training DNNs: Methodology, Analysis and Application," IEEE Trans. Pattern Anal. Mach. Intell., vol. 45, no. 8, pp. 10173–10196, Aug. 2023, doi: 10.1109/TPAMI.2023.3250241.

[42] A. Hertig-Godeschalk, J. Skorucak, A. Malafeev, P. Achermann, J. Mathis, and D. R. Schreier, "Microsleep episodes in the borderland between wakefulness and sleep," Sleep, p. zsz163, Jul. 2019, doi: 10.1093/sleep/zsz163.

[43] M. Besnassi, N. Neggaz, and A. Benyettou, "Face detection based on evolutionary Haar filter," Pattern Anal Applic, vol. 23, no. 1, pp. 309–330, Feb. 2020, doi: 10.1007/s10044-019-00784-5.

[44] N. N. Pandey and N. B. Muppalaneni, "Dumodds: Dual modeling approach for drowsiness detection based on spatial and spatio-temporal features," Engineering Applications of Artificial Intelligence, vol. 119, p. 105759, Mar. 2023, doi: 10.1016/j.engappai.2022.105759.

[45] A. Zankruti and T. Vibha, "Automatic Face Recognition and Detection Using OpenCV, Haar Cascade and Recognizer at Different Angle of Face," International Journal of Engineering Research and Applications, vol. 10, no. 6, pp. 13–19, Jun. 2020.

[46] M. C. Santana, O. Deniz, L. A. Canalis, and J. Lorenzo-Navaro, "FACE AND FACIAL FEATURE DETECTION EVALUATION - Performance Evaluation of Public Domain Haar Detectors for Face and Facial Feature Detection," in Proceedings of the Third International Conference on Computer Vision Theory and Applications, Funchal, Madeira, Portugal: SciTePress - Science and and Technology Publications, 2008, pp. 167–172. doi: 10.5220/0001073101670172.

[47] O. N. Mohammed, "Enhancing Pulmonary Disease Classification in Diseases: A Comparative Study of CNN and Optimized MobileNet Architectures," Journal of Robotics and Control (JRC), vol. 5, no. 2, pp. 427–440, 2024.

[48] K. Dong, C. Zhou, Y. Ruan, and Y. Li, "MobileNetV2 Model for Image Classification," in 2020 2nd International Conference on Information Technology and Computer Application (ITCA), Guangzhou, China: IEEE, Dec. 2020, pp. 476–480. doi: 10.1109/ITCA52113.2020.00106.

[49] P. Verma, V. Tripathi, and B. Pant, "Comparison of different optimizers implemented on the deep learning architectures for COVID-19 classification," Materials Today: Proceedings, vol. 46, pp. 11098–11102, 2021, doi: 10.1016/j.matpr.2021.02.244.

[50] R. Patel and A. Chaware, "Transfer Learning with Fine-Tuned MobileNetV2 for Diabetic Retinopathy," in 2020 International Conference for Emerging Technology (INCET), Belgaum, India: IEEE, Jun. 2020, pp. 1–4. doi: 10.1109/INCET49848.2020.9154014.

[51] Z. Riaz, B. Khan, S. Abdullah, S. Khan, and M. S. Islam, "Lung Tumor Image Segmentation from Computer Tomography Images Using MobileNetV2 and Transfer Learning," Bioengineering, vol. 10, no. 8, p. 981, Aug. 2023, doi: 10.3390/bioengineering10080981.

[52] A. Tripathi, T. Singh, R. R. Nair, and P. Duraisamy, "Improving Early Detection and Classification of Lung Diseases With Innovative MobileNetV2 Framework," IEEE Access, vol. 12, pp. 116202–116217, 2024, doi: 10.1109/ACCESS.2024.3440577.

[53] H. Wang, Q. Qi, W. Sun, X. Li, B. Dong, and C. Yao, "Classification of skin lesions with generative adversarial networks and improved MOBILENETV2," Int J Imaging Syst Tech, vol. 33, no. 5, pp. 1561–1576, Sep. 2023, doi: 10.1002/ima.22880.

[54] C. Buiu, V.-R. Dănăilă, and C. N. Răduţă, "MobileNetV2 Ensemble for Cervical Precancerous Lesions Classification," Processes, vol. 8, no. 5, p. 595, May 2020, doi: 10.3390/pr8050595.

[55] S. Gupta, K. Saluja, A. Goyal, A. Vajpayee, and V. Tiwari, "Comparing the performance of machine learning algorithms using estimated accuracy," Measurement: Sensors, vol. 24, p. 100432, Dec. 2022, doi: 10.1016/j.measen.2022.100432.

[56] H. R. Sofaer, J. A. Hoeting, and C. S. Jarnevich, "The area under the precision - recall curve as a performance metric for rare binary events," Methods Ecol Evol, vol. 10, no. 4, pp. 565‑577, Apr. 2019, doi: 10.1111/2041-210X.13140.

[57] R. Yacouby and D. Axman, "Probabilistic Extension of Precision, Recall, and F1 Score for More Thorough Evaluation of Classification Models," in Proceedings of the First Workshop on Evaluation and Comparison of NLP Systems, Online: Association for Computational Linguistics, 2020, pp. 79–91. doi: 10.18653/v1/2020.eval4nlp-1.9.

[58] C. Bertinetto, J. Engel, and J. Jansen, "ANOVA simultaneous component analysis: A tutorial review," Analytica Chimica Acta: X, vol. 6, p. 100061, Nov. 2020, doi: 10.1016/j.acax.2020.100061.

[59] S. Winarno and H. A. Azies, "The Effectiveness of Continuous Formative Assessment in Hybrid Learning Models: An Empirical Analysis in Higher Education Institutions," International Journal of Pedagogy and Teacher Education, vol. 8, no. 1, p. 1, Jul. 2024, doi: 10.20961/ijpte.v8i1.89693.

[60] J. J. Goeman and A. Solari, "Comparing Three Groups," The American Statistician, vol. 76, no. 2, pp. 168–176, Apr. 2022, doi: 10.1080/00031305.2021.2002188.

[61] C. Ravichandran and G. Padmanaban, "A numerical simulation-based method to predict floor wise distribution of cooling loads in Indian residences using Tukey honest significant difference test," Advances in Building Energy Research, vol. 17, no. 1, pp. 1–29, Jan. 2023, doi: 10.1080/17512549.2022.2129449.

[62] S. Sudha Mishra and A. K. Das Mohapatra, "Weavers' perception towards sustainability of sambalpuri handloom: A Tukey's HSD test analysis," Materials Today: Proceedings, vol. 51, pp. 217–227, 2022, doi: 10.1016/j.matpr.2021.05.242.

[63] Muljono, S. A. Wulandari, H. A. Azies, M. Naufal, W. A. Prasetyanto, and F. A. Zahra, "Breaking Boundaries in Diagnosis: Non-Invasive Anemia Detection Empowered by AI," IEEE Access, vol. 12, pp. 9292–9307, 2024, doi: 10.1109/ACCESS.2024.3353788.

[64] S. H. Majeed and N. A. M. Isa, "Adaptive Entropy Index Histogram Equalization for Poor Contrast Images," IEEE Access, vol. 9, pp. 6402–6437, 2021, doi: 10.1109/ACCESS.2020.3048148.

[65] Md. Nahiduzzaman et al., "Diabetic retinopathy identification using parallel convolutional neural network based feature extractor and ELM classifier," Expert Systems with Applications, vol. 217, p. 119557, May 2023, doi: 10.1016/j.eswa.2023.119557.

[66] X. Deng, Q. Liu, Y. Deng, and S. Mahadevan, "An improved method to construct basic probability assignment based on the confusion matrix for classification problem," Information Sciences, vol. 340–341, pp. 250–261, May 2016, doi: 10.1016/j.ins.2016.01.033.

Random Forest Algorithm for HR Data Classification and Performance Analysis in Cloud Environments

Fangfang Dong
College of Management, Zhengzhou Shengda University of Economics,
Business and Management, Zhengzhou 451191, Henan, China

***Abstract*—This study applies the Random forest algorithm to classify and evaluate the effectiveness of business human resources (HR) data, focusing on its potential in supporting strategic decision-making and enhancing organizational efficiency. The research introduces a model that automates the categorization of HR data, including employee records, performance evaluations, and training activities, using the Random Forest method. By constructing both classification and effectiveness assessment models, the study aims to provide businesses with a robust tool for managing and evaluating employee contributions. Key HR metrics were analyzed and categorized, leading to the creation of an effectiveness evaluation model that offers objective insights into employee performance. The Random forest algorithm's accuracy and stability were validated through cross-validation techniques, proving it to be effective in categorizing employee data and identifying different workforce groups. The models developed in this study are designed to support HR managers in optimizing human resource allocation, improving employee satisfaction, and driving overall business performance. The paper also discusses how the model can be optimized further by expanding data sources and applying it to practical business scenarios.**

Keywords*—Random forest algorithm; business; human resources; data classification

I. Introduction

In recent years, the emphasis on investment and R&D programs has become more pronounced as China moves from a rapid growth model to one that pursues high-quality development. Between 2013 and 2015, the formalization of China's R&D workforce increased rapidly. The growth of R&D companies and the rapidly changing needs of users have contributed significantly to the increase in R&D projects. In order to compress the R&D cycle, it has become an emerging trend in the industry for multiple R&D companies to develop multiple projects in parallel at the same time [1]. For many projects, each project's overall status and profitability must be considered thoroughly. Therefore, achieving high performance with limited resources is much more complex than in a single-design environment and requires more than a rational layout [2]. The planning of human resources of R&D personnel as the main body of innovation takes priority in electronic projects, which highly depends on the rational allocation of resources. However, project planning and human resource allocation have become more complicated due to multitasking conflicts and the shortage of R&D personnel [3]. Construction delays and budget overruns are often triggered when the schedule and staffing cannot be synchronized. Therefore, how to rationally organize the task planning and staff allocation of multiple projects, complete the overall construction cycle in the shortest time, improve the company's economic efficiency, and prioritize the execution of R&D projects has become an essential topic in theory and practice.

As the project progresses and the workforce structure study becomes more in-depth, the R&D program encounters several challenges, particularly at two levels. Given the limited size of the company and the high availability and mobility of R&D staff, these people, who are the core driving force of R&D, often have to work on multiple projects simultaneously. Practically, whenever a developer moves from a current project to a new one, it takes a period of adjustment to familiarize themselves with the new task, including understanding the context, timeline, and other vital elements. For example, the R&D department of a networking company often develops multiple software suites in parallel [3]. Due to limited resources, it is often necessary to share developers between projects. Employees are often reassigned to other projects after completing their current tasks. However, due to the vastly different business environments in which different software projects operate, these R&D staff involved in the transition may need help seamlessly integrating into their new tasks. In addition, R&D personnel involved in the transfer need to have a deep understanding of the latest task requirements, background information, and the project's current progress [4]. It is worth noting that, unlike the redeployment of resources such as machines and equipment, the movement of personnel between projects is limited by geographic location, which is often difficult to achieve. In contrast to actual employee mobility, transportation time is not directly related to the geographic location of an employee. Such employee mobility can lead to delays in task execution, negatively affecting project progress and efficiency, which needs to be taken seriously by company management.

II. Background of the Study

In 2019, the National Development and Reform Commission (NDRC) listed talent services as one of the key sectors to promote the development of the talent and human capital services industry, which undoubtedly brings significant advantages and unlimited opportunities for the talent services industry to flourish. The core of digital human resource management lies in analytics and forecasting. This system reduces the impact of uncertainty on the workforce and dramatically improves the accuracy of "training and retention" strategies in human resource management [5].

Under human resource management's current challenges, building a highly integrated digital HR system with the organization has become a core mission in the HR field. The HRM system and projects planned in this paper play a pivotal role. In order to optimize the capability of multiple R&D projects in depth, this paper studies the deployment time of R&D personnel between projects in depth. It constructs a model closer to the actual needs based on personnel characteristics [6]. The model not only considers the impact of personnel heterogeneity on task duration but also incorporates the consideration of transfer time and strives to realize the optimal allocation of human resources [7]. In addition, the research results of this paper provide valuable methods and ideas for solving problems in the design of actual R&D projects, with both theoretical depth and practical value. The steps of the random forest algorithm are shown in Table I.

TABLE I. STEPS OF THE RANDOM FOREST ALGORITHM

Random Forest Algorithm
Input: The training dataset has P attributes or predictive variables
Output: Random Forest Algorithm Model for Corresponding Datasets
(1) Check if the decision attribute values in the training dataset are the same and exit if they are the same.
(2) Select feature subset: Randomly select M attributes as prediction variables in the training dataset, where $M \leq P$;
(3) Select the predictive variable with the best classification performance as the root node and decompose it into decision sub-nodes and leaf nodes; and
(4) Repeat steps (2) and (3) to generate N base classifiers.
(5) Average the prediction results for each training tree.

The importance of resource constraints in the planning process has been explored in greater detail in current academic sources on project planning. Relying on resource constraints as the infrastructure of project planning, many resource-constrained challenges can be extended based on real-world contexts [8]. As a critical branch of PSGRC (which may refer to a specific type of project planning or resource constraint problem) research, the topic of multi-project research design has always attracted researchers' attention [9]. Compared to traditional construction projects, R&D projects like software development have a high failure rate. This study aims to ensure the proper allocation of budget and resources to achieve efficient, on-time delivery of products [10]. However, current R&D project planning and human resource optimization strategies must be addressed. Human resources, as a unique renewable resource, are an essential core element in the product development process [11]. In project planning, the time allocation of intangible human resources among project tasks must be fully considered, as well as the possible impact of personnel differences on project planning and personnel deployment strategies.

III. RESEARCH METHODOLOGY

A. Data Processing

The data sources were first introduced when constructing the employee turnover prediction model, followed by an in-depth analysis and understanding of the dataset's characteristics. Based on business insights, two key features were successfully created: the number of days absent per year and the actual hours worked per day, respectively [12]. After that, the newly acquired status, survey, and employee performance data were seamlessly integrated into the existing dataset. The integrated data was rationalized into two datasets evaluate the model's performance. Given some of the limitations of the data, a simple and efficient method of integrating measurement units of different natures was used shorten the model's learning and prediction cycle [13]. Data preprocessing steps were also performed, including treating missing values, data substitution, data normalization, and feature selection, which are essential for data integration. The GOSS related process description is shown in Table II.

TABLE II. DESCRIPTION OF GOSS-RELATED PROCESSES

GOSS algorithm description
Inputs: training data, number of iterations d, sampling rate a for extensive gradient data, sampling rate b for small gradient data, loss function, and weak learner
Output: A well-trained, strong learner
(1) it points that have been sorted in descending order, and then randomly select b x (1-a) x 100% sample points from the remaining sample set as a set of minor gradient sample points. Been sorted in descending order, and then randomly select b x (1-a) x 100% sample points from the remaining sample set as a set of minor gradient sample points; and then randomly select b x (1-a) x 100% sample points from the remaining sample set as a set of minor gradient sample points. Points.
(2) Merge the large and small gradient sample sets as the total sample sets for this GOSS sampling.
(3) Multiply the small gradient sample by a weight coefficient (1-a)/b.
(4) Repeat steps (2) and (3) to generate N base classifiers.
(5) Use the sampled samples mentioned above to iteratively generate a new weak learner, repeating it until it reaches the maximum number of iterations or convergence.

Since the raw data was until it reached different files, the processing was broken down into two key steps. First, the incoming data needed to be analyzed in detail, followed by data processing and adding new attributes to this data. Immediately following this, the second step effectively integrates the newly generated data, the survey data, and the employee performance requirements [14]. In the context of this paper, the training process for 4,410 employees is refined into three consecutive phases: analysis of status data, processing of status data, and creation of new status data attributes. Regarding the preprocessing of data, the specific processes are as follows:

1) Data analysis: After in-depth analysis of the data of 4,410 employees over 261 days, it is found that all the employees have been absent for an average of 12 days. The number of days of absence for some of them is even as high as 24 days.

2) Data processing: When all the employees are not present on a particular day, it is regarded as a public holiday, and the relevant test data is directly removed; whereas, when some of the employees have attendance records while the other part does not, the missing value 0 will be filled in the corresponding position.

3) New function creation: The number of absences and the average actual working hours of each employee in 2015 were further calculated. These newly generated attendance, survey,

and employee assignment data can now be found in three separate tables.

Given that the preprocessing steps are the same for the training and test packages, the following will focus on the preprocessing process for the training package data. This preprocessing process covers the handling of missing values, data exchange and normalization, and function selection. In the process of random forest or data study, specific attributes often miss values [15]. There are three ways to deal with these missing values: deleting, filling, or leaving them out. If, in practice, the number of functions and data samples are insufficient, it is not recommended to delete these samples directly before providing examples for missing values. Usually, it is necessary to examine the correlation between the missing values and the attribute features to be retained or deleted [16]. There are three broad types of filling of missing values: missing replacement values, missing match values, and model variables. Missing replacement values refer to replacing missing values by filling in statistical indicators or empirical values that do not contain missing data; missing matches correspond to missing values to other characteristics modeled; and model variables refer to data that new, exported, new, or incomplete data have replaced.

Data classification methods in Eq. (1):

$$HC = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}[(a_i a_j)/(1+l_{ij})]}{A_L^2} \quad (1)$$

It is the sum of the original data and the forward increment of the enterprise.

$$PC = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n} a_i a_j P_{ij}^*}{A_L^2} \quad (2)$$

In Eq. (2), P_{ij}^* the j^{th} probability value of the probability I function is always greater than zero and less than one.

$$RI = 0.5^* IIC + 0.5^* PC \quad (3)$$

In Eq. (3), *RI* is the production value of the firm's data, and 0.5 is the coefficient of the two terms.

B. Feature Selection for Random Forests

In data analysis, the use of different units of measurement often leads to very different interpretations of results. In general, attribute values presented in smaller units of measurement tend to appear more prominent, and these values often carry significant importance or "impact." Further, choosing a simplified and functionally meaningful model can help researchers gain a deeper understanding of data generation mechanisms. The feature selection methods can be categorized into three types: filtering, packing, and embedding [17]. This paper uses the correlation coefficient method of the filtering method. This method filters attributes based on the correlation between attributes or setting different thresholds. If the correlation result between two attributes reaches or exceeds the set threshold, it is recognized that there is a strong correlation between them. This paper chose Pearson's correlation coefficient as a correlation measure.

The determination of estimates plays a pivotal role in the selection of critical steps in the experimental process, and this choice is decisive for model selection and the improvement of forecasting accuracy. Since the data in this project are unbalanced and have yet to be analyzed in depth in the balance sheet, the selection of estimates should be closely dependent on the actual data. After careful reading of relevant literature and data, this paper decides to adopt F1, balance accuracy (BA), geometric mean (G-mean), and AUC as the primary evaluation indexes. F1 is a comprehensive score, and the closer its value is to 1, the better the predictive performance of the model is. On the other hand, Balanced accuracy effectively improves the dataset's accuracy by fusing the two metrics, TPR (actual rate) and TNR (actual negative rate). The G-mean, or geometric mean, is the geometric mean of each accuracy level, which effectively filters out the differences in the number of samples in different categories, making the assessment of learning performance more fair. When the ROC curve is closer to the upper left corner, i.e., the area is larger, the AUC value increases, which signals a higher prediction accuracy of the classifier.

Random forest algorithm iteration results:

```
class A { static void f(){ System.out.println("----------
-------");
//} static double quzheng(double a){ int b; int b.
        System.out.println((b=(int)(a+0.5)));
//return(b);
} static double qiushang(double a,double b){
//System.out.println((a/b));
return(a/b).
} static boolean odd(int c){
//if(c%2==0){
return(false);
} else{ return(true);
} } static int juedui(int d){
//f(d<0){
```

First, the employee turnover prediction model was constructed using a Random forest algorithm by adjusting the parameters before and after optimization. Then, the LXR random forest stack algorithm was further utilized to create a forecasting model for employee turnover. In order to assess the performance of the model entirely, the predictive characteristics of the random forest model before and after optimization were compared and analyzed with the LXR random forest stack model. Simplified methods were introduced to reduce the risk of overload that may arise during the modeling process [18]. These methods include group learning algorithms, traditional data augmentation techniques, and cross-validation methods, which further reduce the risk of model overfitting. In addition, compliance elements were added to construct three specific predictive models: the XGBoost employee intention to leave prediction model, the LightGBM employee intention to leave prediction model, and a two-layer learning logistic regression

model based on the LXR stack. It is worth mentioning that the combined LXR stack model was carefully constructed using cross-validation methods to ensure its stability and accuracy. Stacking algorithm model construction process. As shown in Table III.

TABLE III. STACKING ALGORITHM MODEL CONSTRUCTION PROCESS

Stacking algorithm model construction process
Input: training set 1S, base learner H, meta learner H '
Output: Algorithm model of meta learners on the training set
(1) Divide the training set 1S data into K-fold partitions.
(2) Perform K-fold cross-validation using each base learner iH, with K sets of trained data; the
(3) Combine K pieces of data predicted on the training set to obtain new training samples.
(4) Take the average of the predicted data obtained from the test set as the new predicted data.
(5) Import the dataset from step four into the meta learner H classifier (such as logistic regression) to obtain the final prediction result, which is the algorithm model of the meta learner on the training set.

IV. RESULTS AND DISCUSSION

A. Human Resource Effectiveness in Random Forests

Random forest model, as a powerful tool in machine learning, is not only an innovative expansion of traditional data analysis methods but also demonstrates its excellent performance in various data types and complex scenarios. Compared with the traditional decision tree model, Random Forest significantly improves the stability. All this comes from its core algorithm, which aligns with the classic random forest model. In this section, this study specifically focuses on utilizing the Random Forest algorithm to construct a specific HR capability enhancement model, aiming to provide forward-looking guidance for HR planning in an organization by predicting the trend of employee turnover. For this purpose, the Random Forest Classifier tool from the open-source machine learning library Sklearn is the basis for constructing the model.

The setting and tuning of hyperparameters are crucial to constructing the model. For the random forest model, a default starting value for the hyperparameters, i.e., 0, was used as a starting point. This has the advantage that targeted hyperparameter evaluation and tuning can be performed based on the initial performance of the model. However, relying solely on the default starting value often fails to achieve the desired model performance. Therefore, a more refined parameter setting and tuning strategy is used to optimize the Random Forest algorithm model. Among them, FLAML (Fast Lightweight Automated Machine Learning Library) becomes a powerful assistant. FLAML can efficiently tune the hyperparameters in the Random Forest model and find the parameter combinations that can improve the model performance through automation. The questionnaire attributes are shown in Table IV.

Further manual tuning of the hyperparameters was performed on top of the initial optimization of FLAML. This is because, while automated tools can provide a better starting point, more detailed tuning is often required for specific problems and datasets. During the manual tuning process, the model's AUC value (Area Under the Curve) was always used as an evaluation metric to find the combination of hyperparameters that would optimize the model's performance. Overall, a high-performance employee turnover prediction model was successfully constructed by combining Sklearn's Random Forest Classifier tool and the FLAML automated machine learning library. This model can not only help enterprises better understand the pattern of employee turnover but also provide powerful data support for human resource planning to occupy a more favorable position in the fierce competition in the market. LightGBM, the open-source Gradient Boosting Decision Tree (GBDT) algorithmic framework introduced by Microsoft, has excellent parallel learning capability. GBDT, a classic algorithm in the field of random forests, has the core idea of continuously training and correcting the wrong classifiers to achieve the optimal learning effect while avoiding overfitting problems. In addition, GBDT has become a powerful weapon in data research competitions such as Kaggle. In the hyperparameter tuning session, the GBM optical model of FLAML (an automatic machine learning library) is often used to tune the hyperparameters accurately. After completing the initial optimization settings through FLAML, researchers often manually adjust the parameter settings to improve the model's performance further.

TABLE IV. QUESTIONNAIRE ATTRIBUTES

Feature attribute categories	**Feature attribute name**
Annual attendance data	Employee ID, daily clock-in and clock-out time
Questionnaire survey data	Employee ID, Work Engagement, Last Year's Performance Level, Environmental Satisfaction. Job satisfaction, work-life balance
Work-related detail data	Age, frequency of employee business trips in the previous year, department name, distance from home, education level, education field, number of employees, employee ID, gender, occupational level, professional role, marital status, monthly income, the total number of companies worked for, age 18 or above, salary increase percentage, standard working hours per day, stock options level, total years of work, number of training sessions in the previous year, years of work in the company The following are some examples of the types of training sessions that the company has offered: year, years of work in the company, years since last promotion, and years of working with current direct leaders.

The combined model integrates multiple algorithmic models that have been trained to improve performance while considering the strengths and weaknesses of each model. Combining the ability of primary education students with accurate predictive power strengthens the predictive performance of the overall model. The core modeling strategy can be either a unified model algorithm or a diverse collection of algorithms. Different algorithmic models are usually picked according to the modeling requirements when selecting core strategies. In order to optimize the performance of the stack integration model, the hyperparameter tuning algorithmic

model is adopted as the primary base learning tool. During the training and installation process, new learning materials are generated on the first floor of the database learning facility. Directly employing actual data to create new learning records and materials may result in excessive liability risk. Some elements are placed outside the learning area before creating new content to minimize the risk associated with this inconsistency. After parameter optimization, this paper integrates the training methods of these three main machine learning models [19]. using logistic regression to construct an LXR-integrated model to predict employees' intention to leave. This model is used for human resource management in organizations.

In this study, human resources data were divided into two categories, mainly performance and effectiveness evaluation. In the comparison of 18 sample results, pairwise comparisons of the ratios of the two categories were conducted. Negative values were used for the effectiveness evaluation of human resources data to facilitate the comparison of the two data values. The specific results are shown in Fig. 1.

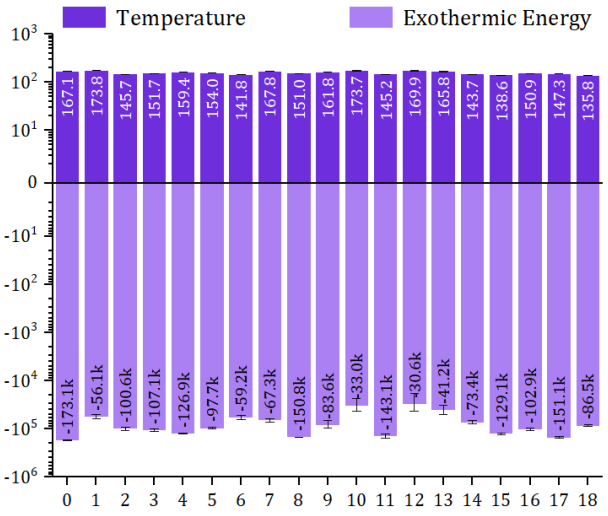


Fig. 1. Human resources data classification.

After going through data integration, missing value filling, data exchange, and standardization, data preprocessing was performed by applying relevant metrics to filter out activities. Three algorithmic models - Random Forest, XGBoost, and Light GBM - were utilized to train the learning toolkit. Given that the second input level is the first core level based on students, the output of the first core level shows a linear correlation with the final classification result. Therefore, a more explanatory model of the logistic regression algorithm was chosen for the second layer of the LXR stack fusion model. After creating new data, the first student used a five-fold cross-validation approach to rank the probability matrix. This strategy effectively reduced the risk of conflict with the second student. When training for Foundation 1 students, optimizing the hyperparameters and subsequently superimposing them is an integral step to obtain superior learning performance. Statistical table for missing feature values in the training set. As shown in Table V.

TABLE V. STATISTICAL TABLE FOR MISSING FEATURE VALUES IN THE TRAINING SET

Attribute Name	Missing quantity	Total number of samples	Missing proportion
Number of companies working	225	8475	0.62%
Total years of service	140	8475	0.65%
Environmental satisfaction	12	8475	0.021%*
Job satisfaction	36	8475	0.63%
Work-Life Balance	552	8475	0.14%

B. Assessment of Human Resources System Design

This paper builds a model to predict employees' propensity to leave their jobs. However, the key to making this model truly useful and user-friendly is seamlessly integrating this turnover prediction model into real-world applications. This ensures that employees across the organization can use the model and supports resource decisions. In terms of data protection, this paper adopts the SM2 algorithm to encrypt critical data to safeguard employees' personal information. In addition, the architecture design of the HRMS mentioned in this paper is based on the B/S model while combining the SpringBoot framework and LayUI to ensure the stability and efficiency of the system.

Data construction for enterprise human resources:

```
    # Define a function to generate a portion of the ASCII art
    def heart_segment(x, y, char).
    return ((x - 2 * y) ** 2 - (x ** 2 - 2 * x * y + y ** 2) ** 2 /
25).substitute(x=x, y=y).replace('**', '^') <= char
    def print_heart(char):
    for y in range(10):
    for x in range(20):
    import turtle
    import math
    turtle.pen()
    t=turtle
    t.up()
    t.goto(0,150)
    t.down()
    t.color('red')
    t.begin_fill()
    if heart_segment(x / 4.0, y, char).
    print(char, end='')
    else.
    print(' ', end=' ')
    print()
    print_heart('*')
```

Before embarking on system development, in-depth research and careful consistency analysis occupy a pivotal position in the system construction process. In this paper, through detailed market research, we have explored users' actual needs and clarified the system architecture's core value and far-reaching significance. In this process, functional and non-functional requirements are explored in detail, and the specific content of system requirements is finally established. Based on related research, it was identified that system users are mainly categorized into three roles: ordinary employee users, employee administrator users, and system administrator users. The tasks commonly involved in the daily operations of

these three roles include logging into the system, logging out of accounts, and changing passwords. Regular employee users may also have access to pay for paychecks and online evaluations. The rating management segment focuses on maintaining and managing rating names, statuses, and flags. Employees can participate only when the assessment mode is activated. The department management module provides users with the ability to store information in their department; the user management module allows authorized users to enter and update information about system users; the role management module not only enables users to manage roles within the system but also ensures that the permissions of each user role are appropriately maintained; and finally, the menu management module is responsible for assigning authorized users the names, paths, and other essential information of the system's menus. Finally, the menu management module specifies the system menus' names, paths, and other essential information for authorized users. The parameters of the random forest are described in Table VI.

TABLE VI. DESCRIPTION OF RANDOM FOREST PARAMETERS

Parameter	Parameter meanings	Default value
(an official) standard	The function that measures the quality of segmentation, with options such as gini, entropy, and log_loss	5565
greatest feature	The size of the random subset of features is considered when dividing nodes. The lower the value, the more the variance decreases, but the more the deviation increases	1124
largest node	The maximum value of leaf nodes, used to limit their growth	12
incremental	The number of base learners is usually better with larger values, but the computation time increases accordingly. When the number of trees exceeds a When the number of trees exceeds a critical value, the performance of the algorithm does not significantly improve.	1
random number	Used to control the randomness of samples during tree construction	6

In this paper, the HR architecture consists of three main layers: the data layer, the control layer, and the interaction layer (i.e., the user interface layer). The data layer is responsible for storing, maintaining, and protecting the system data. The control layer is responsible for receiving requests from the interaction layer, interacting with the data layer, and finally sending the processed results back to the interaction layer. The interaction layer is committed to providing users with an intuitive and easy-to-understand web interface, which transforms complex business logic into a visual interface. This interface allows users to quickly realize all kinds of business needs and form an intuitive user experience. With the rapid development of artificial intelligence technology and the increasingly refined division of labor in society, enterprises have put forward more stringent requirements and cost control standards for the digital management of human resources. In order to quickly adapt to the changing operating environment and market demand, companies must continuously optimize their management and internal processes. Therefore, using the Random Forest method to predict employee turnover has become an effective strategy for HR managers to reduce personnel risks and costs. The random forest algorithm with random correction is shown in Table VII.

TABLE VII. RANDOM FOREST ALGORITHM WITH STOCHASTIC CORRECTION

Variant	Search (1)	Search (2)	Envir (1)	Envir (2)
modified effect	0.1417***	0.0214***	0.0654***	0.0251***
observed value	5147	5147	5147	5147
control variable	be	be	be	be
Annual fixed effects	be	be	be	be
industry fixed effect	be	be	be	be
area fixed effect	clogged	clogged	clogged	be

A specific model for enterprise data effectiveness assessment:

$$X_{new} = x_i + rand(0,1) \times (y_j - x_i)(j = 1,...,P) \quad (4)$$

In Eq. (4) $rand(0,1)$ is the reordering of the independent variables of function x; $Mar(Q,V_T)$ the function is specified as follows:

$$Mar(Q,V_T) = ave(V_T) - E^* \le \frac{\overline{\rho}(1-s^2)}{\delta^2} \quad (5)$$

$$F1 = \frac{2 \times precision \times recall}{precision + recall} \quad (6)$$

In Eq. (5) and Eq. (6), $ave(V_T)$ is the functional form for finding the mean of the *V* function. It $precision \times recall$ is the precision and return value of the function *F1*.

The process of product creation is highly personalized and intelligent. Unlike traditional industrial products, which rely on repetitive mechanical operations, it relies heavily on the ingenuity and innovation of researchers and developers. During the project preparation stage, the R&D staff enjoys the support of abundant resources, such as various types of machinery and equipment. The diversity of human resources refers to the differences in technical expertise, knowledge base, and personal attributes of the company's employees. This diversity has two significant effects on staff allocation: first, the diversity of staff skills directly affects the timeliness of task completion, which is reflected in the different skills of researchers and developers with the same qualifications in terms of age, seniority, experience, and education, which in turn has an impact on performance. Second, employee diversity is also affected by the time between multiple projects. In the actual R&D process, each developer is unique in terms of the underlying design experience he or she possesses. Taking the R&D department of a Web enterprise as an example, any software project can be disassembled into several independent

tasks, each carrying a different workload and content, during the functional analysis and requirements combing phase before the official launch. From the perspective of task allocation, equipping a single task with a combined team with different R&D skills and experience can effectively adjust the project delivery circle.

In the data comparison of Fig. 1, it was found that the performance evaluation data had more significant differences than the performance evaluation data. Therefore, performance evaluation data should be selected for analysis of data density in the study. Fig. 2 shows the process of data density analysis. In order to more significantly highlight the results of the data difference test, polar coordinates were used for this test. The data was divided into intervals of 0-2 π and subjected to extreme segmentation approaching "positive infinity", resulting in a continuous polar coordinate graph of the stability level of the data. The results showed that only at 1/8-3/8 of the data, the stability exceeded the LV3 level, but at other stages, the data exceeded the LV1 level, meeting the testing criteria, as shown in Fig. 2.

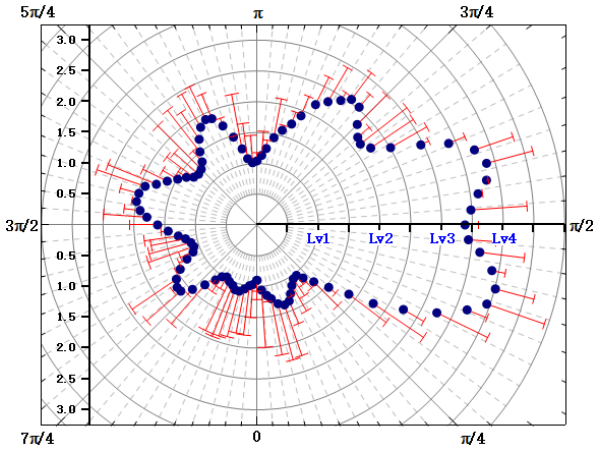


Fig. 2. Human resources effectiveness assessment density.

V. Conclusion

This study has achieved a series of significant findings and results through the classification and effectiveness assessment of enterprise human resource data based on the random forest algorithm. With the continuous development of information technology, effective management of human resources in enterprises has become increasingly important, and the method proposed in this study provides an effective way to process and analyze data, providing deeper insights and decision support for human resource management. First of all, by classifying enterprise human resource data, it is possible to manage and analyze employees more refinery. The classification model constructed based on the Random Forest algorithm can accurately categorize employees according to their characteristics and labels, helping enterprises understand the basic situation of employees, their work characteristics, and potential development direction. This gives enterprises a more comprehensive view of talent management, which helps them develop more personalized training, motivation, and promotion plans for different groups and improves employee job satisfaction and loyalty. Secondly, the performance evaluation model provides an objective and scientific performance evaluation method for enterprises. Analyzing employee performance data and other relevant indicators can assess the contribution and effectiveness level of employees in the organization and help companies identify high-performance employees and potential room for performance improvement. This provides an essential decision-making basis for enterprises and helps optimize the allocation of human resources and improve the overall performance and competitiveness of the organization.

The classification and effectiveness assessment method of enterprise human resource data based on the random forest algorithm has important theoretical significance and practical value. The automated processing and analysis of enterprise human resource data can better understand the characteristics and behaviors of employees and provide more accurate and comprehensive decision support for enterprise managers. In the future, the algorithmic model can be further optimized, combined with more data sources and indicators, and the classification and evaluation system can be improved to cope with the ever-changing market environment and enterprise needs. At the same time, the model can be validated and applied in combination with specific business scenarios and actual cases to improve its accuracy and practicality further and provide more robust support for the sustainable development and innovation of enterprises.

Acknowledgment

This work is supported by Funding project for the construction of disciplines and specialties of Henan Private Ordinary Higher Education Institutions in 2023, " business administration" (Jiaozhengfa [2022] No. 377).

References

[1] Teles, G., Rodrigues, J. J., Rabelo, R. A., & Kozlov, S. A. (2021). Comparative study of support vector machines and random forests machine learning algorithms on credit operation. *Software: Practice and Experience*, 51(12), 2492–2500. https://doi.org/10.1002/spe.2842

[2] Assiri, A. (2021). Anomaly classification using genetic algorithm-based random forest model for network attack detection. *Computers, Materials & Continua*, *66*(1). https://doi.org/10.32604/cmc.2020.013813

[3] Nasar, N., Ray, S., Umer, S., & Mohan Pandey, H. (2021). Design and data analytics of an organization's electronic human resource management activities through the Internet of Things. *Software: Practice and Experience*, *51*(12), 2411–2427. https://doi.org/10.1002/spe.2817

[4] Bazzaz Abkenar, S., Mahdipour, E., Jameii, S. M., & Haghi Kashani, M. (2021). A hybrid classification method for Twitter spam detection based on differential evolution and random forest. *Concurrency and Computation: Practice and Experience*, *33*(21), e6381. https://doi.org/10.1002/cpe.6381

[5] Tassi, A., Gigante, D., Modica, G., Di Martino, L., & Vizzari, M. (2021). Pixel-vs. Object-based Landsat 8 data classification in Google Earth engine using random forest: The Maiella National Park case study. *Remote Sensing*, *13*(12), 2299. https://doi.org/10.3390/rs13122299

[6] Pallathadka, H., Ramirez-Asis, E. H., Loli-Poma, T. P., Kaliyaperumal, K., Ventayen, R. J. M., & Naved, M. (2023). Applications of artificial intelligence in business management, e-commerce, and finance. *Materials Today: Proceedings*, pp. *80*, 2610–2613. https://doi.org/10.1016/j.matpr.2021.06.419

[7] Chaudhary, M., Gaur, L., Jhanjhi, N., Masud, M., & Aljahdali, S. (2022). Envisaging employee churn using MCDM and machine learning. *Intelligent Automation & Soft Computing*,*33*(2). https://doi.org/10.32604/iasc.2022.023417

[8] RL, M., & Mishra, A. K. (2022). Measuring financial performance of Indian manufacturing firms: Application of decision tree algorithms. *Measuring Business Excellence*, *26*(3), 288–307. https://doi.org/10.1108/MBE-05-2020-0073

[9] Javed Mehedi Shamrat, F., Ranjan, R., Hasib, K. M., Yadav, A., & Siddique, A. H. (2022). Performance evaluation among id3, c4. 5, and cart decision tree algorithm. *Pervasive Computing and Social Networking: Proceedings of ICPCSN 2021*, pp. 127–142. https://doi.org/10.1007/978-981-16-5640-8_11

[10] Siahaan, M. (2021). An analysis of contract employee performance assessment using machine learning. *Journal Of Informatics And Telecommunication Engineering*, *5*(1), 121–131. https://doi.org/10.31289/jite.v5i1.5357

[11] Chen, Y., Zheng, W., Li, W., & Huang, Y. (2021). Large group activity security risk assessment and risk early warning based on random forest algorithm. *Pattern Recognition Letters*, pp. *144*, 1–5. https://doi.org/10.1016/j.patrec.2021.01.008

[12] Zhang, T., Su, J., Xu, Z., Luo, Y., & Li, J. (2021). Sentinel-2 satellite imagery for urban land cover classification by optimized random forest classifier. *Applied Sciences*, *11*(2), 543. https://doi.org/10.3390/app11020543

[13] Chen, Y., Chen, W., Chandra Pal, S., Saha, A., Chowdhuri, I., Adeli, B., Janizadeh, S., Dineva, A. A., Wang, X., & Mousavi, A. (2022). Evaluation efficiency of hybrid deep learning algorithms with neural network decision tree and boosting methods for predicting groundwater potential. *Geocarto International*, *37*(19), 5564–5584. https://doi.org/10.1080/10106049.2021.1920635

[14] Yahia, N. B., Hlel, J., & Colomo-Palacios, R. (2021). From big data to deep data to support people analytics for employee attrition prediction. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 60447–60458.

[15] Es-Sabery, F., Es-Sabery, K., Qadir, J., Sainz-De-Abajo, B., Hair, A., García-Zapirain, B., & De La Torre-Díez, I. (2021). A MapReduce opinion mining for COVID-19-related tweets classification using enhanced ID3 decision tree classifier. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 58706–58739.

[16] Zhu, H. (2021). Research on human resource recommendation algorithm based on machine learning. *Scientific Programming*, *2021*, pp. 1–10.

[17] Farhadi, H., & Najafzadeh, M. (2021). Flood risk mapping by remote sensing data and random forest technique. *Water*, *13*(21), 3115. https://doi.org/10.3390/w13213115

[18] Garg, S., Sinha, S., Kar, A. K., & Mani, M. (2022). A review of machine learning applications in human resource management. *International Journal of Productivity and Performance Management*, *71*(5), 1590–1610. https://doi.org/10.1108/IJPPM-08-2020-0427

[19] Zhang, Y., Xu, S., Zhang, L., & Yang, M. (2021). Big data and human resource management research: An integrative review and new directions for future research. *Journal of Business Research*, *pp. 133*, 34–50. https://doi.org/10.1016/j.jbusres.2021.04.019

Feature Selection Methods Using RBFNN Based on Enhance Air Quality Prediction: Insights from Shah Alam

Siti Khadijah Arafin[1], Ahmad Zia Ul-Saufie[2], Nor Azura Md Ghani[3], Nurain Ibrahim[4]*
School of Mathematical Sciences, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia[1, 2, 3, 4]
Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Kompleks Al-Khawarizmi, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia[4]

***Abstract*—This study examines the predictive efficiency of several feature selection approaches in air quality models aimed to predict next-day PM2.5 concentrations in Shah Alam, Malaysia. Air pollution in urban areas is a significant public health concern, and accurate prediction models are essential for timely interventions. However, determining the most important parameters to include in these models remains difficult, especially in complex urban areas with several pollution sources. To address this, we employed three different feature selection methods and applied them to a dataset comprising 43,824 air quality data points provided by the Department of Environmental Malaysia. The data set contained ten variables, such as gas pollutants and meteorological indicators. Each feature selection approach determined top eight variables to include in a Radial Basis Function Neural Network (RBFNN) model. The results showed that ReliefF outperformed Lasso and mRMR in terms of accuracy, specificity, precision, F1 Score, and AUROC, making it the most effective feature selection method for this study. This study contributes to the body of knowledge on air quality modelling by emphasising the relevance of using proper feature selection techniques that are suited to the specific characteristics of the dataset and urban area. Furthermore, it proposes that future study should look into the use of ReliefF-RBFNN in other settings, such as suburban and rural areas, as well as hybrid feature selection approaches to improve prediction performance across several context.**

Keywords*—Lasso; mRMR; PM2.5 concentration; RBFNN; ReliefF

I. Introduction

Globally, air quality has grown to be a major environmental and public health concern, especially in urban areas such as Shah Alam, Malaysia where pollution levels can have a substantial negative influence on people's quality of life. According to study [1], the rapid urbanization in Shah Alam has worsened environmental problems, including air quality deterioration. Predicting air quality, particularly the concentration of dangerous pollutants like PM2.5, is essential for mitigating these risks and providing guidance for public health initiatives. Although various pollutants contribute to air pollution, [2] suggest that PM 2.5 is the most significant affect air pollution. Numerous studies have explored various methods to forecast air quality by utilizing a variety of meteorological and environmental data such as PM10, PM2.5, CO, O3, relative humidity, ambient temperatures and wind speed.

In recent years, there has been a lot of focus on improving the accuracy of air quality predictions using powerful machine learning algorithms. Among these, feature selection approaches help to improve model performance by finding the most relevant variables while minimizing data dimensionality. [3] stated in their study that feature selection can improve model generalization by avoiding overfitting and mitigating the effects of the curse of dimensionality. According to study [4], filter technique, wrapper technique and embedded technique are three technique of feature selection. Various studies have applied different feature selection techniques on air quality data including Lasso, mRMR and reliefF. For instance, [5] used Lasso to find key features that influenced ozone (O3) levels during China's COVID-19 lockdown. Their findings revealed that Lasso efficiently identified key variables, such as O3 and meteorological conditions, which improved the model's interpretability. Moreover, the study in [6] presented a novel method that combines mRMR with Random Forest (RF) and Long Short-Term Memory (LSTM) networks to estimate the Air Quality Index (AQI). Their research showed that mRMR successfully identified key variables influencing AQI, greatly improving the model's predictive capability. Besides, ReliefF was used as a feature selection method for air pollution analysis in the Zonguldak region of Turkey in a study by [7]. They compared the performance of ReliefF with a firefly-based feature selection algorithm and found that even though ReliefF was effective, the firefly-based method outperformed it in classification tasks using Random Forest classifiers. However, most researchers prefer filter approaches because they have a straightforward algorithmic framework and are thus simple to apply [7]. However, the effectiveness of filter and embedded feature selection methods especially in predicting air quality data is still questionable.

Hence, this study aims to determine which feature selection method provides better performance in predicting air quality. This study compares two filter feature selection method and one embedded feature selection method which are Maximum Relevance Minimum Redundancy (mRMR), ReliefF and Least Absolute Shrinkage and Selection Operator (Lasso). The findings of this study will help to build more reliable air quality

forecast models, with consequences for public health and environmental management. This paper is organized as follows: I. Introduction, II. Method, III. Results and Discussion. Then, it followed by the conclusion in Section IV and the reference lists.

II. METHOD

A. Research Flowchart

Fig. 1 below shows the flowchart outlines of this study to predicting next-day PM2.5 levels in Shah Alam, Malaysia, using air quality data from 2018 to 2022 provided by the Department of Environment, Malaysia. Data extraction is the first step in the process, which is then followed by extensive data pre-processing, such as imputation using linear interpolation, converting hourly data to daily figures, binary categorisation of PM2.5 levels, min-max normalisation, and dataset balancing using SMOTE. Next, three feature selection methods which are mRMR, Lasso, and ReliefF are applied to rank and select the top eight variables most relevant to predicting PM2.5. These selected features are then used to train a Radial Basis Function Neural Network (RBFNN), with the model's performance evaluated based on accuracy, specificity, precision, F1 Score, and AUROC. Finally, the best-performing model is identified by combining effective feature selection with the RBFNN.

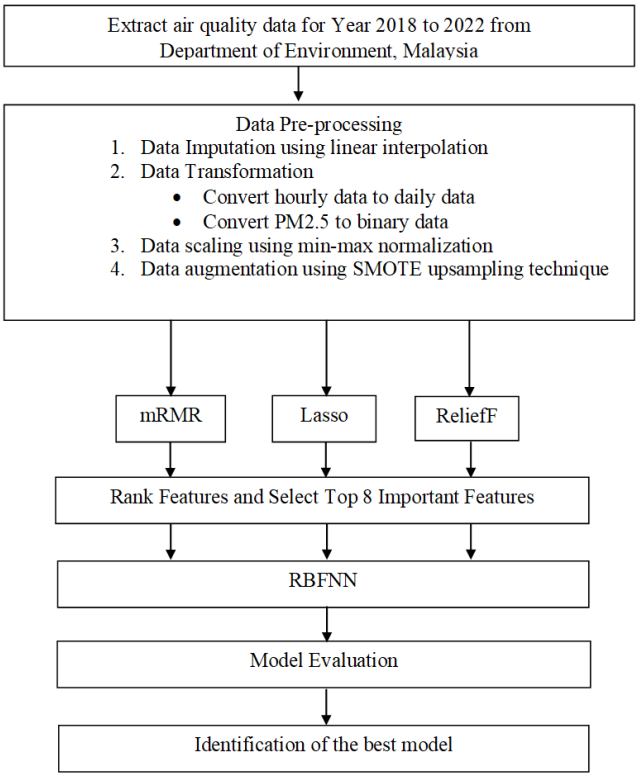


Fig. 1. Research flowchart.

B. Data Description

The Department of Environmental Malaysia provided 43,824 air quality data points for 10 variables, such as gas pollutants and meteorological parameters, collected in Shah Alam. Table I below shows the percentage of missing values for each variable. Based on Table I, all variables have missing values below 10% except NO2 with 12.65% of missing data. In contrast, PM2.5 has a low percentage of missing values with just 1.29% of missing data. Missing values can arise from various sources, including sensor malfunctions, environmental conditions, or data transmission errors. High levels of missing data, particularly in gas pollutants, could introduce biases or reduce the statistical power of the analysis if not properly addressed. Therefore, we applied linear imputation methods to ensure that these gaps do not compromise the accuracy of the predictive models.

TABLE I. PERCENTAGE OF MISSING VALUES

Variable	N	Missing Value
PM2.5	43257	567 (1.29%)
PM10	43151	673 (1.54%)
SO2	41242	2582 (5.89%)
NO2	38280	5544 (12.65%)
O3	41198	2626 (5.99%)
CO	40629	3195 (7.29%)
WD	42925	899 (2.05%)
WS	42868	956 (2.18%)
Humidity	42907	917 (2.09%)
Temperature	42926	898 (2.05%)

To predict the next day's air quality based on PM2.5 levels, we used a binary classification system where 0 represents “not polluted” and 1 represents “polluted”. We followed the methodology of [8], wherein the Air Quality Index (AQI) categories “Good” and “Moderate” were combined into the “not polluted” class, while the other categories were grouped into the “polluted” class. Table II shows the PM2.5 breakpoints (24-hour average) as defined by the U.S. Environmental Protection Agency (EPA).

TABLE II. BINARY LABELS FOR THE RESPECTIVE PM2.5 BREAKPOINT AND AQI CATEGORIES

AQI Category	PM2.5 Breakpoints
Good	0.0-12.0
Moderate	12.1-35.4
Unhealthy for Sensitive Groups	35.5-55.4
Unhealthy	55.5-150.4
Very Unhealthy	150.5-250.4
Hazardous	250.5 and above

C. Feature Selection Method

1) Lasso: The Least Absolute Shrinkage and Selection Operator (Lasso) is an embedded feature selection method that improves model performance by selecting and regularizing variables at the same time. Linear regression assigns weight to each feature, while LASSO regression proposed by Robert Tibshirani removes less significant ones from the subset [9]. Lasso effectively eliminates less significant features from the model by forcing some of the coefficients to be exactly zero by adding a penalty to the loss function that is equal to the absolute value of the magnitude of the coefficients. Furthermore, the study in [10], stated that Lasso method goals

are to lower the variance in models with a high number of unnecessary variables.

The formula to calculate Lasso is shown in Eq. (1) below. Where, $\sum_{j=1}^{p}|\beta_j|$ is known as L_1 penalty term and the value is must below or equal to t, which is the upper bound of the summation of the absolute coefficients. While λ is the tuning parameter which controls the strength of the penalty (Ibrahim, 2020).

$$\hat{\beta} = \min \beta \left\{ \sum_{i=1}^{N} \left(y_i - \beta_0 - \sum_{j=1}^{p} x_{ij}\beta_j \right)^2 + \lambda \sum_{j=1}^{p} |\beta_j| \right\} \quad (1)$$

2) Maximum relevance minimum redundancy (mRMR): Maximum Relevance Minimum Redundancy (mRMR) is a widely used feature selection technique that seeks to reduce redundancy among the independent variables while identifying a subset of features that are most significant to a target variable. This method works especially well with high-dimensional datasets, where the number of features can significantly exceed the number of observations, making traditional modelling techniques less effective. The formula to calculates the maximum relevance shown in Eq. (2):

$$maxD(S,c), D = \frac{1}{|s|}\sum_{x_i \in s} I(x_i, c) \quad (2)$$

Based on the Eq. (2), x_i represents the i-th feature, while $c = \{c_0, c_1\}$ represents the class variables which is not polluted and polluted. L is 2 which denotes the total number of classes, and S indicates the feature subset. Moreover, to calculates the minimum redundancy shown in Eq. (3) below.

$$minR(S), R = \frac{1}{|s|^2}\sum_{x_i, x_J \in S} I(x_i; x_J) \quad (3)$$

3) ReliefF: ReliefF algorithm is an extended version of the Relief algorithm. It is a filter-based feature selection method that used to identify a feature's contribution to a target variable's prediction in order to find relevant features in high-dimensional data [11]. Unlike conventional methods, which just rely on statistical correlations or regression analysis, ReliefF operates by evaluating each feature's ability to differentiate between instances that belong to distinct classes. It has been demonstrated that ReliefF can handle noisy data and identify reelevant features in high-dimensional datasets [12].

The algorithm finds the k-nearest neighbours by repeatedly choosing random examples from training datasets. Finding the k-nearest in distinct classes, M_j (C), (j=1,2,…,k), where Euclidean distance is employed to determine the k-nearest neighbours, and H_j, (j=1,2,…,k) of R inside the same class [13]. The significance of each feature is estimated using the variation in feature values between these neighbours. Features that show significant variation across classes and small variations within the same class are more important. The weight of each characteristic is determined using the Eq. (4) below. While Eq. (5) is how the $diff$ is calculated [13].

$$w(f_i) = w(f_i) - \sum_{j=1}^{k} \frac{diff\left(f_i, R, H_j\right)}{mk} + \sum_{c \neq class(R)} \frac{p(C)}{1 - p\left(class(R)\right)} X \sum_{j=1}^{k} \frac{diff\left(f_i, R, M_j(C)\right)}{mk}, \quad (i = 0,1,\dots,d) \quad (4)$$

$$diff(A, R_1, R_2) = \begin{cases} \frac{|R_1[A] - R_2[A]|}{\max A - \min A}, & if\ A\ is\ continous \\ 0, & if\ A\ is\ discrete\ and\ R_1[A] = R_2[A] \\ 1, & if\ A\ is\ discrete\ and\ R_1[A] \neq R_2[A] \end{cases} \quad (5)$$

where $diff(A, R_1, R_2)$ denotes the difference between samples R_1 and R_2 on feature A. While $R_1[A]$ and $R_2[A]$ indicate the values of sample R_1 and R_2 on feature A (Zhang et al., 2022).

4) Radial basis function neural network: Radial Basis Function Neural Networks (RBFNNs) are a subset of artificial neural networks that used radial basis functions as activation functions. The abilities of the model to describe complex nonlinear interactions makes them especially useful for problems involving function approximation, classification, and regression. There are three important layers in RBFNN which are the input layer, hidden layer, and output layer that are generally connected by weights. Firstly, a source node, also known as the independent variable is connected to the network to its surroundings in the input layer, meanwhile, the hidden layer involves a nonlinear transformation from input space to a high-dimension hidden space. Lastly, the output layer is the outcome of the network that applied to the input layer or called the predicted output. Fig. 2 shows the general framework of RBFNN [14].

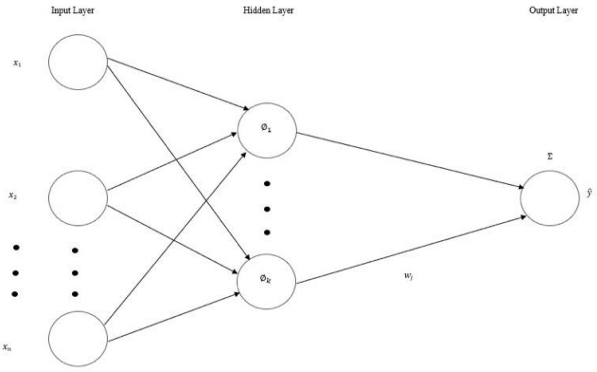


Fig. 2. General framework of a RBFNN.

The hidden layer comprises individual units, each corresponding to a transfer function $\emptyset_j$, which is generally a Gaussian function. The radial basis function (RBF), characterized by its radially symmetric shape, serves as the transfer function in this context. The number of hidden layer units directly corresponds to the number of RBFs used. The Gaussian radial basis function is formally defined in Eq. (6).

$$\emptyset(x) = \exp(-\frac{||x-c||^2}{2\sigma^2}) \quad (6)$$

where x is the input vector, c is the center of the RBF, and σ is the spread (width) parameter. The output of the hidden layer is calculated by taking a weighted sum of these radial basis functions. Specifically, for an input vector $X = \{x_1, x_2, \dots, x_n\}$, the output of the hidden layer is given in Eq. (7).

$$g(X) = \sum_{j=1}^{k} w_j \emptyset_j(r\|X - C_j\|) \quad (7)$$

where w_j are the weights associated with the radial basis functions, C_j are the centers of the RBFs, while r is a scaling factor. In RBFNN, the output layer typically utilizes a logistic (sigmoid) activation function for binary classification tasks. The logistic function, as represented in Eq. (8), is employed to convert the weighted sum of the hidden layer outputs into a probability value within the interval of 0 to 1.

$$\sigma(z) = \frac{1}{1+e^{-z}} \quad (8)$$

Hence, the final output calculation of the RBFNN for binary classification is shown in Eq. (9), where w_0 is a bias term.

$$\hat{y} = \sigma\,(w_0 + \sum_{j=1}^{k} w_j \emptyset_j(r\|X - C_j\|)) \quad (9)$$

D. Model Performances

The performance of developed model in this study will be evaluated based on accuracy, sensitivity, specificity, precision, F1 score and AUROC. The accuracy is the number of correct predictions in a given number of predictions [15]. The formula to calculates accuracy is shown in Eq. (10):

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (10)$$

Sensitivity and specificity are used to explain the relationship between the system's input and output variables and to evaluate the model's resilience in the face of uncertainty. The percentage of real positives that are correctly identified is known as sensitivity, or the True Positive (TP) rate, while the percentage of real negatives that are correctly recognised is known as specificity, or the True Negative (TN) rate. The following Eq. (11) and Eq. (12) provide the formulas for determining specificity and sensitivity, respectively.

$$Sensitivity = \frac{TP}{(TP+FN)} \quad (11)$$

$$Specificity = \frac{TN}{(TN+FP)} \quad (12)$$

Precision quantifies the proportion of correctly classified positive samples out of all samples classified as positive. On the other hand, the F1 score represents the harmonic mean of precision and sensitivity, providing an indication of whether the model's performance is well-balanced. Eq. (13) and Eq. (14) below present the formulas for calculating precision and the F1 score, respectively.

$$Precision = \frac{TP}{(TP+FP)} \quad (13)$$

$$F1\ Score = \frac{2\,x\,Precision\,x\,Sensitivity}{(Precision+Sensitivity)} \quad (14)$$

ROC (Receiver Operating Characteristic) curve examines the relationship between the true positive rate (sensitivity) on the y-axis and the false positive rate (1-specificity) on the x-axis, serving as a tool to assess the performance of the classifier. The AUROC (Area Under the ROC Curve) quantifies the model's ability to distinguish between classes. The AUC value ranges from 0 to 1, where an AUC of 0.0 signifies a model with entirely incorrect predictions, and an AUC of 1.0 indicates a model with perfectly accurate predictions. Hence, high values of accuracy, sensitivity, specificity, F1 score and AUROC indicates that the performance model is good.

III. Results and Discussion

This section displays the result and discussion of this study. Table III presents the descriptive statistics for the independent variables, which shows a broad range of standard deviations from 0 to 48.507, showing different scales for each variable. To address this, the data was standardized using min-max normalization, as described by [16] in their study on prediction of air pollutants for air quality using deep learning methods in a metropolitan city. Furthermore, the histogram for the $PM2.5_{Dt1}$ category in Fig. 3 shows an imbalance in the distribution. Thus, the Synthetic Minority Over-sampling Technique (SMOTE) was used to ensure a balanced dataset, improving the dependability of future results.

The descriptive statistics after data pre-processing are shown in Table IV. Following min-max normalization, all mean and median values now fall within the range of 0 to 1, indicating that the data has been successfully scaled to a standard range. Additionally, the skewness values are now closer to 0, reflecting a more balanced distribution across the dataset. Moreover, Fig. 4 shows the distribution of $PM2.5_{Dt1}$ after the application of SMOTE up sampling to the dataset. It demonstrates that there is a consistent amount of sample sizes in both groups, with 1676 (50.6%) not polluted and 1639 (49.4%) are polluted.

TABLE III. Descriptive Statistics of before Data Pre-Processing

Variable	N	Mean	Median	Std. Dev.	Skewness
PM2.5	1825	23.321	21.187	11.712	4.142
PM10	1825	32.554	30.244	13.739	3.086
SO2	1825	0.001	0.001	0.000	1.330
NO2	1825	0.015	0.015	0.005	0.308
O3	1825	0.020	0.019	0.007	0.800
CO	1825	0.770	0.754	0.266	0.447
WD	1825	206.597	205.583	48.507	0.106
WS	1825	0.820	0.783	0.240	1.468
Humidity	1825	80.138	80.109	6.603	-0.151
Temperature	1825	27.552	27.573	1.247	-0.155

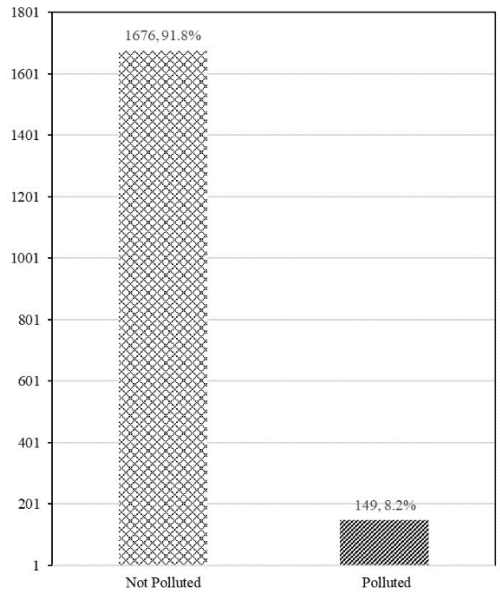


Fig. 3. $PM2.5_{Dt1}$ distribution of (Before SMOTE).

TABLE IV. DESCRIPTIVE STATISTICS OF AFTER DATA PRE-PROCESSING

Variable	N	Mean	Median	Std. Dev
PM2.5	3315	0.176	0.144	0.142
PM10	3315	0.219	0.190	0.146
SO2	3315	0.227	0.215	0.100
NO2	3315	0.426	0.423	0.165
O3	3315	0.333	0.315	0.130
CO	3315	0.395	0.388	0.165
WD	3315	0.522	0.510	0.183
WS	3315	0.214	0.201	0.100
Humidity	3315	0.520	0.517	0.146
Temperature	3315	0.559	0.565	0.118

Table V shows the rankings independent variables according to three feature selection methods which are Lasso, mRMR, and ReliefF on predicting $PM2.5_{D+1}$ in Shah Alam. Each features methods identifies top 8 independent variables to includes in the RBFNN model. The Lasso method ranks PM2.5 as the most critical feature to predict PM2.5 levels of the next day, a result that contrasts with the mRMR and ReliefF methods, where PM2.5 is not included among the top 8 features. However, the mRMR method select PM10 as the most significant feature while Lasso method rank PM10 as second most important features.

ReliefF, on the other hand, identify wind direction as the most important feature. This implies that variations in wind direction can result in significant variations in the dispersion or concentration of pollutants in urban environments. Moreover, [17] investigated the relationship between wind direction and air quality, specifically focusing on fine particulate matter (PM2.5) and its precursor gases. The investigation shows that the distribution and concentration of these contaminants are strongly influenced by wind direction. Moreover, this study shows ReliefF ranks both humidity and temperature as the least important features which is 7 and 8, in contrast to the Lasso and mRMR methods, which assign higher importance to these variables in predicting PM2.5 levels.

Furthermore, all three methods did not select SO2 as top 8 important variables to predict PM2.5 levels of the next day. According to a study by [18] on analysis of air pollution levels in a settlement area using passive sampling methods. Despite of SO2 presence, their results showed that SO2 had a small impact on the area under study's overall air quality index (AQI). This study supports the findings that SO2 may not have a significant impact on air quality projections, especially in areas where other pollutants predominate.

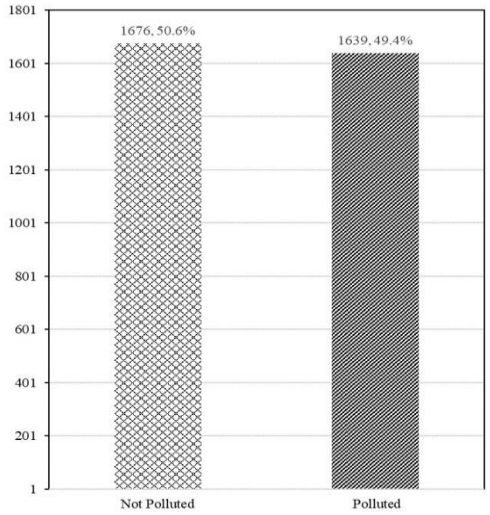


Fig. 4. $PM2.5_{Dt1}$ distribution of (After SMOTE).

TABLE V. FEATURE RANKING ACROSS LASSO, MRMR, AND RELIEFF METHODS

Variable	Lasso	mRMR	reliefF
PM2.5	1	-	5
PM10	2	1	6
SO2	-	-	-
NO2	4	6	2
O3	-	3	4
CO	6	7	3
WD	7	8	1
WS	8	2	-
Humidity	3	5	7
Temperature	5	4	8

Table VI shows the comparison of RBFNN model performance by using different feature selection methods to predict air quality of the next day based on PM2.5 level. According to Table VI, ReliefF outperformed Lasso and mRMR method with higher accuracy, specificity, precision, F1 Score and AUROC value which are 0.757, 0.719, 0.719, 0.758 and 0.759 respectively. This findings contrast with a study by

[9], who found that the Lasso method outperformed the ReliefF method in terms of performance metrics. However, it is important to note that [9] utilized a different classifier, specifically KNN, whereas this study employs RBFNN. Besides, a comparative study by [19], ReliefF was evaluated alongside Lasso and mRMR for survival prediction models. The findings showed that ReliefF was able to consistently find more relevant features than Lasso and mRMR, which had difficulty to maintain stability in their selections.

TABLE VI. COMPARISON MODEL PERFORMANCE

Model	Lasso	mRMR	ReliefF
Accuracy	0.735	0.753	**0.757**
Sensitivity	0.771	**0.818**	0.801
Specificity	0.702	0.703	**0.719**
Precision	0.702	0.703	**0.719**
F1 Score	0.735	0.756	**0.758**
AUROC	0.736	0.756	**0.759**

IV. CONCLUSION

In conclusion, this study's findings highlight the variety in feature selection approaches and their impact on the predictive effectiveness of air quality models in urban area which is Shah Alam, Malaysia. Among the three methods evaluated, ReliefF emerged as the most successful feature selection method for predicting next-day PM2.5 levels, outperforming both Lasso and mRMR in terms of accuracy, specificity, precision, F1 Score, and AUROC. This outcome aligns with some research that underscores ReliefF's ability to reliably detect relevant features, although other studies have favored the Lasso method. This study recommends that future research to explore the application of reliefF-RBFNN method to other type of areas such as sub-urban and rural area. This study also suggests that future studies should be conducted in other urban regions with varying climatic and pollutant features to confirm the generalisability of the findings and to develop more robust air quality prediction models that can be tailored to various situations. Moreover, it is recommended future researcher to explore on hybrid feature selection method such as ReliefF (filter) integrated with Lasso (embedded) feature selection method that might improve prediction performance across a variety of urban settings. However, the output of this study is not generalised to other country as the air quality patterns are differed across country.

ACKNOWLEDGMENT

Authors acknowledge acknowledge the Ministry of Higher Education (MOHE) for funding under the Fundamental Research Grant Scheme (FRGS) (FRGS/1/2023/STG06/UITM/02/8).

REFERENCES

[1] Y. A. Abdullah et al., "Urban Governance Approaches for Low Carbon Cities. The Case of Shah Alam Logal Government, Malaysia," Plan. MALAYSIA, vol. 20, no. 23 SE-Article, Nov. 2022, doi: 10.21837/pm.v20i23.1169.

[2] J. Angelin Jebamalar and A. Sasi Kumar, "PM2.5 prediction using machine learning hybrid model for smart health," Int. J. Eng. Adv. Technol., vol. 9, no. 1, pp. 6500–6504, 2019, doi: 10.35940/ijeat.A1187.109119.

[3] M. Hosni, A. Idri, and A. Abran, "On the value of filter feature selection techniques in homogeneous ensembles effort estimation," J. Softw. Evol. Process, vol. 33, no. 6, pp. 1–38, 2021, doi: 10.1002/smr.2343.

[4] A. Z. Ul-Saufie et al., "Improving Air Pollution Prediction Modelling Using Wrapper Feature Selection," Sustainability, vol. 14, no. 18. 2022, doi: 10.3390/su141811403.

[5] S. Liu et al., "Distinct regimes of O3 response to covid-19 lockdown in China," Atmosphere (Basel)., vol. 12, no. 2, pp. 1–10, 2021, doi: 10.3390/atmos12020184.

[6] H. Wu, T. Yang, H. Li, and Z. Zhou, "Air quality prediction model based on mRMR–RF feature selection and ISSA–LSTM," Sci. Rep., vol. 13, no. 1, pp. 1–15, 2023, doi: 10.1038/s41598-023-39838-4.

[7] E. S. Eşsiz, V. N. Kılıç, and M. Oturakçı, "Firefly-Based feature selection algorithm method for air pollution analysis for Zonguldak region in Turkey," Turkish J. Eng., vol. 7, no. 1, pp. 17–24, 2023, doi: 10.31127/tuje.1005514.

[8] J. Kalajdjieski et al., "Air Pollution Prediction with Multi-Modal Data and Deep Neural Networks," Remote Sensing, vol. 12, no. 24. 2020, doi: 10.3390/rs12244142.

[9] M. S. Hammad, V. F. Ghoneim, M. S. Mabrouk, and W. I. Al-atabany, "A hybrid deep learning approach for COVID-19 detection based on genomic image processing techniques," Sci. Rep., vol. 13, no. 1, pp. 1–22, 2023, doi: 10.1038/s41598-023-30941-0.

[10] N. Ibrahim, "Variable Selection Methods for Classification : Application To Metabolomics Data," University of Liverpool, 2020.

[11] S. S. Md Noh, N. Ibrahim, M. M. Mansor, N. A. Md Ghani, and M. Yusoff, "Hybrid embedded and filter feature selection methods in big-dimension mammary cancer and prostatic cancer data," IAES Int. J. Artif. Intell., vol. 13, no. 3, pp. 3101–3110, 2024, doi: 10.11591/ijai.v13.i3.pp3101-3110.

[12] A. Desiani et al., "The Comparison of ReliefF and C.45 for Feature Selection on Heart Disease Classification Using Backpropagation," IJCCS (Indonesian J. Comput. Cybern. Syst., vol. 17, no. 2, pp. 183–194, 2023, doi: 10.22146/ijccs.82948.

[13] B. Zhang, Y. Li, and Z. Chai, "A novel random multi-subspace based ReliefF for feature selection," Knowledge-Based Syst., vol. 252, p. 109400, 2022, doi: https://doi.org/10.1016/j.knosys.2022.109400.

[14] H. Adeli and M. Wu, "Regularization neural network for construction cost estimation," J. Constr. Eng. Manag., vol. 124, no. 1, pp. 18–24, 1998.

[15] S. S. Md Noh, N. Ibrahim, M. M. Mansor, and M. Yusoff, "Hybrid filtering methods for feature selection in high-dimensional cancer data," Int. J. Electr. Comput. Eng., vol. 13, no. 6, p. 6862, Dec. 2023, doi: 10.11591/ijece.v13i6.pp6862-6871.

[16] B. Das, Ö. O. Dursun, and S. Toraman, "Prediction of air pollutants for air quality using deep learning methods in a metropolitan city," Urban Clim., vol. 46, p. 101291, 2022, doi: https://doi.org/10.1016/j.uclim.2022.101291.

[17] H. Karimian et al., "Spatio-temporal variation of wind influence on distribution of fine particulate matter and its precursor gases," Atmos. Pollut. Res., vol. 10, no. 1, pp. 53–64, 2019, doi: https://doi.org/10.1016/j.apr.2018.06.005.

[18] N. Djamal, A. Suryanto, A. Artiningsih, N. Nasrullah, R. D. T. Manningtyas, and Y. Velina, "Analysis of Air Pollution Level In Settlement Area Using Passive Sampler Method," Int. J. Hydrol. Environ. Sustain., vol. 1, no. 2, pp. 97–107, 2022, doi: 10.58524/ijhes.v1i2.77.

[19] J. Hu et al., "Development of survival predictors for high-grade serous ovarian cancer based on stable radiomic features from computed tomography images," iScience, vol. 25, no. 7, p. 104628, 2022, doi: https://doi.org/10.1016/j.isci.2022.104628.

Optimizing CatBoost Model: AI-Based Analysis on Rail Transit Figma Platform Practice

Ruobing Li[1,*], Hong Qian[2]
College of Innovation and Entrepreneurship, Xi'an Traffic Engineering Institute Xi'an 710300, Shaanxi, China[1, 2]

***Abstract*—The research introduces a novel approach that utilizes the Frilled Lizard Optimization (FLO) algorithm to enhance the hyperparameters of the CatBoost model. First, the Figma platform is analyzed in terms of its innovative design applications in rail transit. Then, the FLO algorithm is applied to optimize the CatBoost model, improving its accuracy in detecting foreign objects on rail tracks. Experiments were conducted using a dataset of 6,000 images from rail transit scenarios, divided into seven categories such as left-turning track, straight track, train, pedestrians, and others. The result showed that the FLO-CatBoost model demonstrated superior performance in accuracy, achieving a Root Mean Square Error (RMSE) of 0.274, significantly outperforming other algorithms like TSA, MPA, and RSA. Furthermore, FLO-CatBoost reduced the Mean Absolute Percentage Error (MAPE) and showed better efficiency in evaluation time. Finally, the FLO-CatBoost model significantly enhances the design and evaluation processes for intelligent rail transit systems on the Figma platform, providing higher accuracy and efficiency in detecting foreign objects and improving system design performance.**

Keywords*—Rail transport; Figma platform innovation design; intelligent analysis and evaluation algorithm; umbrella lizard optimisation algorithm; CatBoost

I. Introduction

Rapidly developing artificial intelligence technology as well as Internet technology has driven the development of software innovation, which has received attention from scholars and experts at home and abroad [1]. Figma software, as an online collaborative and instantaneous design software, can assist designers in creating, collaborating and iterating design projects [2]. Due to the advantages of real-time, collaboration, compatibility, synchronisation, and cloud storage, Figma design platform has an increasingly wide range of application areas, and receives more and more attention and research from experts in the field. In the field of rail transit, with the rapid development of rail transit, the train speed is getting faster and faster, and the way of judging the foreign objects in front of the car by human beings is no longer adapted to the development of the current era [3]. The study of accurate autonomous detection methods of foreign objects in rail transit not only reduces the rate of rail transit accidents, but also strengthens the detection and processing of emergency events in rail transit [4]. In order to generalise the application of autonomous detection system for foreign objects in rail transit and improve the design efficiency of autonomous detection system for foreign objects in rail transit, the combination of Figma design platform has become the development trend and method of intelligent system design. The research on innovative design of rail transit system combined with Figma design platform includes the research on design principle analysis, design method testing and evaluation, etc., in which the design method testing and evaluation includes the research on design effect evaluation index extraction, evaluation system construction, design effect evaluation model construction combined with Figma design platform. Ye et al. [5] analysed the Figma design method for rail transit, and verified the testing accuracy and efficiency of the proposed method through the image dataset. Zhao [6] proposed an innovative design scheme and idea by combining with the Figma design platform. Maricar et al. [7] took the financial service as the background, and used the Figma to innovatively design its management system and made a quantitative analysis of the system. Cheng and Cai [8] proposed a deep learning algorithm based design platform evaluation and analysis method, and used a public dataset to verify the method to improve the design effect. Liu et al. [9] analysed the efficiency of Figma development and design, and gave a qualitative comparative analysis. With the complexity of intelligent systems, the simple Figma design platform effect analysis and evaluation method can no longer meet the assessment of the predictive accuracy effect, and reduces the efficiency of feedback optimisation. The proposal and development of integrated learning technology and intelligent optimisation algorithms accelerate the efficiency and analysis accuracy of Figma design platform application [10].

In order to improve the analysis and evaluation accuracy of the design effect of Figma platform and enhance the design efficiency, this paper proposes an intelligent analysis and evaluation method of Figma platform based on intelligent optimisation algorithm-CatBoost. By analysing the innovative design problems of Figma platform in rail transit, it introduces the related key on seems, and around the Figma platform intelligent analysis and evaluation problems, it combines the umbrella lizard optimization algorithm with CatBoost to construct Figma platform intelligent analysis and evaluation model. The data images of foreign objects in rail transit are brought into the model system for analysis and evaluation, and the results are compared and analysed with those of multiple algorithms to verify the effectiveness of the model in improving the precision and efficiency, as well as the accuracy of the evaluation.

II. Figma Platform for Rail Transport

A. Figma Platform

Figma is a popular online collaborative design tool [11], which supports real-time collaboration and browser-based design, and is widely used for UI/UX design. Figma provides a comprehensive design platform that includes design, prototyping, collaboration, and version control features, as

*Corresponding Author.

shown in Fig. 1. It aims to make design work more powerful, convenient, and approachable for individual designers, teams, and enterprises.

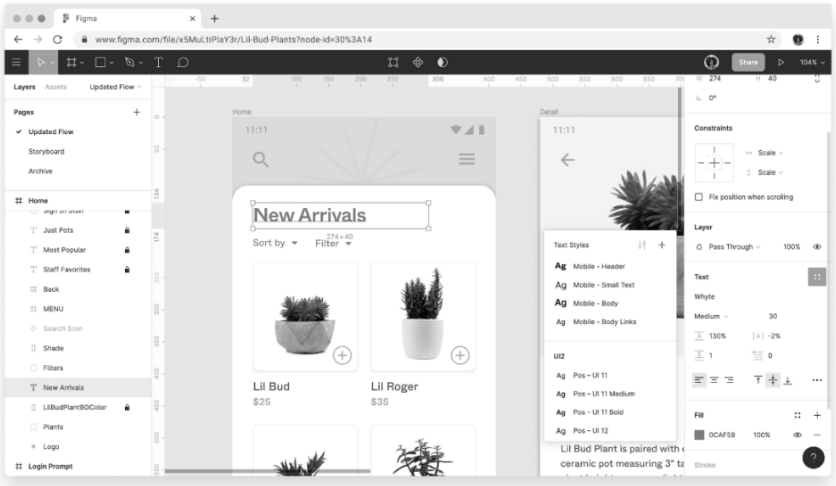


Fig. 1. Figma platform.

1) Figma characteristics: According to the analysis of Figma application, Fig. 2 presents that Figma has the following features and functions [12]:

- Figma allows multiple users to work on the same design file at the same time, while viewing and editing each other's content in real time;
- Many files are stored in Figma Cloud, users can access and edit files on any device at any time, without worrying about file synchronisation;
- Figma has a built-in prototype tool that allows users to create interactive prototypes directly in the design for easy testing and demonstration;
- Figma can record the history function, users can view and restore the past design state;
- In Figma, designers can create reusable components and styles for easy consistency throughout the design;
- Figma supports third-party plug-in development to expand functionality;
- Figma can be used on multiple operating systems and browsers.

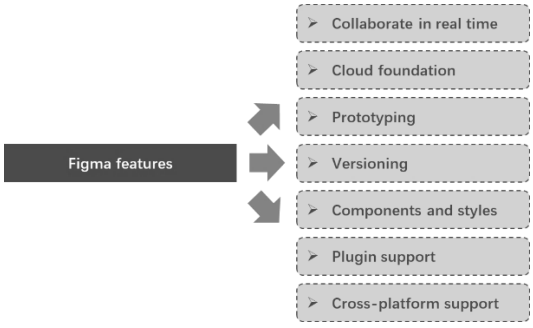


Fig. 2. Figma characteristics.

2) Figma application: Figma has become one of the standard tools in the design world, surpassing competitors such as Sketch, Adobe XD, etc., and has more than 4 million active users in more than 100 countries around the world. Figma's user base includes companies in a wide range of industries such as IT, financial services, advertising, retail, professional training, etc. (Fig. 3), such as Microsoft, Twitter, Dropbox, etc. [13].

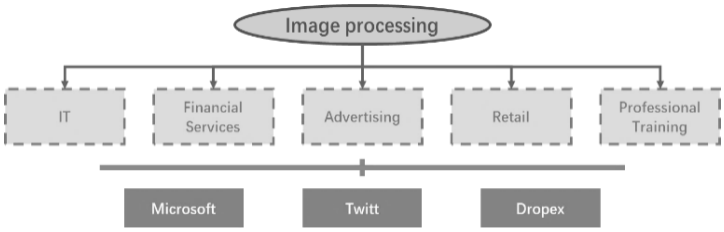


Fig. 3. Current status of Figma applications.

3) Figma design: Figma's design interfaces typically include the following four core components (Fig. 4):

- Canvas (Canvas). This area can hold various design elements such as shapes, text, images, etc.
- Sidebar. This section contains toolbars, layer lists and property panels. Designers can select and modify the properties of design elements through the sidebar.
- Top Menu Bar (Top Menu Bar). This section provides shortcuts to functions such as file management, editing, and view control.
- Component Library (Component Library). This section allows designers to create reusable design elements such as buttons, icons, etc. to be shared and maintained throughout the project [14].

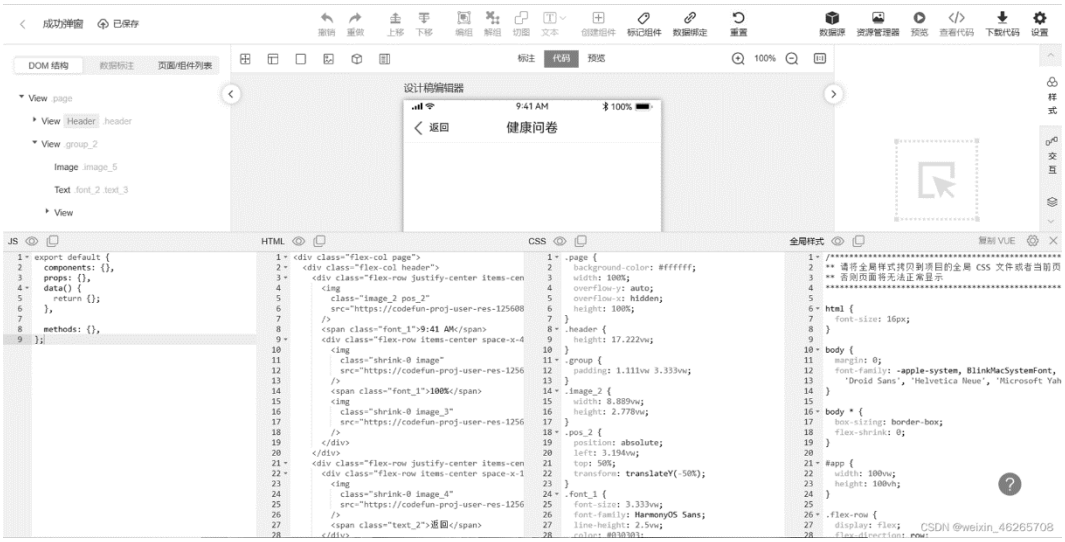


Fig. 4. Figma design interface.

B. Innovative Design Solutions

In order to improve the efficiency of intelligent rail transit autonomous detection system design, this paper proposes an intelligent rail transit autonomous detection system design scheme based on Figma platform, and at the same time, for the effectiveness of the scheme, an efficient machine learning algorithm is used to analyse and evaluate the performance of the intelligent rail transit autonomous detection system design method based on Figma platform.

1) Figma-based platform autonomous detection system: Intelligent rail transit autonomous detection system includes three parts: image acquisition layer, intelligent processing layer, and decision control layer. The system collects images through the starlight camera and inputs them to the image information processing system; the image information processing system analyses the collected data images in real time and identifies the track foreign objects and retrograde with high precision, and then gives correct decision-making information [15], the specific composition diagram is shown in Fig. 5.

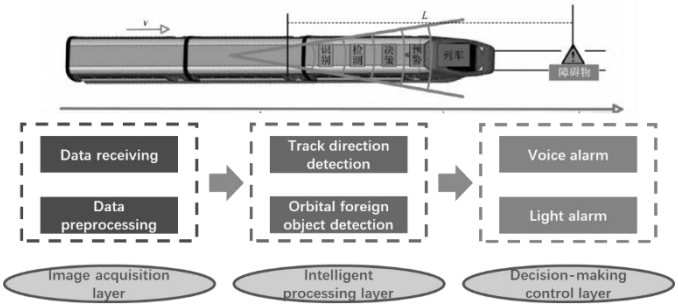


Fig. 5. Autonomous detection system for intelligent rail transit.

Combined with Figma platform, the design scheme of intelligent rail transit autonomous detection system based on Figma platform is proposed, as shown in Fig. 6. The design process of this design scheme is as follows: 1) In-depth study of the characteristics of the rail transit industry, user groups, existing workflows, and challenges, to determine the design objectives and core functional requirements; 2) Based on the results of the requirements analysis, conceptual design and preliminary sketches; 3) Interaction design using Figma, to create low-fidelity and high-fidelity prototypes of autonomous detection for rail transit; 4) Design After the prototype is completed, conduct user testing and collect user feedback; 5) conduct visual design on the basis of interaction design to ensure that the design style is in line with the professional image of the rail transport industry; 6) transform the design into an actual application, while ensuring the feasibility of the design and performance optimization; 7) conduct comprehensive testing after the completion of the development, and then carry out on-line deployment; 8) after the launch of the platform, continuously monitor the platform After going live, continuously monitor the platform's operation status and carry out the necessary maintenance and functional iteration and upgrade according to the feedback.

2) Analysis and evaluation programme: According to the design scheme combining Figma platform, this paper analyses and evaluates the Figma design effect of the rail transit detection system from six aspects [16] (Fig. 7), including the target and core function design A, sketching B, prototyping C, Figma platform interactivity D, operation of the rail transit detection system E, and analysis of the detection results F. By extracting the Figma design effect analysis assessment indicators, construct the assessment indicator set, use data preprocessing methods based on missing value deletion, noise data deletion, normalization, feature selection and other data preprocessing methods to process the assessment indicator dataset, annotate and divide the dataset, and combine with optimized CatBoost technology to construct the mapping relationship between the Figma design effect indicator values and the analysis and evaluation scores, and analyse and compare their performance, the specific overall idea is shown in Fig. 8.

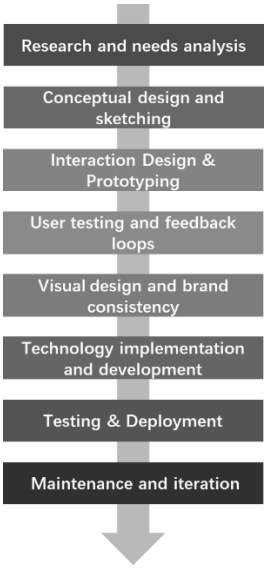


Fig. 6. Autonomous detection system for intelligent rail transit based on Figma platform.

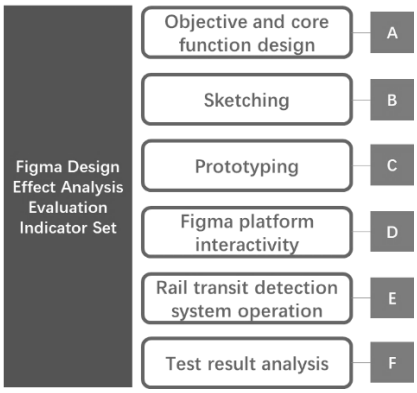


Fig. 7. The evaluation aspects of Figma's design effects analysis.

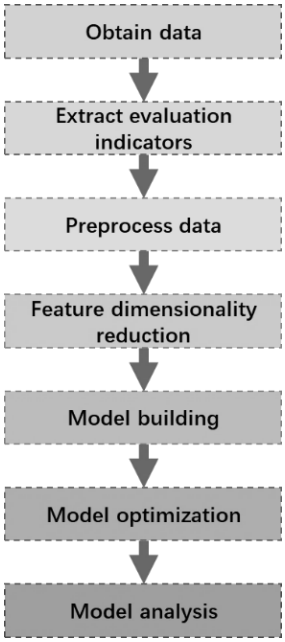


Fig. 8. Ideas for evaluating Figma's design effect analysis.

According to the design idea in Fig. 8, the analysis and evaluation scheme of rail transit detection system combined with Figma design platform includes key technologies such as autonomous detection design of rail transit on Figma platform, data acquisition, extraction of indicator set for analysis and evaluation of Figma design effect, data preprocessing, data annotation and division, and construction and optimisation of model for analysis and evaluation of Figma design effect, etc., and the specific key technologies are shown in Fig. 9. The specific key technologies are shown in Fig. 9.

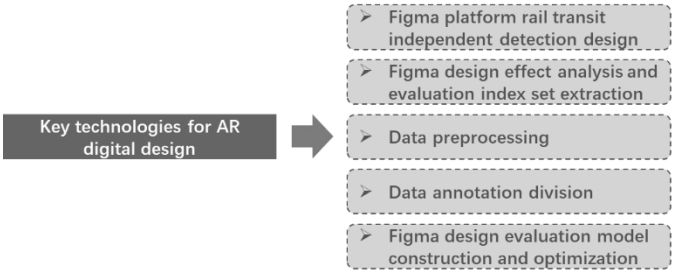


Fig. 9. Figma design effectiveness analysis and evaluation key technology.

III. Analysis and Evaluation Algorithms

A. Analysis of Intelligent Analytics Assessment Issues

According to the analysis of the key technology of Figma design effect analysis and assessment, Figma design intelligent analysis and assessment research as the key technology of the rail transit detection system analysis and assessment system combined with Figma design platform, by using the improved and efficient intelligent machine learning algorithm to fit the mapping relationship between the effect analysis assessment indicator values and assessment scores, as shown in Fig. 10. In this paper, CatBoost is used to construct the mapping relationship between assessment index values and assessment scores, and the umbrella lizard optimisation algorithm is used to optimise the hyper-parameters of CatBoost technology to improve the accuracy of analysis and assessment of the Figma design effect and enhance the effect of Figma design.

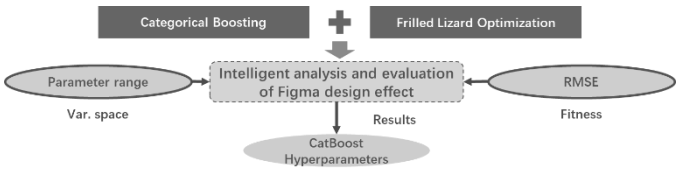


Fig. 10. Figma design analysis and evaluation method based on improved and efficient machine learning algorithm.

B. CatBoost Technology

CatBoost (Categorical Boosting) [17] is a gradient boosting algorithm that consists of two techniques, Categorical and Boosting, which can be used to handle classification and regression problems. It is one of the algorithms belonging to the Gradient Boosting Decision Trees (GBDT) family of algorithms and is well known for its ability to handle categorical features. CatBoost is able to automatically convert categorical features to numerical features, reducing the need for manual feature engineering, and is able to handle high cardinality categorical features without inducing dimensionality disaster, the structure of which is shown in Fig. 11. In addition, CatBoost effectively

reduces the bias of gradient estimation and improves the accuracy and generalisation ability of the model by using symmetric tree and sort boosting methods.

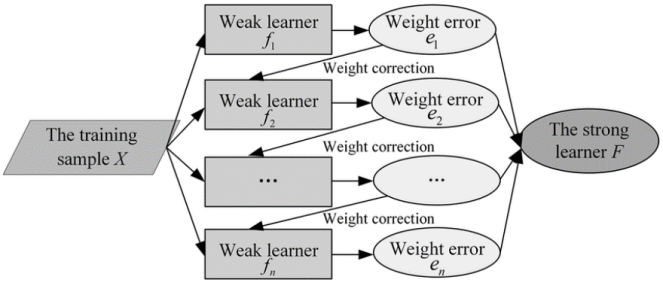


Fig. 11. CatBoost structure.

In CatBoost decision tree, CatBoost uses the Greedy TS method to process the category features [18], and equation changes are made to avoid conditional bias as follows:

$$x_k^i = \frac{\sum_{x_j \in D_k} \left\{ x_k^i = x_j^i \right\} \times y_i + aP}{\sum_{x_j \in D_k} \left\{ x_k^i = x_j^i \right\} + a} \tag{1}$$

Among them, P is the a priori value, which is mainly used to smooth the noise, a is the weight coefficient, and $\left\{ x_k^i = x_j^i \right\}$ is mainly used to judge whether the current sample k and sample j are in the same category, and the same is 1, and vice versa is 0.

Compared with other algorithms in the Boosting cluster class, the CatBoost algorithm is able to handle discrete feature data well and is suitable for problems with multiple input features. The CatBoost algorithm has the following features [19]: 1) automatic processing of category-based features; 2) reduction of gradient bias; 3) handling of missing values; 4) good robustness; 5) ease of use; 6) support for GPU acceleration; 7) Built-in cross-validation, as shown in Fig. 12.

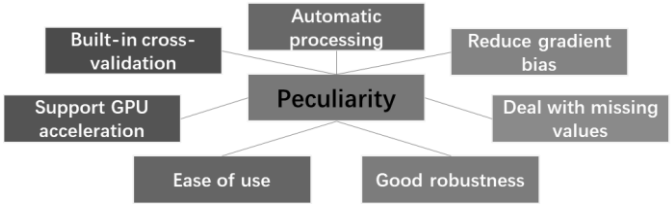


Fig. 12. CatBoost characteristics.

CatBoost is widely used for a variety of machine learning tasks due to its high performance and ease of use, including but not limited to financial risk assessment, recommender systems, bioinformatics, and natural language processing. Its ability to handle large-scale datasets and to deal with complex nonlinear relationships has made it the algorithm of choice in many real-world application scenarios [20-21].

C. Improved CatBoost Evaluation Model Based on Umbrella Lizard Optimisation Algorithm

With the increase of input data dimension, CatBoost algorithm training optimisation will fall into local optimum [21]. In order to improve the regression accuracy of CatBoost algorithm, this paper chooses the umbrella lizard optimisation algorithm to optimise the hyperparameters of CatBoost algorithm, so as to make the Figma platform innovation design analysis and evaluation model error to reach the minimum.

1) Umbrella lizard optimisation algorithm: Frilled Lizard Optimization (FLO) [22], as a biological meta-heuristic based algorithm, simulates the unique hunting behaviour of umbrella lizards in their natural habitat. The algorithm has a unique algorithmic structure and a novel iterative approach with strong adaptive optimisation capabilities.

The main diet of the wrinkled lizard is insects and other invertebrates, although it rarely eats vertebrates as well. Primary prey include centipedes, ants, termites, and moth larvae. The frilled lizard is a sit-and-wait predator, looking for potential prey. Upon seeing prey, the frilled lizard runs quickly on two legs and attacks the prey, catching it and eating it. After feeding, the frilled lizard retreats to a tree.

a) Initialisation: Like other optimisation algorithms, the FLO algorithm uses random initialisation for the population of wrinkled lizards:

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N \times m} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,d} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ x_{i,1} & \cdots & x_{i,d} & \cdots & x_{i,m} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,d} & \cdots & x_{N,m} \end{bmatrix}_{N \times m} \tag{2}$$

$$x_{i,d} = lb_d + r \cdot \left(ub_d - lb_d \right) \tag{3}$$

where X denotes the population of frilled lizards, X_i denotes the ith frilled lizard, $x_{i,d}$ is the d-dimensional position of the ith frilled lizard, and lb_d and ub_d denote the lower and upper boundaries of the d-dimension, respectively.

b) Hunting strategy (exploratory phase): One of the most typical natural behaviours of frilled lizards is hunting strategy animals. The frilled lizard is a sit-and-wait predator that attacks its prey when it sees it. The first stage of the FLO algorithm uses a hunting strategy, which is modelled as follows:

$$x_{i,d}^{P_1} = x_{i,d} + r \cdot \left(SP_{i,d} - I \cdot x_{i,d} \right) \tag{4}$$

$$X_i = \begin{cases} X_i^{P_1} & F_i^{P_1} < F_i \\ X_i & else \end{cases} \tag{5}$$

Where, $x_{i,d}^{P_1}$ denotes the location information of the ith frilled lizard in the dth dimension in the first stage of the FLO algorithm, r is a random number between 0 and 1, $SP_{i,d}$ denotes the location information of the ith frilled lizard in the

dth dimension for selecting the prey, I is a randomly selected number of the 1 and 2 number set, $F_i^{P_1}$ denotes the fitness value of $X_i^{P_1}$, and F_i denotes the fitness value of X_i .

c) Tree-climbing strategy (development phase): After feeding, the frilled lizard retreats to the top of a tree near its location. By modelling the movement of the frilled lizard to the top of the tree, the decision space position of the population individuals is made to change slightly, thus improving the algorithm's ability to exploit local search. In the second stage of FLO, the positions of population individuals in the solution space are updated according to the post-feeding tree-climbing strategy. The specific model is as follows:

$$x_{i,d}^{P_2} = x_{i,d} + (1-2r)\cdot\left(\frac{ub_d - lb_d}{t}\right) \tag{6}$$

$$X_i = \begin{cases} X_i^{P_2} & F_i^{P_2} < F_i \\ X_i & else \end{cases} \tag{7}$$

where, $X_i^{P_2}$ denotes the location information of the ith frilled lizard in the second stage of the FLO algorithm, $x_{i,d}^{P_2}$ denotes the information of the ith frilled lizard in the dth dimension in the second stage, t is the current number of iterations, and $F_i^{P_2}$ denotes the fitness value of $X_i^{P_2}$.

Combining the hunting strategy and tree-climbing strategy of the FLO algorithm, the step-by-step flow of the FLO algorithm (Fig. 13) is as follows:(a)

2) FLO-CatBoost: In order to enhance the design effect of Figma rail transit autonomous detection and improve the accuracy of analysis and evaluation performance, this paper takes CatBoost hyperparameters (number of decision trees, learning rate, maximum depth of the tree and L2 regularisation term) as the optimisation variables, FLO algorithm hunting strategy and tree-climbing strategy as the optimisation method, and RMSE error value as the fitness value function to optimise the CatBoost model. The specific process steps are shown in Fig. 14.

3) Application of FLO-CatBoost in analysing and evaluating the design effect of autonomous detection in Figma platform rail transit: In order to construct the Figma platform rail transit autonomous detection design effect analysis and evaluation model, this paper applies FLO-CatBoost to the Figma platform innovation design intelligent analysis and evaluation problem, and its specific application process is shown in Fig. 15.The application of FLO-CatBoost in Figma platform rail transit autonomous detection design effect analysis and evaluation mainly includes three parts The application of FLO-CatBoost in Figma platform rail transit autonomous testing and design effect analysis and evaluation mainly includes three parts, i.e. Figma platform rail transit autonomous testing and design effect analysis and evaluation index construction part, data pre-processing part, and Figma platform rail transit autonomous testing and design effect analysis and evaluation model construction and optimisation part. In the first part, the assessment indicators are extracted and the assessment indicator system is constructed by analysing the Figma platform innovative design intelligent analysis assessment problem; in the second part, the indicators are feature extracted by abnormal data preprocessing and normalizing the data set; in the third part, the mapping relationship between the values of the effect analysis assessment indicators and the assessment scores is constructed by using the CatBoost technology and the FLO algorithm is used to Optimisation of CatBoost model hyperparameters.

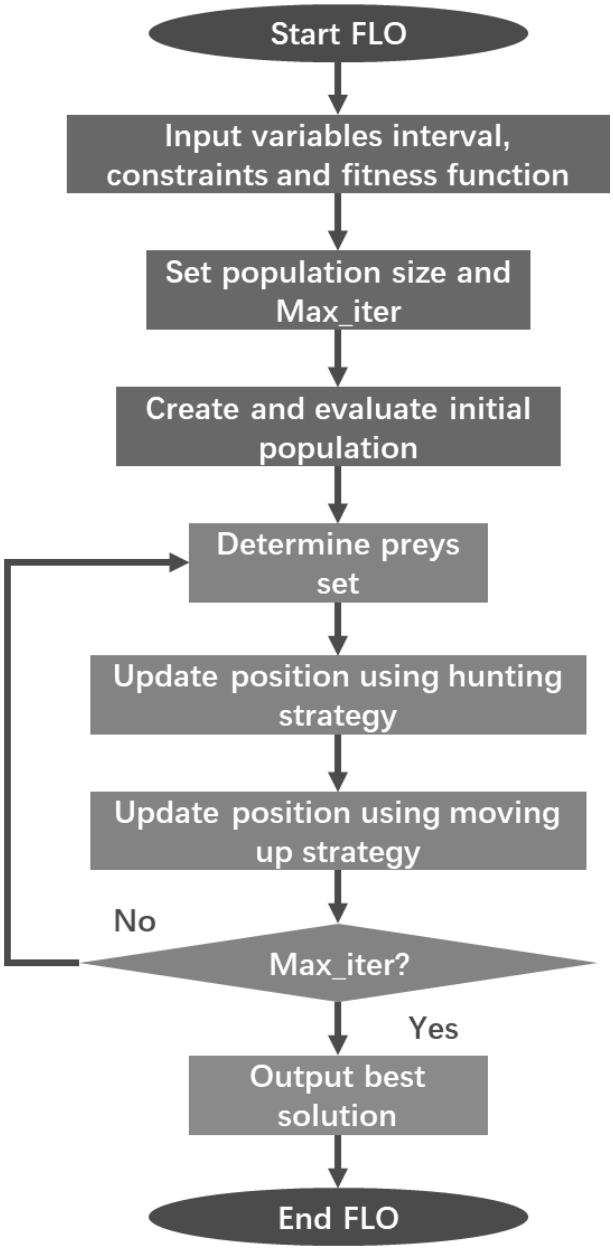


Fig. 13. Flowchart of FLO algorithm.

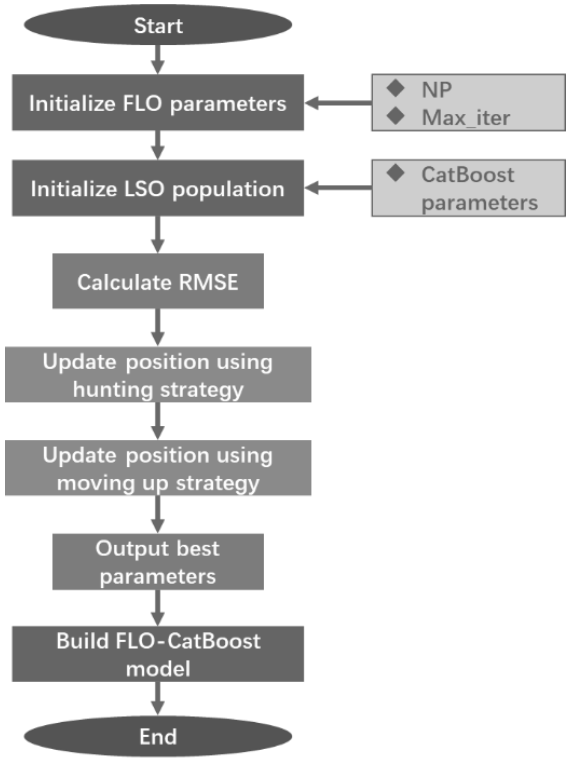


Fig. 14. Flowchart of FLO-CatBoost algorithm.

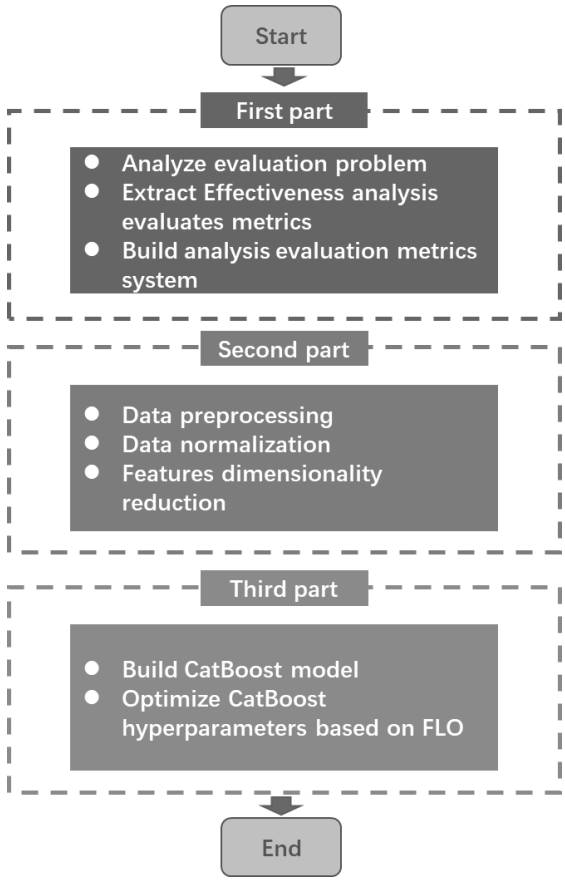


Fig. 15. Application of intelligent analysis and evaluation model for Figma platform combined with FLO-CatBoost.

IV. Simulation Results

A. Experimental Set-up

In this paper, FLO-CatBoost algorithm is simulated and tested in Python 3.7 environment and compared with TSA, MPA, RSA, WSO algorithms. The common parameters of TSA, MPA, RSA, WSO, FLO algorithms include the number of populations, the maximum number of iterations, and their values are set to 100, 1000, respectively. The values of TSA, MPA, RSA , WSO, FLO algorithms other algorithm settings are shown in Table I.

TABLE I. Contrast Algorithm Parameter Settings

No.	Algorithms	Parameter settings
1	CatBoost	Iterations=16, Learning_rate=0.1,depth=5,L2_leaf_reg=1
2	TSA-CatBoost	P_{min}=1, P_{max}=4, c1\c2\c3=rand
3	MPA-CatBoost	P=0.5, R=rand, FADs=0.2, U=0 or 1
4	RSA-CatBoost	Alpha=0.1, Beta=0.01, ES=[-2.2]
5	WSO-CatBoost	F_{min}=0.07, F_{max}=0.75,
6	FLO-CatBoost	No Parameter

In order to analyse the effect of the autonomous detection system of foreign objects in rail transit, this paper collects 6000 images, which are divided into seven categories of foreign object targets, such as left-turning track, right-turning track, straight track, train, pedestrians, wrench and safety, etc., and the sample images are shown in Fig. 16 and the distribution of the number of samples of foreign object targets is shown in Fig. 17.

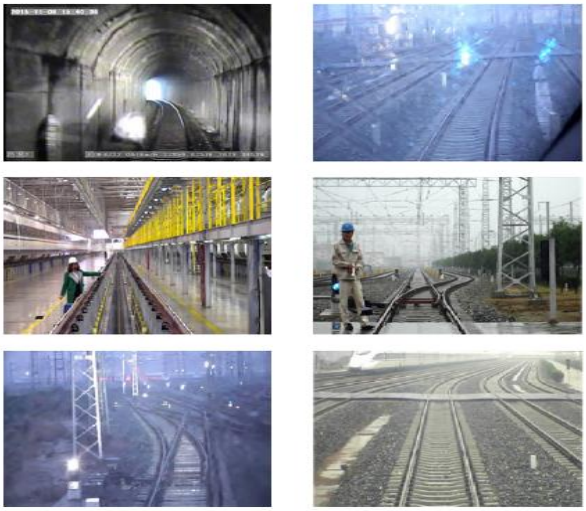


Fig. 16. Sample images.

Testing Figma Platform Intelligent Analytics Evaluation Model Performance Using Figma Platform evaluation metrics data, 1,890 sample data were collected, 1,250 for the training set, 430 for the testing set, and 210 for the validation set.

In order to avoid unexpected results of the experiment, the test optimisation process was repeated independently 10 times and the RMSE, MAPE, and evaluation time means and standard deviations were counted.

B. Algorithm Performance Analysis

1) Analysis of the effectiveness of autonomous detection of foreign objects in railway transportation combined with figma platform: Fig.18 presents the confusion matrix for autonomous detection of foreign objects in rail transport combined with Figma platform. From Fig. 18, it can be seen that the correctness of the detection of seven types of foreign object targets such as left-turn track, right-turn track, straight track, train, pedestrian, spanner and safety is more than 90%, which indicates that the detection results are good.

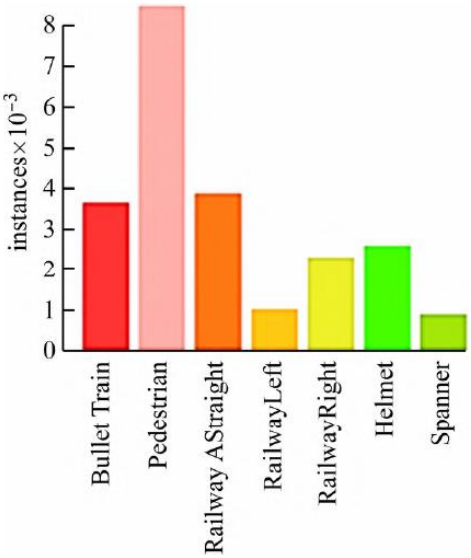


Fig. 17. Distribution of sample data.

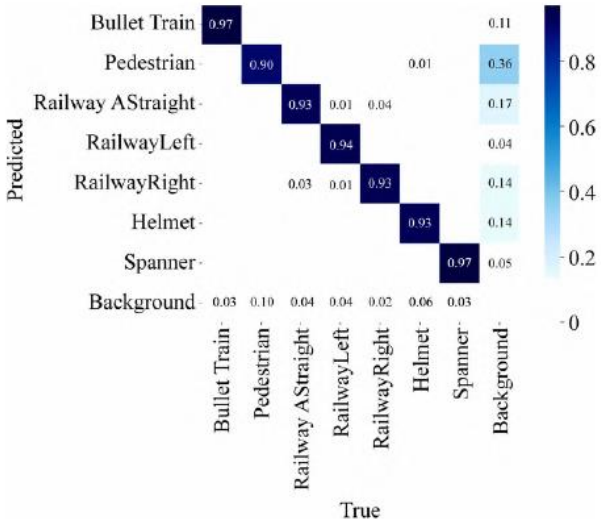


Fig. 18. Confusion matrix for autonomous detection of foreign objects in rail transport combined with Figma platform.

The Precision-Recall curves for autonomous detection of foreign objects in rail transport combined with Figma platform are given in Fig. 19 As shown in Fig. 19 the accuracy-recall curves for the seven categories of foreign object targets, such as left-turn track, right-turn track, straight track, train, pedestrian, spanner and safety, all indicate good detection results.

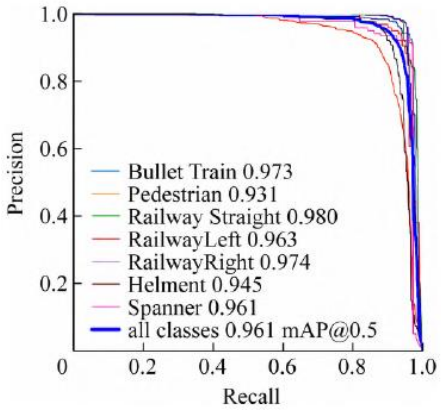


Fig. 19. Precision-Recall curve for autonomous detection of foreign objects in railway combined with Figma platform.

2) Analysis of the results of the assessment: Table II counts the RMSE, MAPE, evaluation time mean and standard deviation of different algorithms for 10 experiments. From Table II it can be seen that in terms of RMSE and MAPE, the analysis and evaluation accuracy of Figma rail transit design platform based on FLO-CatBoost model is better than other algorithms, and the evaluation time is more than that of CatBoost, and is better than that of TSA-CatBoost, MPA-CatBoost, RSA-CatBoost, WSO- CatBoost.This is to show that the optimisation of CatBoost hyperparameters by FLO algorithm makes Figma rail transit design platform analysis and evaluation more efficient.

TABLE II. MEAN AND STANDARD DEVIATION OF RMSE, MAPE, AND EVALUATION TIME FOR DIFFERENT ALGORITHMS

No.	Algorithms	RMSE		MAPE		Evaluation time/s	
		Mean	Std	Mean	Std	Mean	Std
1	CatBoost	1.4523	0.6554	0.5988	0.2673	0.0655	0.0098
2	TSA-CatBoost	0.7667	0.3890	0.4722	0.2178	0.1367	0.0178
3	MPA-CatBoost	0.8904	0.4163	0.5147	0.2893	0.1190	0.0122
4	RSA-CatBoost	0.8389	0.4376	0.5098	0.2865	0.1904	0.0245
5	WSO-CatBoost	0.4731	0.2109	0.2587	0.0988	0.0983	0.0100
6	FLO-CatBoost	0.2744	0.0971	0.1218	0.0674	0.0910	0.0066

Table III gives the results of different optimisation algorithms for optimising CatBoost hyperparameters. As can be seen in Table III the FLO algorithm optimises the CatBoost

hyperparameters with the following final results: the number of decision trees is 15, the learning rate is 0.015, the maximum depth of the tree is 6, and the L2 regularisation is 1.

TABLE III. RESULTS OF DIFFERENT OPTIMISATION ALGORITHMS FOR OPTIMISING CATBOOST HYPERPARAMETERS

Parameters	TSA-CatBoost	MPA-CatBoost	RSA-CatBoost	WSO-CatBoost	FLO-CatBoost
Iterations	17	16	16	17	15
Learning_rate	0.5	0.09	0.07	0.43	0.015
Depth	5	5	6	7	6
L2_leaf_reg	1	1	1	1	1

V. CONCLUSION AND OUTLOOK

Combining Figma platform and CatBoost technology, FLO-CatBoost model is applied to the problem of analysing and evaluating the effect of autonomous detection and design in rail transit. Aiming at problems such as low efficiency of effect analysis and assessment methods, this paper proposes an intelligent analysis and assessment method for Figma platform based on FLO-CatBoost model combined with FLO-CatBoost. The method analyses the innovative design scheme of Figma platform in rail transit, focuses on the Figma platform intelligent analysis and assessment problems, combines FLO and CatBoost algorithms, and constructs the intelligent analysis and assessment model of Figma platform based on FLO-CatBoost. The disclosed data image test shows that the constructed intelligent analysis and evaluation model of Figma platform based on FLO-CatBoost has higher evaluation accuracy than CatBoost, TSA-CatBoost, MPA-CatBoost, RSA-CatBoost, and WSO-CatBoost models, and obtains FLO algorithm optimised CatBoost optimal hyperparameters, i.e., the number of decision trees is 15, the learning rate is 0.015, the maximum depth of the tree is 6, and the L2 regularisation is 1.

However, there are limitations to this study. Firstly, the dataset used may not comprehensively represent all real-world rail transit conditions, which could impact the model's generalizability. Secondly, the proposed method focuses on static image data, limiting its application in dynamic and more complex scenarios. Future research could explore (1) the inclusion of more diverse datasets that capture a broader range of real-time rail transit conditions, (2) the extension of the model to handle video data for more dynamic analysis, and (3) integration with other machine learning algorithms to further enhance performance and robustness in real-world applications.

REFERENCES

[1] Kay S., Oyiliagu C., Ali A.388 Prototyping a mobile phone application for Chimeric Antigen Receptor (CAR) T-cell therapy patient monitoring and data collection post-discharge[J].Journal of Clinical and Translational Science, 2024, 8(s1):115-116.

[2] Odedairo B O.Assessing the Influence of Various Work Breakdown Structures on Project Completion Time[J].engineering technology & applied science research, 2024, 14(2):13773-13779.

[3] Safar L .How Product-Led Localisation Helps 10X Product Adoption Internationally[J].Multilingual, 2022.

[4] Perez-Siguas R , Matta-Solis H , Matta-Solis E .Mobile application Design to help People Suffering from Alzheimer's[J]. Engineering Trends and Technology, 2022, 70(5):258-265.

[5] Ye T., Zheng Z. K, Hao T. C., Xu X. Yu, Li D. S. Design of practical teaching platform for innovation training of university students in rail intelligent transport[J]. Laboratory Research and Exploration,2024,43(01):152-158+198.

[6] Zhao N. Design and implementation of a ticketing system based on Spring Boot[J]. Information Systems Engineering, 2023(7):32-35.

[7] Maricar M A., Pramana D., Edwar E.Pengujian Prototype Pemesanan Creative Gift Menggunakan HEART Framework[J].JURNAL MEDIA INFORMATIKA BUDIDARMA,. 2022.

[8] Cheng F., Cai H .Deep learning-based object detection between train and rail transit platform door[J].International Journal of Grid and Utility Computing, 2022, 13(5):526-537.

[9] Liu J., Canca D., Lv H.Spatiotemporal synchronous coupling algorithm for urban rail transit timetables design under dynamic passenger demand[J]. Applied Mathematical Modelling, 2023.

[10] Shuling H., Yunong G., Peijie C .How to use POE to intervene in the design and renovation of rail transit public buildings[J].Academic Journal of Architecture and Geotechnical Engineering, 2023.

[11] Fei Y. U.Design Strategy of Underground Space of Urban Rail Transit Complex Based on Integration Concept[J]. Landscape Research:English Edition, 2023, 15(1):31-35.

[12] Chen Y., Wang S., Liao H. Y. Design scheme of integrated ticketing management platform system for rail transit[J]. Automation and Instrumentation, 2023, 38(5):105-109.

[13] Chang M., Nan N., Qu D., X., Zhang L.Architecture design and re1iabi1ity eva1uation of a nove1 software defined train contro1 system[J].Urban Rail Transit, 2022 :1-11.

[14] Yan S .Optimal Design of a Short Primary Double-Sided Linear Induction Motor for Urban Rail Transit[J].World Electric Vehicle Journal, 2022, 13.

[15] Pu W. S., Ji T. T. ,Xie H. M. Research on tool selection based on mobile UI design[J]. Wireless Internet Technology, 2023, 20(15):104-107.

[16] Zhang L., Chen Y., Yan Z.Predicting the short-term electricity demand based on the weather variables using a hybrid CatBoost-PPSO model[J]. of Building Engineering, 2023.

[17] Martin R , Watanabe R , Hashimoto Y .Evidence-Based Prediction of Cellular Toxicity for Amorphous Silica Nanoparticles[J].ACS nano, 2023, 17(11):9987-9999.

[18] Ana T., Andrija T., Eljka Z.Machine learning to optimise cerebrospinal fluid dilution for analysis of MRZH reaction[J]. laboratory medicine: CCLM, 2024, 62(3):436-441.

[19] Bian J., Wang J., Yece Q .A novel study on power consumption of an HVAC system using CatBoost and AdaBoost algorithms combined with the metaheuristic algorithms[J].Energy, 2024, 302.

[20] Han C , Gong M , Sun J., Zhao Y., Jing L., Dong C., Zhao Z. .Heat Load Prediction for District Heating Systems with Temporal Convolutional Network and CatBoost[J].Thermal engineering, 2023, 70(9):719-726.

[21] Ibraheem A F, Osama A, Saleh A, Gulnara B, Saikat G, Irina L, Om P M, Frank W, Mohammad D. Frilled Lizard Optimization: a Novel Bio-Inspired Optimizer for Solving Engineering Applications, Computers, Materials & Continua 2024, 79(3), 3631-3678.

[22] Liu Y. H.,Song Y. B., Zhu D. P. A rolling bearing fault diagnosis method based on ELDA dimensionality reduction and MPA-SVM[J]. Noise and Vibration Control,2024,44(03):117-124.

Color Matching and Light and Shadow Processing in Intelligent Interior Environment Art Design Analysis and Application Based on Neural Network

Ji Yang[1]*, Meifen Song[2]
Yancheng Institute of Technology, Yancheng 224000, China[1]
Yancheng Hongxin Decoration Co., Ltd, Yancheng 224001, China[2]

***Abstract*—In recent years, the application of Virtual Reality (VR) technology in the field of interior environmental design has expanded significantly, offering designers innovative methods to present complex design concepts within virtual spaces. However, the current color matching and light and shadow processing in reality are not mature enough, and the deep learning algorithms applied in VR are relatively basic with low running efficiency. The consistency and authenticity of virtual reality are not stable enough. This paper explores the integration of color matching and light-shadow processing in interior environmental design within VR technology, with a particular emphasis on leveraging neural network models to achieve automated design optimization. By incorporating deep learning algorithms, this study proposes a neural network-based approach to enhance color matching and light-shadow processing, aiming to improve the realism and aesthetic appeal of virtual environments. Experimental results demonstrate that this method offers substantial advantages in terms of color matching accuracy, naturalness of light-shadow effects, and computational efficiency, highlighting its broad potential for application in virtual reality.**

***Keywords*—Interior environment design; color matching; virtual reality; neural network; light and shadow processing**

I. Introduction

In recent years, the application of Virtual Reality (VR) technology in the field of interior environmental design has seen substantial growth, offering designers novel means to present complex design solutions within virtual spaces. This technological advancement surpasses the limitations of traditional design methods, providing a more intuitive and immersive user experience. Within a VR environment, users can freely explore virtual spaces and perceive design outcomes with heightened realism, significantly enhancing interactivity and visualization throughout the design process.

In the realm of interior environmental art design, color coordination and light-shadow processing are two critical elements. The choice and combination of colors directly influence the atmosphere and visual perception of a space, while the treatment of light and shadows adds depth and dynamic effects, creating a sense of dimensionality. The integration of these two aspects largely determines users' emotional responses and overall impressions of the space. However, traditional design methods often rely heavily on the designer's experience and subjective judgment, making it challenging to address the complex and variable demands of design. Moreover, achieving automated and personalized design optimization remains particularly difficult. Consequently, the exploration of intelligent design methods has become a crucial topic in the current field of interior environmental art design.

With the rapid advancement of intelligent technologies, breakthroughs in neural networks within the domains of image processing and visual perception have introduced new possibilities for the intelligent development of interior environmental design. By leveraging neural networks, designers can automate the learning and optimization of color coordination and light-shadow processing, thereby reducing the need for human intervention and enhancing both design efficiency and effectiveness.

There are still several challenges in the current field of indoor environmental art design, including:

1) High quality, high-resolution, and efficient color and lighting processing methods are required. Color coordination and light and shadow processing play a crucial role in environmental design. Color not only determines the visual effect of space, but also affects people's emotions and psychological states. Light and shadow processing enhances spatial depth and realism by accurately simulating light sources, shadows, and reflections. In virtual reality, achieving high-quality color and lighting processing while maintaining computational efficiency remains an urgent technological challenge.

2) Currently, neural networks are rarely used for virtual reality implementation in indoor environments, and the methods used are relatively basic. The running efficiency, consistency, and authenticity of virtual reality are not stable enough. In recent years, neural networks, especially convolutional neural networks (CNNs), have made significant progress in image processing and computer vision, opening up new possibilities for automated design. The application of Generative Adversarial Networks (GANs) in image generation and style conversion provides new methods for color coordination and light and shadow processing. However, effectively applying these technologies to environmental design in virtual reality requires further targeted optimization.

*Corresponding Author.

To address this issue, we propose a neural network-based method for color coordination and light and shadow processing in indoor environment design, aimed at improving design efficiency. We explore how to use neural network technology to optimize color matching and lighting processing in indoor environment design, in order to further enhance the design quality and user experience in virtual reality. We propose a neural network algorithm based on deep learning models that can automatically identify and optimize color and light elements in space. This algorithm has demonstrated significant innovation and effectiveness in practical applications, providing a new intelligent solution for color matching and light and shadow processing in indoor environmental art design.

Specifically, by studying the visual characteristics of color in spatial perception and the perception patterns of indoor environment color by spatial users, we proposed the influencing factors of indoor environment color matching and constructed a regression model for evaluating indoor environment color matching based on these factors. This model learns color matching rules from large-scale data through deep learning, forming a systematic indoor environment color matching design method, and successfully applying it to practical design projects. Through this intelligent design approach, we can better meet personalized design needs and enhance users' immersive experience in virtual reality.

Section II of this article introduces the relevant technologies and development status of neural networks, color matching, and light and shadow processing. Section III presents our proposed method, including a detailed neural network model and loss function. Section IV introduces the experimental setup, experimental design, and comparative results. Finally, a summary of the entire text was provided in Section V.

II. Literature Review

In this chapter, we introduce the development of neural networks, color matching and light and shadow processing in interior design, and summarize the research gaps.

A. Neural Network

In recent years, neural network technology has increasingly been applied to intelligent home systems and smart cities, suggesting its potential utility in interior environment design as well. HVAC (Heating, Ventilation, and Air Conditioning) systems are critical for maintaining comfortable indoor environments in buildings and vehicles. To detect HVAC malfunctions, Kim [1] proposed a hybrid model based on transformers, leveraging both temporal and spatial features. Fu [2] introduced an improved version of YOLOv5, specifically designed to enhance the efficiency and accuracy of defect detection in the decorative coverings of car interiors. Zhang [3] developed a color correction method for interior decoration projects, based on a dense convolutional neural network. This method detects color deviation and sets color correction goals such as color matching coordination, harmony, and visual comfort, with a calibrated objective function. Zhang [4] employed the Proximal Policy Optimization (PPO) algorithm to improve the self-planning path capabilities of renovation robots. Liang [5] proposed a pattern recognition method for artificial identification in environments to increase the success rate of target recognition and determine target position and posture in complex settings. Gao [6] introduced a krill swarm algorithm based on a long short-term memory network for interpretable artistic emotion analysis in interior decoration environments. Additionally, Jiang [7] proposed measures to enhance the ecological sustainability of urban waterfront landscapes, including the sponge city construction concept, sewage coupling treatment systems, and information flow monitoring systems. Shan [8] explored the application of traditional Chinese decorative colors in interior design and proposed a model for this application using an improved AlexNet network, optimized with Adam, BN, dropout, and data augmentation algorithms. Lastly, Zhu [9] proposed a system that integrates Mixed Reality (MR), Diminished Reality (DR), and Generative Adversarial Networks (GAN) to provide technological support for designers and other professionals.

In summary, neural network technology can be effectively applied to the artistic design of interior environments, enabling precise control and optimization of color schemes within these spaces.

B. Color Matching and Light Processing

In virtual reality environments, interaction design serves as a crucial source of user engagement [10]. Achieving a highly immersive experience relies heavily on the strategic use of light, which plays an indispensable role in virtual reality interaction design. In the virtual world, the function of light extends beyond mere illumination; it directly influences the realism and authenticity of the scene, thereby affecting various aspects of user engagement and emotional response. From the soft glow of dawn to the intense rays of afternoon sunlight, the dynamic changes in lighting breathe life into virtual interactive scenarios, imbuing virtual reality interaction design with a sense of vitality.

In virtual reality, common types of light sources include ambient light, directional light, point light, and spotlights. Each type of light source possesses distinct illumination characteristics and plays a role in simulating real-world lighting during the rendering process, thus bestowing visual properties upon objects within the scene. By simulating the interaction between light and object surfaces, various visual effects such as shading, shadows, highlights, and reflections can be achieved. The application of light directly impacts the realism and authenticity of rendered images.

Regarding color configuration, Dong [11] developed a green and red color conversion medium (CCM) film for VR/AR micro displays, enhancing color rendering. Wang [12] applied the photometric stereo algorithm to derive surface gradients, which were then used to reconstruct the 3D contours of a scene, significantly improving the dynamic performance of single-pixel 3D reconstruction systems. Stampfl [13] proposed a method for shadow processing that separates shadows from test images by segmenting them into umbra and penumbra regions using a thresholding approach.

In summary, convolutional neural network-based recognition methods have been applied across various fields. Therefore, with the continued development of technology, it is feasible to design more personalized learning recommendation services based on deep learning techniques.

III. Proposed Method

A. Neural Network Model

1) Overall model architecture: In the domain of Virtual Reality (VR) interior environment design, the effective handling and realistic representation of color schemes and lighting effects are crucial for achieving a high-quality immersive experience. Neural networks, particularly those utilizing convolutional structures, have demonstrated significant potential in processing complex visual data, making them well-suited for these tasks. This paper presents a comprehensive neural network architecture specifically designed for VR-based interior environment design, with a focus on color matching and light-shadow processing. The architecture integrates an encoder-decoder framework with a discriminator module, enabling detailed feature extraction, generation, and evaluation of visual elements.

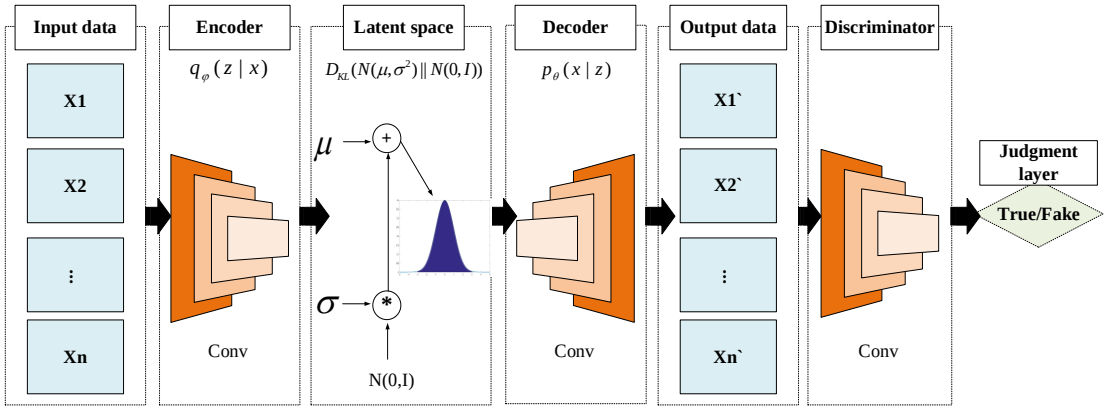


Fig. 1. Overall model architecture.

The neural network model proposed in this study is composed of the following key components:

a) Overall architecture: The architecture consists of three primary components: the encoder, the decoder, and the discriminator, all of which are enhanced by a scalable network. Fig. 1 illustrates this architecture.

b) Input data: The input data comprises a set of images, each depicting a distinct indoor design scenario (X_1, X_2, ..., Xn).

c) Encoder: The encoder employs Convolutional Neural Networks (CNNs) to extract features from the input images. These extracted features are mapped to a latent space, where they are represented by a mean vector (μ) and a standard deviation vector (σ). This latent space is crucial for generating new design samples, such as color schemes or lighting effects. The generator processes a noise vector to produce design outputs.

d) Latent space: The latent space is where the distribution of encoded features is regularized to follow a normal distribution, denoted as $N(0, I)$. This regularization is essential for the decoder to generate consistent and plausible outputs.

e) Decoder: The decoder reconstructs the original images from the latent space, producing outputs (X_1', X_2', ..., Xn') that are similar to the input data.

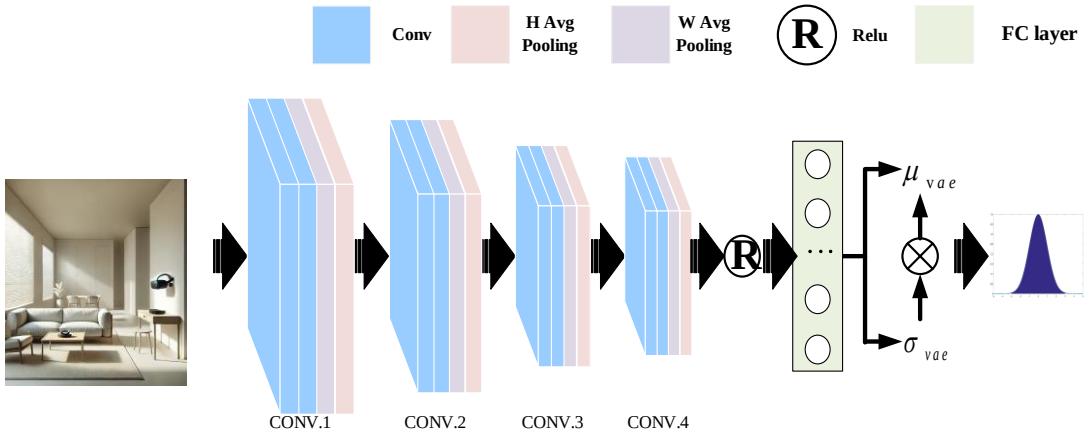


Fig. 2. Encoder structure.

f) Discriminator: The discriminator differentiates between real and generated images, providing feedback to the encoder-decoder system to enhance the quality of the generated images. This setup mirrors the architecture used in Generative Adversarial Networks (GANs), where the output (real/fake) guides the optimization process. The discriminator evaluates the realism of the generator's outputs by comparing generated samples with real samples, thereby providing feedback that drives the generator to refine its outputs continually.

This model framework facilitates the generation of high-quality design samples by integrating these components into a cohesive system that enhances both the quality and diversity of the generated outputs.

Residual mapping is utilized to enhance the model's ability to capture long-range dependencies. In the context of color matching and light-shadow processing, self-attention mechanisms play a critical role. By computing the correlations between different color regions in the input image, the model gains an understanding of the interactions between colors, leading to more harmonious color schemes. Additionally, self-attention facilitates the identification of long-range dependencies between light sources and shadows, ensuring that the generated light-shadow effects are natural and fluid.

The integration of residual mapping with self-attention mechanisms allows the model to address both the intricate color relationships and the complex spatial dependencies associated with light and shadow. This dual approach improves the overall coherence and quality of the generated design outputs, making the model more effective in producing aesthetically pleasing and contextually appropriate results.

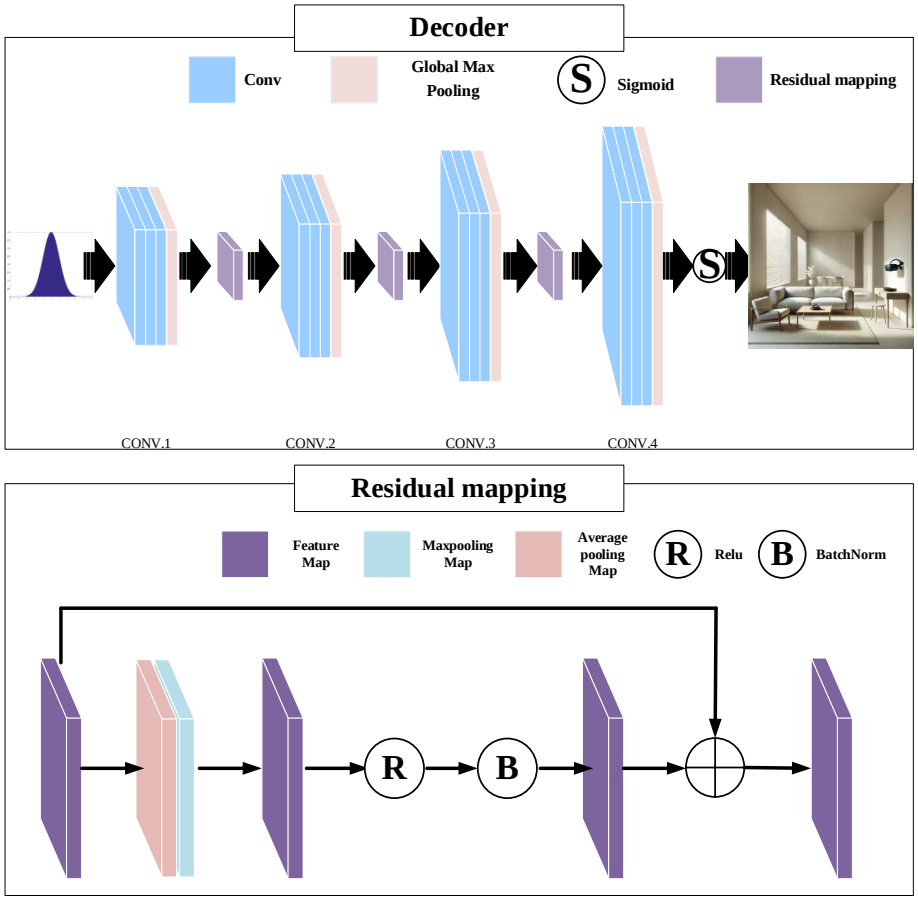


Fig. 3. Decoder structure.

2) Encoder module: As depicted in Fig. 2, the encoder architecture is meticulously crafted to efficiently extract and preserve both spatial and color information from the input images by employing a series of convolutional layers. The encoder comprises four convolutional layers (CONV 1-4), each strategically paired with horizontal (H) and vertical (W) average pooling layers. This design not only reduces the dimensionality of the feature maps but also ensures that critical spatial and color information is retained, facilitating the model's ability to capture the nuanced details of the input images.

Following the convolutional layers, the feature maps undergo a transformation through a fully connected (FC) layer, preceded by the application of the ReLU activation function. This phase is vital for generating the mean vector (μ) and standard deviation vector (σ), which characterize the feature distribution within the latent space. The precision in defining these vectors is paramount as they directly influence the quality of the latent space representation.

Subsequently, latent vectors are sampled from a normal distribution, modulated by the parameters μ and σ. These latent vectors serve as a condensed and informative representation of the input image within the latent space, encapsulating the core information necessary for the decoder to accurately reconstruct the original image. This process not only optimizes the efficiency of the model but also enhances its capability to generate high-fidelity reconstructions, thereby demonstrating the robustness of the encoder's design in capturing complex image features.

3) Decoder module: As depicted in Fig. 3, the decoder plays a crucial role in reconstructing images from latent vectors by employing a structure that mirrors the encoder. This symmetry is vital for ensuring that the reconstruction is as accurate as possible. The decoder's architecture includes a series of convolutional layers (CONV 1-4), which systematically upscale the latent vectors back into full-sized images. To maintain the integrity of high-level features and prevent information loss, each convolutional layer is followed by global max pooling and residual mapping. The incorporation of residual mapping is particularly important as it addresses the vanishing gradient problem, thereby enhancing the flow of gradients during backpropagation. This process involves passing feature maps through a series of transformations, such as average pooling and ReLU activation, before reintegrating them into the main feature stream.

The decoder's final output is generated through a Sigmoid activation function, which produces pixel values for the reconstructed image. These pixel values are then directly compared with the original image to calculate the reconstruction loss, a critical measure of the model's performance.

The encoder-decoder architecture, which includes an integrated encoder, is meticulously designed to handle the complexities of indoor environment design within virtual reality (VR). It effectively captures and reconstructs intricate color schemes and lighting effects, ensuring that the spatial hierarchies are preserved throughout the process. Additionally, latent space regularization is employed to ensure the production of high-quality, consistent outputs. The framework also integrates an adversarial training mechanism, which compels the generator to create outputs that are virtually indistinguishable from real images, thereby significantly enhancing the realism of the final visual content.

This neural network architecture offers a powerful framework for VR-based indoor environment design, with a particular focus on the precise representation of color matching and light-shadow effects. By leveraging state-of-the-art techniques such as latent space regularization, residual mapping, and adversarial training, the architecture provides designers with advanced tools to create highly immersive and realistic VR environments.

B. Loss function

We utilize loss functions to optimize the performance of both the generator and the discriminator. For color matching, the loss function is designed based on color harmony and aesthetic standards, ensuring that the generated color schemes are visually pleasing and coherent. In the context of light-shadow processing, the loss function focuses on the naturalness and realism of the light and shadow effects, aiming to achieve visually accurate and contextually appropriate results.

In the neural network model, the loss function measures the discrepancy between the model's outputs and the ground truth values. Different tasks and objectives necessitate the use of specific loss functions tailored to their respective requirements. The choice of loss function directly influences the model's ability to generate high-quality and realistic outputs, thus playing a crucial role in the overall effectiveness of the model.

1) Color matching loss function: The color harmony loss function is employed to evaluate whether the generated color schemes adhere to aesthetic standards. The color harmony loss is computed using the following formula:

$$L_{color} = \frac{1}{N}\sum_{i=1}^{N} ||c_i^{gen} - c_i^{true}||_2 \quad (1)$$

Let c_i^{gen} denote the RGB value of the i-th generated color, and c_i^{true} represent the RGB value of the i-th true color. Here, N is the total number of colors. The term $||\cdot||_2$ denotes the Euclidean distance. This loss function quantifies the discrepancy between the generated colors and the true colors, with a smaller distance indicating better color harmony.

Color Contrast Loss: To ensure that the generated colors exhibit sufficient contrast, the following loss function can be employed:

$$L_{contrast} = \frac{1}{N}\sum_{i=1}^{N} ||contrast(c_i^{gen}) - contrast(c_i^{true})||_2 \quad (2)$$

$$L_{color\_total} = \alpha \cdot L_{color} + \beta \cdot L_{contrast} \quad (3)$$

$contrast(\cdot)$ represents a function that calculates color contrast. Total loss of coordination with contrast color loses. Where: α and β are weight coefficients, used to balance the impact of the loss of each part.

2) Light processing loss function: The light-shadow realism loss is used to assess how closely the generated light and shadow effects resemble those in real scenes. The light-shadow smoothness loss is designed to ensure that the generated light-shadow transitions are natural, avoiding abrupt shadows or reflections. The combined light-shadow loss integrates both the realism loss and the smoothness loss to achieve a more comprehensive evaluation of the generated effects.

$$L_{shadow} = \frac{1}{M}\sum_{j=1}^{M} ||l_j^{gen} - l_j^{true}||_2 \quad (4)$$

$$L_{smooth} = \frac{1}{P}\sum_{p=1}^{P} ||smooth(l_j^{gen}) - smooth(l_j^{true})||_2 \quad (5)$$

$$L_{shadow\_total} = \gamma \cdot L_{shadow} + \delta \cdot L_{smooth} \quad (6)$$

Among them: l_j^{gen} first j is to generate a light characteristic. l_j^{true} is the first j a real light and shadow. M is the total number of light and shadow features. $smooth(\cdot)$

represents a function for calculating the smoothness of light and shadow. Gamma and δ are the weight coefficients.

IV. Experiment and Verification

In this chapter, we verify the reliability and validity of the proposed method through experiments.

A. Experimental Environment

This study validated the algorithm's effectiveness using an environment comprising an 11th Gen Intel(R) Core (TM) i7-11700K @ 3.60GHz CPU with 32.0 GB of RAM.

B. Data Preparation and Preprocessing

We sourced authentic interior design images and design schemes from various interior design projects, design galleries, and architectural design websites. Each image was annotated with the primary colors, recording their RGB values or coordinates in the color space. Additionally, the position and intensity of light sources, as well as shadow regions, were annotated. The images were further classified by style (e.g., modern, classical, minimalist) and by light-shadow effects (e.g., natural light, artificial lighting, shadow types). The dataset underwent noise reduction and consistency checks to ensure data quality. Finally, the dataset was split into training, validation, and test sets with a ratio of 8:1:1.

C. Evaluation Parameter

The CIEDE2000 metric is employed for the precise calculation of color differences, based on the human eye's perceptual characteristics. The Structural Similarity Index (SSIM) is used to evaluate the structural similarity of images, aligning more closely with human visual perception. The Peak Signal-to-Noise Ratio (PSNR) measures the image quality by focusing on brightness differences. Together, these three metrics provide a comprehensive evaluation of both color and image quality, aiding in the optimization of design effects in virtual reality [14]-[17].

For evaluating color harmony, we assess the aesthetic quality of color schemes through user ratings and expert evaluations. User satisfaction scores are derived from survey results. Additionally, we calculate the color difference between generated and real colors using the CIEDE2000 metric, which is based on the CIELAB color space. CIEDE2000 improves upon the CIE76 and CIE94 formulas to offer a more perceptually accurate measure of color difference, better reflecting human visual perception.

In the CIEDE2000 formula, $\Delta L^{`}$ represents the lightness difference, $\Delta C^{`}$ denotes the chroma difference, and $\Delta H^{`}$ indicates the hue difference. The parameter k is a weighting factor set to 1, and S represents a scaling factor dependent on the color's properties. R_T is a rotation term that accounts for variations in color differences across different hues. CIEDE2000 aligns more closely with human perception of color differences, and a smaller ΔE_{00} value indicates that the colors are visually closer.

For evaluating light and shadow effects, we assess the realism of the generated effects by comparing them to real scenes, using SSIM and PSNR metrics. The Peak Signal-to-Noise Ratio (PSNR) is a metric used to measure image quality and similarity, typically taking paired images as input. Since PSNR is rooted in signal processing and defined using Mean Squared Error (MSE), it is often expressed in decibels (dB). A lower MSE value results in a higher PSNR, indicating better image quality or greater similarity to the source image. Generally, a higher PSNR suggests higher similarity between paired images or better performance in image reconstruction experiments.

Structural Similarity Index (SSIM) is a critical method for assessing the similarity between paired images. It evaluates image similarity by extracting three features—luminance, contrast, and structure—from the test image and comparing these features to human visual perception of pixel structure. SSIM is commonly used as an evaluation metric for paired images and as a loss function improvement in image reconstruction tasks, with l(x,y), c(x,y), and s(x,y) representing the similarity in luminance, contrast, and structure information between images x and y.

$$\Delta E_{00} = \sqrt{\left(\frac{\Delta L^{`}}{k_L \cdot S_L}\right)^2 + \left(\frac{\Delta C^{`}}{k_C \cdot S_C}\right)^2 + \left(\frac{\Delta H^{`}}{k_H \cdot S_H}\right)^2 + R_T \cdot \Delta C} \quad (7)$$

$$PSNR = 10 \cdot log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad (8)$$

$$SSIM = l(x,y)^{\alpha} * c(x,y)^{\beta} * s(x,y)^{\gamma} \quad (9)$$

To evaluate the real-time rendering performance of the model within virtual reality environments, the rendering speed can be assessed by measuring the frame rendering time, typically expressed in frames per second (FPS). This metric provides a quantitative measure of how efficiently the model handles rendering tasks in real-time scenarios, ensuring a smooth and responsive user experience.

D. Test and Evaluation

To validate the effectiveness of the proposed methodology, we carried out a series of rigorous experiments across a diverse range of virtual reality (VR) environments. Our experimental setup involved comparing the performance of our proposed algorithm with three state-of-the-art (SOTA) algorithms: the IRCGAN model [18], the LOHO model [19], and the FTGH model [20]. These algorithms were selected due to their prominence and relevance in the field of VR design and image processing.

As detailed in Table I, our proposed method demonstrates superior performance relative to these SOTA benchmarks across several key metrics. Specifically, in the domain of color matching, our approach consistently achieves higher accuracy in aligning generated colors with target colors, thus producing more aesthetically pleasing and coherent color schemes. The image quality results reveal that our algorithm excels in maintaining high fidelity and detail, surpassing the quality delivered by the IRCGAN, LOHO, and FTGH models.

Furthermore, our method significantly improves real-time performance, which is crucial for practical VR applications where timely and responsive rendering is essential. The enhanced efficiency and reduced computational overhead of our approach ensure that complex VR environments can be rendered smoothly without compromising on visual quality.

The superior performance of our proposed algorithm underscores its potential for advancing virtual reality interior environment design. By offering enhanced color accuracy, superior image quality, and efficient real-time rendering, our method provides a robust tool for designers and developers aiming to create immersive and realistic VR experiences. The results affirm the algorithm's capacity to address the current limitations of existing methods and to contribute effectively to the field of VR design.

TABLE I. ALGORITHM COMPARISON RESULTS

Metric	Proposed Algorithm	IRCGAN	LOHO	FTGH
CIEDE2000	1.23	2.15	1.89	1.56
SSIM	0.98	0.95	0.96	0.97
PSNR (dB)	32.8	30.5	31.1	31.8
FPS	60	45	50	55

The results demonstrate that the neural network-based approach to color matching and light-shadow processing offers significant advantages in the following areas. Compared to traditional methods, neural networks more accurately capture the relationships between colors, generating more harmonious color combinations. The light-shadow effects produced by the model closely resemble real-world scenes, with natural shadow transitions and realistic reflection effects. By optimizing the model structure, our method significantly reduces computation time while maintaining high-quality output, meeting the real-time rendering demands of virtual reality.

TABLE II. ALGORITHM COMPARISON RESULTS

	Satisfaction (%)
IRCGAN	89
LOHO	88
FTGH	93
Proposed Algorithm	100

In addition, we calculated and compared the satisfaction of 100 images generated using the above algorithm, and the comparison results are shown in Table 2. From the table, it can be seen that the satisfaction rate of the images generated using our proposed algorithm is 100%, far higher than other algorithms.

Fig. 4. Generated image.

As illustrated in Fig. 4, the results of our interior environment design demonstrate the effectiveness of the proposed methods in both color matching and light-shadow processing. The generated images exhibit high-quality outcomes, reflecting the model's capability to produce aesthetically pleasing and realistic visual effects.

V. CONCLUSION

The innovations presented in this study are reflected in several key areas:

1) Automated design optimization: By leveraging neural network models, this study achieves automation in color matching and light-shadow processing, significantly reducing the workload of designers.

2) Dynamic color adjustment: The model is capable of adjusting color schemes in real-time based on environmental changes, providing robust technical support for designing dynamic scenes in virtual reality.

3) Efficient light-shadow processing: The use of GANs to generate light-shadow effects not only enhances the realism of the design but also significantly improves computational efficiency, making it suitable for real-time rendering in virtual reality environments.

In terms of applications, the proposed method can be widely applied in various domains such as interior design in virtual reality, game scene development, and virtual exhibition platforms. As neural network technology continues to advance, this method is expected to play an increasingly important role in future virtual reality applications.

ACKNOWLEDGMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] Kim B, Kang JW, Kim CS, Kwon OK, Gwak J. “Hybrid Transformer for Anomaly Detection on Railway HVAC Systems Through Feature Ensemble of Spatial-Temporal with Multi-channel GADF Images.” JOURNAL OF ELECTRICAL ENGINEERING & TECHNOLOGY. 19 (4) , pp.2803-2815. 2024. https://doi.org/10.1007/s42835-024-01844-5

[2] Fu, YZ, Qiu, L, Kong, X, Xu, HF. “Deep Learning-Based Online Surface Defect Detection Method for Door Trim Panel.” ENGINEERING LETTERS. 32 (5) , pp.939-948. 2024.

[3] Chuan-qin Zhang and Hong-tao Xing. “Colour correction method of interior decoration engineering based on dense convolution neural network.” INTERNATIONAL JOURNAL OF ARTS AND TECHNOLOGY. 13 (2) , pp.108-122. 2021.

[4] Zhang L, Qin AM. “Research on Key Technologies of Smart City Building Interior Decoration Construction based on In-Depth Learning.” INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS. 13 (12) , pp.1068-1076. 2022.

[5] Liang, TT, Liu, ZG, Wang, WZ. “Pattern recognition of decorative elements based on neural network.” JOURNAL OF INTELLIGENT &

FUZZY SYSTEMS. 39, 6, 8665-8673. 2020. https://doi.org/10.3233/JIFS-189262

[6] Gao ZQ. "A Novel Long and Short-Term Memory Network-Based Krill Herd Algorithm for Explainable Art Sentiment Analysis in Interior Decoration Environment." Journal of Cases on Information Technology.225(1). 2023. https://doi.org/10.4018/JCIT.324602

[7] Jiang G, Zuo L, Asutosh A T, Zhang J. "Environmental Sustainability Study of Urban Waterfront Landscapes Based on the LCA–Emergy–Carbon Footprint and Artificial Neural Network Method." Builings. 2024, 14, 386. 2024. https://doi.org/10.3390/buildings14020386

[8] Shan WL, Jin RM, Ding XY. "Chinese Decorative Color Based on Improved AlexNet in Interior Decoration Design." MATHEMATICAL PROBLEMS IN ENGINEERING. Sep 23 2022, 2358905. https://doi.org/10.1155/2022/2358905

[9] Zhu YH, Fukuda T, Yabuki N. "A Mixed Reality Design System for Interior Renovation: Inpainting with 360-Degree Live Streaming and Generative Adversarial Networks after Removal." TECHNOLOGIES. 12 (1). 2024. https://doi.org/10.3390/technologies12010009

[10] Jiashan Lu. "Research on influencing factors of virtual reality interaction design from the perspective of embodied cognition." China-arab States Science and Technology Forum,2023(04):111-115.

[11] Dong SC, Jiang YB,Tang CW. "Organic color-conversion media for full-color micro-LED displays." JOURNAL OF THE SOCIETY FOR INFORMATION DISPLAY. 29 (12) , pp.961-967. 2021. https://doi.org/10.1002/jsid.1072

[12] Wang M, Sun MJ, Huang C. "Single-pixel 3D reconstruction via a high-speed LED array." JOURNAL OF PHYSICS-PHOTONICS. 2 (2). 2020. https://doi.org/10.1088/2515-7647/ab83e5

[13] Stampfl V, Ahtik J. "Shadow Segmentation With Image Thresholding for Describing the Harshness of Light Sources." IEEE TRANSACTIONS ON IMAGE PROCESSING. 33, pp.3428-3440. 2024. https://doi.org/10.1109/TIP.2024.3403487

[14] Fu T, Li P, Liu S. "An imbalanced small sample slab defect recognition method based on image generation." Journal of Manufacturing Processes, 2024, 118: 376-388. https://doi.org/10.1016/j.jmapro.2024.03.028

[15] Fu T, Liu S, Li P. "Digital twin-driven smelting process management method for converter steelmaking." Journal of Intelligent Manufacturing, 2024: 1-17. https://doi.org/10.1007/s10845-024-02366-7

[16] Fu T, Li P, Liu S. "A method for quality inspection of continuous casting billet based on infrared flaw detection and two-dimensional image." IEEE Transactions on Instrumentation & Measurement. 2024. https://doi.org/10.1109/TIM.2024.3502874

[17] Fu T, Liu S, Li P. "Intelligent smelting process, management system: Efficient and intelligent management strategy by incorporating large language model." Frontiers of Engineering Management, 2024, 11(3): 396-412. https://doi.org/10.1007/s42524-024-4013-y

[18] Li, L., Wang, C., Zhang, H., & Zhang, B. "SAR Image Ship Object Generation and Classification with Improved Residual Conditional Generative Adversarial Network." IEEE Geoscience and Remote Sensing Letters, 19. 2022. https://doi.org/10.1109/LGRS.2020.3016692

[19] Saha, R.; Duke, B.; Shkurti, F.; Taylor, G.W.; Aarabi, P. "Loho: Latent Optimization of Hairstyles via Orthogonalization." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Nashville, TN, USA, 20–25 June 2021; pp. 1984–1993.

[20] Man, Q., Cho, Y. I., Jang, S. G., & Lee, H. J. "Transformer-Based GAN for New Hairstyle Generative Networks." Electronics (Switzerland), 11(13). 2022. https://doi.org/10.3390/electronics11132106.

Selecting the Best Machine Learning Models for Industrial Robotics with Hesitant Bipolar Fuzzy MCDM

A Comprehensive Framework for Evaluating Industrial Robotics

Chan Gu[1], Bo Tang[2,*]
School of Electrical and Control Engineering, Shaanxi University of Science and Technology, Xi'an 710021, China[1, 2]

***Abstract*—Machine learning models (MLMs) are used in industry to automate complicated activities, minimize human error, and improve decision-making by evaluating large volumes of data in real time. To managing inventory and quality control in the apparel and auto industries, they provide predictive capabilities such as predicting equipment breakdowns, maintenance and detecting fraud in the finance sector and the major key advantages include cost reduction, higher productivity, better product quality, and tailored client experiences. MLM helps the industries to reduce downtime, prevent errors, and gain a competitive edge through data-driven strategies and processing massive volumes of data in real time. So, there is a need to select the best MLMs for industrial robotics and by considering it, this paper addresses this problem as multiple criteria decision-making (MCDM) by exploiting hesitant bipolar fuzzy information, which takes into account both hesitation and bipolarity in decision-maker preferences. This paper introduced the new aggregation operators (AO) based on geometric and arithmetic procedures to efficiently aggregate the data including the hesitant bipolar fuzzy weighted geometric operator (HBFWGO), which is appropriate for multiplicative relationships, and the hesitant bipolar fuzzy weighted average operator (HBFWAO), which gives weighted importance to qualities. Further, the dual operators including the dual hesitant bipolar fuzzy weighted geometric operator (DHBFWGO) and the dual hesitant bipolar fuzzy weighted average operator (DHBFWAO) have been presented that are further applied to create novel strategies for resolving MCDM issues and offering a methodical manner to assess and combine features. Moreover, the example of selecting the optimal MLMs to show the robustness and efficiency of the suggested methodology has been presented which illustrates the applicability and strength of the proposed methodology in actual decision-making situations.**

Keywords*—Machine Learning Model (MLM); Hesitant Bipolar Fuzzy Set (HBFS); Dual Hesitant Bipolar Fuzzy Set (DHBFS); Hesitant Bipolar Fuzzy Aggregation Operators (HBFAO); Dual Hesitant Bipolar Fuzzy Aggregation Operators (DHBFAO); Multi-Criteria Decision-Making (MCDM)

I. INTRODUCTION

The development and evaluation of the highest quality (MLMs) [1] for industrial robotics is an important step toward the improvement of current automation and decision-making systems. Industrial robotics [2] has an enormous effect on manufacturing environments by automating challenging activities, enhancing precision, and minimizing human error. As companies transition to smart manufacturing and Industry 4.0 [3], the demand for advanced robotic systems that can intelligently adapt to dynamic and uncertain surroundings grows. Choosing the best MLM is a challenging process as it involves balancing various criteria [4]. In response, MCDM has grown to be a potent technique for handling complexity and of controlling uncertainty. This decision-making strategy is based on fuzzy set theory (FS) [5], which provides a flexible framework for addressing uncertainty. Zadeh developed the FS notion in 1965 to solve the boundaries of conventional set theory and binary logic [6], in which an individual either fully belongs to a set or does not. Many situations in the real world are not black and white, but rather exist in shades of gray, making it difficult to establish clear boundaries. FS permits the depiction of uncertainty by assigning degrees of membership to elements in a set. This significant development established the way for subsequent advances in decision-making under uncertainty, including the introduction of more advanced ideas like hesitant fuzzy sets (HFS) [7], and then bipolar fuzzy sets (BFS) [8].

FS was created to address difficulties where traditional true/false reasoning was insufficient. Since the traditional set theory implies that an element is either a member of a set or not, which is useful for issues having binary solutions. However, in many practical contexts such as robotics, control systems, and decision-making, real-world data is frequently unclear or missing. To address this, Zadeh's FS developed the concept of partial membership, which allows an element to belong to a set to some extent, represented by values ranging from $[0, 1]$. But, as the research developed, it became clear that the concept of membership alone was not necessarily adequate for modeling all types of uncertainty. This resulted in the creation of increasingly advanced extensions of FS. By considering it, Atanassov presented the concept of an intuitionistic fuzzy set (IFS) [9] in 1986, which expanded Zadeh's FS by including both a membership and non-membership function. This set offers an additional structure for dealing with uncertainty by considering an element's degree of non-membership in addition to its membership. The IFS was especially beneficial when decision-makers needed to indicate hesitancy about whether an element should be included in a set. Later on, researchers such as Alcantud [10] constructed on aggregation operator (AO) for IFS that allows for more flexible ways to aggregate and handle IFS, Ali et al. [11] utilized it for material selection, and Ahn et al. [12] utilized this framework for medical diagnosis. This

*Corresponding author.

approach improved the ability to combine data from numerous sources under uncertainty and it into an effective framework for MCDM which is utilized by various researchers for evaluating decision-making problems. Furthermore, for even more freedom in expressing uncertainty, Torra presented the HFS [13]. In an HFS, an element's membership is represented by a set of alternative values rather than a single value, indicating uncertainty in choosing membership. Additionally, he investigated the connection between IFS and HFS, demonstrating that an IFS is fundamentally contained within the envelope of an HFS. Xia and Xu [14] expanded on previous research on HFS by inventing aggregation algorithms specifically intended for hesitant fuzzy information and applying them to decision-making situations. The bipolar fuzzy set (BFS) [15] has emerged as a potential solution to managing uncertainty in MCDM situations and utilized two values to characterize an object i.e. the positive membership degree and the negative membership degree. Unlike IFS, membership degrees in BFS range from$[-1,1]$. BFS has been widely applied in various domains, such as bipolar fuzzy heat equation [16], traditional Chinese medicine [17], bipolar cognitive mapping [18], decision analysis and organizational modeling [19], biosystem regulation, and graph theory [20]. Moreover, MLMs in industrial robots is selected based on a variety of performance parameters, including speed, accuracy, resilience, and computing efficiency. So, a structured strategy for decision-making due to the abundance of MLMs that are tuned for distinct tasks, such as object recognition, navigation, or manipulation. When evaluating the MLMs, the HFS approach allows decision-makers to express their uncertainty that a model may perform well under some conditions but poorly under others, raising questions about its overall applicability. In such circumstances, HFS offers the ability to depict hesitation and BFS approach extends this concept by allowing decision-makers to consider both the positive and negative elements of any MLM which is beneficial in industrial robots, where the trade-offs between speed and precision, or adaptability and computational cost, must be carefully balanced. By integrating HFS and BFS into the decision-making process, it assists the decision-maker to systematically evaluating various factors while balancing competing aims to get the optimum ML model. Robotic systems can be made far more capable, efficient, and adaptable by choosing the best ML model for industrial robots. So, in the past FS, HFS, and BFS have all been adopted to model uncertainty in decision making, but these methodologies are still limited in terms of dealing with complex and conflicting criteria especially when working in changing arenas like industrial robotic systems. So, this paper aims to introduce the HBFWAO and HBFWGO operators that are more flexible and accurate than the existing ones hence fixing the drawback and improving support in decision making on the choice of ML models for industrial applications. Some of the primary benefits are:

- With the help of MLMs, data is optimized and repeat processes are undertaken without errors in performance to learn from past experiences.
- Traditional models are designed to perform only a few specific tasks since they follow prewritten instructions and cannot adapt to changes but ML on the other hand facilitates real-time data analysis, and enhancing efficiency in performing strategies.
- Through the integration of MLMs, robots can now work together with a human teammate and accomplish diverse tasks with a great level of efficiency.

However, the Industrial robotics faced numerous major obstacles that limited their effectiveness and flexibility prior to the inclusion of ML model, including:

- Before the advent of ML, programming and maintaining robots was an expensive affair, and supervision made them inefficient and very impractical for the modern industries.
- Conventional robots were confined to a certain set of tasks and lacked the quality of adaptability and therefore required expensive changes of programming if there were new tasks or new situations emerged.

A. Motivation of the Research

When it comes to making decisions that are quite complex in nature, the standard fuzzy sets have a lot of difficulties in capturing the preferences especially for those that have hesitations and bipolar judgments. This is addressed by HBFS but new aggregation operators (AOs) must be introduced to deal with the complexity of the existing data sets effectively thus providing the motivation of this research in enhancing MCDM processes.

- In practice, the making of decisions tends to be marred with uncertainty and ambivalent views, for instance in industrial, financial, resource allocation scopes, etc. The HBFS framework depicts this uncertainty but does not apply well in MCDM without sophisticated aggregation methods.
- In this study, the HBFWAO and HBFWGO are introduced in order to aggregate hesitant bipolar fuzzy information for more effective decision-making outputs.
- The research extends these operators to develop flexible decision-making techniques for HBFS and DHBFS, useful in industrial applications like selecting the best ML model for robots.

B. Organization of the Study

For evaluating the MLMs for robot selection, this paper is organized as follows: Section I gives a brief introduction to MLMs and their evaluation as a decision-making problem. Then, the fundamental notions of FS, HFS, BFS, and its operational laws are defined in Section II. Section III proposed the HBF set and DHBF set which are then followed by AOs including averaging and geometric operators. In Section IV, the methodology was proposed by utilizing these AOs to address MCDM concerns and then utilized in evaluating the real-world decision-making problem. Section V provides a comparison between the prior studies and the proposed study and highlights the effectiveness of the proposed operator. In the end, Section VI concludes the whole discussion by defining its limitations and future direction.

II. PRELIMINARIES

This section contains a prior defined definition of FS, BFS, HFS, and its operational laws for the understanding of the readers.

Definition 1 [5]: Let U be a fixed and non-empty set. Then, the FS $\mathcal{B}$ on U is defined as:

which is determined by a membership function MF $\mu_{\mathcal{B}}: \mu_{\mathcal{B}} \in [0,1]$

$$\mathcal{B} = \left\{\left(\sigma_j, \mu_{\mathcal{B}}(\sigma_j)\right) : \sigma_j \in U\right\} \quad (1)$$

Definition 2 [15]: Let U be a fixed and non-empty set. Then, the BFSs $\mathcal{B}$ on U is defined as:

$$\mathcal{B} = \{< \sigma_j(\mu_{\mathcal{B}}^{+}(\sigma_j), \nu_{\mathcal{B}}^{-}(\sigma_j) > | \sigma_j \in U)\} \quad (1)$$

The positive MF function, denoted as $\mu_{\mathcal{B}}^{+}(\sigma_j)$: $U \to [0,1]$, represents the degree to which an element σ_j satisfies the property associated with a bipolar fuzzy set (BFS) $\mathcal{B}$. Conversely, the negative membership degree function, $\nu_{\mathcal{B}}^{-}(\sigma_j)$: $U \to [0,1]$, indicates the degree to which an element σ_j meets an implicit counter property related to the same BFS $\mathcal{B}$. For any σ_j in the set U, the combination of these functions, expressed as $\mathfrak{b}(\sigma_j) = \left(\mu^{+}(\sigma_j), v^{-}(\sigma_j)\right)$, is referred to as a bipolar fuzzy number (BFN), represented by $\mathfrak{b} = (\mu^{+}, v^{-})$, adhering to the conditions $0 \le \mu^{+} \le 1$ and $-1 \le v^{-} \le 0$.

Definition 3 [15]: The following is a description of the basic operations on BFNs.

- $a_1 \oplus a_2 = (\mu_1^{+} + \mu_2^{+} - \mu_1^{+}\mu_2^{+}, -|\nu_1^{-}||\nu_2^{-}|)$
- $a_1 \otimes a_2 = (\mu_1^{+}\mu_2^{+}, \nu_1^{-} + \nu_2^{-} - \nu_1^{-}\nu_2^{-})$
- $\gamma a = (1 - (1 - \mu^{+})^{\gamma}, -|v^{-}|^{\gamma}), \gamma > 0$
- $(a)^{\gamma} = ((\mu^{+})^{V}, -1 + |1 + v^{-}|^{\gamma}), \gamma > 0$
- $a^{c} = (1 - \mu^{+}, |v^{-}| - 1)$
- $a_1 \subseteq a_2, \Leftrightarrow \mu_1^{+} \le \mu_2^{+}$ *and* $\nu_1^{-} \ge \nu_2^{-}$
- $a_1 \cup a_2 = (max\{\mu_1^{+}, \mu_2^{+}\}, min\{\nu_1^{-}, \nu_2^{-}\})$.
- $a_1 \cap a_2 = (min\{\mu_1^{+}, \mu_2^{+}\}, max\{\nu_1^{-}, \nu_2^{-}\})$;

Theorem 1 [15]: Let $a_1 = (\mu_1^{+}, \nu_1^{-})$ and $a_2 = (\mu_2^{+}, \nu_2^{-})$ represents for two BFNs, where $\gamma, \gamma_1, \gamma_2 > 0$. In this context, μ_1^{+} and μ_2^{+} represent the positive membership functions, while ν_1^{-} and ν_2^{-} denotes the negative membership functions. Under these conditions, the following operations can be applied to a_1 and a_2.

- $a_1 \oplus a_2 = a_2 \oplus a_1$
- $a_1 \otimes a_2 = a_2 \otimes a_1$
- $\gamma(a_1 \oplus a_2) = \gamma a_1 \oplus \gamma a_2$
- $(a_1 \otimes a_2)^{\gamma} = (a_1)^{\gamma} \otimes (a_2)^{\gamma}$
- $\gamma_1 a_1 \oplus \gamma_2 a_1 = (\gamma_1 + \gamma_2) a_1$
- $(a_1)^{\gamma_1} \otimes (a_1)^{\gamma_2} = (a_1)^{(\gamma_1 + \gamma_2)}$
- $((a_1)^{\gamma_1})^{\gamma_2} = (a_1)^{\gamma_1 \gamma_2}$

III. HESITANT BIPOLAR FUZZY AGGREGATION OPERATORS (HBFAO)

In this part, a set of innovative and specialized aggregation procedures designed exclusively for HBFAO. These operators are developed to effectively integrate and process HBFAO, boosting their utility in various decision-making and analysis settings. Additionally, the important aspects of these operators by applying fundamental operations have been analyzed which allowing us to obtain deeper insights into their behavior and performance and provide more robust methods for managing unpredictable and bipolar data.

Definition 4: Let U be a fixed and non-empty set. Then, the HBFS $\mathcal{B}^{\mathtt{a}}$ on U is defined as:

$$\mathcal{B}^{\mathtt{a}} = \left\{< \sigma_j, \mathcal{H}_{\mathcal{B}^{\mathtt{a}}(\sigma_j)} > | \sigma_j \in U \right\} \quad (2)$$

where, $\mathcal{H}_{\mathcal{B}^{\mathtt{a}}(\sigma_j)}$ is a collection of BFNs in $\mathcal{B}$. Specifically,

$$\mathcal{H}_{\mathcal{B}^{\mathtt{a}}(\sigma_j)} = \bigcup_{\left(\mu_{\mathcal{B}^{\mathtt{a}}}^{+}(\sigma_j), \nu_{\mathcal{B}^{\mathtt{a}}}^{-}(\sigma_j)\right) \in \mathcal{H}_{\mathcal{B}^{\mathtt{a}}(\sigma_j)}} \left(\mu_{\mathcal{B}^{\mathtt{a}}}^{+}(\sigma_j), \nu_{\mathcal{B}^{\mathtt{a}}}^{-}(\sigma_j)\right)$$

Where $\mu_{\mathcal{B}^{\mathtt{a}}}^{+}(\sigma_j)$ represents the positive MF, indicating the degree to which an σ_j satisfies a given property related to HBFS $\mathcal{B}^{\mathtt{a}}$ and $\nu_{\mathcal{B}^{\mathtt{a}}}^{-}(\sigma_j)$ represents the negative MF which indicates the degree to which σ_j satisfies an opposing or counter-property related to the HBFS $\mathcal{B}^{\mathtt{a}}$.

These membership functions are bounded by the following conditions: $0 \le \mu_{\mathcal{B}^{\mathtt{a}}}^{+}(\sigma_j) \le 1$ and $-1 \le \nu_{\mathcal{B}^{\mathtt{a}}}^{-}(\sigma_j) \le 0$ for every $\sigma_j \in U$.

For ease of reference, the pair $h(\sigma_j) = \left\{\left(\mu^{+}(\sigma_j), v^{-}(\sigma_j)\right)\right\}$ is called a HBFN, denoted as $h = (\mu^{+}, v^{-})$, with the constraints: $0 \le \alpha^{+} \le 1$ and $-1 \le \beta^{-} \le 0$, $(\alpha^{+}, \beta^{-}) \in (\mu^{+}, v^{-})$.

To compare HBFNs, the following comparison laws have been used which give a systematic method for evaluating and distinguishing between different HBFNs and allow us to compare their relative strengths in terms of positive and negative membership functions.

Definition 5: Let $h_i = (\mu_i^{+}, v_i^{-})$ $(i = 1,2)$ be any two HBFNs. Then,

$$\mathfrak{s}(h_i) = \frac{1}{\#\, h_i} \sum_{i=1}^{\#h_i} \frac{1 + \alpha^{+} + \beta^{-}}{2}$$

$\mathfrak{s}(h_i)$ represents the score function of $h_i = (\mu_i^{+}, v_i^{-})$.

Definition 6: Let $h_i = (\mu_i^{+}, v_i^{-})$ $(i = 1,2)$ be any two HBFNs. The accuracy function of $h_i = (\mu_i^{+}, v_i^{-})$,

$$\mathfrak{s}^{*}(h_i) = \frac{1}{\#\, h_i} \sum_{i=1}^{\#h} \frac{\alpha^{+} - \beta^{-}}{2}$$

where $\# h_i$ is the number of elements in h_i.

- If $\mathfrak{s}(h_1) > \mathfrak{s}(h_2)$, then $h_1$is considered superior to h_2, which is represent as $h_1 \succ h_2$;
- If $\mathfrak{s}^*(h_1) = \mathfrak{s}^*(h_2)$, then, $h_1$is equal to h_2, denoted by $h_1 \sim h_2$;
- If $\mathfrak{s}^*(h_1) > \mathfrak{s}^*(h_2)$, then $h_1$is considered superior to h_2, which represent as $h_1 \succ h_2$.

The following operational laws will enable to combine the HBFNs in a variety of ways, making comparisons and analyses easier within the context of HBFS theory and improve the understanding of the links and interactions between various HBFNs.

- $h^{\gamma} = \cup_{(\alpha^+,\beta^-)\in(\mu^+,v^-)} \begin{Bmatrix} (\alpha^+)^{\gamma}, \\ -1+|1+\beta^-|^{\gamma} \end{Bmatrix}, \gamma > 0;$
- $\gamma h = \cup_{(\alpha^+,\beta^-)\in(\mu^+,v^-)} \begin{Bmatrix} 1-(1-\alpha^+)^{\gamma}, \\ |\beta^-|^{\gamma} \end{Bmatrix}, \gamma > 0;$
- $h_1 \oplus h_2 = \cup_{(\alpha_1^+,\beta_1^-)\in(\mu_1^+,v_1^-),(\alpha_2^+,\beta_2^-)\in(\mu_2^+,v_2^-)} \begin{Bmatrix} \alpha_1^+ + \alpha_2^+ - \alpha_1^+\alpha_2^+, \\ -|\beta_1^-||\beta_2^-| \end{Bmatrix}$
- $h_1 \otimes h_2 = \cup_{(\alpha_1^+,\beta_1^-)\in(\mu_1^+,v_1^-),(\alpha_2^+,\beta_2^-)\in(\mu_2^+,v_2^-)} \begin{Bmatrix} \alpha_1^+\alpha_2^+, \\ \beta_1^- + \beta_2^- - \beta_1^-\beta_1^- \end{Bmatrix}$

A. Hesitant Bipolar Fuzzy Weighted Averaging Operators (HBFWAO)

This part defines the HBFAO, which allow us to combine these HBFV in an organized manner for further analysis and decision making.

Definition 7: Let $h_j = (\mu_j^+, v_j^-) \quad (j = 1,2,3,\dots,n)$ represent an entire collection of HBFV. The HBFWAO is defined as:

$$HBFWAO_w(h_1h_2,\dots,h_n) = \sum_{j=1}^{n}(w_j h_j) \tag{3}$$

where, $w = (w_1, w_1, \dots, w_1)^t$ is the weight vector for each h_j for $j = 1,2,3,\dots,n$, with $w_j > 0$ and $\sum_{j=1}^{n}(w_j) = 1$. This operator combines the HBFVs by applying their respective weights.

Theorem 2: The HBFWAO provides a HBFV with

$$HBFWAO_w(h_1h_2,\dots,h_n) = \sum_{j=1}^{n}(w_j h_j)$$

$$HBFWAO_w(h_1h_2,\dots,h_n) = \cup_{(\alpha_j^+,\beta_j^-)\in(\mu_j^+,v_j^-)} \begin{Bmatrix} 1-\prod_{j=1}^{n}(1-\alpha_j^+)^{w_j}, \\ -\prod_{j=1}^{n}|\beta_j^-|^{w_j} \end{Bmatrix} \tag{4}$$

B. Hesitant Bipolar Fuzzy Weighted Geometric Operators (HBFWGO)

This section introduced the hesitant bipolar fuzzy geometric operators (HBFGO) by combining hesitant fuzzy and bipolar fuzzy geometric mean principles. These operators are intended to successfully combine HBFNs by capturing the multiplicative relationships inherent in the dataset. This method not only improves the aggregation process, but it also assures that the output values better reflect the underlying interactions between the components.

Definition 8: The HBFWGO is defined as:

$$HBFWGO_w(h_1h_2,\dots,h_n) = \sum_{j=1}^{n}(h_j)^{w_j} \tag{5}$$

where, $w = (w_1, w_1, \dots, w_1)^t$ is the weight vector for each h_j for $j = 1,2,3,\dots,n$, with $w_j > 0$ and $\sum_{j=1}^{n}(w_j) = 1$. This operator combines the HBFV by applying their respective weights.

Utilizing the established definition and mathematical induction methods, the validity of the following theorem can be demonstrate as;

Theorem 3: The HBFWGO provides a HBFV, and

$$HBFWGO_w(h_1h_2,\dots,h_n) = \sum_{j=1}^{n}(h_j)^{w_j}$$

$$HBFWGO_w(h_1h_2,\dots,h_n) = \cup_{(\alpha_j^+,\beta_j^-)\in(\mu_j^+,v_j^-)} \begin{Bmatrix} \prod_{j=1}^{n}(\alpha_j^+)^{w_j}, \\ -1+\prod_{j=1}^{n}(1+\beta_j^-)^{w_j} \end{Bmatrix} \tag{6}$$

where, $w = (w_1, w_1, \dots, w_1)^t$ is the weight vector for each h_j for $j = 1,2,3,\dots,n$, with $w_j > 0$ and $\sum_{j=1}^{n}(w_j) = 1$.

C. Dual Hesitant Bipolar Fuzzy Aggregation Operators (DHBFAO)

The Dual hesitant bipolar fuzzy AOs (DHBFAO) combine dual hesitant and bipolar fuzzy sets to deal with uncertainty, hesitation, and both positive and negative information. They are used to combine conflicting or uncertain evidence in decision-making, hence improving analysis in complicated, confusing situations.

Definition 9: Let $\mathfrak{h}_j = (\mu_j^+, v_j^-) \quad (j = 1,2,3,\dots,n)$ represent an entire collection of dual hesitant bipolar fuzzy values (DHBFV). Then, the DHBFS $\mathcal{B}^*$ on U is defined as:

$$\mathcal{B}^* = \left\{ < \sigma_j, \left(\mu^+{}_{(\sigma_j)}, v^-{}_{(\sigma_j)}\right) > | \sigma_j \in U \right\} \tag{7}$$

where: positive membership function $\mu^+_{\mathcal{B}^*(\sigma_j)}: U \to [0,1]$ denotes the possible satisfaction function of an element σ_j with respect to the property corresponding to DHBFS $\mathcal{B}^*$ and the negative membership function $v^-_{\mathcal{B}^*(\sigma_j)}: U \to [0,1]$ denotes the

possible satisfaction function of an element σ_j with respect to some implicit counter property corresponding to $\mathcal{B}^*$. For each $\sigma_j \in U$, the following conditions hold:

$$0 \le \alpha^+ \le 1, -1 \le \beta^- \le 0$$

where, $\alpha^+ \in \mu^+{}_{(\sigma_j)}$, $\beta^- \in v^-{}_{(\sigma_j)}$, and $\alpha^{max} \in \mu^+{}_{(\sigma_j)} = \cup_{\alpha^+ \in \mu^+{}_{(\sigma_j)}} max\{\alpha^+\}$, $\beta^{max} \in v^-{}_{(\sigma_j)} = \cup_{\beta^- \in v^-{}_{(\sigma_j)}} max\{\beta^-\}$ for all $\sigma_j \in U$. To make things easier, the pair $\mathcal{B}^*(\sigma_j) = \left(\mu^+{}_{(\sigma_j)}, v^-{}_{(\sigma_j)}\right)$ is called dual hesitant bipolar fuzzy values (DHBFV) denoted by $\mathcal{B}^*(\sigma_j) = (\mu^+, v^-)$.

Definition 10: The dual hesitant bipolar fuzzy weighted aggregation operator (DHBFWAO) is defined as:

$$DHBFWAO_w(\mathfrak{h}_1, \mathfrak{h}_2, \dots, \mathfrak{h}_n) = \sum_{j=1}^{n} (w_j \mathfrak{h}_j) \tag{8}$$

where, $w = (w_1, w_1, \dots, w_1)^t$ is the weight vector for each $\mathfrak{h}_j$ for $j = 1,2,3, \dots, n$, with $w_j > 0$ and $\sum_{j=1}^{n}(w_j) = 1$. This operator combines the DHBFV by applying their respective weights.

The basic definition and principle of mathematical induction can be used to show Theorem 4. The following theorem uses the inductive reasoning and ensuring that it applies appropriately in all relevant cases.

Theorem 4: The DHBFWAO provides a hesitant bipolar fuzzy value (HBFV) with

$$DHBFWAO_w(\mathfrak{h}_1, \mathfrak{h}_2, \dots, \mathfrak{h}_n) = \sum_{j=1}^{n} (w_j \mathfrak{h}_j)$$

$$DHBFWAO_w(\mathfrak{h}_1, \mathfrak{h}_2, \dots, \mathfrak{h}_n) = \cup_{\left(\alpha_j^+ \in \mu_j^+\right), \left(\beta_j^- \in v_j^-\right)} \begin{Bmatrix} \left\{1 - \prod_{j=1}^{n}\left(1 - \alpha_j^+\right)^{w_j}\right\}, \\ \left\{-\prod_{j=1}^{n}\left|\beta_j^-\right|^{w_j}\right\} \end{Bmatrix} \tag{9}$$

D. Dual Hesitant Bipolar Fuzzy Geometric Operators

Dual hesitant bipolar fuzzy geometric operators (DHBFGOs) use dual hesitant and bipolar fuzzy sets to deal with uncertainty, reluctance, and both positive and negative information.

Definition 11: The dual hesitant bipolar fuzzy weighted geometric operator (DHBFWGO) is defined as:

$$DHBFWGO_w(\mathfrak{h}_1, \mathfrak{h}_2, \dots, \mathfrak{h}_n) = \sum_{j=1}^{n} \left(\mathfrak{h}_j\right)^{w_j} \tag{10}$$

where, $w = (w_1, w_1, \dots, w_1)^t$ is the weight vector for each $\mathfrak{h}_j$ for $j = 1,2,3, \dots, n$, with $w_j > 0$ and $\sum_{j=1}^{n}(w_j) = 1$. This operator combines the DHBFV by applying their respective weights.

The basic definition and principle of mathematical induction can be used to show Theorem 5. The following theorem uses the inductive reasoning and ensures that it applies appropriately in all relevant cases.

Theorem 5: The DHBFWGO provides a hesitant bipolar fuzzy value (HBFV) with

$$DHBFWGO_w(\mathfrak{h}_1, \mathfrak{h}_2, \dots, \mathfrak{h}_n) = \sum_{j=1}^{n} \left(\mathfrak{h}_j\right)^{w_j}$$

$$DHBFWGO_w(\mathfrak{h}_1, \mathfrak{h}_2, \dots, \mathfrak{h}_n) = \cup_{\left(\alpha_j^+ \in \mu_j^+\right), \left(\beta_j^- \in v_j^-\right)} \begin{Bmatrix} \left\{\prod_{j=1}^{n}\left(\alpha_j^+\right)^{w_j}\right\}, \\ \left\{-1 + \prod_{j=1}^{n}\left(1 + \beta_j^-\right)^{w_j}\right\} \end{Bmatrix} \tag{11}$$

IV. Evaluation of Best Machine Learning Models for Industrial Robotics

To evaluate the best machine learning models by applying the proposed hesitant bipolar AOs (HBAO), consider the collection of alternatives as $\mathcal{A} = \{\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_m\}$, and the collection of criteria denoted by $\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_n\}$. The weight vectors for the criterias are given by $w = \{w_1, w_2, \dots, w_n\}$, where $w_j \ge 0 \; \forall \; j = 1,2, \dots, n$, and $\sum_{j=1}^{n}(w_j) = 1$. Assume $H = \left[h_{ij}\right]_{m \times n} = \left[\left(\mu_{ij}^+, v_{ij}^-\right)\right]_{m \times n}$ which represent the hesitant bipolar fuzzy decision matrix. Here μ_{ij}^+ and v_{ij}^- and represent positive and negative functions, respectively, assessed by the decision-maker for the effectiveness of alternative $\mathcal{A}_i$ meets criteria $\mathcal{C}_j$. These functions lie within ranges $\mu_{ij}^+ \in [0,1]$ and $v_{ij}^- \in [0,1]$, where $i = 1,2, \dots, m$ and $j = 1,2, \dots, n$.

The methodology for using the HBFWAO or HBFWGO operator to solve a MCDM problem is explained below:

Step 1: To evaluate the MCDM problem, formation of decision matrix based on hesitant bipolar fuzzy environment.

Step 2: Applying the HBFWAO and HBFWG operator to process the information in matrix H. Calculate the overall values $h_i (i = 1,2, \dots, m)$ of alternative $\mathcal{A}_i$.

$$HBFWAO_w(h_{i1} h_{i2}, \dots, h_{in}) = \sum_{j=1}^{n} (w_j h_{ij})$$

$$= \cup_{\left(\alpha_{ij}^+, \beta_{ij}^-\right) \in \left(\mu_{ij}^+, v_{ij}^-\right)} \begin{Bmatrix} 1 - \prod_{j=1}^{n}\left(1 - \alpha_{ij}^+\right)^{w_j}, \\ -\prod_{j=1}^{n}\left|\beta_{ij}^-\right|^{w_j} \end{Bmatrix} \tag{12}$$

$$HBFWGO_w(h_{i1}, h_{i2}, \dots, h_{in}) = \sum_{j=1}^{n} \left(h_{ij}\right)^{w_j}$$

$$= \cup_{\left(\alpha_{ij}^{+},\beta_{ij}^{-}\right)\in\left(\mu_{ij}^{+},\nu_{ij}^{-}\right)} \left\{ \begin{matrix} \prod_{j=1}^{n}\left(\alpha_{ij}^{+}\right)^{w_j}, \\ -1+\prod_{j=1}^{n}\left(1+\beta_{ij}^{-}\right)^{w_j} \end{matrix} \right\} \quad (13)$$

Step 3: Determine the score by $s(h_i) = \frac{1}{\#h_i}\sum_{i=1}^{\#h_i}\frac{1+\alpha^{+}+\beta^{-}}{2}$, where $s(h_i)$ $(i = 1,2,\dots,m)$.

Step 4: Rank all the alternatives $\mathcal{A}_i$ (for $i = 1,2,\dots,m$) based on their scores $s(h_i)$ (for $i = 1,2,\dots,m$). If two scores $s(h_i)$ and $s(h_j)$ are identical, then calculate the accuracy functions $s^{*}(h_i)$ and $s^{*}(h_j)$ to differentiate and rank alternatives $\mathcal{A}_i$and $\mathcal{A}_j$.

Step 5: Select the most suitable alternatives based on their score values.

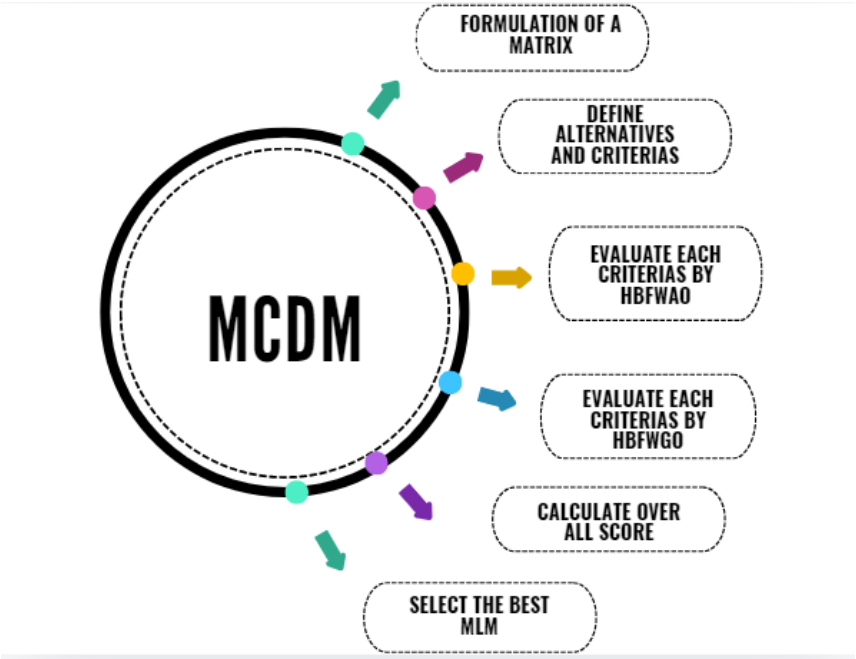


Fig. 1. Methodology of MCDM.

The pictorial representation of methodology to evaluation of best ML models is shown in Fig. 1.

A. Illustrative Example

Consider a manufacturing business that specializes in electronic device assembly. To boost their production efficiency, they decide to adopt an industrial robotic arm that can independently handle duties such as assembly and quality control. To maximize performance, however, choosing the best ML model for the robotic arm's functioning is essential. The main objective is to maximize the robotic arm's performance on the assembly line by selecting the best ML model from a pool of candidates using HBFAO. In this section, an empirical case study to assess the quality of ML model for industrial robots. The objective of the study is to evaluate which ML model, among several options that maximizes robotic performance in assembly line activities. The ML model for industrial robotic systems is shown in Fig. 2.

Fig. 2. Some ML models for industrial robotic system.

So, for the evaluation of the ML model, consider the following machine learning models (alternatives) which are evaluated based on the following criteria including accuracy of the model, training period, robustness, and interpretability which can be formulated as an MCDM problem.

The five machine learning models (alternatives) based on the following criteria are:

- $\mathcal{A}_1$ is Support Vector Machines (SVM): A high-dimensional space classification algorithm that locates the hyperplane dividing distinct classes
- $\mathcal{A}_2$ is Random Forest (RF): An ensemble technique for reliable regression and classification with insights into feature relevance that uses several decision trees.
- $\mathcal{A}_3$ is Deep Neural Networks (DNN): A flexible model with numerous layers capable of learning complicated patterns from vast datasets.
- $\mathcal{A}_4$ is Gradient Boosting Machines (GBM): An ensemble technique that creates models in a step-by-step manner, fixing mistakes in earlier models to increase accuracy.
- $\mathcal{A}_5$ is k-Nearest Neighbors (k-NN): A straightforward technique that relies on the closest training instances in the feature space to classify have been recognized.

These models will be assessed by a panel of experts who will make decisions based on the following four criteria:

- $\mathcal{C}_1$: Accuracy of the model
- $\mathcal{C}_2$: Training time required for the model.
- $\mathcal{C}_3$: Robustness of the model under various operational conditions.
- $\mathcal{C}_4$: Interpretability of the model results.

The weight values assigned by the decision makers (hypothetically) to each criterion represented by weighting vector $w = (0.20,0.10,0.30,0.40)$.

The decision-making problem i.e. evaluation of the ML model is evaluated by utilizing the above-defined methodology as follows;

Step 1: To evaluate the MCDM problem, the formation of a decision matrix from the opinion of the decision-maker based on a hesitant bipolar fuzzy environment is shown in Table I.

TABLE I. DECISION MATRIX

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$
$\mathcal{A}_1$	$\{(0.7,0.8,0.1),(-0.7,-0.4,-0.1)\}$	$\{(0.4,0.6,0.8),(-0.4,-0.3,-0.2)\}$	$\{(0.6,0.8,0.7),(-0.6,-0.3,-0.1)\}$	$\{(0.3,0.8,0.1),(-0.6,-0.4,-0.1)\}$
$\mathcal{A}_2$	$\{(0.6,0.7,0.2),(-0.6,-0.2,-0.7)\}$	$\{(0.6,0.7,0.1),(-0.6,-0.5,-0.1)\}$	$\{(0.5,0.7,0),(-0.3,-0.7,-0.1)\}$	$\{(0.5,0.7,0),(-0.3,-0.6,-0.2)\}$
$\mathcal{A}_3$	$\{(0.8,0.6,0),(-0.4,-0.3,0)\}$	$\{(0.5,0.6,0),(-0.4,-0.3,0)\}$	$\{(0.4,0.6,0.8),(-0.2,-0.5,-0.2)\}$	$\{(0.7,0.6,0.3),(-0.2,-0.4,-0.2)\}$
$\mathcal{A}_4$	$\{(0.6,0.7,0.8),(-0.4,-0.3,-0.3)\}$	$\{(0.7,0.8,0.2),(-0.2,-0.5,-0.4)\}$	$\{(0.6,0.7,0),(-0.2,-0.4,-0.1)\}$	$\{(0.6,0.7,0.8),(-0.2,-0.2,-0.4)\}$
$\mathcal{A}_5$	$\{(0.8,0.5,0),(-0.3,-0.4,-0.1)\}$	$\{(0.6,0.8,0),(-0.3,-0.5,-0.4)\}$	$\{(0.4,0.5,0.8),(-0.5,-0.4,-0.6)\}$	$\{(0.4,0.5,0),(-0.5,-0.3,-0.4)\}$

Step 2: By following above step 2, applying the HBFWAO and HBFWGO to process the information in a decision matrix H. Calculate the overall values $h_i(i = 1,2,\dots,m)$ of each alternative $\mathcal{A}_i$ corresponds to the criteria, shown in Table II.

TABLE II. AGGREGATION OF DECISION MATRIX

	HBFWAO	**HBFWGO**
$\mathcal{A}_1$	$\{(0.5081,0.7856,0.4431),(-0.5942,-0.3565,-0.1072)\}$	$\{(0.4503,0.7773,0.2207),(-0.6067,-0.3618,-0.1105)\}$
$\mathcal{A}_2$	$\{(0.5324,0.7000,0.0537),(-0.3693,-0.4953,-0.1947)\}$	$\{(0.5281,0.7000,0.0),(-0.4082,-0.5690,-0.3108)\}$
$\mathcal{A}_3$	$\{(0.6416,0.6000,0.4650),(-0.2462,-0.3923,0)\}$	$\{(0.5877,0.6000,0.4650),(-0.2661,-0.4050,-0.1446)\}$
$\mathcal{A}_4$	$\{(0.6113,0.7119,0.6277),(-0.2297,-0.2927,-0.2491)\}$	$\{(0.6093,0.7094,0.6277),(-0.2447,-0.3183,-0.3012)\}$
$\mathcal{A}_5$	$\{(0.5375,0.5438,0.3830),(-0.4290,-0.3646,-0.3424)\}$	$\{(0.4785,0.5241,0.0),(-0.4469,-0.3734,-0.4238)\}$

Step 3: Compute the score function of the evaluated decision matrix by step 3 and display in Table III.

TABLE III. SCORE VALUE

	$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}_3$	$\mathcal{A}_4$	$\mathcal{A}_5$
HBFWAO	0.1679	0.1227	0.2068	0.2179	0.1328
HBFWGO	0.1369	0.0940	0.1372	0.1455	0.0758

Step 4: Rank all the ML model $\mathcal{A}_i$ (for $i = 1,2,\dots,5$) in according with the score function $s(h_i) = h_i(i = 1,2,\dots,5)$ and demonstrate in Table IV.

TABLE IV. RANKING OF THE BEST ML MODEL FOR INDUSTRIAL ROBOTIC

	Ranking Value
HBFWAO	$\mathcal{A}_4 \succ \mathcal{A}_3 \succ \mathcal{A}_1 \succ \mathcal{A}_5 \succ \mathcal{A}_2$
HBFWGO	$\mathcal{A}_4 \succ \mathcal{A}_3 \succ \mathcal{A}_1 \succ \mathcal{A}_2 \succ \mathcal{A}_5$

Step 5: The most suitable alternatives based on their score values are shown in Table V.

TABLE V. SUITABLE ML MODEL FOR INDUSTRIAL ROBOTIC

	Ranking Value	Suitable ML (Alternative)
HBFWAO	$\mathcal{A}_4 \succ \mathcal{A}_3 \succ \mathcal{A}_1 \succ \mathcal{A}_5 \succ \mathcal{A}_2$	$\mathcal{A}_4$
HBFWGO	$\mathcal{A}_4 \succ \mathcal{A}_3 \succ \mathcal{A}_1 \succ \mathcal{A}_2 \succ \mathcal{A}_5$	$\mathcal{A}_4$

The graphical representation of the ranking of alternatives is shown in Fig. 3(a) and Fig. 3(b).

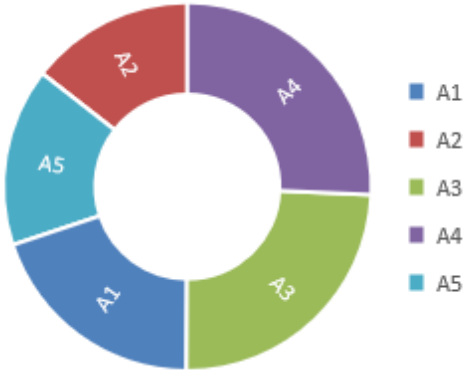


Fig. 3. Ranking of alternatives.

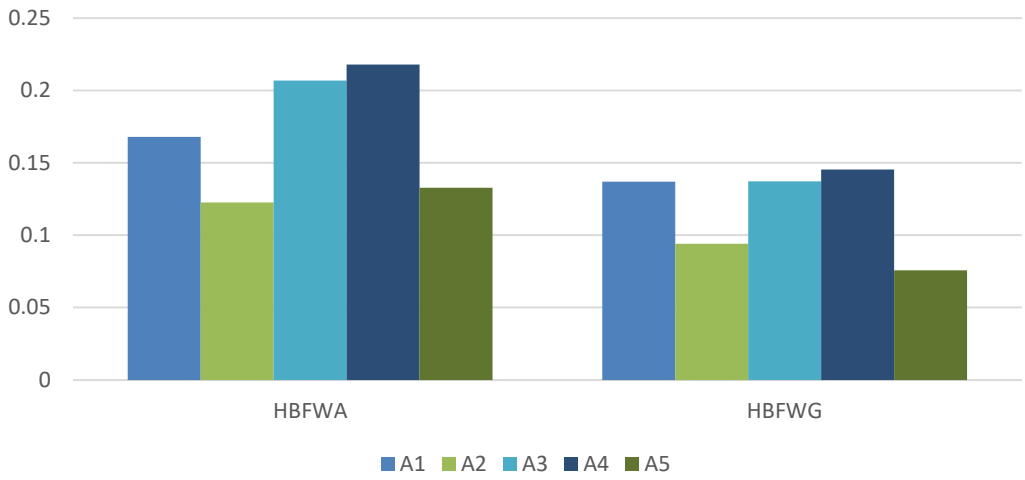


Fig. 4. Ranking of alternatives.

B. Result and Discussion

To evaluate the MLMs that are best suited for industrial robotics, the following Aos HBFWAO and HBFWGO have been employed, in this study. The proposed operators show that the Gradient Boosting Machines (GBM) model i.e. A_4 ranks higher than the other models, as shown by Table IV i.e. ranking of the ML model for industrial robotics based on these operators. By utilizing both AOs i.e. HBFWAO and HBFWGO, the results show that $\mathcal{A}_4$ is the most appropriate model, followed by $\mathcal{A}_3, \mathcal{A}_2$, and so on. The ultimate rankings in Table 5 indicate that $\mathcal{A}_4$ is the best-fit ML model based on both operators. The constancy of these operators' rating findings demonstrates their competence in decision-making, guaranteeing that the best model is chosen for industrial robotics jobs.

V. COMPARATIVE ANALYSIS

To check the validity and effectiveness of the proposed operator, this comparison study demonstrates the benefits and drawbacks of several fuzzy-based operators, from the simpler FS to the more sophisticated HBFAO. While HFS adds the capacity to model uncertainty but lacks flexibility, FS are limited in their ability to handle complicated attribute interactions. Although BFS introduces both positive and negative attribute dimensions, they are still insufficient for parametric flexibility, which hinders decision-making. Flexibility is further increased by operators like HBFWAO and HBFWGO, which consider the weighted relationships between criteria. We have compared the proposed AOs with the prior operators as shown in Table VI, which demonstrates how inadequate and ineffective the previous approaches are at handling connections between attribute values. To close this gap, we developed the HBFWAO and HBFWGO, which support optimal decision-making by thoroughly addressing these constraints.

TABLE VI. COMPARISON BETWEEN PRIOR APPROACHES AND THE PROPOSED APPROACH

Approaches	Connection Between Two Attributive Values	Relationships between Various Attributive Values	Reduced Adverse Effects	Parametric Method Increases Flexibility	Scalability	Robustness
FS [5]	✗	✗	✗	✗	✗	✗
HFS [13]	✓	✗	✗	✗	✗	✗
BFS [15]	✓	✓	✗	✓	✗	✗
HFAO [21]	✓	✓	✓	✗	✗	✗
BFAO [22]	✓	✓	✓	✓	✓	✗
HFGO [21]	✓	✓	✓	✗	✓	✗
BFGO [22]	✓	✓	✓	✓	✓	✗
HBFAWO (Proposed Operator)	✓	✓	✓	✓	✓	✓
HBFGWO (Proposed Operator)	✓	✓	✓	✓	✓	✓

So, the above Table VI demonstrate the proposed operators has the ability to highlights the relation between the various attributive values and reducing the adverse effects which make it flexible, efficient and versatile operator which assists the decision makers in making decisions. The proposed HBFWAO and HBFWGO operators are advanced and less laborious approaches to decision making under uncertainty, conflict, and incompleteness. Compared to earlier works, they afford a superior incorporation of uncertainty and flexibility with respect to complex with many criteria and objectives problems, especially those relating to industrial robotics, which have been the focus of this study.

VI. CONCLUSION

The MLMs are increasingly utilized in industrial applications to automate the complex activities, reduce human error, and enhance decision-making by analyzing large volumes of data in real-time. In this paper, a comprehensive novel approach for evaluating the best MLMs in industrial robots has been developed by utilizing the hesitant bipolar fuzzy and dual hesitant bipolar fuzzy AOs within the averaging and geometric framework. i.e. HBFWAO, HBFWGO, DHBFWAO, and DHBFGO. These operators, inspired by arithmetic and geometric operations, effectively address MCDM challenges and capturing the uncertainties associated with hesitancy and bipolarity which enabling a robust evaluation of positive and negative attributes. To demonstrate the effectiveness and robustness of proposed operator, an exemplary case study has been defined which is evaluated by utilizing the proposed decision-making algorithm. The proposed operators demonstrated their practical utility, providing precise and adaptable solutions for real-world applications in industrial robotics.

Moreover, a rigorous comparative analysis demonstrates the superiority of the proposed approach over existing methods and highlighting its robustness, accuracy, and flexibility. The parametric adaptability of the framework ensures its broad applicability across various decision-making scenarios, minimizing errors and optimizing the outcomes in complex industrial environments.

A. Limitations and Future Direction

To demonstrate the thorough evaluation and defines the balanced perspective, it is necessary to discuss the limitations of the proposed approach.

- The proposed approach offers complexity in handling a large data set, resulting in a high processing time and memory consumption.
- The proposed operators may be sensitive towards the various parameters and then improper selection may affect the accuracy and effectiveness.
- The complex nature of integrating the hesitant and bipolar environment can lead to complex situations in evaluating decision-making problems.
- Although the proposed operators show flexibility and robustness, however, it is not applicable in a highly dynamic framework and demands further modification.

So, to improve the precision and adaptability of decision-making, future research could concentrate on merging the proposed operators with sophisticated fuzzy logic systems [23], Intuitionistic fuzzy framework [24], and Pythagorean fuzzy set (PyFS) [25] framework, Neutrosophic framework [26] that may handle hesitation and more complex decision scenarios precisely. Furthermore, it can be extended by utilizing the AOs [27], [28], [29], [30] that can be useful for dealing with noisy or incomplete data. More resilient and adaptable decision-making models can be created by fusing these operators with sophisticated fuzzy techniques. Moreover, it could expand the applicability of these models beyond industrial robots to industries where uncertainty is crucial, such as healthcare, finance, and autonomous systems. Including different sectors, such as healthcare in diagnostic decision support systems, finance in risk assessment tools and autonomous systems for vehicle navigation or resource allocation, in the research

activities or case studies developed would serve to indicate the extensibility of the methods suggested. This wider perspective reveals not only the usefulness of the methods in practice across different sectors, but also the desire to appeal to a larger audience. Such examples would emphasize how these types of models can be adapted to different industries yet remain internally consistent and accurate in the face of uncertainty when making decisions.

REFERENCES

[1] Y. Behbehani and T. Messay-Kebede, "A Novel Multi-Sensor Fusion System with a Machine Learning-Based Human-Machine Interface for Automating Industrial Robots," in NAECON 2024-IEEE National Aerospace and Electronics Conference, IEEE, 2024, pp. 230–236. Accessed: Oct. 05, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10670644/

[2] M. Soori, B. Arezoo, and R. Dastres, "Optimization of energy consumption in industrial robots, a review," Cogn. Robot., vol. 3, pp. 142–157, 2023.

[3] Z. M. Çınar, A. Abdussalam Nuhu, Q. Zeeshan, O. Korhan, M. Asmael, and B. Safaei, "Machine learning in predictive maintenance towards sustainable smart manufacturing in industry 4.0," Sustainability, vol. 12, no. 19, p. 8211, 2020.

[4] S. Raschka, "Model Evaluation, Model Selection, and Algorithm Selection in Machine Learning," Nov. 11, 2020, arXiv: arXiv:1811.12808. Accessed: Nov. 18, 2024. [Online]. Available: http://arxiv.org/abs/1811.12808

[5] L. A. Zadeh, "Fuzzy sets," Inf. Control, vol. 8, no. 3, pp. 338–353, Jun. 1965, doi: 10.1016/S0019-9958(65)90241-X.

[6] A. Kechris, Classical descriptive set theory, vol. 156. Springer Science & Business Media, 2012. Accessed: Jun. 21, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=WR3SBwAAQBAJ&oi=fnd&pg=PR15&dq=classical+set+theory&ots=b9zsHqh7CB&sig=3m_0Gf19SqlqxclWZ4tDtJ3xIRs

[7] [7] H. Liao, G. Si, Z. Xu, and H. Fujita, "Hesitant Fuzzy Linguistic Preference Utility Set and Its Application in Selection of Fire Rescue Plans," Int. J. Environ. Res. Public. Health, vol. 15, no. 4, Art. no. 4, Apr. 2018, doi: 10.3390/ijerph15040664.

[8] K. Ullah, T. Mahmood, N. Jan, S. Broumi, and Q. Khan, "On bipolar-valued hesitant fuzzy sets and their applications in multi-attribute decision making," The nucleus, vol. 55, no. 2, pp. 93–101, 2018.

[9] K. T. Atanassov, "Intuitionistic fuzzy sets," Fuzzy Sets Syst., vol. 20, no. 1, pp. 87–96, Aug. 1986, doi: 10.1016/S0165-0114(86)80034-3.

[10] J. C. R. Alcantud, "Multi-attribute group decision-making based on intuitionistic fuzzy aggregation operators defined by weighted geometric means," Granul. Comput., vol. 8, no. 6, pp. 1857–1866, Nov. 2023, doi: 10.1007/s41066-023-00406-w.

[11] S. Ali, H. Naveed, I. Siddique, and R. M. Zulqarnain, "Extension of Interaction Geometric Aggregation Operator for Material Selection Using Interval-Valued Intuitionistic Fuzzy Hypersoft Set," J. Oper. Intell., vol. 2, no. 1, pp. 14–35, 2024.

[12] J. Y. Ahn, K. S. Han, S. Y. Oh, and C. D. Lee, "An application of interval-valued intuitionistic fuzzy sets for medical diagnosis of headache," Int. J. Innov. Comput. Inf. Control, vol. 7, no. 5, pp. 2755–2762, 2011.

[13] V. Torra, "Hesitant fuzzy sets," Int. J. Intell. Syst., vol. 25, no. 6, pp. 529–539, 2010.

[14] M. Xia and Z. Xu, "Hesitant fuzzy information aggregation in decision making," Int. J. Approx. Reason., vol. 52, no. 3, pp. 395–407, Mar. 2011, doi: 10.1016/j.ijar.2010.09.002.

[15] W.-R. Zhang, "(Yin) (Yang) bipolar fuzzy sets," in 1998 IEEE International Conference on Fuzzy Systems Proceedings. IEEE World Congress on Computational Intelligence (Cat. No.98CH36228), May 1998, pp. 835–840 vol.1. doi: 10.1109/FUZZY.1998.687599.

[16] M. Akram and M. Bilal, "Analytical solution of bipolar fuzzy heat equation using homotopy perturbation method," Granul. Comput., vol. 8, no. 6, pp. 1253–1266, Nov. 2023, doi: 10.1007/s41066-023-00415-9.

[17] S.-P. Chen, S.-T. Yang, K.-C. Hu, S. K. Satyanarayanan, and K.-P. Su, "Usage Patterns of Traditional Chinese Medicine for Patients with Bipolar Disorder: A Population-Based Study in Taiwan," in Healthcare, MDPI, 2024, p. 490. Accessed: Oct. 03, 2024. [Online]. Available: https://www.mdpi.com/2227-9032/12/4/490

[18] W.-R. Zhang, "Bipolar fuzzy sets and relations: a computational framework for cognitive modeling and multiagent decision analysis," in NAFIPS/IFIS/NASA'94. Proceedings of the First International Joint Conference of The North American Fuzzy Information Processing Society Biannual Conference. The Industrial Fuzzy Control and Intellige, IEEE, 1994, pp. 305–309. Accessed: Jun. 25, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/375115/

[19] N. S. K. Devi et al., "An integrated bipolar picture fuzzy decision driven system to scrutinize foodwaste treatment technology through assorted factor analysis," CMES-Comput. Model. Eng. Sci., 2024, Accessed: Oct. 07, 2024. [Online]. Available: https://acikerisim.medipol.edu.tr/xmlui/handle/20.500.12511/12763

[20] M. Akram, "Bipolar fuzzy graphs," Inf. Sci., vol. 181, no. 24, pp. 5548–5564, 2011.

[21] J. Peng, J. Wang, X. Wu, and C. Tian, "Hesitant intuitionistic fuzzy aggregation operators based on the Archimedean t-norms and t-conorms," Int. J. Fuzzy Syst., vol. 19, pp. 702–714, 2017.

[22] C. Jana, M. Pal, and J. Wang, "A robust aggregation operator for multi-criteria decision-making method with bipolar fuzzy soft environment," Iran. J. Fuzzy Syst., vol. 16, no. 6, pp. 1–16, 2019.

[23] A. Ali et al., "Enhanced Fuzzy Logic Zone Stable Election Protocol for Cluster Head Election (E-FLZSEPFCH) and Multipath Routing in wireless sensor networks," Ain Shams Eng. J., vol. 15, no. 2, p. 102356, Feb. 2024, doi: 10.1016/j.asej.2023.102356.

[24] J. C. R. Alcantud, "Multi-attribute group decision-making based on intuitionistic fuzzy aggregation operators defined by weighted geometric means," Granul. Comput., vol. 8, no. 6, pp. 1857–1866, Nov. 2023, doi: 10.1007/s41066-023-00406-w.

[25] S. N. Abbasi, S. Ashraf, M. Akram, C. Jana, V. Simic, and D. Pamucar, "A Pythagorean fuzzy Ž-number-based neutrality aggregation model for AI-enabled energy efficiency management," Appl. Soft Comput., vol. 161, p. 111753, 2024.

[26] M. N. Jafar, R. Imran, S. H. A. Riffat, and R. Shuaib, Medical diagnosis using neutrosophic soft matrices and their compliments. Infinite Study, 2020. Accessed: Sep. 16, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=D2r7DwAAQBAJ&oi=fnd&dq=raiha+imran+topsis&ots=_gOuAHMiph&sig=vyso2uHh8sWV9lPsw-Qo6HqB-DU

[27] R. Imran, K. Ullah, Z. Ali, M. Akram, and T. Senapati, "The theory of prioritized Muirhead mean operators under the presence of complex single-valued neutrosophic values," Decis. Anal. J., vol. 7, p. 100214, 2023.

[28] M. E. Ullah, M. Idrees, S. Muhammad, and M. Shuaib, "Numerical investigation of heat transfer enhancement in magnetohydrodynamics ternary ferrofluids on nonlinear stretching sheet," Case Stud. Therm. Eng., vol. 59, p. 104470, 2024.

[29] R. Imran, K. Ullah, Z. Ali, and M. Akram, "An Approach to Multi-Attribute Decision-Making Based on Single-Valued Neutrosophic Hesitant Fuzzy Aczel-Alsina Aggregation Operator," Neutrosophic Syst. Appl., vol. 22, pp. 43–57, Oct. 2024, doi: 10.61356/j.nswa.2024.22387.

[30] M. Amin, K. Ullah, M. Akram, R. Imran, and M. S. Nazeer, "Advancing AI-Based Biometric Authentication in Multi-Criteria Decision Approach Using Complex Circular Intuitionistic Fuzzy Logic and Dombi Operators," 2024, Accessed: Jul. 18, 2024. [Online]. Available: https://www.researchsquare.com/article/rs-4483111/latest

Real-Time Data Acquisition in SCADA Systems: A JavaWeb and Swarm Intelligence-Based Optimization Framework

Lingyi Sun[1], Tieliang Sun[2], Ruojia Xin[3], Feng Yan[4], Yue Li[5], Hengyu Wang[6], Yecen Tian[7], Dongqing You[8], Yun Liu[9], Muhao Lv[10]
Pipe China Oil and Gas Control Center, Beijing, 10020, China[1, 2, 4, 5, 6, 7, 8, 9, 10]
Kunlun Digital Technology Co., Ltd. Beijing, 10020, China[3]

***Abstract*—This paper aims to improve the accuracy and efficiency of SCADA software design and testing for oil and gas pipelines. It proposes a JavaWeb-based SCADA software solution optimized by the Bird Foraging Search (BFS) algorithm combined with an Echo State Network (ESN) for enhanced testing and analysis. A multi-tiered distributed SCADA software architecture based on the Java EE framework was designed to provide real-time data acquisition, monitoring, control, and data analysis. The BFS algorithm was used to optimize the hyperparameters of the ESN model to improve testing accuracy and convergence speed. The BFS-ESN model was compared with other optimization algorithms such as PSO and DE. Experimental results show that the BFS-ESN model achieved a testing accuracy of 97.33% and faster convergence within 700 iterations. It outperformed other algorithms in both accuracy and convergence speed. The JavaWeb-based SCADA software design for oil and gas pipelines is feasible, and the BFS-ESN model significantly enhances the accuracy and efficiency of SCADA software testing. This approach demonstrates the potential for application in SCADA systems, with future research needed to simplify the model and extend its applicability for large-scale deployment.**

***Keywords*—JAVAWeb; oil and gas pipelines; SCADA software; design analysis; bird foraging search algorithm**

I. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) is a kind of industrial control system for long-distance data acquisition and monitoring [1], which is widely used in long-distance oil and gas pipelines [2], and its ability to work properly directly affects the production and operation of oil and gas pipelines and even the national oil and gas industry [3]. In recent years, with the great development of pipeline construction, the normal operation of the pipeline has had a direct impact on the production and operation of oil and gas pipelines and even the national oil and gas industry [3]. In recent years, with the great development of pipeline construction, the pipeline scale is getting bigger and bigger, the demand for SCADA system software is getting higher and higher, the database management scale reaches millions of nodes, the supported devices are diversified, and the number of collection devices is required to reach hundreds or even thousands [4]. In order to improve the efficient, stable and safe operation of the system, combined with Java Web technology, the design of SCADA software, to build multi-level, distributed applications [5]. In the consideration of safe production, after the SCADA software for oil and gas pipelines passes the software test in the laboratory simulation environment, it is also necessary to select real scenarios at the operation site and use the SCADA software to carry out a controlled range of trial operation [6]. Therefore, the study of SCADA software analysis for oil and gas pipelines based on Java Web technology is of great significance for software design, which is not only conducive to the efficiency of software design, but also contributes to the efficient, stable and safe operation of SCADA systems [7].

The research on the design and analysis of SCADA software for oil and gas pipelines based on Java Web technology mainly includes the research on the demand analysis of SCADA system for oil and gas pipelines, Java Web development of SCADA software, and test analysis of SCADA software [8]. Oil and gas pipeline SCADA system requirements analysis is mainly to improve the performance of oil and gas pipeline SCADA system, study in [9] from the perspective of market research, analysed the existence of pipeline transmission characteristics, for this feature, designed a long-distance oil and gas pipeline SCADA system; study in [10] from the perspective of economic benefits, research on oil and gas pipeline SCADA project construction specific design ideas. SCADA software Java Web development is mainly to study the process of developing SCADA software based on Java Web technology, study in [11] used Java Web technology to develop SCADA software for oil and gas pipelines, and introduces the relevant functions and structure. SCADA software testing and analysis research is mainly the use of software testing process, according to the test indexes, analyse the effectiveness and functionality of SCADA software. The effectiveness and functionality of SCADA software is analysed according to the testing indexes. Currently, data-driven algorithms are used to test SCADA software, including neural networks [12], SVM [13], LSTM [14] and other methods. Although scholars at home and abroad have done a lot of rich research on the design and analysis of SCADA software for oil and gas pipelines based on Java Web technology, there are still some problems [15]: firstly, there are fewer research studies on the development of SCADA software for oil and gas pipelines based on Java Web technology; secondly, there are fewer methods for testing SCADA software for oil and gas pipelines; and lastly, the testing methods for SCADA software accuracy is not high enough.

In order to improve the accuracy of SCADA software testing and analysis methods for oil and gas pipelines based on Java Web technology, this paper provides relevant ideas for the design problems of SCADA software for oil and gas pipelines based on Java Web technology, focusing on the key problems of SCADA software design and testing for oil and gas pipelines, combining the Echo State Network [16] with the Bird Foraging Search Algorithm [17], and proposing a method based on the BFS-ESN network in Java Web framework of oil and gas pipeline SCADA software design testing method. The experimental results of relevant data analysis show that the SCADA software design method for oil and gas pipelines based on BFS-ESN network under the Java Web framework realises the SCADA software design and analysis problems of oil and gas pipelines, and improves the accuracy and efficiency of the SCADA software design test.

II. SCADA Software for Oil and Gas Pipelines

A. Java Web Technologies

Java Web is a web development framework based on Java technology [18] for building dynamic websites and enterprise applications. It includes a variety of technologies and server-side components, such as Servlet, JSP (JavaServer Pages), Spring, Hibernate, as well as web servers and application servers, such as Apache Tomcat, Jetty, GlassFish and WildFly. The Java Web technology system covers the full range of development needs from front-end presentation to back-end logic processing. Java Web technology system covers a full range of development needs from the front-end display to the back-end logic processing. Java Web schematic diagram shown in Fig. 1.

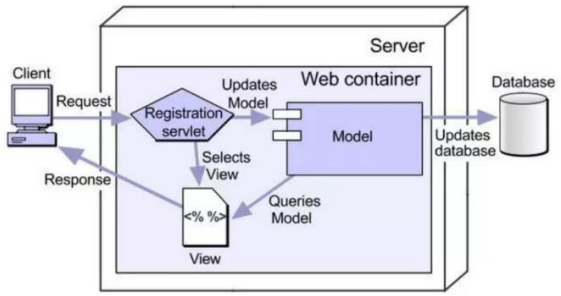


Fig. 1. Java web technology.

The technology system of Java Web includes front-end technologies (HTML, CSS, JavaScript) and back-end technologies (Servlet, JSP, MVC frameworks, database interaction technologies) [19]. Developers can use these technologies to create dynamic web pages, handle user requests, access databases, and implement business logic. The Java Web technology system and roles are shown in Fig. 2.

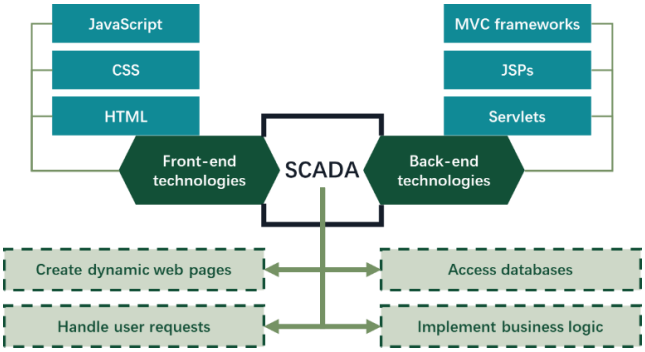


Fig. 2. Java Web technology system and role.

Java Web servers usually work based on a B/S (Browser/Server, browser and server) model (Fig. 3). The client sends an HTTP request to the server through the browser, and the server receives the request and processes it according to the type of request (static resource or dynamic resource). If it is a dynamic resource, the server forwards the request to the Web container (Tomcat), which loads the Servlet or JSP page, executes the corresponding business logic, and returns the generated dynamic content to the client browser.

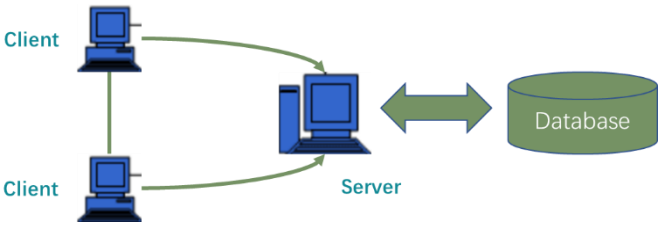


Fig. 3. Java web server fundamentals.

B. SCADA System for Oil and Gas Pipelines

Oil and gas pipeline SCADA (Supervisory Control And Data Acquisition) [20] systems are key industrial control systems used to monitor and control oil and gas transmission processes. Java Web-based SCADA software design typically involves the use of the Java EE (Jakarta EE) technology stack to build multi-tiered, distributed applications that provide real-time data acquisition, monitoring, control, and data analysis, as shown in Fig. 4.

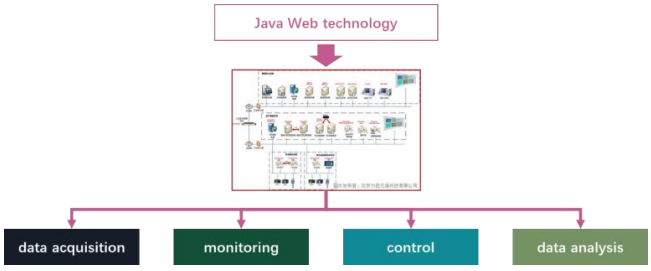


Fig. 4. Logical relationship between SCADA and Java Web.

In designing Java Web-based SCADA software for oil and gas pipelines, the multi-tier architecture provided by the J2EE platform can be used, including the client layer, Web layer, business logic layer, and enterprise information system layer [21]. Such an architecture helps to improve the modularity, maintainability, and scalability of the system.1) The client layer can be a Web-based interface for remote access; 2) the Web layer handles HTTP requests and responses and provides the user interface; 3) the business logic layer contains components that process data and execute control logic; and 4) the enterprise information system layer is responsible for integrating with external systems such as energy Management System (EMS). Fig. 5 shows Java Web-based SCADA software design architecture.

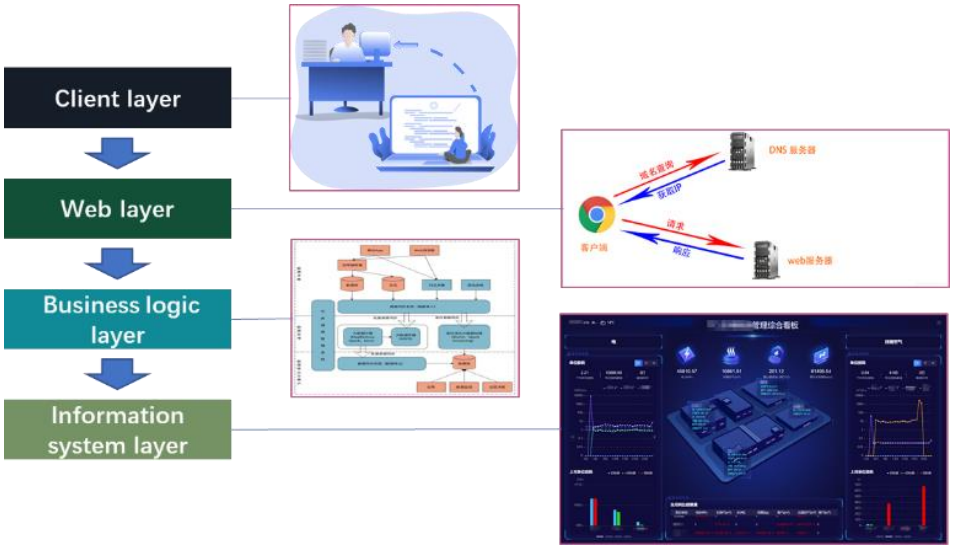


Fig. 5. Java Web-based SCADA software design architecture.

C. Design Thinking

According to the Java Web-based SCADA software design architecture for oil and gas pipelines, this paper uses various technologies and services provided by Java EE (Servlet, JavaServer Pages (JSP), Enterprise JavaBeans (EJB), Java Message Service (JMS), Java Transaction API (JTA)) to achieve high performance, reliability and security of the system; using a database management system (DBMS) to store historical data and real-time data; the use of Web services and RESTful APIs to achieve inter-system communication and data exchange, as shown in Fig. 6.

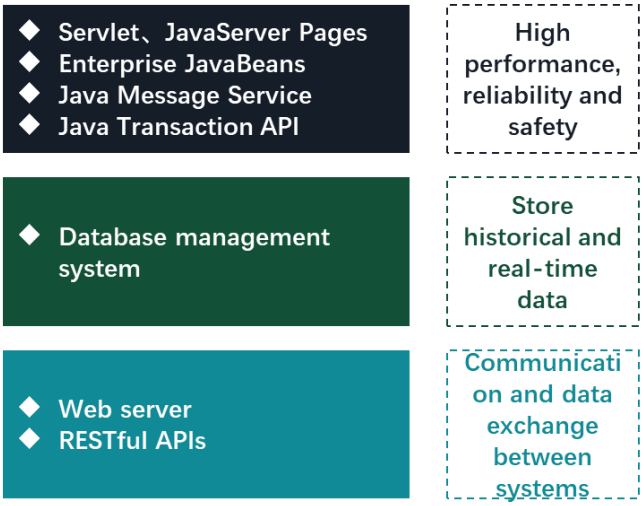


Fig. 6. Key technologies and tools.

With the help of these tools and technologies, security and reliability are fully considered to ensure that real-time data monitoring and control response can be provided, and interface interaction is designed to enable operators to easily monitor pipeline status and perform necessary control operations. The design flow of Java Web-based SCADA software is shown in Fig. 7.

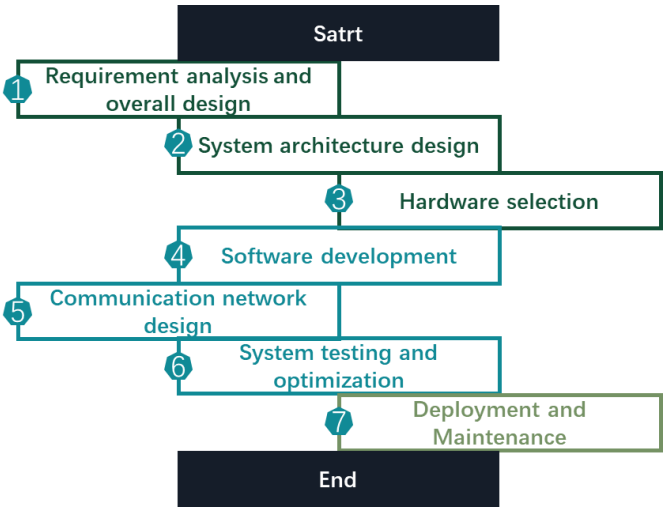


Fig. 7. Design flow.

III. Software Design Application and Test Analysis

A. Echo State Network

One type of recursive neural network is the echo state network (ESN) [22], which is typically used for time series

prediction [19] and builds the network hidden layer using the "reserve pool" technique. The input layer, storage layer, and output layer comprise the vast majority of ESN. Fig. 8 illustrates its precise configuration. Following the initial randomization, the connection weights between the input layer and the storage pool $\boldsymbol{W}_{in}^{r\times n}$ are not trained and won't be altered. Similarly, the state feedback weight $\boldsymbol{W}^{r\times r}$ is arbitrarily initialized and does not require training, while the reserve pool input is derived from the output of the previous state of the input layer and the reserve pool, respectively. A reserve pool for the output layer weights $\boldsymbol{W}_{out}^{m\times r}$ must be trained, typically using the Ridge regression (Ridge regression) method for connection weights. This method is expressed as follows:

$$\boldsymbol{W}_{out}=\boldsymbol{Y}_{long}\boldsymbol{H}^{T}\left(\boldsymbol{H}\boldsymbol{H}^{T}+\lambda_{r}\boldsymbol{I}\right)^{-1} \tag{1}$$

The storage pool state and the regularization factor are represented by $\boldsymbol{H}$ and λ_r, respectively. The condition $\boldsymbol{H}$ of the pool is depicted below:

$$\boldsymbol{H}\left(t\right)=\tanh\left(\boldsymbol{W}_{in}\boldsymbol{X}_{long}\left(t\right)+\boldsymbol{W}\boldsymbol{H}\left(t-1\right)\right) \tag{2}$$

where the hyperbolic tangent activation function is indicated by tanh.

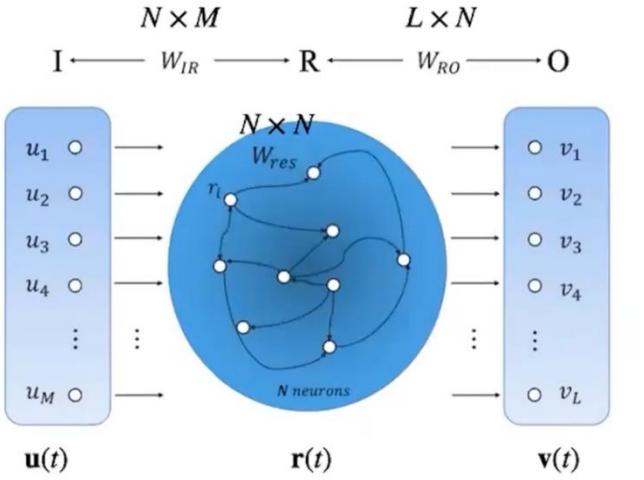


Fig. 8. Echo state neural network.

The Echo State Network (ESN) algorithm consists of two main phases: the initialization of weight parameters and the training process. During the initialization phase, the connection weights within the network are randomly generated. Specifically, the connection weights between neurons in the reservoir (or storage pool) are sparsely distributed, meaning that not all neurons are connected, which helps reduce computational complexity. In the training phase, only the weights connecting the reservoir to the output layer are adjusted, typically using methods like Ridge regression, while other weights remain fixed [23], where the ESN hyperparameters include the size of the storage pool N_r, the spectral radius SR, and the input scaling factor IS, storage pool sparsity SD.

A key characteristic of ESNs is the relatively large number of neurons present in the reservoir, which allows the network to capture complex dynamics. However, the performance of an ESN is highly dependent on its hyperparameters, making hyperparameter tuning a crucial step for optimal performance. The key hyperparameters include the size of the reservoir, which determines how much internal memory the network has; the spectral radius, which controls the stability and dynamic range of the network; the input scaling factor, which influences the sensitivity of the reservoir to input signals; and the sparsity of the reservoir, which affects the degree of connectivity between neurons. Proper adjustment of these hyperparameters is essential for improving the prediction accuracy of the ESN, especially in time series forecasting and other complex tasks.

B. Bird Foraging Search Algorithm

Drawing inspiration from the diverse behaviors exhibited by birds while foraging, this paper introduces a new swarm intelligence optimization algorithm known as the Birds Foraging Search (BFS) algorithm [17]. Each phase contributes uniquely to the optimization process.

In the flight search behavior phase, birds engage in exploratory movements, mimicking how birds scout for food sources over large areas. This phase primarily focuses on exploration, allowing the algorithm to cover a wide search space. The domain behavior phase, on the other hand, emphasizes exploitation, where birds refine their search within specific territories to locate better resources more precisely. The balance between these two phases—exploration and exploitation—is essential for optimizing the algorithm's performance. The cognitive behavior phase enhances the algorithm's search efficiency by allowing individual birds to learn from their past experiences. This phase simulates self-learning, enabling birds to adjust their strategies based on previously gathered information, which helps in avoiding redundant searches and accelerating convergence. The detailed search strategies for each phase are illustrated in Fig. 9.

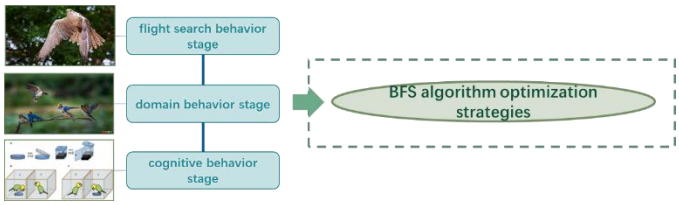


Fig. 9. Search strategy of the BFS algorithm.

The initial position of the bird in space is represented as follows:

$$X_i=UB-r_1\cdot(UB-LB) \tag{3}$$

where X_i denotes the position of the ith bird, UB and LB denote the upper and lower bounds of the search space, respectively, and r_1 is a random value.

1) Flight search behaviour stage: Birds of prey, like falcons, typically choose areas with high potential for finding prey and hover over these regions while searching for food. Through extensive research, scientists have observed that the flight patterns of these raptors closely resemble a logarithmic spiral. This spiral movement allows the birds to efficiently cover a specific area, increasing their chances of locating prey. The spiral pattern is mathematically defined, and its unique structure enables the predator to maintain focus on a targeted zone while gradually expanding or contracting their search radius, optimizing their hunting strategy (as shown in Fig. 10):

$$X_i^{iter+1} = D_{i-p} \cdot e^{\theta} \cdot \cos(2\pi\theta) + PA^{iter} \quad (4)$$

where $i \in [1, 2, 3, \ldots, N]$, and N is the population size. θ is a random number between -1 and 1. $D_{i-p} = \left| X_i^{iter} - PA^{iter} \right|$ denotes the distance from the i[th] bird to the potential region, X_i^{iter} denotes the position of the i[th] bird at iter iteration, and PA^{iter} denotes the position of the potential region at iter iteration.

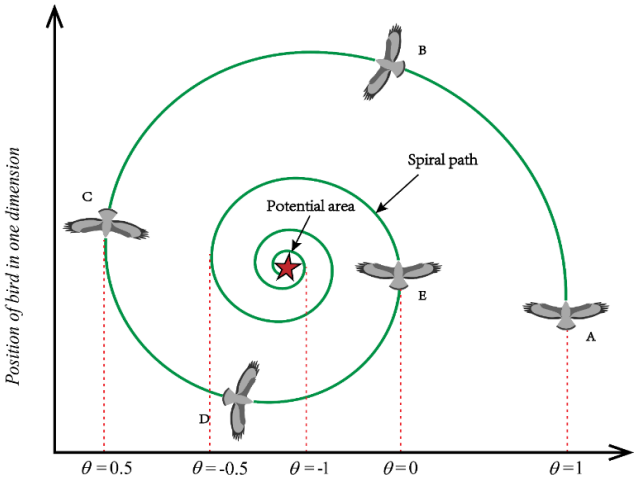


Fig. 10. Logarithmic spiral flight pattern.

2) Stages of domain behavior: In the Birds Foraging Search (BFS) algorithm, these two types of birds follow different movement behaviors. The territorial bird focuses on patrolling a small region around its current position, both to search for better food sources and to defend its territory from other competing birds. This localized exploration allows the territorial bird to refine its current solution while preventing others from entering its domain. Meanwhile, the invasive birds attempt to enter the territory in search of resources. The behavior of the territorial bird, balancing exploration and defense, can be mathematically modeled as follows:

$$X^{T,iter+1} = X^{T,iter} + r_d \cdot \lambda \quad (5)$$

Where, $X^{T,iter}$ is the position of the territorial bird at iterth iteration; r_d is a random value between -1 and 1, representing the search direction of the territorial bird; λ is a scale factor, which is generally set to $(X^{T,iter} - X^{S,iter})$, and $X^{S,iter}$ is the position of the suboptimal individual.

Once a territorial bird has claimed a region as its exclusive domain, all invading birds will begin moving toward that area in search of resources. At this stage, the territorial bird takes defensive action to protect its claimed space, using warning calls or chirping to deter the invaders. This defense mechanism can lead to two possible outcomes.

a) Scenario 1: In this case, the invasive bird's position is updated as it moves closer to the territory. The invasive bird's persistence reflects a focus on resource acquisition, and the algorithm models this movement as a rapid progression toward the territorial bird's domain, following a predefined mathematical update rule. This allows the invasive bird to keep adjusting its position despite the territorial bird's efforts to protect its resources.

$$X_j^{I,iter+1} = X_j^{I,iter} + r_2 \cdot (X^{T,iter} - IF \cdot X_j^{I,iter}) \quad (6)$$

Where, $X_j^{I,iter}$ is the position of the jth invasive bird at the iterth iteration, r_2 is a random number between 0 and 1; IF is the invasion factor, which determines how the position of the invasive bird changes, and the specific effects are shown in Fig. 11.

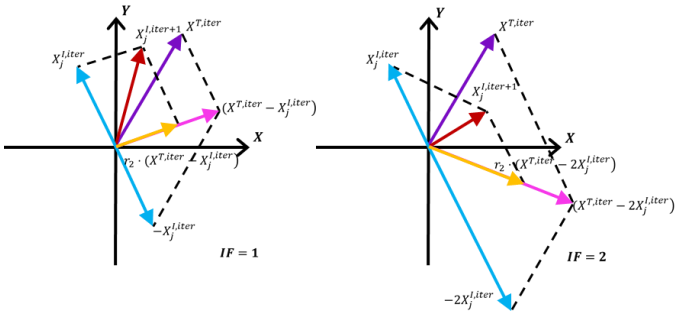


Fig. 11. Vector representation of invasive bird movements with different invasion factors.

b) Scenario 2: When the bird continues its search but fails to discover an improved solution, its current position remains unchanged from the previous one($X_i^{iter} = X_i^{iter-1}$). In this scenario, the bird's movement is modeled using a Gaussian distribution, allowing for random variations in its search path. This randomness helps the bird explore new areas more effectively.

$$X_{j,d}^{I,iter+1} = X_{j,d}^{I,iter} + r_3 \cdot (X_{k,d}^{I,iter} - X_{m,d}^{I,iter}) + r_4 \cdot (X_{l,d}^{I,iter} - X_{h,d}^{I,iter}) \quad (7)$$

The Scenarios 1 and 2 optimisation process is summarised as:

$$\begin{cases} X_j^{I,iter+1} = X_j^{I,iter} + r_2 \cdot (X^{T,iter} - IF \cdot X_j^{I,iter}) & if\ P^{iter} \le rand \\ X_{j,d}^{I,iter+1} = X_{j,d}^{I,iter} + r_3 \cdot (X_{k,d}^{I,iter} - X_{m,d}^{I,iter}) + r_4 \cdot (X_{l,d}^{I,iter} - X_{h,d}^{I,iter}) & otherwise \end{cases} \quad (8)$$

3) Cognitive behavioural stage: Cognitive behavior in birds is essentially a self-learning process that draws on accumulated experience. Birds use the information gathered from previous searches to refine their strategies, helping them avoid redundant or inefficient searching. This self-guided learning enhances their foraging efficiency, allowing them to focus on more promising areas. Cognitive behavior can be broken down into two distinct parts.

a) Scenario 1: In this case, the birds are continuously discovering better food sources, which means their current position differs from the previous one $X_i^{iter} \neq X_i^{iter-1}$. Here, the birds actively learn by leveraging the gradient information from their previous searches. By following this targeted search approach, they adjust their movements in a way that is guided by prior successes, which ultimately helps them refine their foraging strategy. This focused learning process not only allows them to zero in on better resources but also significantly speeds up the algorithm's convergence. The efficiency gained from this self-learning behavior means the birds are more likely to optimize their search pattern faster, avoiding unnecessary wandering and making the overall process more streamlined. The specific mathematical calculations for updating their positions during this phase are based on their learning from previous gradients.

$$X_i^{iter+1} = X_i^{iter} + r_5 \cdot (X_i^{iter} - X_i^{iter-1}) \quad (9)$$

Where X_i^{iter} and X_i^{iter-1} are the i-th bird at iter-th iteration and iter-1 iteration position respectively; r_5 is a random number between 0 and 1.

b) Scenario 2: The bird continues to search but fails to find a better result. That is, the current position is the same as the previous position ($X_i^{iter}=X_i^{iter-1}$). The process is implemented based on Gaussian distribution:

$$X_i^{iter+1}=Gaussian(X_{best}^{iter},\ \xi) \quad (10)$$

Where $Gaussian(X_{best}^{k},\ \xi)$ denotes a Gaussian distributed random number with mean X_{best}^{k} and standard deviation ξ ; X_{best}^{iter} is the population optimal solution for iter iteration number.

$$\xi = (\log(iter)/iter)\cdot abs(X_{best}^{iter} - r_6 \cdot X_i^{iter}) \quad (11)$$

where r_6 is a random value and $\log(iter)/iter$ denotes the size used to adjust the standard deviation.

To prevent such ineffective searches, BFS introduces a boundary control policy:

$$X_{i,d}^{iter} = UB - r_7 \cdot (UB - LB) \quad if \quad X_{i,d}^{iter} < LB \ or \ X_{i,d}^{iter} > UB \quad (12)$$

where $X_{i,d}^{iter}$ denotes the position of the dth dimension of the ith individual at the iter iteration number and r_7 denotes the random value.

According to the optimisation strategy of the BFS algorithm, the pseudo code is shown in Table I.

TABLE I. BIRD FORAGING SEARCH ALGORITHM

	Algorithm 1: Bird Foraging Search Algorithm
1	Set the parameter values UB, LB, N and Max_iter;
2	Random initialisation of bird populations in the solution space;
3	iter=1;
4	While iter<=Max_iter do
5	// Perform flight search phase
6	Individuals are generated by logarithmic spiral flight;
7	// Behavioural stages in the field of implementation
8	/* Territorial birds */
9	Generate a new location for the territorial bird;
10	/* Invasive bird */
11	Calculate the new location of the invasive bird;
12	// Implementation of the cognitive-behavioural stage
13	Consolidation of stocks;
14	Detecting transgressive constraints;
15	Evaluate the new location of the individual bird, update the location
16	End while
17	Output the optimal solution.

C. BFS-ESN Method

In order to improve the feasibility and accuracy of SCADA software design test for oil and gas pipelines based on Java Web technology, this paper uses to optimise the hyperparameters of ESN network using BFS algorithm to construct the SCADA software design test model, and the specific structure is shown in Fig. 12.

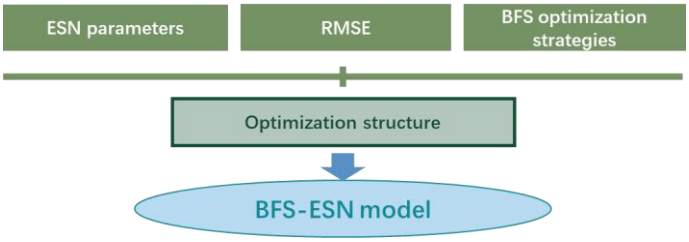


Fig. 12. BFS-ESN structure.

BFS-ESN uses ESN hyperparameters, i.e., storage pool size N_r , spectral radius SR , input scale factor IS , and storage pool sparsity SD as the optimisation variables, and the coding mode is real number coding mode, the specific coding structure is shown in Fig. 13.

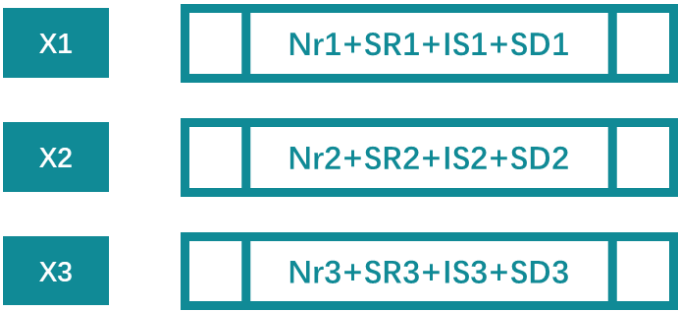


Fig. 13. BFS-ESN coding structure.

BFS-ESN uses RMSE as the optimisation fitness value and the on-the-fly search behavioural phase, domain behavioural phase, and cognitive behavioural phase of the BFS algorithm as the ESN optimisation strategy.

D. Test and Analysis Method for Designing SCADA Software

Taking the BFS-ESN model as the software testing model, in order to solve the oil and gas pipeline SCADA software design testing analysis, this paper proposes the oil and gas pipeline SCADA software design testing analysis method based on the BFS-ESN model, and the specific application flowchart is shown in Fig. 14. The application process of the BFS-ESN algorithm consists of the following processes: 1) According to the user's security and reliability of the system The application process of the BFS-ESN algorithm includes the following processes: 1) according to the user's demand for system safety and reliability, specify the actions and functions to be achieved by the control object; 2) design the topology of the SCADA system; 3) develop the front-end interface and the back-end logic of the SCADA software by using the JavaWeb technology; and 4) test the system by using the BFS-ESN model after the completion of the software development.

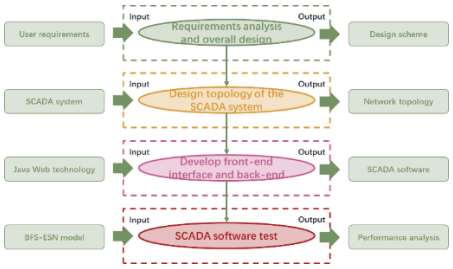


Fig. 14. Flow of BFS-ESN algorithm application.

IV. Results and Discussion

A. Experimental Set-up

In order to verify the effectiveness and feasibility of the method proposed in this paper, this paper adopts the oil and gas pipeline SCADA system software and related data as the analysis data, and selects PSO, DE, ABC, CS, GSA, FA as the comparison algorithms of hyperparameter optimisation of the ESN network, and the parameter settings of each algorithm are shown in Table II. The population sizes of PSO, DE, ABC, CS, GSA, FA algorithms are chosen as 100 and the maximum number of iterations is set to 1000.

TABLE II. Parameter Settings of the Optimisation Algorithm for the Comparison Model

Arithmetic	Parameterisation
PSO	w=0.6, c1=c2=2
DE	F=0.5, CR=0.9
ABC	limit=(N*D)/2, hired bees=scout bees=0.5N
CS	G0=100, α=20
GSA	β = 1.5, p = 0.25
FA	α = 0.2, β0 = 1 and γ = 1
BFS	Parameter-free optimisation algorithm

The experimental simulation system is Wins 10 and the programming language is Matlab2024a.

B. Analysis of Test Results

1) BFS optimisation performance analysis: In order to analyse the optimisation performance of BFS algorithms, in this section, the single peak benchmark functions (F01-F06) are used to analyse and compare the BFS, PSO, DE, ABC, CS, GSA and FA algorithms, and the basic information of the functions is shown in Table III.

The optimisation curves of the BFS, PSO, DE, ABC, CS, GSA and FA algorithms are given in Fig. 15. From Fig.15, it can be seen that in terms of convergence speed, BFS is significantly better than the remaining six algorithms; in terms of convergence accuracy, BFS is significantly better than the other optimisation algorithms.

TABLE III. Test Function Description

Test function	name (of a thing)	dimension (math.)	realm	optimum value
F01	Sphere	30	[-100,100]	0
F02	Schwefel2.22	30	[-10,10]	0
F03	Schwefel 1.2	30	[-100,100]	0
F04	Schwefel2.21	30	[-100,100]	0
F05	Rosenbrock	30	[-30,30]	0
F06	Step	30	[-100,100]	0

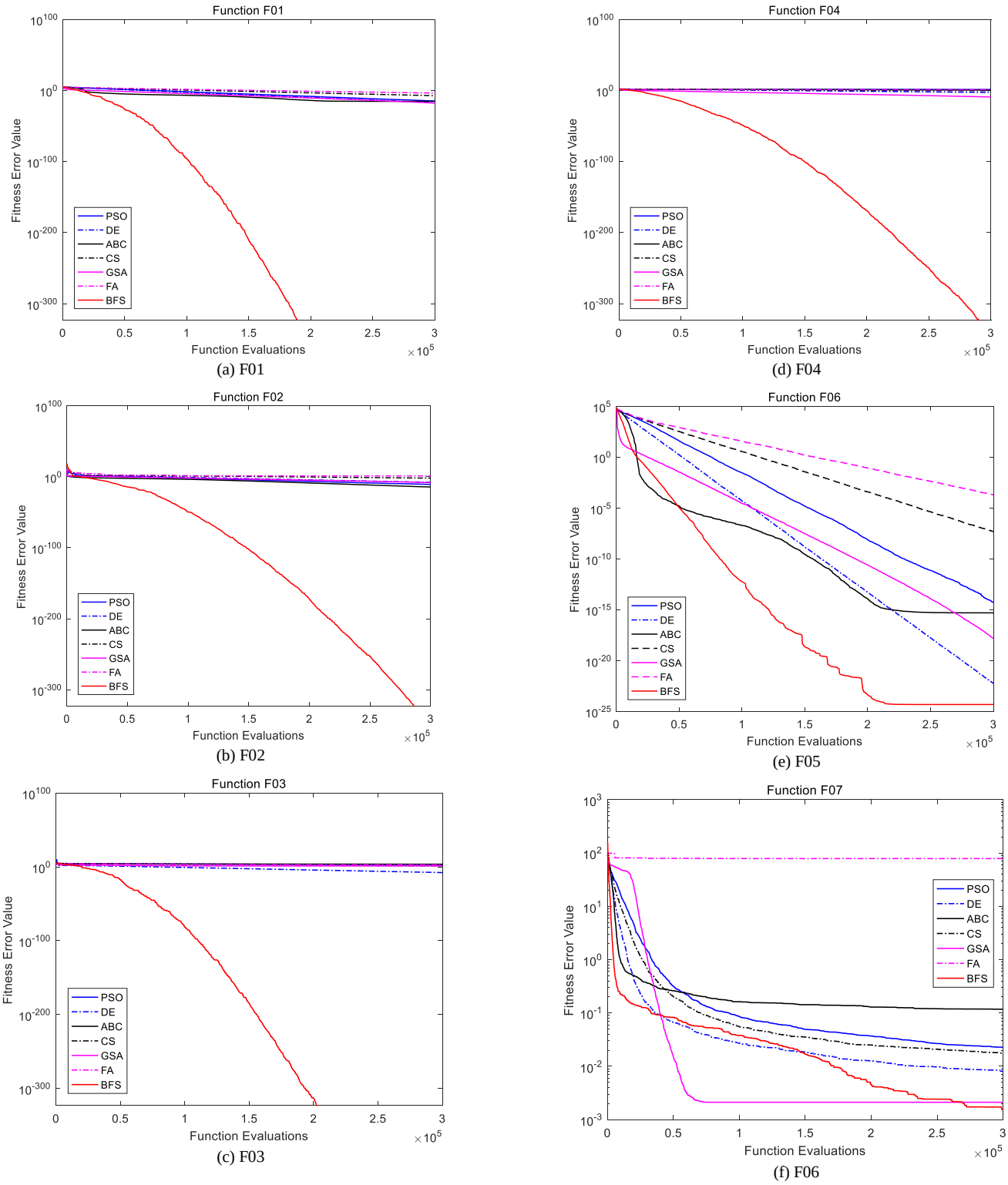


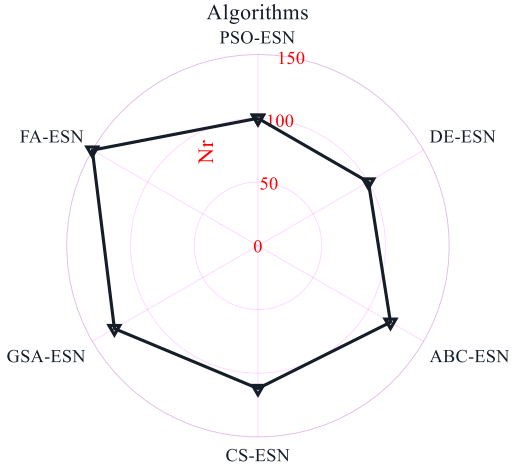
Fig. 15. Flow of BFS-ESN algorithm application.

2) Java web design software effectiveness analysis: Using Java Web technology, this paper designs SCADA system software for oil and gas pipelines, and the specific effect diagram is shown in Fig. 16. As can be seen from Fig. 16 the oil and gas pipeline SCADA system software achieves the functions of real-time data acquisition, monitoring, control and data analysis.

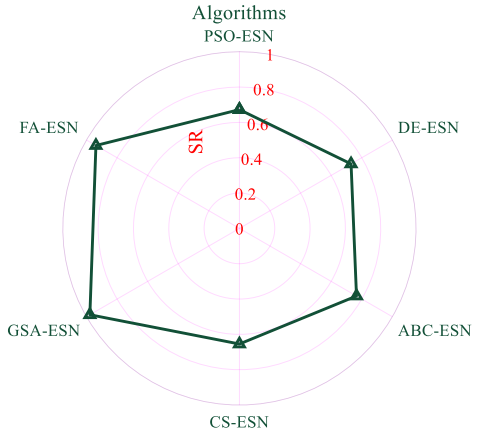
Fig. 16. Flow of BFS-ESN algorithm application.

3) SCADA software test and analysis: In order to verify the validity and feasibility of the SCADA software testing and analysis method based on the BFS-ESN model, this section uses PSO, DE, ABC, CS, GSA, FA algorithms to optimise the ESN model for comparative analysis with the BFS-ESN, and the results are shown in Fig. 16 and Fig. 17.

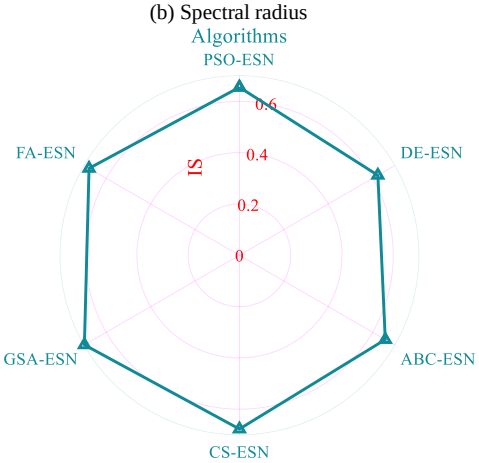
Fig. 17 gives the results of optimising the ESN hyperparameters for the comparison algorithms. As can be seen from Fig. 17, the results obtained by BFS for optimising the hyperparameters of the ESN model are as follows: storage pool size $N_r = 150$, spectral radius $SR = 0.9381$, input scale factor $IS = 0.6772$, storage pool sparsity $SD = 0.4951$.



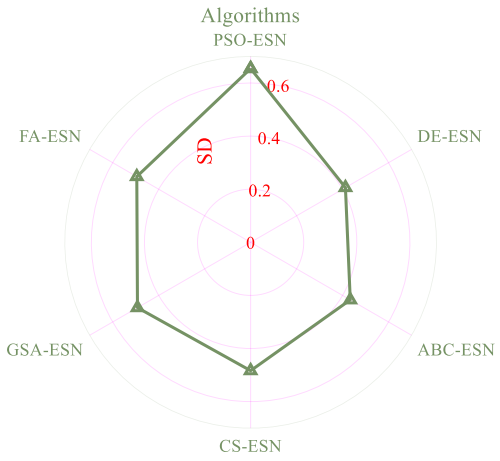
(a) Size of storage tanks



(b) Spectral radius



(c) Input scale factor



(d) Sparsity of storage tanks

Fig. 17. Contrasting algorithms to optimise ESN hyperparameters results.

The optimisation iteration curves of the compared algorithms are given in Fig. 18. From Fig. 18, it can be seen that the test accuracy of SCADA software design for oil and gas pipelines in Java Web framework based on BFS-ESN model is better than other algorithms, the optimisation iterations converge faster than other algorithms, and an accuracy of 97.33% is obtained at 700 iterations.

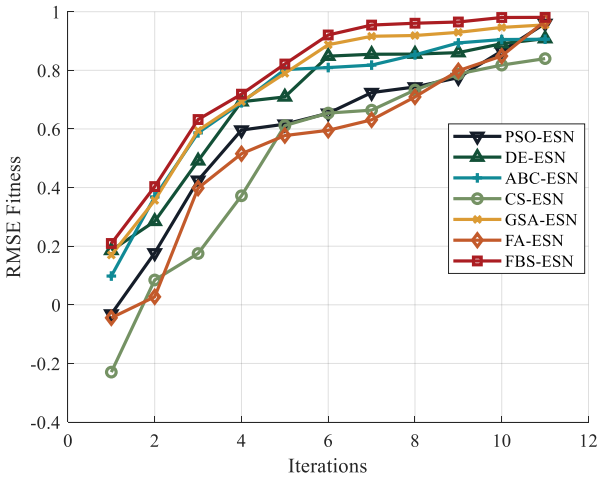


Fig. 18. Contrasting algorithm optimisation iteration curves.

V. Conclusion and Outlook

This paper presents the design and testing methods for oil and gas pipeline SCADA software based on JavaWeb technology, with the aim of improving accuracy, efficiency, and real-time data monitoring. The key innovation lies in the integration of the Bird Foraging Search (BFS) algorithm with the Echo State Network (ESN) to optimize the SCADA software design and testing process.

1) The paper outlines a multi-tiered software architecture using Java EE technologies to ensure the efficient operation of SCADA systems for oil and gas pipelines. The design includes real-time data acquisition, monitoring, control, and data analysis functionalities.

2), A novel combination of the Bird Foraging Search algorithm and Echo State Network is proposed to optimize the software testing process. This method enhances accuracy and convergence speed in SCADA system testing, outperforming other algorithms like PSO and DE.

3), Experimental results using actual SCADA data confirm the feasibility of the BFS-ESN model, showing significant improvements in testing accuracy, reaching 97.33% accuracy with faster convergence rates compared to traditional methods.

We also find some shortcomings: Firstly, the validation is based on specific SCADA data from oil and gas pipelines, which may limit the generalizability of the proposed method to other industrial applications. Secondly, while the model improves accuracy, its complexity might pose challenges in real-world implementation, particularly in terms of computational resource requirements. Finally, although the paper discusses system security briefly, the analysis of potential cybersecurity risks and scalability issues, particularly in larger pipeline networks, is not fully explored.

Future studies could extend the BFS-ESN approach to different SCADA systems in industries beyond oil and gas, to verify its broader applicability and performance. Reducing the computational complexity of the BFS-ESN model to make it more suitable for large-scale deployments in real-time environments. Exploring the integration of advanced security protocols and testing methods could strengthen the robustness of SCADA systems against potential cyber threats.

References

[1] Chen X. Zhou F., Hao X., Gong X., Lin X. Development Status, Challenges and Suggestions of SCADA System in China[J]. Industrial Technology Innovation, 2015, 2(1): 103-114.

[2] Moynihan B , Tronci E M , Hughes M C ,Moaveni B, Hines E.Virtual sensing via Gaussian Process for bending moment response prediction of an offshore wind turbine using SCADA data[J].Renewable Energy, 2024, 227.

[3] Deshpande S N , Jogdand R .A novel scheduling algorithm development and analysis for heterogeneous IoT protocol control system to achieve SCADA optimization: a next generation post covid solution[J].International Journal of Information Technology, 2023, 15:2123 - 2131.

[4] Gill S .SCADA/HMI software market to grow and drive digital transformation[J].Control Engineering Europe, 2023(05).

[5] Morrison R , Liu X , Lin Z .Anomaly detection in wind turbine SCADA data for power curve cleaning[J].Renewable Energy, 2022, 184.

[6] Rabie O B J , Balachandran P K , Khojah M , Selvarajan S. A Proficient ZESO-DRKFC Model for Smart Grid SCADA Security[J].Electronics, 2022, 11(24):4144 .

[7] Ma J , Yuan Y .Application of SCADA data in wind turbine fault detection - a review[J].Sensor Review, 2022.

[8] Mckinnon C , Tartt K , Carroll J , Mcdonald A. Comparison of novel SCADA Data Cleaning Technique for Wind Turbine Electric Pitch System[J]. Physics: Conference Series, 2022, 2151(1).

[9] Chretien A , Tahan A , Pelletier F .Wind Turbine Blade Damage Evaluation under Multiple Operating Conditions and Based on 10-Min SCADA Data[J]. energies, 2024, 17(5).

[10] Zhang G , Li Y , Zhao Y .A novel fault diagnosis method for wind turbine based on adaptive multivariate time-series convolutional network using SCADA data[J].Advanced Engineering Informatics, 2023.

[11] Dao P B , Barszcz T , Staszewski W J .Anomaly detection of wind turbines based on stationarity analysis of SCADA data[J].Renewable Energy, 2024, 232.

[12] Zhang L , Zhu H .A Simple Method of Non-Intrusive Load Monitoring Based on BP Neural Network[J].Journal of Physics: Conference Series, 2022, 2237(1) :012010.

[13] Laxmisagar H S , Hanumantharaju M C .FPGA implementation of breast cancer detection using SVM linear classifier[J].Multimedia Tools and Applications, 2023:1-24.

[14] Diqi M , Ordiyasa I W .Enhancing Stock Price Prediction in the Indonesian Market: a Concave LSTM Approach with Runrelu[J]. Mobile Robotics and Intelligent Systems, 2024, 18(3):69-77.

[15] Dbrowski T , Bednarek M ,A. Rosiński, Olchowik W.Engineering Application of a Product Quality Testing Method within the SCADA System Operator Education Quality Assessment Process[J].Applied Sciences, 2023.

[16] Ma Z F, Han J. J., Wang B , Zhang B, Sun K , Chen X. Ground resistance prediction of transmission line based on IPSO-NESN algorithm[J]. Intelligent Power,2024,52(06):116-122.

[17] Zhang Z, Huang C, Dong K, Huang H. Birds foraging search: a novel population-based algorithm for global optimisation[J]. Memetic Computing, 2019, 11(3):221-250.

[18] Wang F., Liu S. Java Web-based knowledge base management platform for optimised design of CNC machine tools[J]. Machine Tools and Hydraulics, 2022, 50(20):82-89.

[19] Wang J. , Gong J. X , Lin Z Q, Zhang X J. A multidimensional depth oriented fuzzy testing approach for Java Web[J]. Information Network Security, 2024(2):282-292.

[20] Huang H, Zhang W, Qi G. C. , Yan F , Chen P. Security Risks of Data Transmission in SCADA System of Oil and Gas Pipelines and Their Solutions[J]. Natural Gas Industry, 2013, 33(11): 115-120.

[21] Liu B , Zhang M. Design and application of SCADA system based on multi-control platform[J]. Electrotechnology,2023,(10):8-13+16.

[22] Bai Y. R., Lun S. X. Optimising time series prediction of echo state networks based on war strategy algorithm[J]. Journal of Bohai University(Natural Science Edition),2024,45(02):154-160.

[23] Guo Q. H., Lin H. Z., Li Y., Xie L. L., Liu T. Y. Short-term electricity price prediction based on NGO-VMD-SSA-ESN[J]. Electrotechnology,2024,(02):130-136.

Cyber Resilience Model Based on a Self Supervised Anomaly Detection Approach

Eko Budi Cahyono[1], Suriani Binti Mohd Sam[2], Noor Hafizah Binti Hassan[3], Amrul Faruq[4]
Faculty of Artificial Intelligence, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia[1, 2, 3]
Faculty of Engineering, Universitas Muhammadiyah Malang, Malang, Indonesia[1, 4]

***Abstract*—Cyber resilience plays an important role in dealing with cybersecurity and business continuity uncertainty in the post-COVID-19 era. The fundamental problem of cyber resilience is the complexity of real-world problems. Therefore, it is necessary to reduce the complexity of real-world problems to be simple and easy to analyze through cyber resilience model. The first part is the representational model by utilizes world models. It utilizes the stochastic nature of latent data to generate log-likelihood values by data-generating process. The second part is the inference model. This concludes the observation of log-likelihoods using a self-supervised anomaly detection approach. This is related to optimizing decision boundary in anomaly detection, which is achieved by supervising two competing hypotheses based on bias-variance alignment and likelihood ratios. The optimization operates a dynamic threshold supervised by a supervisory signal from the underlying structure of log-likelihoods. The paper contributes by conducting research on the cyber resilience model from the perspective of statistical machine learning. It enhances the representational modeling of world models with the Gaussian mixture model for multimodal regression (GMMR). Additionally, it examines the issue of misleading log-likelihood for out-of-distribution inputs caused by the generalization error and optimizes decision boundary in minimizing the generalization error with a new metric named the harmonic likelihood ratio (HLR). Finally, it aims to boost the performance of anomaly detection using self-supervised learning.**

Keywords*—Cybersecurity; anomaly detection; cyber resilience model; statistical machine learning; data generating process; bias variance alignment; likelihood ratios; self-supervised learning

I. Introduction

In the post-COVID-19 era, cyber resilience plays an important role in dealing with cybersecurity and business continuity uncertainty. The problems and methodology for cyber resilience, especially in the scope of small and medium enterprises (SMEs), have been described systematically in the cyber resilience progression model [5], [6]. The model helps SMEs prioritize cyber resilience proposing the natural evolution of implementation. It designed to be more flexible based on available resources. It focuses on insights into operationalizing cyber resilience strategies by describing ten domains. One of the ten domains is detection processes and continuous monitoring has been chosen as the central domain [4]. In description, it is explained that there are two strategies for this domain: actively monitor the company's assets and define a detection process that specifies when to escalate anomaly into incidents [5], [6]. This description allows self-supervised anomaly detection technology that works fully automatically to detect and monitor processes.

The cyber resilience model that will be studied refers to technical architectures in [4]. The technical architecture was built on five layers. The five layers were services, data, generative models, data analysis, and resilience scale [4]. Each layer had different structures and functions but was part of a system. The technical architectures are necessarily simplified without changing the fundamental architecture so that the complexity of the problem is reduced and more focused on anomaly detection. The fundamental architecture that continues to go is Gaussian mixture models (GMMs), one of the first-generation generative models with high flexibility in handling data distribution, statistical modeling, and inference. GMMs are the fundamental architecture of cyber resilience with the underlying structure of a probabilistic model approach [4]. However, GMMs fail if applied directly as the basis of cyber resilience model. GMMs fail in high-dimensional data. GMMs can be used for density estimation but the perfect density model cannot guarantee anomaly detection [23]. Also, GMMs work in an unsupervised setting that often produces high false positive rates in a dynamic system [28]. The paper studies GMMs as a reliable generative model for anomaly detection.

The cyber resilience model designed by a two-part model: the representational model in layers 1 to 3, which play a role in data collection, and the inference model in layers 4 and 5, which play a role in data analysis. The complexity of real-world problems of cyber resilience encapsulated by data collection and analysis as the key of a data-driven approach. The paper studies critically the problems of the representational and inference model to set up the appropriate cyber resilience model, such as misleading log-likelihood, the bias-variance alignment, and two competing hypotheses.

As the core of the representational model, the world model [14] that lies in layer 2 takes the principal role in data-generating process to strengthen a data-driven approach. Hence, it needs to be enhanced to become part of the representational model that meet the requirements for data collection in a new setting. That is different from it utilized previously. For developing the data-generating process, the world model needs to avoid generating misleading log-likelihood [3]. Also, it needs to be integrated in a supervised setting [11], [12] to align the self-labeling problem of an unsupervised learning algorithm [1], [28].

The inference model in layers 4 and 5 focuses more on inferring the observed samples with data analysis directed by anomaly detection. The concept of anomaly detection explains that samples can be distinguished into normal and anomaly

samples [28], [35] with a two-class decision boundary [1], [8] determined by two competing hypotheses [33], [41]. The factual problem is aligning a two-class decision boundary with two competing hypotheses so that the model can perform anomaly detection properly, which will be studied in this paper.

II. Review of Existing Techniques

One fundamental study as the basis of cyber resilience model is anomaly detection [4]. Anomaly detection, in this case, is similar tasks to novelty detection (ND) [1], one-class classification (OCC) [29], and out-of-distribution (OOD) [8], [27], [33], [41]. An anomaly is an observation that deviates significantly from some concepts of normality [35]. This definition is also suitable for ND, OCC, and OOD [16], [35]. If the distribution of normal instances is P, an anomaly is a sample drawn from any distribution other than P. Furthermore, ND has a new region of P; OCC has a one-class decision boundary of P; OOD has fine-grained P during training [28], [35]. Thus, there is a shared concept between anomaly detection and ND, OCC, OOD.

The cyber resilience model represents a cyber resilience system as a technical framework to measure the resilience scale. The resilience scale denotes a scale of the service resilience against cyber threats. In the domain of cyber resilience, numerous services like Domain Name System (DNS), firewall, web services, resource planning, and supply chain are required to explore anomaly detection for monitoring the continuity of services. It is necessary for one specific service to bring about the model as suggested in [4] which points to DNS. This choice is reasonable because DNS used by most services and applications of the Internet, even critical infrastructures of the Internet. Also, DNS provides an authentic data distribution of anomalies by the system so that anomaly detection works in factuality. DNS is the hierarchical name system that uses the globally distributed database and stores the information about every Internet domain [39]. DNS information is stored on DNS servers and can be accessed anytime based on user queries. DNS is like a phone book. It contains addresses that make it easier for users to access the Internet in cyberspace. Each address has a unique identity and is different from one another. This identity is called an Internet Protocol (IP) address. DNS translates these numbers into names because IP addresses are complicated for users to remember. DNS is made simple to solve IP address resolution issues, however, it does not come with a security proficiency by nature [4]. Therefore, a DNS measurement method is needed to enable security proficiency by design.

DNS measurement methods are categorized into two types: passive and active DNS. Passive DNS [39] allows observation of DNS ecosystem limited to clients, resolver servers, authoritative servers and the networks between the three. Active DNS allows observing a global hierarchical DNS ecosystem. It involves very large DNS networks. It does not pay attention to the complete contents of the query and response from a particular client, so it has difficult to apply for data collection and analysis. The mechanism for DNS queries only supports one type of query. One query of the domain name and one response of an IP address. Other lookup keys must be converted to domain names before being used in DNS queries. Thus, passive DNS provides advantages over active DNS in reconstructing specific queries/responses useful for anomaly detection.

Passive DNS, as a local representative of the active DNS ecosystem, contributes to efficient traffic data collection. Many DNS traffic analysis uses passive DNS including anomaly detection. The earlier DNS anomaly detection is based on supervised model. The model produce high precision, low false positive rates, and efficient anomaly detection in specific patterns [28]. However, the model depend on training data. The ability to recognize anomaly patterns depends on the anomaly patterns that have been trained during training time [16], [28], [35]. The trained anomaly patterns are limited to the capacity of datasets. While DNS ecosystem is always evolving, threats to DNS security never stop, and DNS resilience needs to be monitored continuously. Therefore, supervised models are less suitable for DNS traffic anomaly detection in dynamic real world environments.

Since DNS traffic is dynamic, unsupervised model is inherently suitable for anomaly detection. Labeling normal and anomaly traffic are not necessary during training time. The model accepts all types of unlabeled traffic and classify it with certain rules into two classes that can distinguish normal or anomaly traffic. The model does not depend on training data [16], [28], [35]. The ability to recognize anomaly patterns does not depend on the trained anomaly patterns during training time. The model can recognize new anomaly patterns using a classifier algorithm. However, the model often produces high false positive rates and fails to recognize patterns from the genuine labeled data [28]. The model's ability to recognize normal and anomaly patterns is not as precise as the supervised model because there is no strong connection between the model and the genuine labeled data [28]. In this model, the genuine labeled data is not defined. Normal and anomaly labels are not explicitly defined.

A machine learning algorithm that makes use of the structure within data for self-labeling is self-supervised model [16], [32]. Self-supervised model has been designed as a hybrid approach of supervised and unsupervised models. The model produces pseudo-labels, but the model directs pseudo-labels to follow the underlying structure of the genuine labeled data. Anomaly detection can utilizes self-supervised model based on likelihood ratios [32], [33], [41]. Likelihood ratios can manage the relationship between supervised and unsupervised models. Likelihood ratios have signal to measure the performance of regression and classification functions in a supervised setting [19], [22], [25], [37]. Likelihood ratios also have signal to control self-labeling in an unsupervised setting [1], [2], [19], [21], [33], [41].

III. Methodology

Cyber resilience plays an important role in facing business continuity uncertainty. Outside of business matters, business continuity uncertainty can be affected by data uncertainty in data collection and analysis. Various sources, such as noisy data, incomplete data, sampling errors, measurement errors generalization errors, and anomalies, which will cause data uncertainty. It is necessary to manage data uncertainty to

improve the reliability of data collection and analysis. One of the approaches chosen to address the problem of data uncertainty is to study anomaly detection in more depth. It has several indicators that will be used to obtain reliable data collection and analysis. The indicators are bias, variance, and likelihood ratios.

This section explains the research methodology of cyber resilience model, consist of the representational model to realize reliable data collection using data-generating process and the inference model to realize reliable data analysis based on likelihood ratios. Process flow diagram of the methodology as seen in Fig, 1.

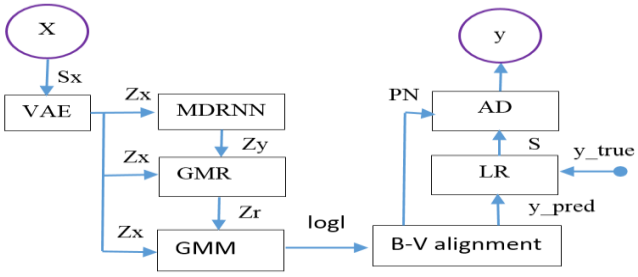


Fig. 1. Process flow diagram of the methodology.

A. Characteristics of Raw Datasets

The raw dataset is a collection of data from a network capture-based DNS logger. The raw dataset was taken from November 2018 to February 2020 on DNS servers (dnsanalyzer.info) amount 1,000 samples (Sx). The tool used to collect the raw dataset is GoPassiveDNS [26].

The raw dataset contains three feature vectors (X): TTL (x_1), latency (x_2), and throughput (x_3). The K-Means algorithm was used to collect data for classifying positive and negative classes from the raw dataset. The negative class have fine grain structure with two type subdistributions: the sample variance of subdistributions in one standard deviation (inliers) and the sample variance of subdistributions more than two standard deviations (outliers). Inliers of the negative class represent DNS normal. Inliers of the negative class have the lowest anomaly level in the resilience scale. The positive class have fine grain structure with three type subdistributions: the sample variance of subdistributions in one standard deviation (inliers), the sample variance of subdistributions more than two standard deviations (outliers), and anomaly. Anomaly refers to the response of RCODE more than 0 (zero) by GoPassiveDNS. RCODE more than 0 indicates DNS failure [26]. Otherwise, RCODE equal to 0 indicates DNS normal. The anomaly subdistribution have the highest anomaly level in the resilience scale.

The raw dataset exhibit different data characteristics named the generator of in-distribution, which is the source of normal datasets, and the generator of out-of-distribution, which is the source of anomaly datasets. The raw dataset needs to be further processed to generate reliable datasets.

TABLE I. CHARACTERISTICS OF RAW DATASETS

Datasets	In distribution		Out-of-distribution		
Classes	Negative		Positive		
Types	Inlier	Outlier	Inlier	Outlier	Anomaly
Variances	≤68%	>95%	≤68%	>95%	-
RCODE	0	0	0	0	>0
Subdistributions	1	2	3	4	5
Samples	500	25	75	200	200
Anomaly levels	1	2	3	4	5

Table I presents two sources of raw datasets: In-distribution (ID) and out-of-distribution (OOD). The ID dataset comes from the generator of in-distribution. The OOD dataset comes from the generator of out-of-distribution. Conceptually, the two generators should produce different two sources of datasets and naturally not overlap each other. However, in practice, the two generators cannot avoid producing two overlapping datasets.

Table I explains that the overlap occurs due to the two approaches taken in data collection. The first approach, data collection uses DNS sensors. The sensors are limited in representing data from the real world with only three feature vectors. The sensors are also limited in responding accurately to RCODE. Furthermore, the sensors can only classify DNS events by default based on the value of RCODE.

TABLE II. DNS RESPONSE CODE

RCODE	**Message**	**Description**
0	NOERROR	DNS query completed successfully
1	FORMERR	DNS query format error
2	SERVFAIL	Server failed to complete the DNS request
3	NXDOMAIN	Domain name does not exist
4	NOTIMP	Function not implemented
5	REFUSED	The server refused to answer for the query
6	YXDOMAIN	Name that should not exist, does exist
7	XRRSET	RRset that should not exist, does exist
8	NOTAUTH	Server not authoritative for the zone
9	NOTZONE	Name not in zone

Table II defines the DNS response code which have been implemented in GoPassiveDNS [26]. It describes RCODE values of the various types of DNS events that occur most

frequently. Refers to Table I that RCODE produces high false negative rates. Subdistribution 1, 2, 3, and 4 are classified as DNS normal even though some are DNS failure according to K-Means. In contrast, the second approach, data collection uses K-Means to classify two different datasets. Table I shows that K-Means produce high false positive rates. Subdistribution 3, 4, and 5 are classified as the positive class even though some are the negative class according to RCODE. The problem of the first approach is that normal and anomaly labeling in the raw dataset is based on RCODE even though many failure functions cannot be recognized by RCODE. The second approach uses the algorithm of machine learning. The K-Means is the simplest unsupervised learning algorithm for basic self-labeling. It can be utilized to classify the raw dataset into two classes on a specific rule.

It is a similarity between the two approaches. None of anomaly samples in subdistribution 5 that has been classified by the first approach are part of normal samples that has been classified by the second approach. In other words, anomaly samples from the first approach is the same as anomaly samples from the second approach. So, it is concluded that the classification of one sample as anomaly and another sample as not anomaly is true. However, there are anomaly samples from the second approach that are not anomaly samples from the first approach such as samples in subdistribution 3 and 4. Therefore, the first approach is not able to recognize new patterns of anomaly other than those already recognized by RCODE. This urges the use of machine learning algorithms to better recognize new patterns of anomalies. Meanwhile, the second approach is able to recognize new patterns of anomaly other than those already recognized by the first approach. However, not all of the new anomaly patterns of the second approach are true due to the limitations of K-Means based on a specific shape of the decision boundary and no training to do for anomaly samples.

B. Data Collection

The representational model are useful in improving the reliability of data collection. The reliability of data collection is improved by modeling the raw dataset into latent samples (Zx), a sequence of latent samples (Zy), and a density of latent samples (logl).

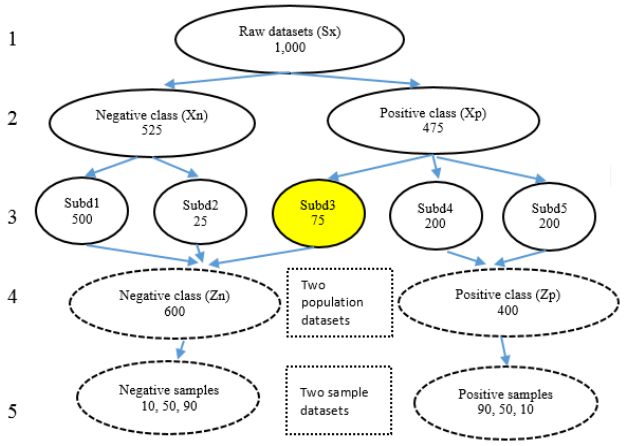


Fig. 2. Process flow diagram of data collection.

Fig. 2 describes process flow diagram of data collection which consists of five steps. The first step is initial data collection which produces raw datasets as 1,000 samples (Sx). The samples are a data distribution of 200 data points so raw datasets are 200,000 data points in size. The samples are designed as a data distribution to understand the underlying generator of datasets through latent variable models. The samples have parameters from a data distribution that show the principal component of datasets.

The second step classifies positive (Xp) and negative (Xn) classes from raw datasets using the K-Means algorithm. The positive class are samples that assert the presence of anomaly. The negative class are samples that assert the absence of anomaly. The K-Means algorithm succeeded in classifying raw datasets into 525 negative samples and 475 positive samples from selected samples.

In the third step, each class is divided into two subdistributions, namely inliers and outliers, so that in total there are four subdistributions plus one specific subdistribution produced by DNS sensors as the ground truth of anomaly samples. So the total becomes five subdistributions, each of 500, 25, 75, 200, and 200 selected samples respectively. Inliers and outliers are formed using an outlier detection technique [42].

The fourth step as the key of reliable data collection is processes that generate data specifically event, memory, and density processes. The three processes set up the data-generating process properly. A detailed explanation of each process is in the following subsection. Furthermore, one sample subdistribution differs from another. It estimated by the Expectation-Maximization (EM) algorithm [9].

TABLE III. EM AS A SAMPLE CLASSIFIER

	subd2	**subd3**	**subd4**
subd1	1.419	2.949	5.026
subd5	5.423	3.893	1.816
DI	4.004	0.944	3.210

abbreviations: subd = subdistribution, DI = difference index

Table III explains the process of classifying normal and anomaly samples using EM. Two polars are defined as the centroids of normal and anomaly classes. Subdistribution 1 with the lowest anomaly level selected as the polar of normal class. Subdistribution 5 with the highest anomaly level selected as the polar of anomaly class. The smaller difference between a subdistribution and two polars defines the label of subdistribution. As subdistribution 2 and 3 are closer to subdistribution 1 than 5, subdistribution 2 and 3 are classified as normal class. As well subdistribution 4 is closer to subdistribution 5 than 1, subdistribution 4 is classified as anomaly class. It can be seen that K-Means and EM are the same in classifying subdistribution 1, 2, 4, and 5 but different in classifying subdistribution 3. K-Means classify subdistribution 3 as anomaly class while EM classify subdistribution 3 as normal class. K-Means classify patterns with a specific shape for all subdistributions, while EM classifies patterns dynamically following the underlying

structure of each subdistribution. It seems EM is more flexible than K-Means. EM is not limited by shape but depends on unobserved latent variables performed properly by data-generating process.

The output of data-generating process is primary datasets (logl) that consist of 1,000 samples treated as a population of observation. The samples come from five subdistributions of raw datasets, each of 500, 25, 75, 200, and 200 respectively. In the last step, the observation sample is generated as a random variable of normal and anomaly samples. One hundred random variables configure the observed samples that are taken randomly from the population. Be appointed, the sample size is 10% of the population provided for any observation. The data-generating process will consider data collection more appropriate as required.

C. The Event Process

The event process is the first part of data-generating process. It encodes DNS events into a latent variable model. It reproduces the idea from the world model [14] that pattern recognition was performed indirectly through a latent variable model. The model in latent space provides more advantages than in data space. The pattern encoded as a principal component is more concise. The principal component has information sufficiency that can be further encoded in another process smoothly, so it is easier to analyze in the next part of data-generating process. VAEs take the task of encoding for a latent variable model.

Variational autoencoders (VAEs) are an artificial neural network architecture in which the latent space has good properties to enable generative processes [21] utilizing stochastic backpropagation [34]. It plays a role in transforming data distribution in data space (X) into data distribution in latent space (Zx) by the latent variable model. It recognizes the characteristic of data distribution through EM by estimating the joint distribution between X and Zx [9]. EM will maximize the similarity between the two. If the joint distribution Zx is a close approximation of X, then Zx will be indistinguishable from X. Analysis of compressed data distribution produces a principal component. This is called dimensionality reduction. Principal components in latent space are more ready to use to recognize the behavior of data distribution than feature vectors in data space. It summarize the pattern of data distribution without eliminating the principal information substance.

VAEs use two neural networks: encoder (generative model) and decoder (variational approximation) [21]. The encoder part transforms samples of discrete data distribution from DNS events into continuous latent variables by taking the characteristic of probability distribution. In this case, probability distribution as the core of a latent variable model that has two parameters: mean (μ) and standard deviation (Σ). The mean represents the expected value of DNS events, and the standard deviation represents the variability of DNS events. The type of probability distribution to generate the latent sample is Gaussian distribution. So, a latent variable model may be called a Gaussian model. The use of VAE encoder as a generator of latent samples refers to the vision model of world models [14].

One important component of neural networks that quantifies the difference between the predicted and actual outputs is the loss function. There are two loss functions for VAEs: Mean Square Error (MSE) and Kullback–Leibler Divergence (KLD). These two loss functions are standard for measuring how fit a model explains the data. The decoder part reconstructs latent samples into the predicted outputs (S'x). In the experiment, the decoder part is only needed at training to measure how fit a Gaussian model has been encodes DNS events by comparing the difference between the predicted and actual outputs (S'x-Sx). Flow diagram of VAEs as seen in Fig. 3.

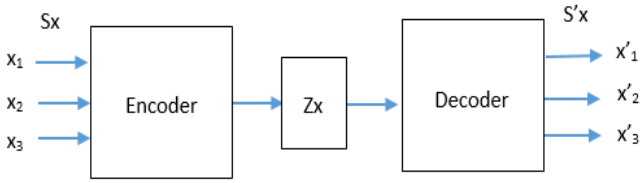


Fig. 3. Flow diagram of VAEs for the event process.

The performance of training can be evaluated from training and testing loss. Suppose the loss gets smaller for larger epochs, the loss shift convergence to a specific value, testing loss is smaller than training loss, that are indicating that VAE training has achieved appropriate performance tasks. Latent variables at training are set to $\mu + \Sigma \times \varepsilon$. The ε is random noise added to the latent variable so that the loss will always converge to a specific value [21], [34]. Some of the reasons testing loss is smaller than training loss are that at training: (1) the latent variable overloaded with random noise, whereas, at testing, it does not, (2) testing loss measured after training, and (3) training loss measured for all epochs while testing loss measured once after completing the training epoch. However, training and testing loss are limited to optimizing the loss function in estimating the difference between the actual (Sx) and predicted (S'x) DNS events and not optimizing model parameters. The model parameter is optimized by the architecture of encoder and decoder, hyperparameter tuning, and using more flexible prior distributions. This means that the model parameter of training is better than those of testing because it is used as a reference for testing. The performance of VAEs training as seen in Fig. 5(a).

VAEs are built with one input layer for three feature vectors, two hidden layers, each with sizes 64 and 16, and one output layer for training purpose only. One data distribution of the input layer come from two hundred data points. One latent sample is composed of two hundred latent vectors, in other words, the two hundred dimensions of Zx. Then, a μ vector of length two hundreds and a Σ vector of length also two hundreds, so the VAE parameters are four hundreds. In these configuration, two hundred latent vectors are a good sample size to reduce the log-likelihood of sampling errors. The observed samples need to be ensured to be independent (one discrete data of DNS events does not depend on other discrete data of DNS events in the same data distribution) and identically distributed (in one data distribution of DNS events, the probability distribution of data distribution is the same).

Consequently, a latent sample which generated by the model meets the criteria of independent and identically distributed (i.i.d) as a stochastic random sample, making it well-suited for addressing an observation sample of DNS events in latent space.

D. The Memory Process

The memory process is the second part of data-generating process that play a role in encoding a sequence of latent samples from the event process into a latent dynamics model. A latent sample which is the output of the event process does not have the sequence because it is an i.i.d sample. Meanwhile, one observation consists of many latent samples to form a sequence. The event process needs to be extended with another process called the memory process so that it can encode the sequence. Hence, the memory process is an extended event process.

Mixture density-recurrent neural networks (MDRNNs) are one specific neural network architecture that combines mixture density networks (MDNs) and recurrent neural networks (RNNs) to build a latent dynamics model. MDNs encode the output of a neural network parametrize a mixture of Gaussian distribution, which can model general conditional probability densities [2]. RNNs are an artificial neural network architecture of dynamic models that have been used to generate sequences [13], [15]. Dynamic models simplified representations of real-world problems by algorithms, such as dynamic models of signal processing, automatic speech recognition (ASR), and time-series forecasting. As a sequence generator, MDRNNs encode a sequence of latent samples Zx generated by a Gaussian model to latent samples Zy generated by a latent dynamics model. The use of MDRNNs as a sequence generator refers to the memory model of world models [14].

RNNs are used as the forefront of a sequence generator. RNNs have a recurrent layer (a cell) to remember its previous inputs by internal memory. A recurrent layer works with iterative sampling from the output, then feeding in the sample as input at the next step [13]. The problem with standard RNNs is that it is used only for basic sequential data tasks and cannot be used to store information about previous inputs for a very long time [13]. Hence, a type of RNNs called long short-term memory networks (LSTMs) [15] was designed to address the problem of standard RNNs. LSTMs can be used for advanced sequential data and artificial long-time lag tasks [15], such as tasks to predict a sequence of latent samples, and then store information in internal memory with memory cells and gating mechanisms for long-term. Memory cells store information from the previous step and use it to update the cell output for the current step. Gating mechanisms remove unimportant information, store new information, and encode information from the cell state to the output layer.

Practically, LSTMs need MDNs for modeling advanced sequential data. LSTMs and MDNs are compatible with each other. MDNs consist of two components: a feed-fordward neural network and a mixture model [2]. The output layer of LSTMs is the final layer of a feed-fordward neural network and a fully connected layer that connects all units in the layer directly to every unit in the previous layer, so it can be utilized as an interface between LSTMs and MDNs.

MDNs can smoothly encode the outputs of LSTMs to form the parameters of a mixture model, generally with Gaussian models for each mixture component [2], [10]. These parameters are mean (μ), standard deviation (Σ), and weight (π). The mean represents the expected value of DNS events, the standard deviation represents the variability of DNS events, and the weight represents mixing each Gaussian distribution of DNS events into a mixture distribution. These parameters involve shaping probability density functions (PDFs) for each mixture component and categorical distribution from the mixture weights [2], [10]. Additionally, there are two reasons why LSTMs require MDNs: different mixture components represent different stochastic events and different situations [10]. In other words, MDNs are able to model different stochastic events and situations for any DNS events in Gaussian models for each mixture component. Therefore, LSTMs and MDNs can seamlessly work together in MDRNNs. Flow diagram of MDRNNs as seen in Fig. 4.

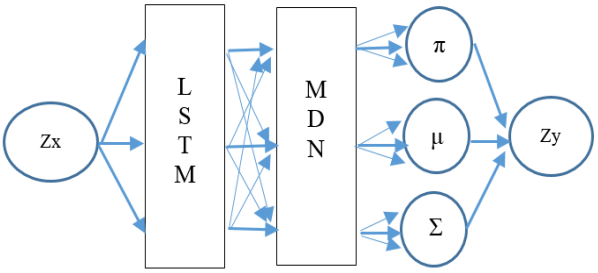


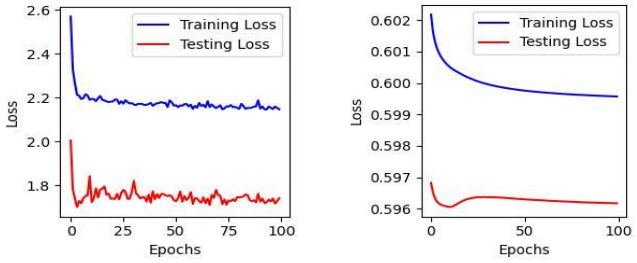
Fig. 4. Flow diagram of MDRNNs for the memory process.

One observation consists of some latent samples. In a sequence, one latent sample is related to other latent samples. MDRNNs training recognize the underlying generator of a sequence by making relationships between one sample and another using a time-series regression approach. Some samples are treated as independent variables, while the dependent variable is taken from the independent variable itself which has been shifted in a sequence. In this case, the independent variable is Zx while Zy is constructed from shifted Zx with a sequence length of four.

LSTMs have been applied to realize this time-series regression. Because LSTMs can memorize previous input, then for each latent sample, MDNs would encode the output of LSTMs into a mixture component that was a combination of individual distributions in the form of a mixture distribution. To identify that MDRNNs training has been able to recognize the underlying generator of a sequence, it was evaluated using the logsumexp function. The logsumexp function is a smooth approximation to the maximum function in a logarithmic scale. This provides a numerically stable estimation of PDFs for each sequence and sample. The logsumexp is used to measuring the similarity between the sequence and sample by maximizing the log-likelihood.

MDRNNs are built with one input layer, a single hidden LSTM layer, the output layer of LSTMs as the input of MDNs, a sequence length is four at training time, and a

mixture distribution from three Gaussian distributions as a mixture model. Three Gaussian distributions were chosen because the input distribution is not complex, it only consists of three feature vectors. One data distribution of the input layer comes from two hundred latent vectors. A single hidden layer with sixteen units is enough to perform computations on the input which consists of two hundred latent vectors. MDNs aim to model a sequence of latent samples that can be drawn from one of several possible distributions with a certain probability. Several possible distributions come from three Gaussian distributions. Each parameter of three Gaussian distributions needs two hundred vectors, so MDNs parameterize 3×3×200 = 1,800 parameters. These parameters will generate two hundred latent vectors as the output of MDRNNs (Zy). MDRNNs training uses the data of VAEs training so that the performance of MDRNNs training follows of VAEs training such as shown in Fig. 5.



a. The performance of VAEs training b. The performance of MDRNNs training

Fig. 5. The performance of VAEs and MDRNNs training.

E. The Density Process

The density process is the last part of data-generating process that play a role in producing the density (logl) from a sequence of latent samples. The density process works to enhance the density of the memory process. The memory process is designed to encode a sequence of latent samples, not the density. It is not sufficient to produce reliable density because a standard MDN as part of the memory process is prone to mode collapse [25]. Mode collapse happens when a standard MDN fail to generate data samples from the underlying probability distribution of Zx. It will turn multimodal learning [38] into unimodal so that all of the generated samples are very similar [25]. To overcome the problem, a joint distribution was built on Zx and Zy, denoted p(Zx, Zy). In this case, Zx and Zy represent the input and target variables respectively. The relationship between the input and target variables has been initialized by LSTMs in the memory process through time-series regression. It is the conditional distribution, which is the probability that Zy happens given Zx has happened, denoted p(Zy|Zx). It is created to build a more proper regression that is the joint probability density functions (joint PDFs). All the statistical information of the input and target variables is stored in the joint PDFs [37]. Furthermore, learning the joint PDFs of the input and target variables is a form of supervised learning [12]. It is a statistical approach to transform from unsupervised learning of the event process, denoted p(Zx), into supervised learning of the density process, denoted p(Zx, Zy). The joint PDFs and the conditional distribution are the statistical basis for multimodal regression.

An important factor in the joint PDFs is to predict target variables from input variables. A type of supervised learning algorithm that has been used to predict target variables from input variables as part of the joint PDFs is Gaussian mixture regression (GMR) [11], [12], [20], [36], [37], [40]. GMR is a regression approach that models probability distributions of latent samples from the event process and the memory process into multimodal regression using Gaussian mixture models (GMMs). It can be used to predict distributions of variables Zy by computing the conditional distribution p(Zy|Zx). The first process in GMR is to learn the joint PDFs through EM, then compute the conditional distribution to predictions. Training is the same procedure as in GMMs [11].

GMMs and GMR can seamlessly work together called the Gaussian mixture model for multimodal regression (GMMR), which applies two functions in one: the prediction function and the score function. The prediction function to predict target variables from input variables, this is the role of GMR. The score function to estimate the new joint PDFs of the input and class label, this is the role of GMMs. The realization of GMMR is in two steps. Step 1 is to predict target variables Zr from input variables (Zx, Zy) or Zxy using the prediction function. This target variable Zr is also used to predict class labels. Step 2 is to produce log-likelihood (logl) from bivariate data (Zx, Zr) or Zxr using the score function. Therefore, GMMR specifically is designed to enhance the reliability of the log-likelihood estimation produced by world models [14]. Flow diagram of GMMR as seen in Fig. 6.

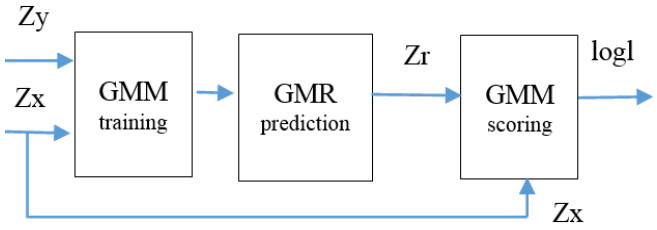


Fig. 6. Flow diagram of GMMR for the density process.

In step 1, GMMR has utilized the mixture of experts (MoE) [20] for developing the GMR prediction. MoE gives a simple approach to combine parametric and nonparametric regression methods by taking the analytic advantages of parametric and the flexibility of nonparametric [12], [19], [37]. The parametric method has been realized by a mixture of linear models [36] and the nonparametric method has been realized with divide-and-conquer principles [20]. In fact, the model log-likelihood function disregards the global data density [32], because the global maximum that indicates the global data density does not smoothly regress all local maxima. Then, MoE replaces a single global model with a weighted sum of local models (experts) [11], [12], [20], [40] to achieve the stability of multimodal regression as follows:

$$p(Zx, Zy) = \sum_{k=1}^{K} \pi_k N_k(Zx, Zy|\mu(Zxy_k), \Sigma(Zxy_k)) \quad (1)$$

$$p(Zy|Zx) = \sum_{k=1}^{K} \pi(Zy|Zx_k) N_k(Zy|\mu(Zy|Zx_k), \Sigma(Zy|Zx_k)) \quad (2)$$

Eq. (1) is the joint PDFs of GMMs via the EM algorithm [9]. $N_k(Zx, Zy|\mu(Zxy_k), \Sigma(Zxy_k))$ are Gaussian distributions with means $\mu(Zxy_k)$, covariances $\Sigma(Zxy_k)$, five Gaussian components (K=5). Weights $\pi_k \in [0, 1]$ are priors that sum up to one. EM is an iterative method for fitting GMMs to the negative class label of latent samples (Zx, Zy) or Zxy in an OCC setting. Eq. (2) is GMR model via the MoE to predict distributions of variables Zr by computing the conditional distribution p(Zy|Zx). The conditional distribution of each Gaussian distribution is $N(Zx,Zy|\mu(Zxy),\Sigma(Zxy))$ then the conditional distribution of a mixture of Gaussian distributions is $N_k(Zy \mid \mu(Zy \mid Zx_k), \Sigma(Zy \mid Zx_k))$ with means $\mu(Zy|Zx_k)$ and covariances $\Sigma(Zy|Zx_k)$. Weights $\pi(Zy|Zx_k) \in [0, 1]$ are priors that sum up to one.

In step 2, GMMR has utilized EM [9] for developing the score function. EM has a role for fitting GMMs to the negative class label of latent samples (Zx, Zr) or Zxr in an OCC setting again. The joint PDFs are used to store the statistical information of the input and target variables such in Eq. (3). The target variable is assumed class labels. In this case, class labels for the global model are missing, then EM is used to compute the parameters of each mixture component and estimate the maximum log-likelihood of GMMs as the score function such in (4).

$$p(Zx, Zr) = \sum_{k=1}^{K} \pi_k N_k(Zx, Zr|\mu(Zxr_k), \Sigma(Zxr_k)) \quad (3)$$

$$logl = \log p(Zx, Zr) \quad (4)$$

Fig. 7 demonstrates GMMR with five local models, which yield the predicted outcome Zr_pred in the output space y-axis when conditioning by Zx on the input space x-axis. GMMR has worked well to combine linear and non-linear models. The key model of GMMR is p(Zy|Zx) which produces p(Zx, Zy) from p(Zx) that can be well represented by a set of Gaussians [36] so that GMMR can be analyzed easily using a mixture of linear models. For this reason, the evaluation of GMMR is carried out on the linear regression model. It is linear in the parameters. The linearity of parameters is shown by a linear relationship between the predictor (Zx), observed outcome (Zy), predicted outcome (Zr) in performing local regression [19], [20], [36] at the query point on demand. The query point on demand using: (1) the nearby training observations [19], (2) a nested sequence of regions [20], and (3) a small set of close points [36], to build a mixture of linear models. From global regression into local regression referred to as a memory-based procedure [19] of experts and gates. It can predict the outcome according to the memory of experts, each expert specializes in one local regression, and the gate defines the regions where the memory of an individual expert are trustworthy.

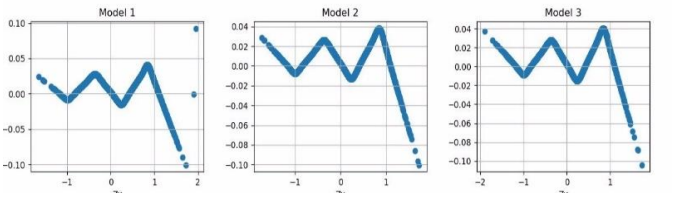


Fig. 7. GMMR with five local models.

The mechanism of GMMR with the local models has been explained specifically in hierarchical mixtures of experts (HME) [20]. The mechanism works on a set of experts and gates collaborating to solve a nonlinear function by dividing the input space into a nested sequence of regions [20], [40]. The experts learn the simple parameterized surfaces in these partitions of these regions, and the gate makes a soft split of the input space. The simple parameterized surface in both experts and gates can be learned using the EM algorithm [9].

The common metric to evaluate a regression model is root mean squared error (RMSE) and R-squared (R^2) [22]. RMSE is a function of the model residuals which is the difference between Zr_true and Zr_pred: in [0, ∞], the smaller the better. R^2 can be interpreted as the proportion of the variance in Zr_pred which is explained by the model: in [−∞, 1], the closer to 1 the better. R^2 is a measure of correlation, not accuracy [22]. The other metric is mean absolute error (MAE) which is the average of the absolut difference between Zr_true and Zr_pred: in [0, ∞], the smaller the better. The performance of GMMR for three selected models is shown in Table IV.

TABLE IV. MEASURING PERFORMANCE OF GMMR

Model	RMSE↓	R^2↑	MAE↓
1	0.0022	0.9752	0.0010
2	0.0010	0.9928	0.0009
3	0.0011	0.9926	0.0009

F. The Bias-Variance Alignment

The center point of cyber resilience model is in GMMs which build the fundamentals of representational and inference models. GMMs work on a probabilistic model to estimate maximum log-likelihood via the EM algorithm [9]. GMMs are a simple generative model that utilizes a mixture of Gaussian distributions to build a weighted sum of PDFs but GMMs have high flexibility in the predictive and inference modeling. The weakness is that GMMs fail in high-dimensional data [4]. To address the problem, the three methods take into account. The first method, dimensionality reduction to summarize important information from feature vectors into latent samples. The method uses VAEs for analyzing latent samples and MDRNNs for generating sequences of latent samples. The second method, multimodal regression to transform the non-linear function of latent samples into a mixture of linear models so that latent samples are easier to analyze just using linear regression but more stable in handling the density with local regression. The method uses MoE to combine parametric and nonparametric estimates of the model for a regression function. The third method, decision boundary optimization to conclude log-likelihood. The method uses the bias-variance alignment described in this subsection and likelihood ratios described in the next subsection.

The bias-variance tradeoff and alignment have similarities in decomposing the generalization error into bias and variance. The bias-variance tradeoff is often used to analyze

the generalization error in a regression setting [19], [22], while the bias-variance alignment is more suitable used to analyze the generalization error in a classification setting [7]. Quantitative measures of the generalization error in regression are derived from the mean squared error (MSE) which also can be calculated by squaring RMSE. The expected test MSE can be decomposed into bias and variance [19], [22] as follows:

$$E[MSE] = \sigma^2 + (\text{model bias})^2 + \text{model variance} \quad (5)$$

The first part (σ^2) is an irreducible error. It cannot be eliminated in predictive modeling. It shows intrinsic noise in the model due to unknown variables. The second part is the squared bias of the model. It shows the relationship between the predictor (Zx) and the outcome (Zr_true and Zr_pred) of the model. High bias means the model is unable to relate accurately between the predictor and the outcome, Zr_pred is very different from Zr_true that indicates underfitting. The third part is the model variance. It shows the sensitivity of predictive modeling to different datasets. High variance means the model learns more about the noise than the underlying patterns in datasets. More fitting in training data but poor in testing data indicates overfitting. The expected test MSE simultaneously achieves low bias and low variance.

Eq. (5) also works to multimodal regression via MoE. The variance model of multimodal regression can be expressed as the sum of two parts: the first part is related to the variance of the expert networks and the second part is related to the covariance of the expert networks [18]. This shows that a model that can be analyzed using a regression function means it can also be analyzed using bias-variance tradeoff, including GMMR.

TABLE V. TWO SAMPLES FOR CLASSIFICATION

Model	N(Zn)	N(Zp)	H
1	10	90	Hp
2	50	50	Hp
3	90	10	Hp
1	10	90	Hn
2	50	50	Hn
3	90	10	Hn

Table V describes two samples for classification. The samples size is one hundred for one observation. Positive samples denoted Zp and the size denoted N(Zp). Negative samples denoted Zn and the size denoted N(Zn). The hypothesis of classification models denoted H. There are two hypotheses: a positive hypothesis (Hp) and a negative hypothesis (Hn). A positive hypothesis is an observation that tests log-likelihood in an expected finding of the presence of an anomaly if the hypothesis is true. Quantitative measures of the presence of an anomaly are indicated by the positive likelihood ratio (PLR). Low log-likelihood is an instance from the presence of an anomaly. A negative hypothesis is an observation that tests log-likelihood in an expected finding of the absence of an anomaly if the hypothesis is true. Quantitative measures of the absence of an anomaly are indicated by the negative likelihood ratio (NLR). High log-likelihood is an instance from the absence of an anomaly.

The idea of using two samples for classification is motivated by the one-class classification method that suffered spurious detection [29] and perfect density models that could not guarantee anomaly detection [23]. One-class classification in the density process aims to learn a one-class decision boundary by GMMR that minimizes false positive rate (FPR) [35]. In this problem, the underlying patterns of negative samples is well-recognized by the model. However, because positive samples were not trained on the model, the model did not know the underlying patterns of positive samples. As a consequence, it suffers from spurious detection. The next problem, even though the data-generating process produces reliable log-likelihood, it does not mean that low log-likelihood is identical to the presence of an anomaly and vice versa. If the inference model of log-likelihood is not well-defined, high log-likelihood may be interpreted as the presence of an anomaly [8], [27]. The low and high log-likelihood of the representational model need to be proven quantitatively as the decision boundary that discriminates the two [33]. Therefore, anomaly detection using a single-sample distributional test is impossible [41]. The existency of positive and negative samples is a must for developing two competing hypotheses [33], [41]. The samples may be derived from ground truth or without. The model will learn from the samples and justified by two competing hypotheses. However, one-class classification is still required to define initial assumptions about the samples before modeling two competing hypotheses.

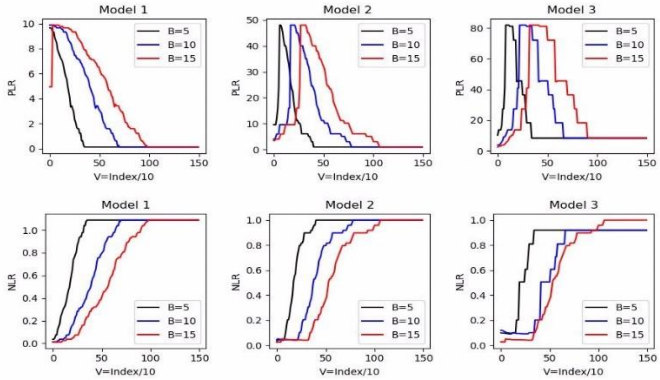


Fig. 8. The bias-variance alignment.

Fig. 8 describes the bias-variance alignment. The bias-variance alignment plays a role in decision boundary optimization to conclude log-likelihood. GMMR as part of data-generating process that produces log-likelihood is not free from the generalization error. The generalization error causes the estimated log-likelihood to shift from the true log-likelihood. This is called misleading and weak log-likelihood. However, the bias-variance tradeoff does not completely explain the phenomenon in a classification setting [7] as follows:

$$(\text{model bias})^2 \approx \text{model variance} \quad (6)$$

Eq. (6) about the phenomenon, which is different from bias-variance tradeoff in general that models of low capacity have high bias but low variance and vice versa. While in Eq. (6) shows the flexibility of bias-variance tradeoff. The model that has high bias does not tend to have low variance or vice versa. Eq. (6) suggests that the bias-variance alignment is specific to large neural networks. Meanwhile, for the small model as in Fig. 8 shows the same results that bias and variance are aligned at a sample level although squared bias does not approximately equal variance, as seen in a full and not-full concave curve of optimal likelihood ratios. It means that the effect of bias-variance tradeoff does not lost at all in a classification setting. Fig. 8 shows that decision boundary in a classification setting has optimized by bias-variance alignment. The relation between decision boundary and bias-variance alignment is as follows:

$$\text{aligned\_logl} = \text{logl-B}\times\mu(\text{Ze})\times\text{logl} \quad (7)$$

$$T = \mu(\text{aligned\_logl})\text{-V}\times\Sigma(\text{aligned\_logl}) \quad (8)$$

$$\text{y\_pred} = \begin{cases} 1, & \text{aligned\_logl} < T \\ 0, & \text{aligned\_logl} \geq T \end{cases} \quad (9)$$

In Eq. (7), aligned_logl has related to a bias factor (B) and the mean of the predictors at testing time μ(Ze). Meanwhile, a decision boundary threshold (T) has related to a variance factor (V), means μ(aligned_logl), and standard deviations Σ(aligned_logl). Eq. (7) shows that log-likelihood needs to be aligned so that it shifts closer to the true log-likelihood, then aligned_logl performs as a parameter in determining the variability of thresholds together with a variance factor.

In Eq. (9), the threshold T creates a decision boundary that classifies log-likelihood into two classes: low log-likelihood if aligned_logl < T and high log-likelihood if aligned_logl ≥ T. Low log-likelihood being labeled positive samples (predicted positive/PP) and high log-likelihood being labeled negative samples (predicted negative/PN). Eq. (9) applies if the bias-variance alignment has achieved the optimal likelihood ratio.

G. Likelihood Ratios

A likelihood (L) is the relative probability of the observed data given a hypothesis parameter value [3]. It refers to the probability or density of a sample under a distribution [41]. It is related to the observed data, statistical models, and statistical hypotheses. It indicates the hypothesis for the goodness of fit of a model to the observed data. With these roles, the data-generating process is designed to produce the likelihood datasets that construct hypothesis. A hypothesis is a prediction for the observed data that can be tested for truth. Hypothesis testing is an important step to ensure that a model being built fits the observed data. Together with the observed data, statistical models, and statistical hypotheses are actual components to be able to draw inferences. The likelihood ratio (LR) is the ratio of two likelihoods for parameter values for two different hypotheses H_1 over H_2 given the observed data x [3] that can be written as follows:

$$LR = L(H_1|x)/L(H_2|x) = P(x|H_1)/P(x|H_2) \quad (10)$$

The likelihood ratio LR represents and measures statistical evidence. The LR is not a probability but a relative measure of evidence for competing two hypotheses. The likelihood of a hypothesis H given the observed data x (L(H|x)) is proportional to the probability of the observed data x under a hypothesis H (P(x|H)). L(H|x) builds a likelihood model. As a consequence, the LR builds a model to represent statistical evidence. Then, the LR model performs as an evidence measure for the observed data. Two different evidences will be measured: evidence from ground truth datasets (y_true) as explained in the subsection III.B and evidence from the bias-variance alignment (y_pred).

In the LR, hypotheses can be easily derived from the model and vice versa. Eq. (7) represents the observed data in a model and (9) is the hypothesis of the model. Eq. (9) formulates the positive hypothesis H_1 (align_logl<T) and the negative hypothesis H_2 (align_logl≥T). In contrast, the hypotheses formulated in (9) together with ground truth datasets build a new model, as seen in Fig. 9(b). The LR model measures statistical evidence by support, denoted S. Statistical evidence for two hypotheses on the graded scale can be seen in Table VI.

TABLE VI. INTERPRETING SUPPORT [3]

LR (1/LR)	Support (log LR)	Interpretation H_1 over H_2
1 (1.00)	0	No evidence
2.7 (0.37)	1	Weak evidence
7.4 (0.14)	2	Moderate evidence
20 (0.05)	3	Strong evidence
55 (0.02)	4	Extremely strong evidence

Table VII shows likelihood intervals or support intervals and their corresponding frequentist confidence intervals (CI) for the standard Gaussian distribution. Similar to confidence intervals, likelihood intervals describe the accuracy and reliability of estimation obtained from the observed data. Likelihood intervals measure the level of confidence in the estimation that expected parameters fall within a certain range. Likelihood intervals are a need to interpret likelihood clearly that the likelihood evidence points are confidence within a certain range.

TABLE VII. LIKELIHOOD INTERVALS [3]

S	LR	1/LR	% CI
1.6	4.95	0.202	92.6
2	7.39	0.135	95.4
3	20.09	0.050	98.6
4	54.60	0.018	99.5
5	148.4	0.007	99.8
6	403.4	0.0025	99.95
7	1096.6	0.0009	99.98
8	2981.0	0.0003	99.99

The LR is about the relative strength of evidence for two competing hypotheses. In contrast, the frequentist approach use of type I and type II errors allows one to specify the probability of rejecting the null hypothesis when it is true, and of not rejecting it when it is false [3]. The LR was built to test two hypotheses: predicted label as an outcome and true label as a reference standard. The two hypotheses compete to measure the relative strength of evidence.

In this paper, a competition is performed by considering ground truth datasets as a reference standard to test the hypothesis in (9) as predicted label. It will produce the outcome of a test: (1) y_pred=1 for a positive label, (2) y_pred=0 for a negative label, and (3) the relative strength of evidence for the observed data. Therefore, the outcome of a test by the LR is not to reject or not reject the null hypothesis (H_0 or H_2). If the relative strength of evidence is not misleading and not weak, the hypothesis may be accepted.

The 2×2 contingency table describes a matrix format used to display a frequency distribution of two variables with the vertical columns denoting instances of reference standard, or true label and the horizontal rows denoting instances of outcome of a test, or predicted label [24]. The relative strength of evidence is measured using the 2×2 contingency table as seen in Fig. 9.

	align_logl<T	align_logl≥T
y_pred=1	TP	FP
y_pred=0	FN	TN

a. The 2×2 contingency table to evaluate the performance indicator of a model

	y_true=1	y_true=0
y_pred=1	TP	FP
y_pred=0	FN	TN

b. The 2×2 contingency table to assess the relative strength indicator of evidence

Fig. 9. The 2×2 contingency table for binary classification.

Table VIII defines a measure factor in the 2×2 contingency table and its derivative. The limitation in the evidential approach is that no observed values are zero [3]. The generalization error controlled by the bias-variance alignment is only a reducible error part not all error conditions [19], [22]. A measure factor of TPR, TNR, FPR, and FNR is an error-based measure. A measure factor, such as TPR or TNR, has a test's ability to detect correctly a condition when it is present and to rule it out correctly when it is absent. A measure factor, such as FPR or FNR, has a test's propensity to detect incorrectly a condition when it is absent and not to detect it correctly when it is present [24]. Therefore, a measure factor of TP, TN, FP, and FN is considered to be not zero.

PLR measures the change in pre-test to post-test odds and diagnostic gain. It also combines information about TPR and FPR [24]. If a sample from population tested positive, PLR represents the relative strength of evidence that a sample is an anomaly given a positive test result. However, the relative evidence of PLR also depends on the explicit prior in the Bayesian approach which is not discussed in this paper. To reduce uncertainty due to factors that influence it, PLR utilizes information from NLR.

Ideally the PLR value is 1/NLR [3], but in practice, the PLR value is sometimes greater than 1/NLR so that the relative strength of evidence for the observed data is less properly. It is necessary to combine PLR and NLR for a single test value as the performance indicator of a model and the relative strength indicator of evidence. Basically, PLR and NLR are the ratio of paired measures [24]. Hence the approach taken is based on the harmonic mean method [43] to combine PLR and NLR that gets a new measure factor, namely, the harmonic likelihood ratio (HLR):

$$HLR = 2\times PLR/(1+(PLR\times NLR)) \quad (11)$$

TABLE VIII. A MEASURE FACTOR IN THE 2×2 CONTINGENCY TABLE AND ITS DERIVATIVE

Term	Denoted	Formula	Description
True positive	TP	TP > 0	Correct predictions of anomaly
True negative	TN	TN > 0	Correct predictions of normal
False positive	FP	FP > 0	Incorrect predictions of anomaly
False negative	FN	FN > 0	Incorrect predictions of normal
True positive rate	TPR	TP/(TP+FN)	The rate of an anomaly sample tested positive
True negative rate	TNR	TN/(TN+FP)	The rate of a normal sample tested negative
False positive rate	FPR	1-TNR	The rate of a normal sample tested positive
False negative rate	FNR	1-TPR	The rate of an anomaly sample tested negative
Positive likelihood ratio	PLR	TPR/FPR	The ratio of an anomaly sample tested positive and a normal sample tested positive
Negative likelihood ratio	NLR	FNR/TNR	The ratio of an anomaly sample tested negative and a normal sample tested negative

The idea of a self-supervised binary classifier is to utilize the structure within data from the samples (logl) to build a supervisory signal for the classifier. A supervisory signal comes from the underlying structure of the samples realized in producing two samples using (7), (8), and (9). A supervisory signal first finds the bias B and variance V that give the maximum likelihood ratios of the two samples. For simplicity, the bias B is assumed to be 10 refers to the B value in the description of the bias-variance alignment in Fig. 8 and the variance V is tried to find iteratively within a certain range on the PLR or HLR value is the maximum, denoted _PLR_ and _HLR_. This maximum value indicates the relative strength of evidence for two samples that the classifier has worked to classify the two samples properly.

The performance evaluation of classifiers involves three models, two groups of observation, and five indicators. Classification is designed in two stages. The first stage is about training samples with a one-class classification method for fine-grained negative samples from subdistributions 1, 2, and 3. Three types of training samples were realized with a negative sample size of 10, 50, and 90, respectively. Training samples were taken from ground truth datasets randomly.

Training samples were the initial assumptions about the prior distribution implicitly (the implicit prior). The second stage is about testing samples with a binary classification method for fine-grained negative samples from subdistributions 1, 2, and 3 and positive samples from subdistributions 4, and 5. Ninety-nine types of testing samples were realized with a negative sample size from 1 to 99 and a positive sample size from 99 to 1, respectively. Testing samples were taken from ground truth datasets randomly. The second stage applies (7), (8), and (9).

Table IX shows that 4 out of 5 performance indicators of the group of observation _HLR_ are better than the group of observation _PLR_. This proves that HLR as a single test value of performance indicators has worked well to evaluate the performance of binary classifier even though the absence of the explicit prior. This correspond to the result of the area under the receiver operating characteristic (AUROC). While the area under the precision-recall curve (AUPRC) is almost the same.

TABLE IX. THE METRIC TO EVALUATE THE PERFORMANCE OF BINARY CLASSIFIERS

Model	Model 1		Model 2		Model 3	
Group	_PLR_	_HLR_	_PLR_	_HLR_	_PLR_	_HLR_
V	1.148	0.576	1.556	0.741	1.352	0.683
T	3.815	5.127	3.868	5.114	3.908	5.067
PLR↑	36.128	22.432	36.664	20.053	37.811	22.591
NLR↓	0.207	0.076	0.211	0.082	0.200	0.079
HLR↑	11.608	16.072	11.041	14.805	10.966	15.492
AUROC↑	0.894	0.941	0.895	0.938	0.897	0.938
AUPRC↑	0.922	0.935	0.927	0.931	0.926	0.939

IV. EXPERIMENTAL RESULTS

The study in this paper was conducted using an experimental method. The experiment was conducted in four stages. The first stage was an experiment with raw datasets that produce ground truth datasets: true or to be true positive (TP) samples and true or to be true negative (TN) samples using the K-Means and EM algorithms.

The second stage was an experiment with the LR as the performance indicator of a model (HLR). The experiment uses data-generating process to produce the logl. The bias-variance alignment enhances likelihood by shifting the logl closer to true likelihood thereby producing the LR model. An indication that the logl closer to true likelihood if the LR model is not misleading and not weak refers to Table VI. The LR model constructs two hypotheses: a positive hypothesis (H_1) and a negative hypothesis (H_2). A measure factor HLR facilitates the resolution of two hypotheses to obtain the variance V properly based on the underlying structure of the two samples. The variance V is proper if the HLR has reached its maximum within a certain range of variance. Together with the bias B, the variance V constructs a supervisory signal for the classifier by a threshold T. Referring to (9), the LR model produces predicted datasets: predicted positive (PP) samples and predicted negative (PN) samples. In the LR, two samples present two models and two hypotheses. Otherwise, two models and two hypotheses represent two samples.

The third stage was an experiment with the LR as the relative strength indicator of evidence (S). Evidence comes from ground truth and predicted datasets which construct two hypotheses: a primary hypothesis (H_1) and a null hypothesis (H_0). Once again, a measure factor HLR makes it easier to resolve two hypotheses to get the relative strength of evidence.

The fourth stage was an experiment to build up a self-supervised anomaly detection (AD) approach. The resilience scale (RS) and anomaly score (AS) can be written as follows:

$$RS = 2\times IPN\times S/(IPN+S) \quad (12)$$

$$AS = 4-RS \quad (13)$$

In (12), the support S is the natural logarithm of a measure factor HLR. It assumes the highest relative strength of evidence is 4 that refers to Table VI. Also, the highest index of PN is 4, because PN is in the range of 0 to 100, the index of PN (IPN) is PN/25. So that the IPN and S have the same ratio from 0 to 4, then both variables can be estimated smoothly using a harmonic mean method [43] to derive (12). Eq. (13) assumes the resilience scale and anomaly score are complements to the support S.

The experiments were realized using a Python programming language, a deep learning library Pytorch [30] to implement an artificial neural network, a Python module Scikit-learn [31] to implement a machine learning model, a Python library gmr [11] to implement a mixture of experts, a Python toolbox PyOD [42] for benchmarking anomaly detection methods, and a 2D graphics package Matplotlib [17] for the visualization of observational and experimental results.

TABLE X. THE LOG-LIKELIHOOD SCORE OF EACH SUBDISTRIBUTION

subd	1	2	3	4	5
Zx	-1.238	-1.199	-1.281	-1.372	-1.475
Zxy	-1.217	-1.193	-1.233	-1.278	-1.335
Zxr	5.078	5.104	5.057	4.985	4.921
Zxr, B=5	6.211	5.514	4.726	3.652	2.712
Zxr, B=10	7.344	5.925	4.395	2.318	0.502
Zxr, B=15	8.477	6.335	4.064	0.985	-1.707

Table X presents the log-likelihood score of each subdistribution for some latent variables and the bias factor that affects the log-likelihood score. The latent variable Zx is the latent samples generated by VAEs. The latent variable Zxy is the latent samples generated by VAEs and MDRNNs also known as world models [14]. The latent variable Zxr is the

latent samples generated by VAEs, MDRNNs, and GMMR also called the representational model.

Table X proves that the log-likelihood score of Zx and Zxy is too low, below zero. GMMR can increase the log-likelihood score significantly from Zxy to Zxr. However, the log-likelihood score generated by GMMR is not strong enough to be used as evidence. The log-likelihood scores of one subdistribution and the others are difficult to distinguish as normal and anomaly classes. It shows that the classification of the two samples is not clear. The reason is that the latent samples are generated by the model, while a model is not free from the generalization error.

In Table X, the bias factor B as one of a supervisory signal straightens the weak evidence by shifting the log-likelihood score closer to the true classification of the two samples. A higher B value has implications for a higher log-likelihood score of subdistributions 1, and 2 and a lower log-likelihood score of subdistributions 3, 4, and 5. This simple experiment explains that subdistributions 1, and 2 tend to be samples of normal class and subdistributions 3, 4, and 5 tend to be samples of anomaly class.

Fig. 10 gives three indicators of the cyber resilience model: the predicted negative PN, the support S, and the resilience scale RS. The predicted negative PN about two samples needed in a likelihood ratio model. One sample represents a reference standard used as an example (ground truth datasets). The other sample represents the observed data (predicted datasets). Ground truth and predicted datasets construct a likelihood ratio model. In the context of cyber resilience, the samples that need to be monitored are the predicted negative (PN) as part of the predicted datasets. PN is the total number of elements labeled as belonging to the negative class. PN is true negative (TN) + false negative (FN). True negative (TN) is as part of the ground truth datasets while false negative (FN) indicates incorrect predictions of the negative class. So, FN is the difference between PN and TN. The PN indicator proves the relationship between PN and the number of negative samples N(Zn), TN, FN.

The support S about the relative strength indicator of evidence. Two samples in a likelihood ratio model construct two competing hypotheses. A measure factor HLR makes it easier to resolve two competing hypotheses to get the support S. From the experiment, it is known that the support S is not affected by the number of negative samples linearly in the training and testing phases except for extreme numbers, such as less than 10 or more than 90 if the sample size is 100. As a consequence, the number of negative samples of 10 has met the requirement as training data.

The resilience scale RS about the resilience scale of the service. It is the indicator to measure the behavior of cyber resilience model. The cyber resilience model requires two data to realize (12): the predicted negative (PN) and the support (S). Because RS derives from the PN and S, which refers to Table VI, the resilience scale RS also has an interpretation that refers to Table VI.

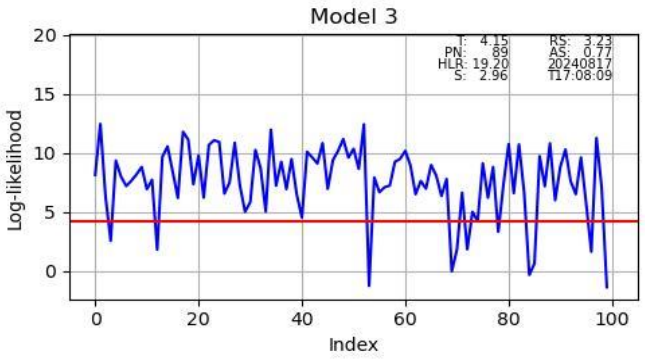


Fig. 10. The cyber resilience model.

Referring to this experimental results, it is known that the cyber resilience model is identical to a likelihood ratio model (LRM). A likelihood ratio model is effectively carried out based on anomaly detection. In anomaly detection, two samples are clearly defined. LRM summarizes complete information about the observed data, statistical models, and statistical hypotheses of DNS events. It identifies the individual and group behavior of each sample shown by the PN and S indicator.

The PN indicator can be used to estimate the status of the data. High PN shows that DNS events are normal and low PN shows otherwise. In addition, LRM provides information about the stability of the model in predicting the observed data. The stability of the model can be seen from the S indicator. A high S shows that the model has the ability to predict the data normally and a low S shows otherwise. Furthermore, the two indicators are used to test the hypothesis of DNS events. A high anomaly score or low resilience scale indicates a DNS anomaly. A low anomaly score or high resilience scale indicates a DNS normal. Table VI will help interpret both in a more understandable form. Therefore, the anomaly score AS is a complement to the resilience scale RS as has been formulated in (13).

Anomaly detection is designed using a specific binary classification task to build a reliable anomaly detection method in dealing with dynamic models. The binary classification task goes through two stages. The first stage is fitting data using regression to obtain the initial value of the relationship between the model and the genuine labeled data (the implicit prior) and the second stage classifies the log-likelihood by a decision boundary threshold to define high and low log-likelihoods. The complete differences between some anomaly detection methods (PyOD) and the tested method (LRM) in the experiment can be seen in Table XI.

TABLE XI. THE DIFFERENCE OF PYOD AND LRM IN THE EXPERIMENT

PyOD	LRM
Input from the log-likelihood score of latent samples (logl) about 100 samples	Input from latent samples (Zxr) about 2×200×100 latent samples
Fitting and predicting in classification	Fitting in regression Predicting in classification
Fitting is done on the negative samples	Fitting is done on the negative latent samples
Predictors are the negative and positive samples	Predictors for regression are the negative latent samples Predictors for classification are the negative and positive samples
Not using latent samples but directly using the log-likelihood score as the observed samples	For each latent sample, the maximum log-likelihood score is taken as the observed samples

Some anomaly detection methods that have been compared: Angle-Based Outlier Detection (ABOD), Isolation Forest (IForest), K-Nearest Neighbors (KNN), and One-Class Support Vector Machines (OCSVM). The methods represent four different anomaly detection methods that have been implemented in PyOD [42]. The results of the benchmarking show that LRM has high performance and stability as an anomaly detection method as seen in Table XII.

TABLE XII. BENCHMARKING THE FOUR METHODS AND LRM

Model	Indicator	ABOD	IForest	KNN	OCSVM	LRM
1	HLR↑	6.003	14.236	14.236	17.626	17.626
	AUROC↑	0.856	0.933	0.933	0.944	0.944
	AUPRC↑	0.984	0.993	0.993	0.994	0.994
2	HLR↑	10.212	13.458	13.458	13.458	32.441
	AUROC↑	0.910	0.930	0.930	0.930	0.970
	AUPRC↑	0.928	0.943	0.943	0.943	0.980
3	HLR↑	10.862	10.124	10.124	9.478	19.203
	AUROC↑	0.961	0.956	0.956	0.950	0.994
	AUPRC↑	0.794	0.778	0.778	0.763	0.955

V. DISCUSSION AND FUTURE WORK

Two samples can be well-modeled with the LR model so that the interpretation of the observed data is more objective, depending only on the data itself. It is relevant to be used for anomaly detection. It is also relevant to be used for normal detection (resilience). Based on a self-supervised anomaly detection approach, self-labeling in a dynamic model can be realized with measurable supervision. Self-labeling directed by a supervisory signal consisting of a bias factor B, a variance factor V, and a threshold T. The evaluation of regression and classification models with results as follows: RMSE=0.0014, R^2=0.9869, MAE=0.0009 for fitting 3 regression models at training time and HLR=15.456, AUROC=0.939, AUPRC=0.935, S=2 (2.738) with the S-2 likelihood interval for 297 (3×99) classification models at testing time. It means that the LR model does not generally produce misleading and weak log-likelihood. In this LR, the relative strength of evidence is defined by a primary hypothesis that models self-labeling and a null hypothesis that models a standard reference of the samples. In the experiment, it has been proven that a primary hypothesis is accepted, S=2 with a 95% confidence level.

The difference index (DI) of likelihood in the EM as a sample classifier is the difference between a subdistribution classified as positive and negative samples. The larger DI, the larger the disjoint support between the distribution of positive and negative samples. In Table III, subdistribution 2 has a DI of 4.004, subdistribution 3 has a DI of 0.944, and subdistribution 4 has a DI of 3.210. It means the difference index of subdistribution 3 is small, then the disjoint support is also small. As a consequence, subdistribution 3 is less reliable as a standard reference of samples.

To address the problem of misleading and weak log-likelihood required aligning bias-variance and optimizing likelihood-ratios. In Table X, the bias factor B has been worked properly for subdistributions 1, 2, 4, and 5 but not for subdistribution 3. This is correlated with the analysis of Table III that the disjoint support of subdistribution 3 is small so subdistribution 3 produces anomaly interpretation: some parts tend to be negative samples and others tend to be positive samples.

Referring to the facts in Table III and X, it is necessary that a null hypothesis may need to be redesign. A null hypothesis represents ground truth datasets as examples of positive and negative samples that declare a reference standard of the observed samples in two competing hypotheses. The next study focused on enhancing the ground truth datasets, especially to address the problem of subdistribution 3 that produces a stronger relative strength indicator of evidence. Furthermore, predictive modeling only relies on examples of positive and negative samples from those trained to the model as the implicit prior.

VI. CONCLUSION

There is a relationship between the cyber resilience and likelihood ratio models. The likelihood ratio model (LRM) is useful in building the cyber resilience model. It meets the requirements needed to realize the representational and inference models in practice. The representational model has been realized with likelihood maximization inside data-generating process and the inference model has been realized with likelihood ratios inside two competing hypotheses. In the representational model, the Gaussian mixture model for multimodal regression (GMMR) enhances the ability of world models produces log-likelihood. The log-likelihood needs to be aligned by the bias-variance factor to be worthy of being used as evidence. In the inference model, evidence from ground truth datasets and evidence from the model build two competing hypotheses to handle anomaly detection tasks in self-supervised settings. Evidence from the model has been labeled through a self-labeling technique that supervised by three supervisory signals: a bias factor, a variance factor, and a threshold to optimize decision boundary in minimizing the generalization error of predictive modeling with the harmonic likelihood ratio (HLR).

ACKNOWLEDGMENT

This study was conducted in collaboration between Universitas Muhammadiyah Malang and Universiti Teknologi Malaysia. The authors fully acknowledge to Rector of Universitas Muhammadiyah Malang for the research grant (E.5.c/1693/UMM/XII/2020) that helps in funding the research works. Special thanks to all the reviewers for their valuable feedback.

REFERENCES

[1] C.M. Bishop, "Novelty detection and neural network validation," In: S. Gielen, B. Kappen (eds), ICANN '93, Springer, 1993.

[2] C.M. Bishop, Mixture density networks, Technical Report, Aston University, 1994.

[3] P.M.B. Cahusac, Evidence-based statistics: An introduction to the evidential approach-from likelihood principle to statistical practice, John Wiley & Sons, 2020.

[4] E.B. Cahyono, S.M. Sam, N.H. Hassan, N. Mohamed, N.B. Ahmad, and Y.M. Yusuf, "A review on cyber resilience model in small and medium enterprises," 4th International Conference on Smart Sensors and Application (ICSSA), pp. 114-119, 2022.

[5] J. F. Carías, M. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, "Systematic approach to cyber resilience operationalization in smes," IEEE Access, vol. 8, pp. 174200-174221, 2020.

[6] J. F. Carías, S. Arrizabalaga, L. Labaka, and J. Hernantes, "Cyber resilience progression model," Applied Sciences, vol. 10, iss. 21, pp. 7393, 2020.

[7] L. Chen, M. Lukasik, W. Jitkrittum, C. You, and S. Kumar, "On bias-variance alignment in deep models," International Conference on Learning Representations, 2024.

[8] H. Choi, E. Jang, and A.A. Alemi, "WAIC, but why? Generative ensembles for robust anomaly detection," arXiv, abs/1810.01392, 2018.

[9] A.P. Dempster, N.M. Laird, and D.B. Rubin, "Maximum likelihood from incomplete data via the em," Journal of the Royal Statistical Society, Series B (Methodological), vol. 39, no. 1, pp. 1-38, 1977.

[10] K.O. Ellefsen, C.P. Martin, and J. Tørresen, "How do mixture density rnns predict the future?," ArXiv, abs/1901.07859, 2019.

[11] A. Fabisch, "gmr: Gaussian mixture regression," Journal of Open Source Software, vol. 6, no. 62, pp. 3054-3057, 2021.

[12] Z. Ghahramani, and M.I. Jordan, "Supervised learning from incomplete data via an em approach," Neural Information Processing Systems, 1993.

[13] A. Graves, "Generating sequences with recurrent neural networks," ArXiv, abs/1308.0850, 2013.

[14] D.R. Ha, and J. Schmidhuber, "World models," ArXiv, abs/1803.10122, 2018.

[15] S. Hochreiter, and J. Schmidhuber, "Long short-term memory," Neural Computation, vol. 9, pp. 1735-1780, 1997.

[16] H. Hojjati, T.K. Ho, and N. Armanfard, "Self-supervised anomaly detection: A survey and outlook," ArXiv, abs/2205.05173, 2022.

[17] J.D. Hunter, "Matplotlib: A 2D graphics environment," Computing in Science & Engineering, vol. 9, no. 3, pp. 90-95, 2007.

[18] R.A. Jacobs, "Bias/variance analyses of mixtures-of-experts architectures," Neural Computation, vol. 9, pp. 369-383, 1997.

[19] G.M. James, D.M. Witten, T.J. Hastie, and R. Tibshirani, An introduction to statistical learning with applications in r, Second Edition, Springer Texts in Statistics, 2021.

[20] M.I. Jordan, and R.A. Jacobs, "Hierarchical mixtures of experts and the em algorithm," Neural Computation, vol. 6, pp. 181-214, 1993.

[21] D.P. Kingma, and M. Welling, "Auto-encoding variational Bayes," ArXiv, abs/1312.6114, 2013.

[22] M. Kuhn, and K. Johnson, Applied predictive modeling, Springer, 2013.

[23] C.L. Lan, and L. Dinh, "Perfect density models cannot guarantee anomaly detection," Entropy, vol. 23, no. 12, 2020.

[24] A. J. Larner, The 2x2 matrix: Contingency, confusion and the metrics of binary classification, Second Edition, Springer, 2024.

[25] O. Makansi, E. Ilg, O. Çiçek, and T. Brox, "Overcoming limitations of mixture density networks: A sampling and fitting framework for multimodal future prediction," IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 7137-7146, 2019.

[26] P. Martin, GoPassiveDNS: Network-based dns logging in go, GitHub repository, https://github.com/Phillipmartin/gopassivedns, 2016.

[27] E.T. Nalisnick, A. Matsukawa, Y.W. Teh, D. Görür, and B. Lakshminarayanan, "Do deep generative models know what they don't know?," International Conference on Learning Representations, 2019.

[28] G. Pang, C. Shen, L. Cao, and A. Van Den Hengel, "Deep learning for anomaly detection: A review," ACM Computing Surveys, vol. 54, no. 2, pp. 1-38, Research Collection School Of Computing and Information Systems, 2022.

[29] J. Park, J. Moon, N. Ahn, and K. Sohn, "What is wrong with one-class anomaly detection?," ICLR 2021 Workshop on Security and Safety in Machine Learning Systems, 2021.

[30] A. Paszke, S. Gross, F. Massa, A. Lerer, J. Bradbury, G. Chanan, T. Killeen, Z. Lin, N. Gimelshein, L. Antiga, A. Desmaison, A. Köpf, E. Yang, Z. DeVito, M. Raison, A. Tejani, S. Chilamkurthy, B. Steiner, L. Fang, J. Bai, and S. Chintala, "Pytorch: An imperative style, high-performance deep learning library," 33rd Conference on Neural Information Processing Systems, 2019.

[31] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, G. Louppe, P. Prettenhofer, R. Weiss, R.J. Weiss, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in python", Journal of Machine Learning Research, vol. 12, pp. 2825-2830, 2011.

[32] P. Poklukar, "Seeing the whole picture instead of a single point: Self-supervised likelihood learning for deep generative models," 2nd Symposium on Advances in Approximate Bayesian Inference, 2019.

[33] J. Ren, P.J. Liu, E. Fertig, J. Snoek, R. Poplin, M.A. DePristo, J.V. Dillon, and B. Lakshminarayanan, "Likelihood ratios for out-of-distribution detection," 33rd Conference on Neural Information Processing Systems, 2019.

[34] D.J. Rezende, S. Mohamed, and D. Wierstra, "Stochastic backpropagation and approximate inference in deep generative models," International Conference on Machine Learning, 2014.

[35] L. Ruff, J.R. Kauffmann, R.A. Vandermeulen, G. Montavon, W. Samek, M. Kloft, T.G. Dietterich, and K. Muller, "A unifying review of deep and shallow anomaly detection," Proceedings of the IEEE, vol. 109, no. 5, pp. 756-795, 2020.

[36] F. Stulp, and O. Sigaud, "Many regression algorithms, one unified model: A review," Neural networks: the official journal of the International Neural Network Society, vol. 69, pp. 60-79, 2015.

[37] H.G. Sung, Gaussian mixture regression and classification, PhD thesis, Rice University, 2014, unpublished,

[38] M. Suzuki, and Y. Matsuo, "A survey of multimodal deep generative models," Advanced Robotics, vol. 36, pp. 261-278, 2022.

[39] F. Weimer, "Passive dns replication," 17th annual FIRST conference on computer security incident, 2005.

[40] S.E. Yüksel, J.N. Wilson, and P.D. Gader, "Twenty years of mixture of experts," IEEE Transactions on Neural Networks and Learning Systems, vol. 23, pp. 1177-1193, 2012.

[41] L.H. Zhang, M. Goldstein, and R. Ranganath, "Understanding failures in out-of-distribution detection with deep generative models," Proceedings of machine learning research, vol. 139, pp. 12427-12436, 2021.

[42] Y. Zhao, Z. Nasrullah, and Z. Li, "Pyod: A python toolbox for scalable outlier detection," Journal of Machine Learning Research, vol. 20, pp. 1-7, 2019.

[43] D. Ziou, "Pythagorean centrality for data selection," ArXiv, abs/2301.10010, 2023.

Evaluation of the Optimal Features and Machine Learning Algorithms for Energy Yield Forecasting of a Rural Rooftop PV Installation

Boris Evstatiev[1], Katerina Gabrovska-Evstatieva[2], Tsvetelina Kaneva[3], Nikolay Valov[4], Nicolay Mihailov[5]
Faculty of Electrical Engineering, Electronics and Automation, University of Ruse Ange Kanchev, Ruse, Bulgaria[1, 3, 4, 5]
Faculty of Natural Science and Education, University of Ruse Angel Kanchev, Ruse, Bulgaria[2]

***Abstract*—The stability and reliability of the electric grid strongly depend on the ability to schedule and forecast the energy output of all sources. Even though the share of photovoltaic installation in the energy mix is continuously increasing, they have one major drawback: their dependence on different environmental parameters, such as solar irradiance, ambient temperature, cloudiness, etc., which have a highly variable nature. Six machine learning algorithms are compared in this study, regarding their ability to forecast the power generation of a rural rooftop photovoltaic installation using different combinations of the input data. The features selected for investigation are solar radiation, ambient temperature, and wind speed, obtained from a meteorological station, as well as two additional time-based variables – the time of the day and the month of the year. During the validation and testing phases, four models performed better – artificial neural network (ANN), k-Nearest neighbor (kNN), Decision tree (DT), and Random Forest (RF), with ANN achieving the best results in all cases. The optimal combination of input data includes solar radiation, ambient temperature, wind speed, and hour of the day, though the difference with the other scenarios was small. The optimal ANN model achieved R^2, MAE, and RMSE of 0.995, 6.71 Wh, and 13.7 Wh, respectively. The results obtained in this study indicate that the yield of PV installations located in rural areas could be forecasted with high probability using a limited number of meteorological data.**

Keywords*—PV yield; forecasting; machine learning; deep learning; features; solar radiation; ambient temperature; wind speed; hour of the day

I. Introduction

Renewable energy technologies have greatly developed during the last decades, with photovoltaics holding the largest share. Many reasons exist for this, such as their low maintenance costs [1, 2], abundant availability of solar energy [3], the possibility for building integration [4], relatively easy installation, reliability [4], etc. However, one major drawback could be defined for PV installations: their strong dependence on weather conditions and especially on solar radiation, which has a highly variable nature. For this reason, the output of photovoltaic power in a stations changes wide range over time and is generally difficult to forecast. One of the options to deal with this problem is the application of energy storage systems, allowing energy charging during daylight hours and using it according to the requirements of the load profile [5, 6]. However, with the current development of energy storage technologies, this approach is still too expensive and its return on investment is too low without government incentives and subsidies [7]. Furthermore, the batteries' life expectancy is still relatively low, which requires additional investment during the PV park operation for battery replacement [8].

Reducing power uncertainties in the electric grid is a major task, which is required to ensure its energy balance. Therefore, forecasting the output of photovoltaic installations is crucial for maximizing the economic benefit and ensuring customers receive electric energy of acceptable quality and reliability [9]. The power production of PV installations depends on many environmental factors, such as solar irradiance, cloudiness, ambient temperature, wind speed [10, 11, 12], and even relative humidity and rainfall. [13, 14]. Moreover, when a photovoltaic installation is installed in an urban or suburban environment, additional factors affecting power production are introduced or enhanced, such as soiling [15, 16], shading [17, 18], panel degradation [19, 20], etc.

Different forecasting approaches exist mostly based on statistical methods (ARIMA, ARCH, GARCH) and machine learning methods, even though physical and hybrid approaches are also used [21, 22]. Machine learning has many applications in the renewable energy field, such as yield forecasting [23], condition monitoring [24], fault detection [25, 26], PV cell degradation [27], MPPT tracking [28], energy management [29], etc. When it comes to PV yield or power forecasting, different machine learning regression algorithms are used, such as Support Vector Machine (SVM), Linear regression (LR), Random Forest (RF), Regression tree (RT), etc. For example, in study [30] the global horizontal irradiance and atmospheric temperature were used, obtained from a meteorological station with a 5-minute timeframe. Several regression models were investigated, such as Gaussian process regression (GPR), LR, RT, and SVM. All models achieved similar performance, with R^2 varying between 92% and 96%, yet the RT achieved the highest score. Similarly, in the study [31] the 5 min horizontal global radiation and ambient temperature in Berlin were used as input data for a machine learning algorithm. It predicted the generated AC energy of a photovoltaic installation and achieved a coefficient of determination of 0.87.

A study for Jordan used nine features to predict the power of a PV installation: irradiation, air temperature, module temperature, as well as several time-based features – day of the week, month number, day type, week number, hour of the day

and year type [32]. RF achieved the highest performance, closely followed by Bagging-REFTree. In study [33], the possibility of forecasting PV energy output in numerous regions with limited plant-specific data was investigated. The authors enriched the features by adding 1-hour-lagged meteorological data and tested different machine-learning regression methods, such as Kernel Ridge and RF. The models achieved a normalized root mean square error (NRMSE) of 3% in the case of lagged power used as input, corresponding to a 1-h time horizon.

Three types of forecasting exist when it comes to photovoltaic output: short-term, medium-term, and long-term [34]. In study [35], a predictive model for PV power generation in Korea was presented, based on a recurrent neural network (RNN) and meteorological data. Four predictive features were selected: air temperature, relative humidity, solar radiation, and wind speed. Error rates of 13.8% and 13.2% were reported, respectively for the single- Long Short-Term Memory (LSTM) and multi-LSTM models. In another study, nine input parameters were used to train an artificial neural network that forecasts the output of a photovoltaic installation – global horizontal irradiance, global diffuse radiance, ambient temperature, precipitation, wind speed, air pressure, sunshine duration, relative humidity, and surface temperature [36]. The reported error rates vary between 72.64% and 0.74% for low and high insulation values, respectively. In study [37] the 24 h PV yield was forecasted using solar radiation and ambient temperature as input data. The authors proposed an artificial neural network (ANN) Multi-Layer Perceptron (MLP) model, which achieved an R^2 between 96% and 99% for sunny days and between 0.88% and 92% for cloudy days. Similarly, in [38] ultra-short PV power forecasting was investigated based on neural networks and four features – global horizontal irradiance, wind speed, ambient temperature, and relative humidity. The different models achieved an R^2 between 0.889 and 0.967 in the validation phase and between 0.910 and 0.971 in the testing phase.

Some studies have also compared the performance of the machine learning and deep learning approaches. In [39] the temperature of the PV surface, the solar irradiance, and the wind speed were used to predict the power output of a rooftop photovoltaic installation in Russia. A comparison between ANN and regression models showed the first had better performance with error rates between 0% and 30% for the different days. Similarly, in study [40] the power of a PV installation in Egypt was forecasted using three models – RF, Facebook Prophet, and LSTM. The features used are different components of the solar irradiance, wind speed at 10 m, temperature at 2 m, and sun height. The best-performing model was Prophet with R^2=0.93, which was confirmed by its mean square error (MSE) and MAE coefficients. In study [23] were used seven machine learning algorithms for short-term prediction of photovoltaic generation - extreme gradient boosting algorithm (XGB), support vector regressor (SVR), random forest (RF), classic MLP, and three LSTM-based models. Their achieved R^2 values varied from 0.90 to 0.91 for 15-minute-ahead forecasting, from 0.88 to 0.89 for 30-minute-ahead forecasting, and from 0.86 to 0.89 for 1-hour-ahead forecasting.

However, one of the key factors for forecasting the PV yield is the availability of reliable predictions for solar radiation. This task can also be implemented using either machine or deep learning. In study [41] different machine learning algorithms were evaluated in their ability to forecast solar radiation and ambient temperature, which are considered to have the highest impact on the PV output. Similarly, in study [42] predictions of the hourly solar radiation were made for time horizons h+1 and h+6 in Odeillo, France. They were based on ANN and RF models and the past solar radiations as input data. The RF algorithm achieved better results at forecasting the global horizontal irradiation with an NRMSE of 19.65% for the h+1 timeframe and 27.78% for the h+6 timeframe.

Other studies combined the forecasting of solar energy and PV power. In study [43], the MLP ANN method to forecast the PV power was used with a 10-minute discretization step. The authors investigated two scenarios – one with measured solar irradiance data and the other with predicted one. The precision of the models was estimated using different errors. The best-performing scenario achieved a 7% error for a scenario, which relies on three days of previous solar radiation data. Similarly, in study [44] two hybrid models were investigated for PV power forecasting. A statistical model for estimating solar radiation and a physical or statistical (ANN) model for estimating output power were trained. The ANN-based model achieved lower relative root mean square error, varying from 3.59% to 8.65% for 3 days ahead forecasting and from 5.25% to 11.85% for 6 days ahead forecasting.

The analysis of previous studies shows that a wide range of input data is used for forecasting photovoltaic power. Basic meteorological data, such as solar irradiance, ambient temperature, wind speed, relative humidity, rainfall, and cloudiness is used, as well as some parameters of the PV installations, such as module temperature and yield. Additional time-based features are often added, such as day of the week, month number, day type, week number, hour of the day, year type, etc. Previous authors have reported different accuracies of the existing models, which can be explained by the influence of local factors, such as shading, soiling, etc., and the chosen features. Furthermore, there isn't an obvious winner amongst the used approaches, such as machine learning and deep learning.

The agricultural sector has a great potential for creating additional value with the help of energy from photovoltaic installations. Such applications include powering of irrigation systems [45], animal farms [46,47], etc., and are commonly rooftop mounted. Rural areas are characterized with lack of high-rise buildings and other artificial objects, which could potentially influence the energy production of photovoltaics by creating shadings. Considering the above mentioned, it is important to investigate the possibilities for precise forecasting of the output PV power under such conditions.

This study aims to investigate the influence of different features on the performance of machine learning and deep learning models for forecasting the yield of PV installations located in rural areas.

II. Materials and Methods

A. Data Acquisition

This study relies on two data sources: a mid-scale PV park and a dedicated meteorological station. They are located in the village of Staro Selo, near the city of Tutrakan, Bulgaria, coordinates 43°59'11"N 26°32'49"E (Fig. 1).

Fig. 1. Geographic location of the experimental facility.

The photovoltaic park is installed on the roof of a building and its total power is 68.040 kWp. It is built of 378 monocrystalline modules SPV180M-24 by Sinski PV Co., Ltd. (Wuxi, Jiangsu, China). They are characterized by 180 Wp peak power, 14.1% efficiency, 45V open-circuit voltage, and 5.3 A short-circuit current under standard testing conditions. The orientation of the PV modules has an azimuth angle of 3° and an angle of inclination of 30°. The installation also contains 9 Sunny Mini Central 6000TL single-phase grid-connected inverters by SMA Solar Technology AG (Niestetal, Germany). Their key characteristics are 97.7% efficiency, 1 MPPT with four inputs, and an MPP voltage range of 333 V to 500 V. The inverters are connected to the internet via a Sunny WebBox and all data is stored on the SunnyPortal platform with a 1-hour time step.

The meteorological data is collected using a Sunny Sensor box by SMA Solar Technology AG (Niestetal, Germany), which includes:

- A solar radiation sensor with a measuring range 0÷1500 W/m^2 and an accuracy of 8%.
- A temperature sensor with a measuring range -30÷80 °C and an accuracy of 0.5°C.
- An anemometer with a measuring range of up to 40 m/s and an accuracy of 0.5%.

It is installed near the PV panels and similarly to the inverter, transmits data to the SunnyPortal platform via the Sunny WebBox with a 1-hour time step.

B. Methodology for Data Processing and Data Analysis

In this study, we have applied a data analysis methodology, which includes the following steps (Fig. 2): data preparation, feature preparation and engineering, model optimization, and features evaluation.

1) Step 1. Data preparation: In this step, the data is extracted from the cloud platform. The four datasets are exported in Microsoft Excel format and are merged into a single file with five columns – timestamp, energy yield, solar radiation, temperature, and wind speed. During the merging process, special attention should be paid to the correspondence of the timestamps of the records.

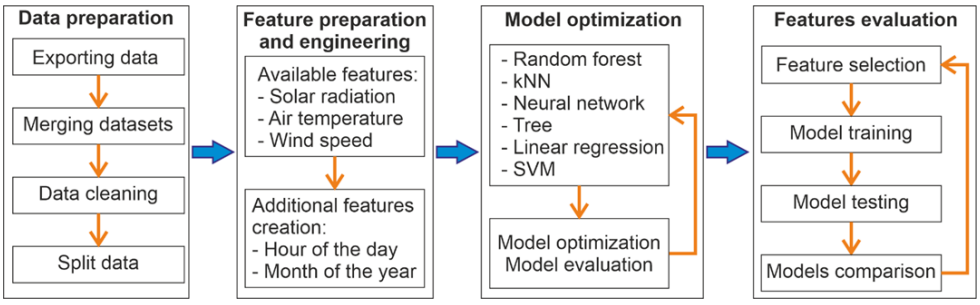


Fig. 2. Overview of the methodology used.

Next, the created dataset is analyzed for inconsistencies, such as:

- Empty or invalid values;
- The solar radiation is non-zero, while the PV yield is zero and vice-versa.

All records with such inconsistencies are removed from the dataset. Finally, the available data is divided into training/validation and testing datasets.

2) Step 2. Features preparation and engineering: In this step, the main features of the machine learning are selected. As previous authors have stated, the factors with the highest influence on the energy yield of photovoltaic installations are solar radiation, ambient temperature, and wind speed [22, 48]. Therefore, they are selected as the main features for model training. Secondary features, which are known to be correlated with solar radiation are the "month of the year" and the "hour of the day". They are extracted from the timestamp of the datasets using Microsoft Excel's "Month" and "Hour" functions. This way the "month of the year" feature takes values from 1 to 12 and the "hour of the day" feature takes values from 0 to 23.

3) Step 3. Model optimization: This step aims to obtain the optimal parameters of each of the selected machine-learning models, using all available features. In this study, we

have chosen the Orange Data Mining v3.36 tool, developed by the University of Ljubljana (Ljubljana, Slovenia) [49]. The reason for choosing it is the wide range of available components for training regression models, evaluation and comparison, modification of the input and output data, etc.

The goal is to train regression models, which can forecast the photovoltaic energy yield using the available features, i.e. the output of the models should be the predicted energy. Based on the results of previous studies, the following machine-learning algorithms are selected for evaluation:

- *Decision tree (DT)* – builds regression organized as a tree structure.
- *Random forest (RF)* – works by creating numerous DTs during the training phase. Each tree is constructed using a random subset of the dataset to measure a random subset of features in each partition. It can be used for both classification and regression tasks. Overfitting is a common problem that may worsen the model performance, which is commonly dealt with by adding enough trees in the forest.
- *K-nearest neighbor (kNN)* – a supervised machine learning algorithm that can be used for classification and regression tasks. It requires more time and memory and is commonly useful with smaller datasets.
- *Artificial neural network (ANN)* – a set of algorithms designed for recognizing patterns in data. They are modeled after the structure and function of the human brain and have shown acceptable results in all spheres of science.
- *Support vector machine (SVM)* – a selective classifier formally defined by dividing the hyperplane. The SVM algorithm intends to find a hyperplane in an N-dimensional space that classifies the data points.
- *Linear regression (LR)* – computes the linear relationship between the dependent variable and one or more independent features by fitting a linear equation to observed data.

The output of the abovementioned regression models is additionally modified (if required), to make sure no energy production is forecasted during the dark hours of the day:

$$E_{pred.m} = \begin{cases} E_{pred};\ Solar\ radiation \geq 0 \\ 0;\ Solar\ radiation < 1 \end{cases} \quad (1)$$

During this step, the parameters of each model are changed and their performance is assessed with the help of a 5-fold cross-validation. Several statistical metrics are used that allow to evaluate the difference between the original and the predicted values:

- Coefficient of determination (R^2) - it takes values between 0 and 1 and shows how well a model predicts the outcome:

$$R^2 = 1 - \frac{\sum_i^n (y_i - \widehat{y_i})^2}{\sum_i^n (y_i - \bar{y})^2}, \quad (2)$$

where, y_i and $\widehat{y_i}$ are the i^{th} samples of the actual and predicted variables and $\bar{y}$ is the mean of the actual values. It is known that when multiple regression models are evaluated, it is better to use the adjusted R^2 metric, which penalizes the additional features. However, this is true only when the number of records is relatively low. When the number of records is significantly higher than the number of features, R^2 and the adjusted R^2 have insignificant differences. That is why in this study the application of R^2 is considered appropriate.

- Mean square error (MSE) – measures the average squared difference between the actual and the predicted values with extra penalty to large errors:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \widehat{y_i})^2 \quad (3)$$

- Root mean square error (RMSE) – measures the average magnitude of the errors in the prediction and is the square root of MSE:

$$RMSE = \sqrt{MSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \widehat{y_i})^2}. \quad (4)$$

- Mean absolute error (MAE) – measures the average magnitude of the errors in the prediction and is useful when large errors should not be given extra penalty:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \widehat{y_i}|. \quad (5)$$

- Non-zero mean absolute error (NZMAE) – measures the average magnitude of the errors in the prediction using only the non-zero records. This metric gives more accurate results, as excludes nighttime records, where no energy is generated and no error is expected.

This step is repeated numerous times with different parameters of each regression model until a peak R^2 value is achieved.

4) Step 4. Features evaluation: This step aims to evaluate the influence of the selected features on the performance of the trained models. The following variants are considered:

- Variant 1. Only solar radiation;
- Variant 2. Solar radiation and ambient temperature;
- Variant 3. Solar radiation, ambient temperature, and wind speed;
- Variant 4. Solar radiation, ambient temperature, wind speed, and hour of the day;
- Variant 5. Solar radiation, ambient temperature, wind speed, hour of the day, and month of the year.

For each of the abovementioned variants:

- The training dataset is modified to include only the corresponding features. This is implemented directly in the Orange Data Mining software, by selecting the necessary columns from the Files component.
- The six models are trained again with the selected features.

- The testing dataset is modified similarly to the training one.
- The trained models are applied to the testing dataset and the metrics from Step 3 are evaluated.

Next, the evaluated metrics are compared and the performance of each model with the different feature variants is obtained. The optimal variant and model are determined.

Other than the hourly generated energy, another important parameter of photovoltaic installations is the cumulative daily generated energy. Therefore, during this phase is also estimated the cumulative energy production for each of the testing days according to:

$$E_D = \sum_{i=0}^{23}(E_H), \quad (6)$$

where, E_H is the hourly energy production. The estimated daily energy productions can be compared to each other to identify problems where a model's predictions are dominantly above or below the actual values.

III. Results and Discussion

The datasets were prepared using data obtained in the period from 4 January 2020 to 20 December 2022. Previous studies have recommended the datasets for accurate PV forecasting to be at least 1 full year [38], therefore the used data conforms to this recommendation. Following the proposed methodology, four datasets were exported with 1 h timestep: specific yield in kWh/kWp, solar radiation in W/m^2, ambient temperature in °C, and wind speed in m/s. Thereafter, they were merged, and all records with missing, incomplete, or inconsistent data were removed. The data was split into training and testing datasets as follows:

- The training data includes 13781 records from 4 January 2020 to 31 July 2021;
- The testing data includes 3394 records from 1 August 2021 to 20 December 2021.

Next, the two additional features ("month of the year" and "hour of the day") were added to the datasets. A sample from the prepared training dataset is shown in Fig. 3. The first column (Timestamp) is not used as a feature but is kept as metadata for easier analysis. The last column contains the target variable (the specific energy yield, produced by the PV installation for 1 h), which should be forecasted.

Timestamp	Month of the year	Hour of the day	Solar rad, W/m2	Tavg, °C	Wind speed m/s	specific_yield, Wh/kWp
05.01.2020 06:00	1	6	1.86	4.8	2.89	0
05.01.2020 07:00	1	7	1.97	4.28	4.15	0
05.01.2020 08:00	1	8	1.83	3.72	5.37	0
05.01.2020 09:00	1	9	2.2	3.09	3.76	0
05.01.2020 10:00	1	10	14.8	2.63	0.56	8
05.01.2020 11:00	1	11	25.81	2.06	0.23	17
05.01.2020 12:00	1	12	93.64	2.78	0	79
05.01.2020 13:00	1	13	120.53	3.11	0.2	105
05.01.2020 14:00	1	14	183.53	4.31	1.27	158

Fig. 3. A sample from the prepared training data.

Next, the training and testing procedure were implemented in Orange Data Mining, as shown in Fig. 4. According to step 3 of the methodology, the optimal parameters of the six machine learning algorithms were obtained experimentally using all available features so that their R2 values were as close to 1 as possible. Their optimal parameters are summarized in Table I.

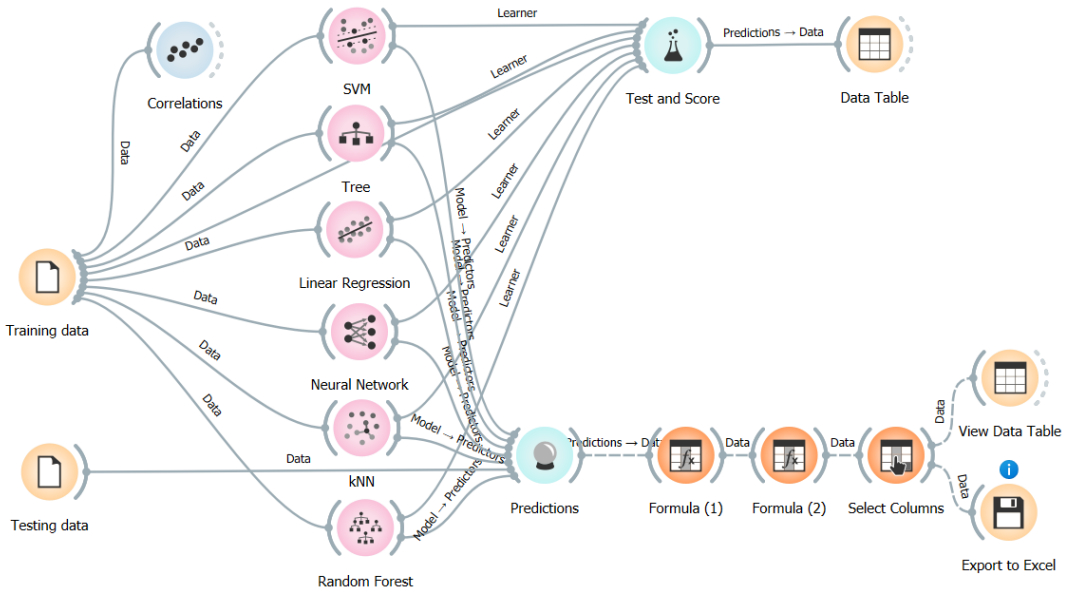


Fig. 4. Implementation of the training and testing methodology in orange data mining.

TABLE I. PARAMETERS OF THE OPTIMAL MODELS

Model	Parameters
Random forest	Number of trees: 6 Number of attributes considered at each split: not checked Replicable training: checked Balance class distribution: not checked Limit depth of individual trees: not checked Do not split subsets smaller than: not checked
K nearest neighbor	Number of neighbors: 5 Metric: Euclidean Weight: Uniform
Artificial neural network	Neurons in hidden layers: 20 Activation: ReLu Solver: L-BFGS-B Regularization, α=0: Maximal number of iterations: 300 Replicable training: checked
Linear regression	Fit intercept: checked Regularization: No regularization
Decision tree	Induce binary tree: not checked Min number of instances in leaves: 12 Do not split subsets smaller than: not checked Limit the maximal tree depth to: not checked Stop when majority reaches: 95%
Support vector machine	SVM type: SVM Cost (C): 1.40 Regression loss epsilon (ε): 0.10 Kernel: Linear Numerical tolerance: 0.0010 Iteration limit: 20 000

The model is validated using 5-fold cross-validation, which means that 20% of the records are randomly chosen for validation and the remaining 80% are used for training. The results from the models' training and validation are summarized in Table II, ordered decreasingly by their R^2 value. The best-performing algorithm is the ANN, RMSE, and MAE, with R^2 respectively 0.995, 18.3, and 7.5.

TABLE II. COMPARISON OF THE MODELS' VALIDATION PERFORMANCE

Model	MSE	RMSE	MAE	R^2
ANN	336	18.3	7.50	0.995
RF	383	19.6	6.94	0.994
kNN	390	19.8	7.31	0.994
DT	411	20.3	7.74	0.994
LR	952	30.9	18.7	0.985
SVM	1041	32.3	15.5	0.984

The order of the next three models is disputable for the following reasons:

- The RF has the second-best R^2 equal to 0.994; however, its MAE (6.94) is the lowest. In other words, if we choose the optimal model based on its MAE then the RF model performs slightly better than the trained ANN.
- The kNN model has the same R^2 as RF, and its MAE (7.31) is also lower than ANN's.
- The DT has the same R^2 as RF and kNN, and almost the same MAE (7.74).

In general ANN, RF, kNN, and DT perform almost equally well in our study. The other two models (LR and SVM) perform slightly worse, though their R^2 values are still impressive – 0.985 and 0.984, respectively. However, their MAE metrics are more than twice as bad (18.7 and 15.5, respectively), which means their forecasts contain more errors. This is also indicated by their RMSE metrics (30.9 and 32.3, respectively), which penalize large errors.

Next, according to the developed methodology, the performance of the models was evaluated for the different feature variants. For each one the corresponding features were selected from the training and testing datasets and the models were retrained and reevaluated with the testing dataset. The results from Variants 1, 2, 3, 4, and 5 are summarized in Table III, Table IV, Table V, Table VI, and Table VII, respectively.

TABLE III. RESULTS FROM THE TESTING OF VARIANT 1 (ONLY SOLAR RADIATION)

Model	MSE	RMSE	MAE	NZMAE	R^2
ANN	567	23.8	10.2	21.2	0.990
DT	638	25.3	10.8	22.6	0.989
kNN	691	26.3	11.3	23.7	0.988
RF	838	29.0	12.6	26.6	0.986
LR	985	31.1	13.8	28.8	0.983
SVM	1021	32.0	13.8	28.9	0.983

TABLE IV. RESULTS FROM THE TESTING OF VARIANT 2 (SOLAR RADIATION AND AMBIENT TEMPERATURE)

Model	MSE	RMSE	MAE	NZMAE	R^2
ANN	323	18.0	6.41	13.4	0.994
kNN	352	18.8	6.72	14.3	0.994
DT	347	18.6	6.83	14.3	0.994
RF	406	20.1	7.15	15.2	0.993
LR	930	30.0	13.5	28.3	0.984
SVM	1022	32.0	13.9	28.9	0.983

TABLE V. RESULTS FROM THE TESTING OF VARIANT 3 (SOLAR RADIATION, AMBIENT TEMPERATURE, AND WINDSPEED)

Model	MSE	RMSE	MAE	NZMAE	R^2
ANN	314	17.7	6.12	12.8	0.995
kNN	358	18.9	6.61	14.1	0.994
DT	355	18.8	6.90	14.5	0.994
RF	383	19.6	6.84	14.5	0.993
LR	930	29.9	13.60	28.4	0.984
SVM	1025	32.0	13.86	28.9	0.983

TABLE VI. RESULTS FROM THE TESTING OF VARIANT 4 (SOLAR RADIATION, AMBIENT TEMPERATURE, WINDSPEED, AND HOUR OF THE DAY)

Model	MSE	RMSE	MAE	MZMAE	R^2
ANN	299	17.3	5.71	11.9	0.995
kNN	357	18.9	6.65	14.2	0.994
DT	358	18.9	6.93	14.6	0.994
RF	372	19.3	6.56	14.1	0.993
LR	930	30.5	13.6	28.4	0.984
SVM	1022	32.0	13.9	28.9	0.983

TABLE VII. RESULTS FROM THE TESTING OF VARIANT 5 (SOLAR RADIATION, AMBIENT TEMPERATURE, WINDSPEED, HOUR OF THE DAY, AND MONTH OF THE YEAR)

Model	MSE	RMSE	MAE	NZMAE	R^2
ANN	335	18.3	6.44	13.4	0.994
kNN	367	19.2	6.65	13.7	0.994
DT	373	19.3	6.93	14.0	0.994
RF	436	20.9	6.56	14.1	0.993
LR	936	30.6	16.2	28.4	0.984
SVM	1023	32.0	14.0	28.9	0.983

If we take a look at the obtained coefficients of determination, several things can be noticed:

- The ANN models have the best performance in all five variants of the input features with R2 ranging between 0.990 and 0.995;
- The RF, kNN and DT models return very close results in all cases with R2 between 0.986 and 0.994;
- The SVM and the LR models have the worst performance in all cases, although it is not significantly worse. They are practically the same in all five variants; i.e., if these algorithms are selected, solar radiation can be used as the only feature.

All models in all variants achieved excellent coefficients of determination, ranging between 0.983 and 0.995. At first glance, the last statement means that there is not any significant difference between the six algorithms. That is why a closer look should be taken at the other metrics. For Variant 1 (Table III) the ANN model achieved an MAE of 10.2 Wh/kWh/h, which means that for the investigated testing period (3394 hours or approximately five months) the expected cumulative error is 34.6 kWh/kWp. However, if only the non-zero records are accounted for, as no error is expected during the dark hours of the day, the NZMAE metric is 21.2 Wh/kWh/h, i.e. approximately twice as high as MAE. For the worst-performing model (SVM) the MAE and NZMAE are 13.8 Wh/kWp/h and 28.0 Wh/kWhp/h, respectively, corresponding to a cumulative error of 46.837 kWh/kWp.

For Variant 2, ANN's MAE and NZMAE reach 6.41 Wh/kWp/h and 13.4 Wh/kWp/h, respectively (i.e., a cumulative error of 21.8 kWh/kWp), and for Variant 3 – 6.12 Wh/kWp/h and 12.8 Wh/kWp/h, respectively (a cumulative error of 20.8 kWh/kWp). The best performance was achieved for Variant 4, where ANN's MAE and NZMAE reached 5.71 Wh/kWp/h and 11.9 Wh/kWp/h (a cumulative error of 19.4 kWh/kWp), while for Variant 5 the score was slightly worse.

If the RMSE metric is analyzed, which adds a penalty to higher errors, once again the optimal value is achieved by the ANN model with Variant 4 – 17.3 Wh/kWp/h and the lowest by the SVM model, which is 32.0 Wh/kWp/h for all five variants.

For a better understanding of the precision of the trained models, the worst-case (Variant 1) and best-case (Variant 4) models are further compared. In Fig. 5 statistics about the total daily absolute error of the models for Variant 1 is presented. The minimal daily errors for the different models vary between 0.6 (SVM) and 4.0 (kNN) Wh/kWp/Day. The maximum daily errors vary between 523 (ANN) and 711 (LR) Wh/kWp/Day. The average daily error is the lowest for DT (169.973 Wh/kWp/Day and the highest for SVM (218.508 Wh/kWp/Day). The cumulative daily error for the investigated period is the lowest for DT (24136 Wh/kWh) and the highest for SVM (31028.2 Wh/kWh).

Similarly, in Fig. 6 the total daily absolute errors for Variant 4 (best-case) are presented. It is interesting to notice that the maximal daily errors are higher in this situation and vary between 596 (kNN) and 767 (RF) Wh/kWp/Day. Nevertheless, the cumulative errors for the investigated period are significantly lower for all algorithms except SVM and LR. The lowest cumulative error was achieved by ANN (10813 Wh/kWp) and the highest again by SVM (31045.4 Wh/kWp). Similarly, the lowest average daily error was achieved by ANN (76.82 Wh/kWp/Day) and the highest again by SVM (218.63 Wh/kWp/Day).

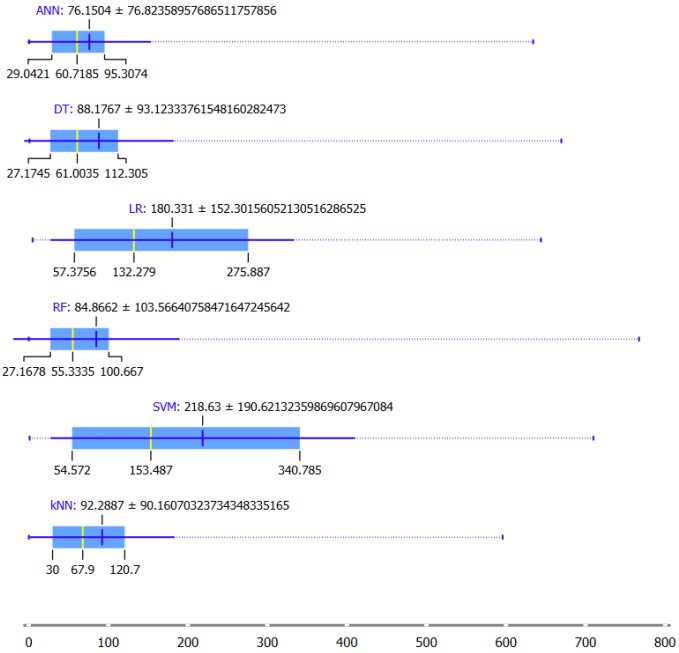


Fig. 5. Cumulative absolute daily errors of the 6 models for Variant 4 of the selected features: dark blue vertical line – mean value; thin blue – standard deviation; yellow line – the median; blue highlighted area – the values between the first and the third quartile.

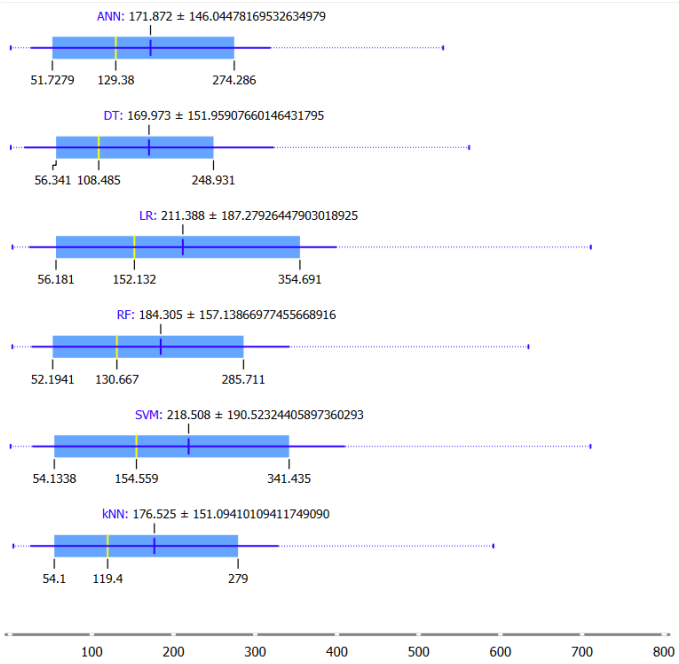


Fig. 6. Cumulative absolute daily errors of the 6 models for Variant 1 of the selected features: dark blue vertical line – mean value; thin blue – standard deviation; yellow line – the median; blue highlighted area – the values between the first and the third quartile.

Furthermore, the following examples of the actual and predicted hourly PV yields with high errors are demonstrated:

- Example 1: Hourly data forecasts of one of the days with the worst cumulative absolute error of the ANN model in Variant 1 (4 August 2022) and the corresponding predictions in Variant 4 (Fig. 7).
- Example 2: Hourly data forecasts of one of the days with the worst cumulative absolute error of the ANN model in Variant 4 (27 November 2022) and the corresponding predictions in Variant 1 (Fig. 8).

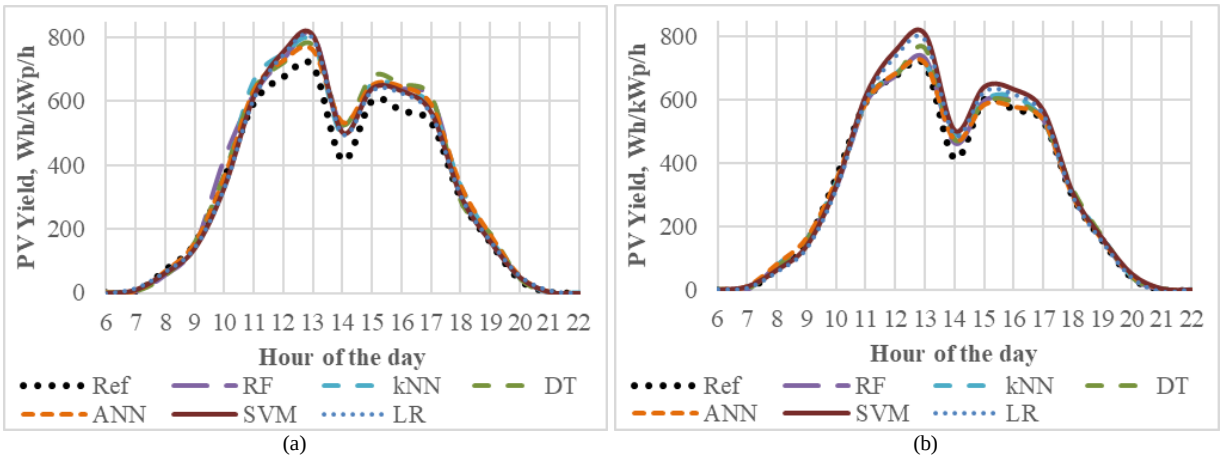


Fig. 7. Sample data from 4 August 2022 for Variant 1 (a) and Variant 4 (b) of the used features.

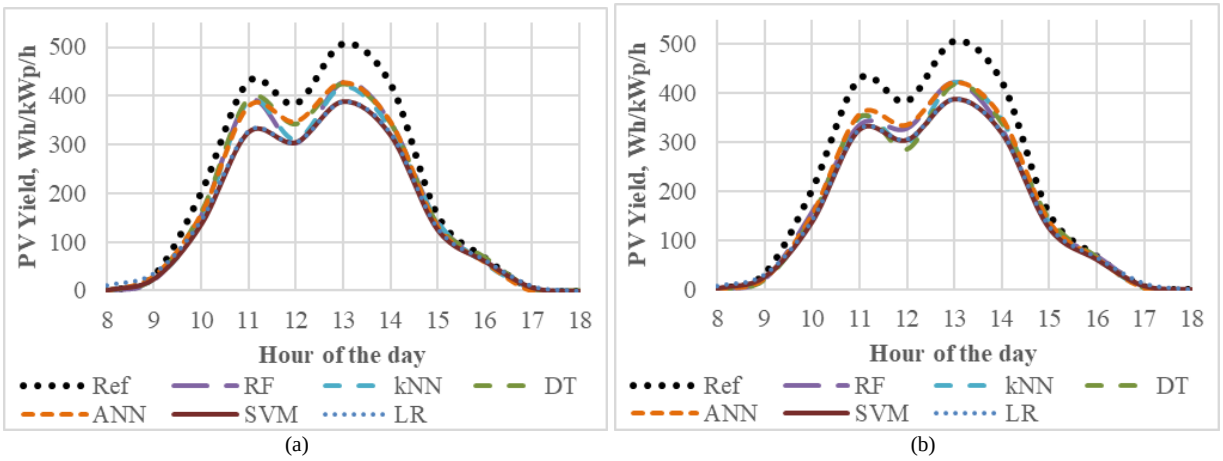


Fig. 8. Sample data from 27 November 2022 for Variant 1 (a) and Variant 4 (b) of the used features.

Both examples show that the higher errors occur mostly on days with varying cloudiness. This behavior is expected, because of the increased errors when estimating the average hourly solar radiation introduced by the period of discretization. Nevertheless, in both situations, the obtained forecasts by the ANN model are slightly better in Variant 4, compared to Variant 1, in which only solar radiation is used as a feature. Other examples are presented in Fig. 9(a) and Fig. 9(b), where the actual and forecasted values from 25 September to 27 September 2022 are shown, representing the models from Variants 1 and Variant 4, respectively. In this case, no significant deviations are observed from the actual values and this refers to both variants of the features used. The maximum absolute difference of the ANN model from the observed values does not surpass 50 Wh/kWp/h for Variant 1 and 36 Wh/kWp/h for Variant 4.

Finally, predicted vs. actual scattered graphs were prepared for all six models with Variant 4 of the selected features, which should provide a clear understanding of their performance. They are presented in Fig. 10, where the models are ordered in the decreasing order of their coefficient of determination.

The following observations could be made:

- One anomaly with all 6 models could be noticed, most likely caused by a maintenance procedure or some technical fault with the PV installation.
- The best performance of the ANN models is also confirmed by the lowest scattering of the predicted vs. actual points [(Fig. 10(a)].
- The kNN [(Fig. 10(b)] and DT [(Fig. 10(c)] models perform almost as well as ANN; however, several points are separated slightly from the main group, which explains their lower score.
- Two of the points of the RF model [(Fig. 10(d)] are significantly separated from the main group. However, if these records are excluded from the testing dataset, the RF model could be a contender for the top spot.
- The performance of the LR [(Fig. 10(e)] and SVM [(Fig. 10(f)] models is significantly worse, and it can be noticed that their predicted vs. actual graph can be better approximated with a polynomial, rather than a straight line.

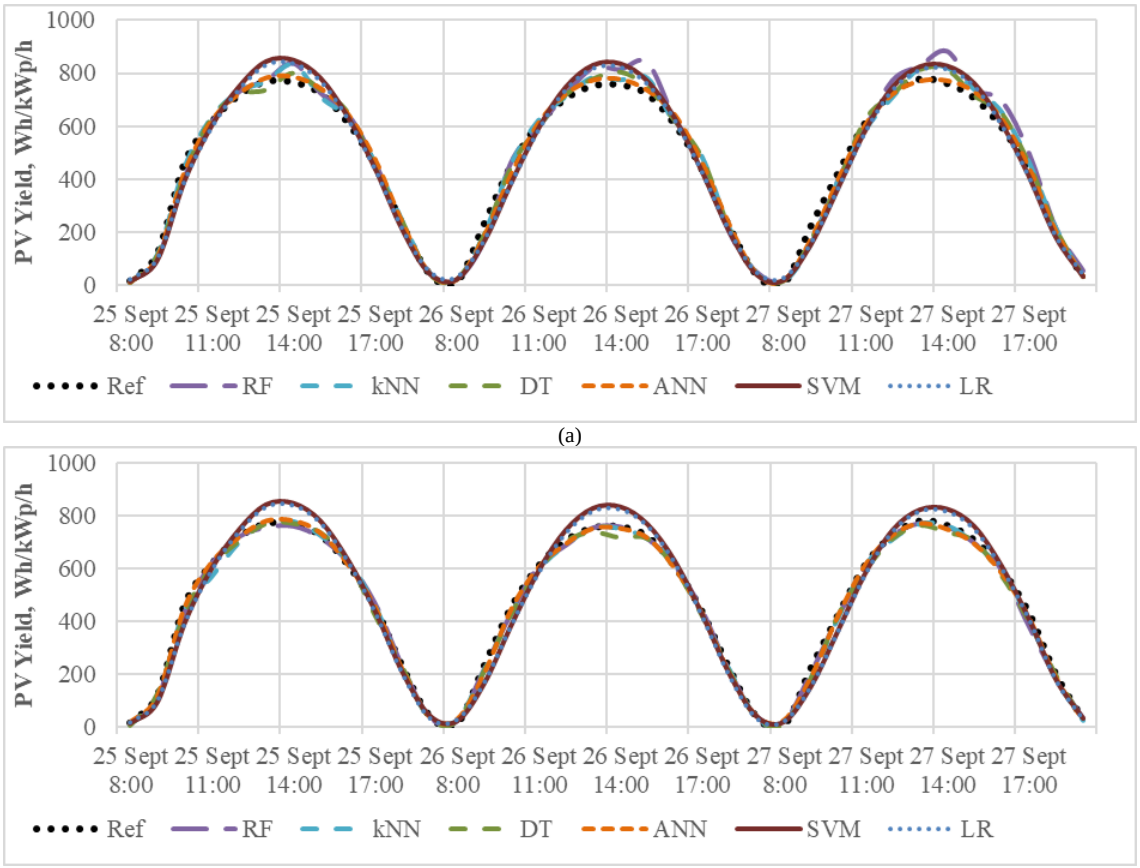


Fig. 9. Sample data from the daylight hours of 25-27 September 2022 for variant 1 (a) and variant 4 (b).

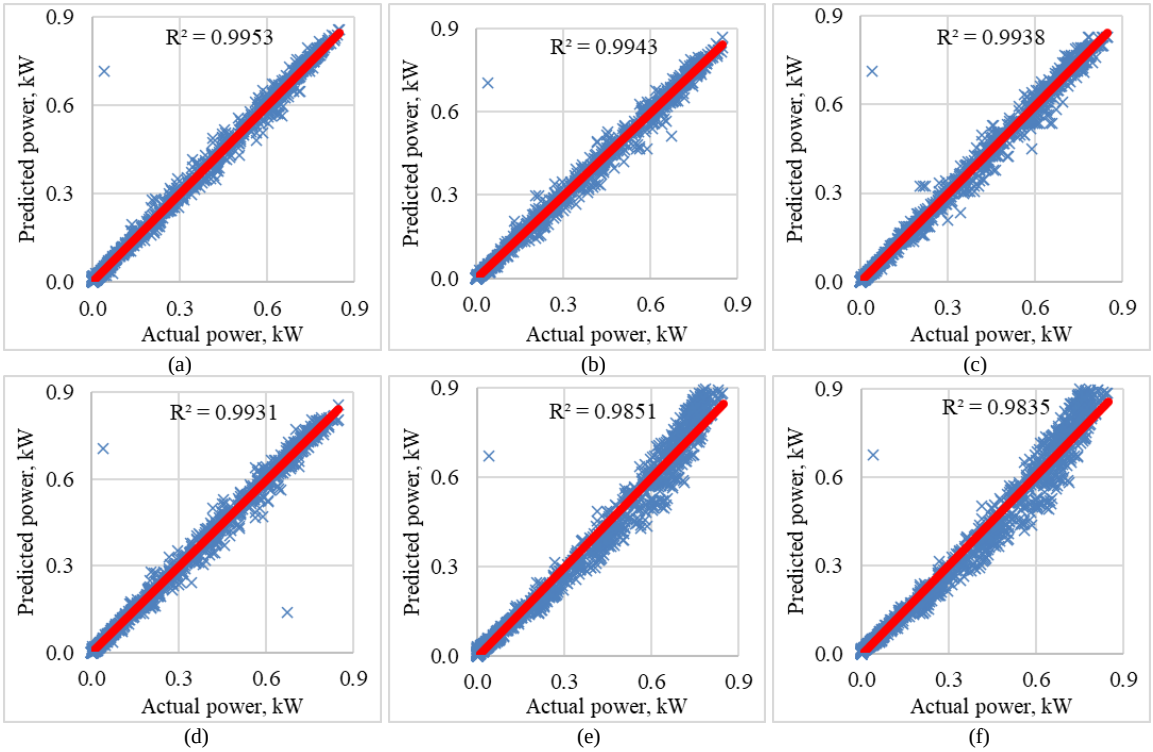


Fig. 10. Comparison between actual and predicted specific yields for the six models with variant 4 of the features: a) ANN; b) kNN; c) DT; d) RF; e) LR; f) SVM.

The performance of the trained models could be compared with that achieved in previous studies. In [32] different machine learning algorithms for forecasting the power of a PV installation were evaluated using eight features. The best-performing model was RF, which achieved an R^2 of 0.95 and an MAE of 68.7 W. Similarly, in study [30] different machine-learning models using ambient temperature and solar irradiance as features were compared. The Fine tree model achieved the highest R^2 and RMSE, 0.959 and 5.83 W, respectively.

If compared with studies relying on deep learning, our results are also ranked very well. In study [35] several meteorological parameters, the day, and time were used as features to predict the PV yield. The multiple LSTM neural network achieved an RMSE of 37.1 Wh and an error rate of 13.2%; however, no MAE and R^2 were reported. Similarly, in [40] solar irradiance, windspeed, ambient temperature, and the Sun height were used as input data to predict the PV power. The optimal model was Facebook Prophet, which achieved an R^2 of 0.93, an MAE of 8.77 W, and an RMSE of 3.28 W.

A significantly different approach was used in study [23], where the previous PV yield was used as input data for ANN models to predict the 1-hour-ahead yield. The optimal model achieved R^2, MAE, and RMSE of 0.89, 13.4 Wh, and 27.5 Wh, respectively. A similar approach in [43], where the 3 days ahead solar radiation was used, led to an MAE of 0.00 kW and a RMSE of 35.4 kW with a MLP ANN; though no info was provided about the coefficient of determination.

In study [50] was used a hybrid machine learning model, combining variational mode decomposition (VMD), whale optimization algorithm (WOA), and long short-term memory neural network (LSTM) to forecast power. The study relied on the ambient temperature, relative humidity, global and diffuse horizontal radiation to achieve an R^2 of 0.997.

The above-mentioned is summarized in Table VIII and allows us to conclude that our results position themselves very well. Out of the papers that provided a coefficient of determination, we achieved the second-best results with an R^2 of more than 99%, and were outperformed only by the hybrid model, proposed in study [50]. Similarly, the MAE we achieved is the lowest, compared to the previous studies; however, in terms of RMSE, our optimal models are ranked 3rd. The last information indicates that the models trained in this study returned several wrongly forecasted values, which differ significantly from the actual ones.

TABLE VIII. COMPARISON OF THE ACHIEVED RESULTS WITH THOSE OF PREVIOUS STUDIES

Article	Regression model	Features	Target	R^2	MAE	RMSE
Alhmoud et al [32]	RF	Irradiation, air temperature, module temperature, day of the week, month number, day type, week number, hour of the day, and year type	PV power in W	0.95	68.7 W	N/A
Zulkifly et al. [30]	Fine tree	Ambient temperature, solar irradiance	PV power in W	0.96	34.9 W	5.83 W
Park et al [35]	Multiple LSTM ANN	Ambient temperature, humidity, direct solar radiation, diffuse solar radiation, wind speed, day, and time	PV yield in Wh	N/A	N/A	37.1 Wh
Allam et al [40]	Facebook Prophet	Solar irradiance, wind speed, ambient temperature, sun height	PV power in W	0.93	8.77 W	3.28 W
Cantillo-Luna et al [23]	ConvLSTM1D ANN	Lagged PV yield	1 h ahead PV yield in Wh	0.89	13.4 Wh	27.5 Wh
Stoyanov and Draganovska [43]	MLP ANN	3 days ahead solar radiation	PV power in kW	N/A	0.00 kW	35.4 kW
Hou et al [50]	A hybrid VMD, WOA and LSTM model	Ambient temperature, relative humidity, global and diffuse horizontal radiation	PV power in kW	0.997	15.247	19.753 kW
Ours	ANN kNN DT RF	Solar radiation, wind speed, ambient temperature	Specific PV yield in Wh	0.995 0.994 0.994 0.993	5.71 Wh 6.65 Wh 6.93 Wh 6.56 Wh	17.3 Wh 18.9 Wh 18.9 Wh 19.3 Wh

IV. CONCLUSIONS

The performance of different machine learning algorithms (ANN, kNN, DT, RF, LR, and SVM) for forecasting the yield of a rural photovoltaic installation was evaluated in this study. An almost complete hourly dataset from 2020 and 2021 was used and divided into training/validation and testing datasets. Five combinations of the input features (solar radiation, ambient temperature, wind speed, hour of the day, and month of the year) were evaluated.

During the 5-fold cross-validation step the ANN achieved the highest R^2 (0.995), closely followed by RF, kNN, and DT (0.994). LR and SVM returned a lower coefficient of determination (0.985 and 9.984, respectively), though it is not significantly lower. During the testing stage, the worst results were achieved with solar radiation as the only feature, and the best results with solar radiation, ambient temperature, wind speed, and hour of the day. In all cases, the ANN model had the highest performance in terms of R^2, MAE, RMSE, and NZMAE, though once again it was very closely followed by kNN, DT, and RF.

The obtained results allow us to conclude that when a PV installation is located in a rural or ruruban area, which is characterized by a lack of significant shadings influencing its operation:

- the optimal combination of features for forecasting the output power is solar radiation, ambient temperature, wind speed, and hour of the day;
- the optimal models are ANN, kNN, DT, and RF;
- in case of limited availability of meteorological data, it is acceptable (in terms of forecasting errors) to use solar

radiation and ambient temperature or only solar radiation data as features.

The results obtained in this study could be useful to energy experts and farm owners, who are trying to maximize their profit and added value. However, it should not be forgotten that with such an approach the models also need reliable input data, such as solar radiation, ambient temperature, and wind speed. Therefore, it is also important to investigate the influence of the forecasted feature errors on the precision of the trained models, i.e. if a certain error is added to the meteorological data, what absolute and relative difference will it create. Moreover, in the present paper, we accepted that the PV installation produces only active power, which is not always the case. The presence of reactive consumers in the industry might be a significant problem when PV installations produce only active power and require a thorough investigation. The abovementioned problems were not addressed in this study and are an object for future research.

ACKNOWLEDGMENT

This research is financed by the Bulgarian National Science Fund under Project КП-06-Н77/2 “Research and optimization of hybrid system with renewable energy sources for power supply of livestock farm”.

This research is supported by the European Union-NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, project № BG-RRP-2.013-0001-C01.

REFERENCES

[1] K. Manohar, R. Ramkissoon, A. Adeyanju, “Cost benefit analysis of implementing a solar photovoltaic system,” International Journal of Innovative Research in Science, Engineering and Technology, vol. 4, no. 12, pp. 1-8, 2015, doi: https://doi.org/10.15680/IJIRSET.2015.0412006

[2] Y. Wang, R. Das, G. Putrus, R. Kotter, “Economic evaluation of photovoltaic and energy storage technologies for future domestic energy systems – A case study of the UK,” Energy, vol. 203, 2020, doi: https://doi.org/10.1016/j.energy.2020.117826

[3] K. Natesan, C.K. Nagaraj, N.K. Chandran, “Studies on improvement of solar PV panel performance,” Journal of Chemical Technology and Metallurgy, vol. 58, no. 6, pp. 1065-1070, 2023, doi: http://dx.doi.org/10.59957/jctm.v58i6.145

[4] L.P. Panagoda, R.A. Sandeepa, W.A. Perera, D.M. Sandunika, S.M. Siriwardhana, M.K. Alwis, S.H. Dilka, “Advancements in Photovoltaic (PV) Technology for Solar Energy Generation,” Journal of Research Technology & Engineering, vol. 4, no. 30, pp. 30-72, 2023, https://www.jrte.org/wp-content/uploads/2023/07/Advancements-In-Photovoltaic-Pv-Technology-for-Solar-Energy-Generation.pdf

[5] D. Rekioua, “Energy Storage Systems for Photovoltaic and Wind Systems: A Review,” Energies, vol. 16, no. 9, 2023, doi: https://doi.org/10.3390/en16093893

[6] A.S. Hassan, L. Cipcigan, N. Jenkins, “Optimal battery storage operation for PV systems with tariff incentives,” Appl. Energy, vol. 203, pp. 422–441, 2017, doi: https://doi.org/10.1016/j.apenergy.2017.06.043

[7] G.G. Zanvettor, M. Casini, A. Vicino, “Optimal Operation of Energy Storage Facilities in Incentive-Based Energy Communities,” Energies, vol. 17, no. 11, 2024, doi: https://doi.org/10.3390/en17112589

[8] H. Beltran, P. Ayuso, E. Pérez, “Lifetime Expectancy of Li-Ion Batteries used for Residential Solar Storage,” Energies, vol. 13, no. 3, 2020, doi: https://doi.org/10.3390/en13030568

[9] K.J. Iheanetu, “Solar Photovoltaic Power Forecasting: A Review,” Sustainability, vol. 14, no. 24, 2022, doi: https://doi.org/10.3390/su142417005

[10] A. Rhouma, Y. Said, “Solar Energy Forecasting Based on Complex Valued Auto-encoder and Recurrent Neural Network,” International Journal of Advanced Computer Science and Applications(IJACSA), vol. 14, no 4, 2023, doi: https://dx.doi.org/10.14569/IJACSA.2023.0140443

[11] Z.R. Tahir, A. Kanwal, M. Asim, M. Bilal, M. Abdullah, S. Saleem, M.A. Mujtaba, I. Veza, M. Mousa, M.A. Kalam, “Effect of Temperature and Wind Speed on Efficiency of Five Photovoltaic Module Technologies for Different Climatic Zones,” Sustainability, vol. 14, no. 23, 2022, doi: https://doi.org/10.3390/su142315810

[12] M.H. Alomari, O. Younis, S. Hayajneh, “A Predictive Model for Solar Photovoltaic Power using the Levenberg-Marquardt and Bayesian Regularization Algorithms and Real-Time Weather Data,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 9, no.1, 2018, doi: http://dx.doi.org/10.14569/IJACSA.2018.090148

[13] H.A. Kazem, M.T. Chaichan, I.M. Al-Shezawi, H.S. Al-Saidi, H.S. Al-Rubkhi, K. Alsinani, A.H. Al-Waeli, “Effect of Humidity on the PV Performance in Oman,” Asian Transactions on Engineering, vol. 2, no. 4, pp. 29–32, 2012.

[14] D.S. Hasan, M.S. Farhan, H. Alrikabi, “Impact of Cloud, Rain, Humidity, and Wind Velocity on PV Panel Performance,” Wasit Journal of Engineering Sciences, vol. 10, no. 2, pp. 34-43, 2022, doi: https://doi.org/10.31185/ejuow.Vol10.Iss2.237

[15] B. Stankov, A. Terziev, M. Vassilev, M. Ivanov, “Influence of Wind and Rainfall on the Performance of a Photovoltaic Module in a Dusty Environment,” Energies, vol. 17, no. 14, 2024, doi: https://doi.org/10.3390/en17143394

[16] M.R. Maghami, H. Hizam, C. Gomes, M.A. Radzi. M.I. Rezadad, S. Hajighorbani, “Power loss due to soiling on solar panel: A review,” Renewable and Sustainable Energy Reviews, vol. 59, pp. 1307-1316, 2016, doi: https://doi.org/10.1016/j.rser.2016.01.044

[17] P. dos Santos Vicente, E.M. Vicente, M.G. Simoes, E.R. Ribeiro, “Shading position effects on photovoltaic panel output power,” International Transactions on Electrical Energy Systems, vol. 30, no. 1, e12163, 2020, doi: https://doi.org/10.1002/2050-7038.12163

[18] D. Wang, T. Qi, Y. Liu, Y. Wang, J. Fan, Y. Wang, H. Du, “A method for evaluating both shading and power generation effects of rooftop solar PV panels for different climate zones of China,” Solar Energy, vol. 205, pp. 432-445, 2020, doi: https://doi.org/10.1016/j.solener.2020.05.009

[19] H. Yang, J. Chang, H. Wang, D. Song, “Power degradation caused by snail trails in urban photovoltaic energy systems,” Energy Procedia, vol. 88, pp. 422-428, 2016, doi: https://doi.org/10.1016/j.egypro.2016.06.018

[20] R.A.G. Burbano, G. Petrone, P. Manganiello, “Early Detection of Photovoltaic Panel Degradation through Artificial Neural Network,” Applied Sciences, vol. 11, no. 19, 2021, doi: https://doi.org/10.3390/app11198943

[21] S. Baratsas, F. Iseri, E.N. Pistikopoulos, “A hybrid statistical and machine learning based forecasting framework for the energy sector,” Computers & Chemical Engineering, vol. 188, 2024, doi: https://doi.org/10.1016/j.compchemeng.2024.108740

[22] A. Gholami, M. Ameri, M. Zandi, R.G. Ghoachani, S.J. Gerashi, H.A. Kazem, A.H. Al-Waeli, “Impact of harsh weather conditions on solar photovoltaic cell temperature: Experimental analysis and thermal-optical modeling,” Solar Energy, vol. 252, pp. 176-194, 2023, doi: https://doi.org/10.1016/j.solener.2023.01.039

[23] S. Cantillo-Luna, R. Moreno-Chuquen, D. Celeita, G. Anders, “Deep and Machine Learning Models to Forecast Photovoltaic Power Generation,” Energies, vol. 16, no. 10, 2023, doi: https://doi.org/10.3390/en16104097

[24] T. Berghout, M. Benbouzid, T. Bentrcia, X. Ma, S. Djurović, L.-H. Mouss, “Machine Learning-Based Condition Monitoring for PV Systems: State of the Art and Future Prospects,” Energies, vol. 14, no. 19, 2021, doi: https://doi.org/10.3390/en14196316

[25] E. Garoudja, A. Chouder, K. Kara, S. Silvestre, “An enhanced machine learning based approach for failures detection and diagnosis of PV systems,” Energy Convers. Manag., vol. 151, pp. 496–513, 2017, doi: http://doi.org/10.1016/j.enconman.2017.09.019

[26] A. Eskandari, J. Milimonfared, M. Aghaei, “Line-line fault detection and classification for photovoltaic systems using ensemble learning model

based on I-V characteristics," Sol. Energy, vol. 211, pp. 354–365, 2020, doi: http://doi.org/10.1016/j.solener.2020.09.071

[27] M. Dhimish, "Defining the best-fit machine learning classifier to early diagnose photovoltaic solar cells hot-spots," Case Stud. Therm. Eng., vol. 25, 2021, doi: http://doi.org/10.1016/j.csite.2021.100980

[28] K.Y. Yap, C.R. Sarimuthu, J.M. Lim, "Artificial intelligence based MPPT techniques for solar power system: A review," Journal of Modern Power Systems and Clean Energy, vol. 8, no. 6, pp. 1043-1059, 2020, doi: https://doi.org/10.35833/MPCE.2020.000159

[29] M. Gautam, S. Raviteja, R. Mahalakshmi, "Household energy management model to maximize solar power utilization using machine learning," Procedia Computer science, vol. 165, pp. 90-96, 2019, doi: https://doi.org/10.1016/j.procs.2020.01.075

[30] Z.A. Zulkifly, K.A. Baharin, C.K. Gan, "Improved machine learning model selection techniques for solar energy forecasting applications," International Journal of Renewable Energy Research (IJRER), vol. 11, no. 1, pp. 308-319, 2021, doi: https://doi.org/10.20508/ijrer.v11i1.11772.g8135

[31] S. Wendlandt, F. Popescu, "Photovoltaic Energy Yield Prediction Using an Irradiance Forecast Model Based On Machine Learning For Decentralized Energy Systems," The European Photovoltaic Solar Energy Conference and Exhibition (EU PVSEC), France, pp. 1860–1864, 2019, doi: https://doi.org/10.4229/EUPVSEC20192019-6CV.1.6

[32] L. Alhmoud, A.M. Al-Zoubi, I. Aljarah, "Solar PV power forecasting at Yarmouk University using machine learning techniques," Open Engineering, vol. 12, pp. 1078–1088, 2022, doi: https://doi.org/10.1515/eng-2022-0386

[33] M. Tucci, A. Piazzi, D. Thomopulos, "Machine Learning Models for Regional Photovoltaic Power Generation Forecasting with Limited Plant-Specific Data," Energies, vol. 17, no. 10, 2024, doi: https://doi.org/10.3390/en17102346

[34] S.M. Babbar, C.Y. Lau, K.F. Thang, "Long Term Solar Power Generation Prediction using Adaboost as a Hybrid of Linear and Non-linear Machine Learning Model," International Journal of Advanced Computer Science and Applications(IJACSA), vol. 12, no. 11, 2021, doi: https://dx.doi.org/10.14569/IJACSA.2021.0121161

[35] M.K. Park, J. Lee, J.; W.H. Kang, J.M. Choi, K.H. Lee, "Predictive model for PV power generation using RNN (LSTM)," Journal of Mechanical Science and Technology, vol. 35, no. 2, pp. 795-803, 2021, doi: http://doi.org/10.1007/s12206-021-0140-0

[36] K.R. Kumar, M.S. Kalavathi, "Artificial intelligence based forecast models for predicting solar power generation," Materials today: proceedings, vol. 5, no. 1, pp. 796-802, 2018, doi: https://doi.org/10.1016/j.matpr.2017.11.149

[37] A. Mellit, A.M. Pavan, "A 24-h forecast of solar irradiance using artificial neural network: Application for performance prediction of a grid-connected PV plant at Trieste, Italy," Solar energy, vol. 84, no. 5, pp. 807-821, 2010, doi: https://doi.org/10.1016/j.solener.2010.02.006

[38] M.A. Hassan, N. Bailek, K. Bouchouicha, S.C. Nwokolo, "Ultra-short-term exogenous forecasting of photovoltaic power production using genetically optimized non-linear auto-regressive recurrent neural networks," Renewable Energy, vol. 171, pp. 191-209, 2021, doi: https://doi.org/10.1016/j.renene.2021.02.103

[39] D.V. Tai, "Solar photovoltaic power output forecasting using machine learning technique," Journal of Physics: Conference Series, vol. 1327, 2019, doi: https://doi.org/10.1088/1742-6596/1327/1/012051

[40] G.H. Allam, B.E. Elnaghi, M.N. Abdelwahab, R.H. Mohammed, "Using Machine Learning to forecast Solar Power in Ismailia," International Journal of Scientific and Research Publications (IJSRP), vol. 11, no. 12, pp. 238-44, 2021, doi: http://doi.org/10.29322/IJSRP.11.12.2021.p12033

[41] W. Tercha, S.A. Tadjer, F. Chekired, L. Canale, "Machine Learning-Based Forecasting of Temperature and Solar Irradiance for Photovoltaic Systems," Energies, vol. 17, no. 5, 2024, doi: https://doi.org/10.3390/en17051124

[42] L. Benali, G. Notton, A. Fouilloy, C. Voyant, R. Dizene, "Solar radiation forecasting using artificial neural network and random forest methods: Application to normal beam, horizontal diffuse and global components," Renewable energy, vol. 132, pp. 871-884, 2019, doi: https://doi.org/10.1016/j.renene.2018.08.044

[43] L. Stoyanov, I. Draganovsk, "Application of ANN for forecasting of PV plant output power–Case study Oryahovo," 2021 17th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2021, doi: https://doi.org/10.1109/ELMA52514.2021.9503087

[44] L. Stoyanov, I. Draganovska, "Comparison of hybrid models for pv power output forecasting—application to Oryahovo, Bulgaria," 2023 18th Conference on Electrical Machines, Drives and Power Systems (ELMA), Varna, Bulgaria, 2023, doi: https://doi.org/10.1109/ELMA58392.2023.10202257

[45] A.M. García, R.G. Perea, E.C. Poyato, P.M. Barrios, J.R. Díaz, "Comprehensive sizing methodology of smart photovoltaic irrigation systems," Agricultural Water Management, vol. 229, 105888, 2020, doi: https://doi.org/10.1016/j.agwat.2019.105888

[46] A.S. Maia, E. de Andrade Culhari, V.D. Fonsêca, H.F. Milan, K.G. Gebremedhin, "Photovoltaic panels as shading resources for livestock," Journal of Cleaner Production. vol. 258, 120551, 2020, doi: https://doi.org/10.1016/j.jclepro.2020.120551

[47] A. M. Bartkowiak, "Energy-saving and low-emission livestock buildings in the concept of a smart farming," Journal of water and land development, vol. 51, 2021, pp. 272-278, doi: https://doi.org/10.24425/jwld.2021.139935

[48] J.K. Kaldellis, M. Kapsali, K.A. Kavadias, "Temperature and wind speed impact on the efficiency of PV installations. Experience obtained from outdoor measurements in Greece," Renewable energy, vol. 66, pp. 612-624, 2014, doi: https://doi.org/10.1016/j.renene.2013.12.041

[49] J. Demsar, T. Curk, A. Erjavec, C. Gorup, T. Hocevar, M. Milutinovic, M. Mozina, M. Polajnar, M. Toplak, A. Staric, M. Stajdohar, L. Umek, L. Zagar, J. Zbontar, M. Zitnik, B. Zupan, "Orange: Data Mining Toolbox in Python," Journal of Machine Learning Research, vol. 14, pp. 2349−2353, 2013.

[50] Z. Hou, Y. Zhang, Q. Liu, X. Ye, "A hybrid machine learning forecasting model for photovoltaic power," Energy Reports, vol. 11, 2024, pp. 5125-5138, doi: https://doi.org/10.1016/j.egyr.2024.04.065

Edge Computing in Water Management: A KPCA-DeepESN and HOA-Optimized Framework for Urban Resource Allocation

Hanchao Liao[1*], Miyuan Shan[2]
School of Civil Engineering, Changsha, Changsha 410022, Hunan, China[1]
Business School of Hunan University, Changsha 410002, Hunan, China[1, 2]

***Abstract*—This paper presents a novel approach to optimizing urban water resource allocation by integrating Kernel Principal Component Analysis (KPCA) with a Deep Echo State Network (DeepESN), further optimized using the Hiking Optimization Algorithm (HOA). The proposed model addresses the issue of achieving an optimal balance between water supply and demand in urban environments, utilizing advanced machine learning techniques to enhance prediction accuracy and allocation efficiency. KPCA is employed to reduce the dimensionality of key water resource indicators, capturing nonlinear relationships in the dataset. DeepESN, a deep recurrent neural network model, is then applied to predict water consumption trends. HOA, a meta-heuristic algorithm inspired by hiker behavior, is used to fine-tune the DeepESN network parameters, ensuring faster convergence and higher accuracy. The experimental setup includes water resource data from January 2010 to December 2023, divided into training, testing, and validation sets. The model's performance is compared with other approaches, such as PCA-DeepESN and standalone DeepESN. Results show that the KPCA-HOA-DeepESN model achieves the lowest prediction error and fastest convergence, making it a superior solution for urban water management. Optimized network parameters include a reservoir size of 140, a spectral radius of 0.3, an input scaling factor of 0.22, and a reservoir sparsity degree of 0.72. This study demonstrates the applicability of distributed computing techniques in water resource management by utilizing cloud-based data processing and real-time predictions. The proposed approach not only improves resource allocation but also showcases the potential for edge computing to enhance the responsiveness of water management systems.**

Keywords*—KPCA Method; water supply and demand equilibrium; allocation of resources in urban water environment; optimization strategy for hiking; DeepESN

I. INTRODUCTION

Water, being an essential natural resource for the existence of humans, is intricately linked to both social stability and economic progress [1]. The fast expansion of civilization and population increase have resulted in an uneven distribution of water resources and pollution produced by human activities. This has led to a crisis in water resources, which is a pressing problem for every country and industry. In recent years, professionals and academics in the area have paid attention to the evaluation of water resources usage efficiency, recognizing its importance in the best allocation of water resources [2]. Studying objective and accurate approaches for optimizing the allocation of urban water resources may assist the water resources management department in enhancing the efficiency of water resource utilization and improving the precision of water usage solution control [3]. The analysis of water resources encompasses the evaluation of water resource utilization efficiency, the examination of water resource policies and regulations, the creation and implementation of water resource management strategies, the study of variables that influence water resources, and the evaluation of water resource utilization efficiency [4]. The efficient distribution of water resources is a crucial aspect of water resources analysis. The use of water resources is assessed by identifying key areas for review and employing data analysis methods to construct mathematical models that optimize resource distribution.

Presently, the water resource optimal allocation techniques encompass the fuzzy comprehensive assessment method, Tobit regression analysis method, machine learning algorithms, neural networks, deep learning networks, and other approaches [5]. Aghu and Reddy [6] employ an enhanced fuzzy set and fuzzy comprehensive evaluation method to assess and analyze the carrying capacity of water resources. The principal component analysis technique is combined with the particle swarm optimization algorithm, using an improved projection tracing model method, to evaluate the hierarchical water resources carrying capacity [7]. The inefficient use of urban water resources is simulated and analyzed using the least squares method and the Tobit regression model [8]. Lv et al. [9] examine the problem of water resource sustainability through a multi-level fuzzy comprehensive evaluation model and provides relevant water use measures. In literature [10], the random forest algorithm is utilized to predict and analyze water balance and forecast data. Lastly, Mangal et al. [11] introduces a deep echo state network based on a multi-layer self-coder and applies it to the evaluation of urban water resources. While there have been significant achievements in researching the best way to allocate urban water resources both domestically and internationally, there are still certain limitations and flaws in the methodologies used for water resource analysis. Firstly, the analysis method relies on subjective evaluation, which can easily compromise the objectivity of the results. Additionally, relying solely on evaluation or allocation methods can impact the accuracy of the results. Moreover, the optimization model used for water resources allocation in the local area fails to adequately reflect equilibrium and does not contribute to enhancing the overall utilization rate of water resources [12].

This study utilizes the hiking optimization algorithm and deep echo state network to address the issue of optimal allocation of urban water resources, with the aim of analyzing the current research situation. The structure of this paper is:

- Examine the problem by considering water resources analysis and water resources optimization.
- Design the appropriate index parameters and optimize the parameters of the deep echo state network using the hiking optimization algorithm.
- Develop a method for optimizing and allocating urban water resources based on the HOA-DeepESN model.
- Suggested approach is utilized in the examination of data about the allocation of urban water resources.
- Contrasted with alternative models in order to confirm its superiority and correctness.

II. Water Allocation Challenges

A. Examination of Water Resources

Water resources analysis is the application of systems analysis techniques to comprehensively examine the design, planning, management, and challenges related to water resources. Its aim is to develop a scientifically sound and rational program. The analysis of urban water resources typically involves the selection of indicators, processing without dimensions, finding a solution for weighting, calculating a comprehensive score, and analyzing the efficiency of the city's water benchmarking by considering spatial and temporal differences. Additionally, a seven-step analysis is conducted to assess the potential for water conservation, as depicted in Fig. 1.

Regarding indicator selection, this paper opts for four urban water resources analysis indicators: 10,000 RMB GDP water consumption A, 10,000 RMB industrial output value water consumption B, per capita comprehensive water consumption C, and per capita living water consumption D [13], as depicted in Fig. 2.

Furthermore, this study uses Z-score methodology to standardize the analysis indicators for urban water resources. It utilizes principal component analysis to determine the weights of the indicators and develops complete assessment indicators using the weighted average approach.

B. Efficient Distribution of Water Resources

1) Guidelines for efficient distribution of water resources: To achieve the best allocation of water resources, it is recommended to utilize the comprehensive score obtained from analyzing urban water resources as an explanatory variable. Additionally, select the influencing factors of each field at each level as explanatory variables and employ the regression algorithm to construct the water resources allocation model. The water resource optimization allocation process involves many key processes, including indicator selection, correlation analysis, building of an allocation model, and optimization of the allocation model [14]. These steps are illustrated in Fig. 3.

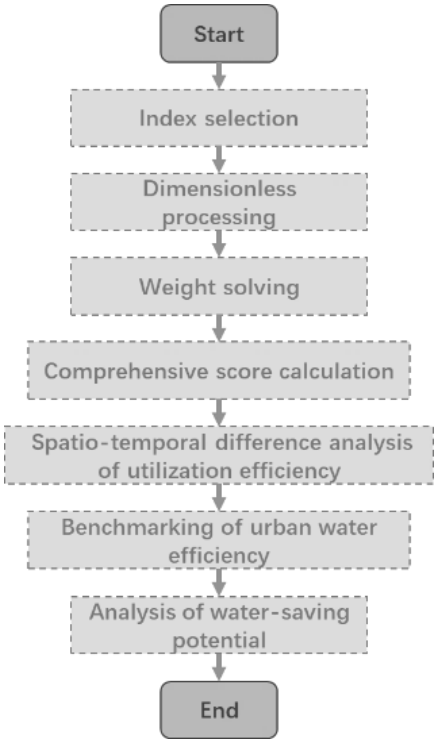


Fig. 1. Sequential process of assessing urban water resources.

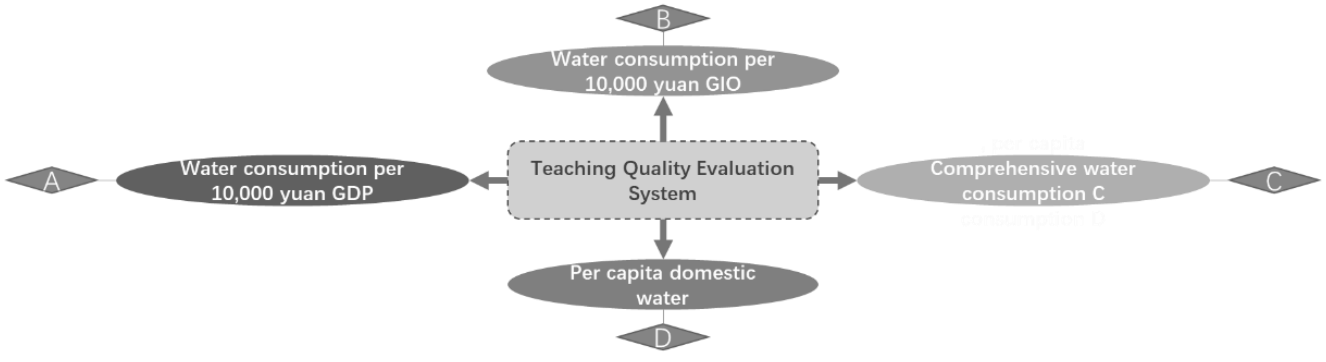


Fig. 2. Indicators used to analyze urban water resources.

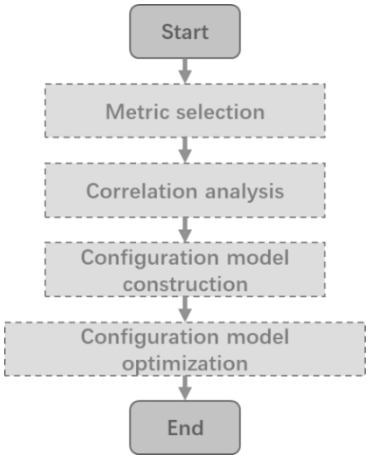


Fig. 3. Steps for optimal allocation of urban water resources.

2) Choosing appropriate indicators for efficient distribution of water resources: Several variables influence the efficiency of water resource consumption, such as natural factors, economic considerations, scientific and technological factors, and the organization of industrial water use. Hence, this article chooses water resource optimization indicators based on four viewpoints: natural factors, economic aspects, scientific and technical considerations, and industrial water usage structure [14]. 1) Natural factors indicators consist of total annual water supply (S1), per capita water possession (S2), and per capita regional gross domestic product (S3). 2) Economic factors indicators include the proportion of the first industry (J1), the proportion of the second industry (J2), and the proportion of the third industry (J3). 3) Scientific and technological factors indicators include the investment cost of wastewater treatment (K1). 4) Industrial investment cost of wastewater management (K1) is also an indicator of scientific and technological factors. 5) Indicators of industrial water use structure include agricultural water use (C1), industrial water use (C2), domestic water use (C3), and ecological water use (C4). Fig. 4 shows selection of indicators for optimal allocation of urban water resources.

3) Optimal allocation modeling of water resources: Water resource optimization and allocation model construction is the use of machine learning algorithms or mathematical agent model analysis training to construct a nonlinear mapping relationship between the water resource optimization and allocation indicators and the comprehensive score of water resource utilization efficiency. In this paper, we propose to use the deep learning algorithm to construct the water resources optimization model, and at the same time, we adopt a meta-heuristic optimization algorithm inspired by the hiker's travel experience to optimize the parameters of the deep learning algorithm to optimize the prediction accuracy of the water resources optimization model, which is shown in Fig. 5.

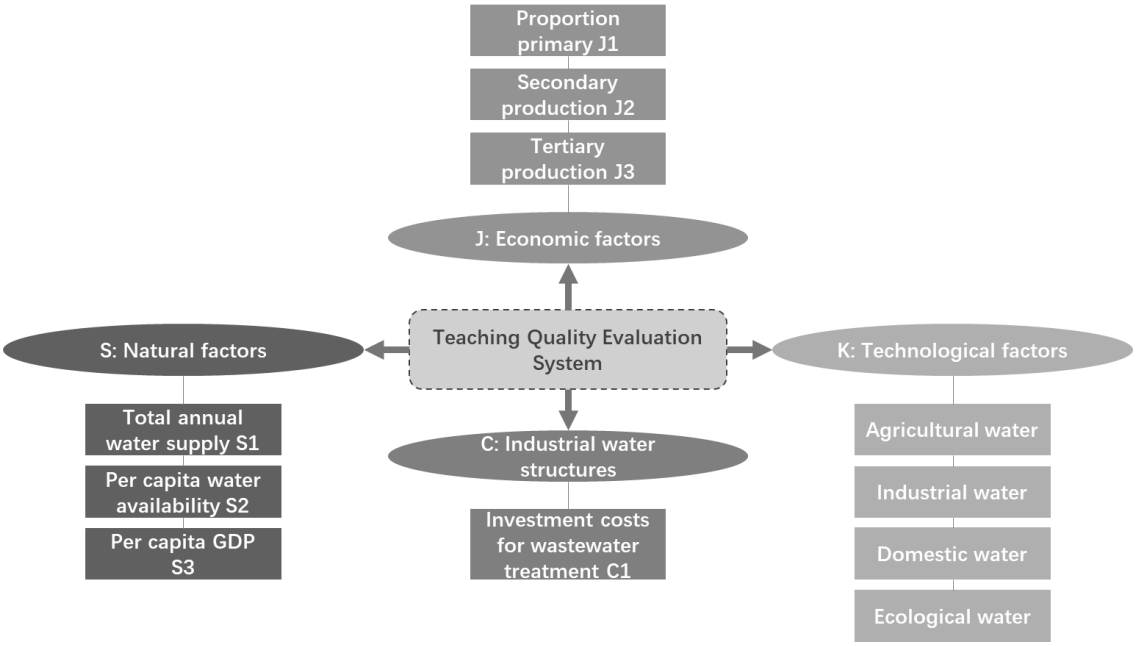


Fig. 4. Selection of indicators for optimal allocation of urban water resources.

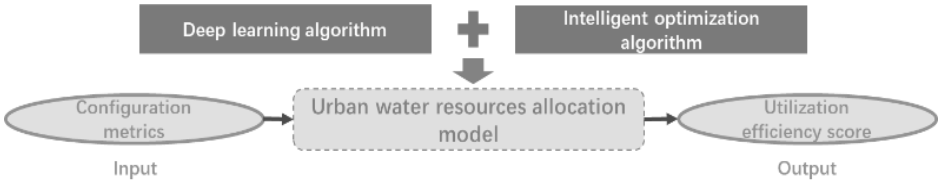


Fig. 5. Model construction of optimal allocation of urban water resources.

III. Risk Assessment Problems

A. Kernel Principal Component Analysis (KPCA)

Kernel Principal Component Analysis (KPCA) [15] is an enhanced version of Principal Component Analysis (PCA) [16] that addresses nonlinear data structures by transforming the data into a feature space with a higher dimensionality. KPCA, unlike classic PCA, does not directly calculate the covariance matrix and eigenvectors in the original data space. Instead, it employs a kernel function to transform the data into a new feature space and then calculates the principal components in this transformed space. Some frequently employed kernel functions include the linear kernel, Gaussian kernel (also known as radial basis function), polynomial kernel, and others. KPCA effectively captures the non-linear characteristics of the data and is particularly useful for datasets that cannot be accurately represented using linear approaches in their original form. Fig. 6 provides a schematic representation of the precise structure.

The fundamental procedures of KPCA are as follows: 1) Choose a suitable kernel function, such as the radial basis function; 2) Calculate the kernel matrix; 3) Center the kernel matrix; 4) Perform eigenvalue decomposition; 5) Normalize the eigenvectors; 6) Select the principal components; 7) Compute the nonlinear principal components; 8) Reconstruct the data.

KPCA is mostly employed in pattern recognition, image processing, bioinformatics, and fault detection, as seen in Fig. 7. It aids researchers in identifying intricate patterns in data, decreasing data dimensionality, and enhancing the efficiency and precision of future analysis.

B. HOA-DeepESN Network

1) Algorithm for optimizing hiking: The Hiking Optimization method (HOA) [17] is a meta-heuristic optimization method that draws inspiration from the act of hiking. Hikers consciously or unconsciously consider the incline of the land when they try to reach the top of mountains, hills, or rocks. This activity is a well-liked recreational pursuit that acknowledges the resemblance between the search landscape of an optimization problem and the rugged terrain that hikers navigate, as depicted in Figure. The number 9. The mathematical model of HOA is based on the Tobler hiking function, which considers the height of the terrain and the distance walked to calculate the walking pace of the hiker (agent). During the optimization phase, the Tobler hiking function (THF) is employed to ascertain the precise whereabouts of the hiker.

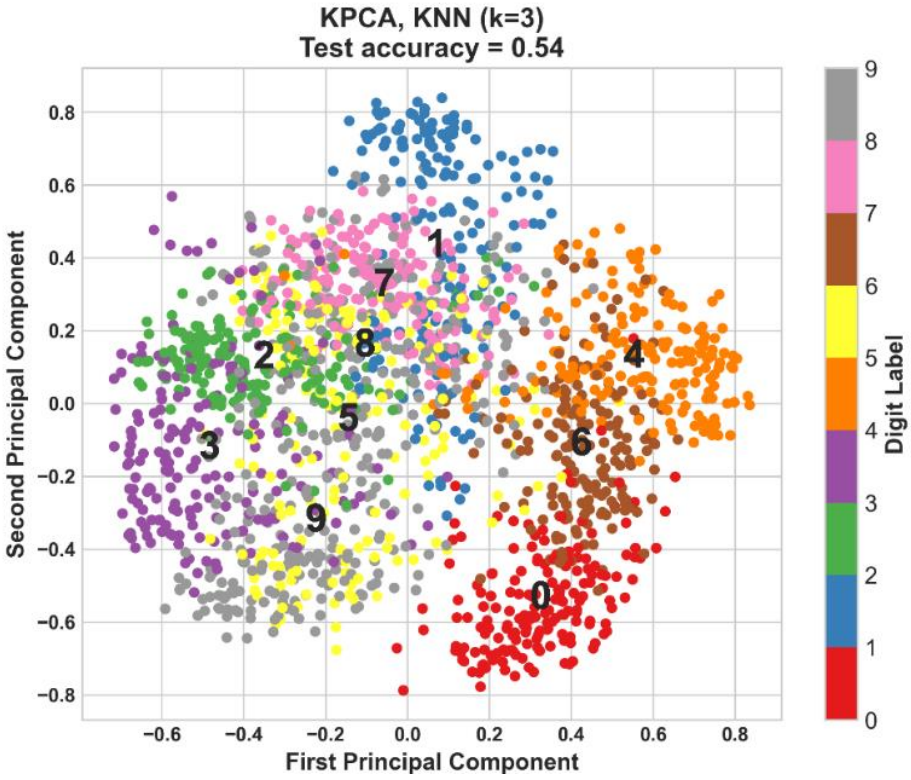


Fig. 6. KPCA structure.

Fig. 7. Types of machine learning algorithms.

a) Principles of Homeowners Association (HOA): The mathematical basis of HOA is derived from the renowned Tobler Hiking Function, initially introduced by Waldo Tobler, a Swiss-American geographer and cartographer. The Tobler Hiking Function is an exponential function that calculates the velocity of a hiker, considering the incline or slope of the terrain or path. The precise mathematical model of the THF is as follows:

$$W_{i,t} = 6e^{-3.5\left|S_{i,t}+0.05\right|} \tag{1}$$

Where, $W_{i,t}$ denotes the speed of hiker i in km/h; and $S_{i,t}$ denotes the slope of the terrain, which is calculated as follows:

$$S_{i,t} = \frac{dh}{dx} = \tan\theta_{i,t} \tag{2}$$

Where, dh is the hiker elevation gradient, dx is the difference in hiker distance, and θ denotes the angle of terrain inclination, typically at [0, 50°].

HOA algorithms hikers as a group for the benefit of social thinking and individual hikers for the benefit of their personal cognitive abilities. The updated or actual speed of a hiker is a function of the initial speed determined by the THF, the position of the leading hiker, the actual position of the hiker, and the sweep factor. Thus, the current speed of hiker i is calculated as follows:

$$W_{i,t} = W_{i,t-1} + \gamma_{i,t} \cdot \left(\beta_{best} - \alpha_{i,t}\beta_{i,t}\right) \tag{3}$$

where $\gamma_{i,t}$ is a uniformly distributed random number; β_{best} is the position of the lead hiker; $\alpha_{i,t}$ is the scan factor SF for hiker i, which lies between 1 and 3; SF ensures that hikers do not stray too far from the lead hiker so that they can see the direction of the lead hiker and receive signals from the lead hiker.

The location update for hiker i is calculated as follows:

$$\beta_{i,t+1} = \beta_{i,t} + W_{i,t} \tag{4}$$

In addition, the HOA algorithm initializes the hiker population as follows:

$$\beta_{i,t+1} = \phi_j^1 + \delta_j\left(\phi_j^2 - \phi_j^1\right) \tag{5}$$

where δ_j is a uniform distribution and ϕ_j^1 and ϕ_j^2 denote the upper and lower bounds of the jth dimension of the optimization problem.

The exploratory and exploitative tendencies of the HOA algorithm are influenced by the SF parameter. When the SF range increases, the HOA algorithm tends to the developmental stage; when SF decreases, the HOA algorithm enters the exploratory stage.

b) Sequential progression of the HOA algorithm: Table I displays the pseudo-code for the hiking optimization method.

TABLE I. HIKING PSEUDO-CODE

	Algorithm 1: Hiking Optimization Algorithm
1	Nout upper and lower limits, Max_iter, Np, d;
2	Intislize hikers' position randomly;
3	Calculate fitnss and output best fitness;
4	For t = 1:Max_iter
5	Determine best fitness of hikers;
6	Determine trail/terrain angle of elevation;
7	Compute the slope;
8	Determine the actual velocity of hiker;
9	Update hiker's position;
10	Bound position using upper and lower limits;
11	Update best hiker position;
12	End
13	Output best solution.

2) DeepESN network: The Deep Echo State Network (DeepESN) [18] is a customized deep recurrent neural network designed for the processing of temporal data. The model is an expansion of the Echo State Network (ESN) [19]. DeepESN is an advanced technique used to create recurrent neural networks that are trained efficiently. It involves combining multiple recurrent layers to create a network that can represent temporal information at different time scales. This makes DeepESN more effective at processing data that changes over time. The precise configuration is illustrated in Fig. 8.

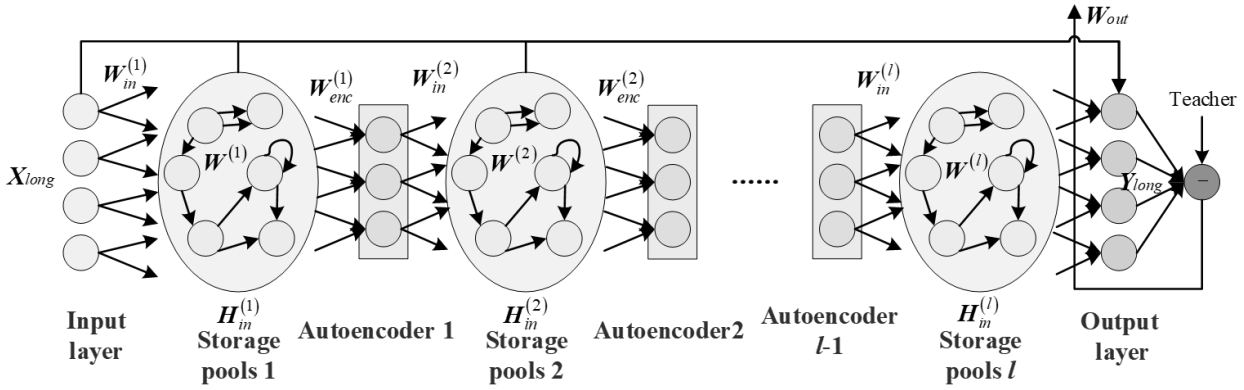


Fig. 8. DeepESN structure.

DeepESN is a variant of Echo State Networks (ESNs) that enhances the depth of the reservoir by employing a self-encoder mapping. In the DeepESN network architecture, the preceding reservoir echo state is compressed to lower dimensions using an Autoencoder (AE). This compressed state is then fed into the subsequent reservoir pool, and the process continues until reaching the last layer. In the final layer, all the echo states are organized and the ultimate result is outputted to the network. The mathematical model is precisely defined as follows:

$$\boldsymbol{H}_{in}^{(l)}(t)=\boldsymbol{W}_{in}^{(l)}\boldsymbol{X}_{in}^{(l)}(t)+\boldsymbol{W}^{(l)}\boldsymbol{H}^{(l)}(t-1) \tag{6}$$

$$\boldsymbol{X}_{in}^{(l)}(t)=\begin{cases}\boldsymbol{X}_{long}(t), l=1\\ f_{enc}\left(\boldsymbol{W}_{enc}^{(l-1)}\boldsymbol{H}^{(l-1)}(t)\right), l>1\end{cases} \tag{7}$$

$$\boldsymbol{H}^{(l)}(t)=\left(1-SD^{(l)}\right)\boldsymbol{H}^{(l)}(t-1)+SD^{(l)}\tanh\left(\boldsymbol{H}_{in}^{(l)}(t)\right) \tag{8}$$

$$\boldsymbol{Y}_{long}(t)=g\left(\boldsymbol{W}_{out}\boldsymbol{H}(t)\right) \tag{9}$$

Where, $\boldsymbol{H}_{in}^{(l)}(t)$ denotes the weighted input data of storage pool in layer *l* at moment *t*, $\boldsymbol{W}_{in}^{(l)}$ denotes the connection weight from input to storage pool in layer *l*, $\boldsymbol{X}_{in}^{(l)}(t)$ denotes the input in layer *l* at moment *t*, $\boldsymbol{W}^{(l)}$ denotes the state feedback weight of storage pool in layer l, $\boldsymbol{H}^{(l)}(t-1)$ denotes the state of storage pool in layer *l* at moment t-1, $\boldsymbol{W}_{enc}^{(l-1)}$ denotes the projection weight of the self-encoder in layer l-1 at moment t, $f_{enc}(\cdot)$ denotes the activation function of the self-encoder, $\boldsymbol{X}_{long}(t)$ denotes the input variable at moment t, $\boldsymbol{H}^{(l)}(t)$ denotes the state value of storage pool in layer l at moment t, and denotes the degree of sparsity of storage pool in layer l at moment t. represents the state value of storage pool in layer *l at* time t, and $SD^{(l)}$ is the sparsity degree of storage pool in layer *l*. The state value of storage pool in layer l at time t is the state value of storage pool in layer l. $\boldsymbol{H}(t)$ The vector formed for the states of all storage pools is denoted as $\left[\boldsymbol{H}^{(1)}(t),\boldsymbol{H}^{(2)}(t),\cdots,\boldsymbol{H}^{(l)}(t)\right]$; $g(\cdot)$ denotes the activation function of the output layer. The DeepESN neural network training process is generally solved by regularized ridge regression.

The core strength of DeepESN is its deep structure, which allows the network to learn features on different time scales. Its cascading structure not only helps to achieve multi-timescale representations, but also improves unsupervised reservoir adaptation and network design. Application scenarios for DeepESN [20-25] include environmentally-assisted living, medical diagnosis, speech and music processing, weather forecasting, energy prediction, transportation forecasting, and financial market forecasting (Fig. 9).

3) DeepESN network model based on hiking optimization algorithm: In order to increase the design effect of the optimal urban water resources allocation scheme, this paper takes the parameters of DeepESN network (storage pool size N_r , spectral radius SR , input scale factor IS , storage pool sparsity SD) as the optimization decision variables, HOA algorithm hiker optimization strategy as the optimization method, and MAPE error value as the fitness function, and the specific process steps are shown in Table II.

TABLE II. HOA-DEEPESN PSEUDO-CODE

Algorithm 2: DeepESN based on HOA	
1	Determine optimized variables, including Nr, SR, IS, SD;
2	Set HOA algorithm parameters;
3	Encode hikers population;
4	Calculate fitness using MAPE, and update best hiker;
5	For i = 1:Np
6	Updated hiker velocity
7	Updated hiker position
8	End
9	Output best parameters of DeepESN;
10	Build HOA-DeepESN model.

C. Application of KPCA and HOA-DeepESN

This study utilizes the KPCA (Kernel Principal Component Analysis) and HOA-DeepESN (Higher Order Autoregressive-Deep Echo State Network) algorithms to identify the main factors affecting urban water resources allocation. The aim is to enhance the effectiveness and precision of water resources optimization and allocation. The specific procedure is illustrated in Fig. 10. The urban water resources optimization allocation method consists of five main components: water resources analysis, extraction of water resources allocation index, principal component analysis of allocation index, preprocessing of allocation index data, and construction of optimal allocation model. These components are based on the KPCA and HOA-DeepESN method.

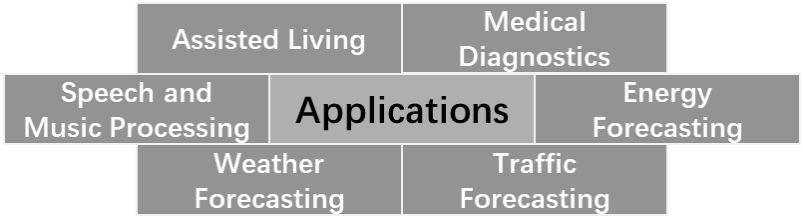


Fig. 9. DeepESN application.

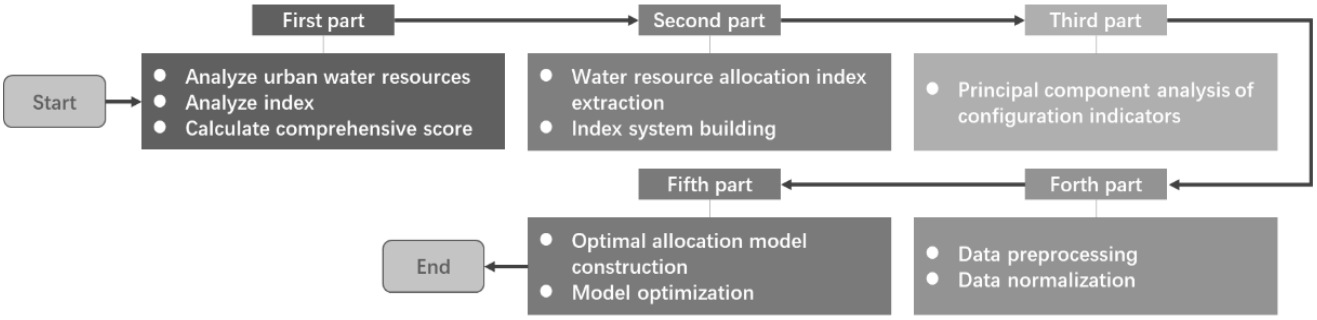


Fig. 10. KPCA with HOA-DeepESN algorithm application.

IV. Case Study

The operating system on which the instance analysis program operates is Windows 10, and the software utilized for the analysis technique is Matlab 2019b. The experiment will utilize the urban water environment resource-related index data from January 2010 to December 2023. The data will be divided into training, test, and validation sets in a ratio of 7:2:1. To analyze the impact of the principal components of the KPCA technique, we will compare the performance of DeepESN, PCA-DeepESN, and KPCA-DeepESN. The specific configurations for these models are described in Table III.

TABLE III. Parameter Settings of the Comparison Algorithm

No.	Algorithms	Descriptions
1	DeepESN	SD=0.7, Nr=100, SR=0.2, IS=0.25, 3layers of AE with 50 nods per layer of AE
2	PCA-DeepESN	PCA technique, 3 layers of AE with 50 nodes in each layer.
3	KPCA-DeepESN	Kernel Principal Component Analysis (KPCA) technique, Radial Basis Function (RBF) was selected, three layers of AE with 50 nodes per layer
4	KPCA-HOA-DeepESN	Kernel Principal Component Analysis (KPCA) technique, Radial Basis Function(RBF) selection, Three layers of AE with 50 nodes per layer, HOA algorithm to optimise DeepESN parameters

This paper aims to validate the effectiveness of the HOA algorithm in enhancing the efficiency of urban water environment resource allocation using the DeepESN network. To achieve this, the SCA, BBO, KMA, and QIO algorithms are employed to optimize the DeepESN network and the HOA algorithm. A comparative analysis of the specific algorithm parameter settings can be found in Table IV. The dimensions of the storage pool, the spectral radius, the input scale factor, and the range of sparsity parameters for the storage pool are displayed in Table V.

TABLE IV. Parameter Settings of Intelligent Optimization Algorithm for Optimizing DeepESN Network

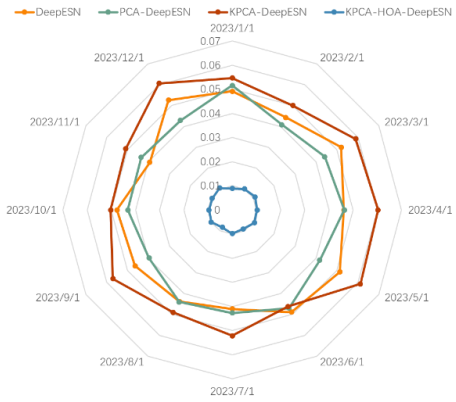
No	Algorithms	Parameter Settings
1	SCA-DeepESN	A reduce linearly 2 to 0
2	BBO-DeepESN	Probability of modifying a habitat is 1
3	KMA-DeepESN	Mlipir rate=0.5, Female mutation rate=0.5, Female mutation radius=0.5
4	QIO-DeepESN	No
5	HOA-DeepESN	Angle of inclination is [0,50], SF=[1,3]

TABLE V. Decision Range Settings for Parameters to be Optimized in the DeepESN Network

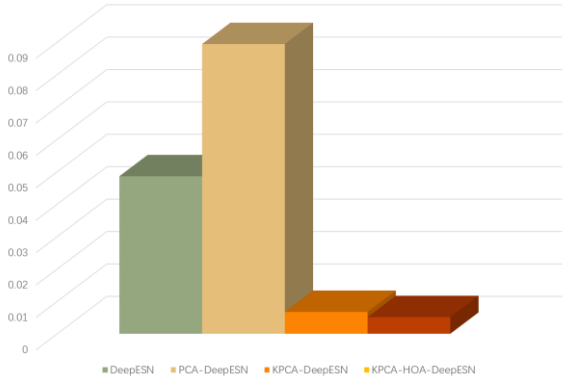
No	Variables	Range Settings
1	Nr	[50,300]
2	SR	[0.4,0.9]
3	IS	[0.1,0.8]
4	SD	[0.1,0.5]

A. Evaluation of the Impact of using the KPCA Approach

This article examines the efficiency of resource allocation in the urban water environment for four models: DeepESN, PCA-DeepESN, KPCA-DeepESN, and KPCA-HOA-DeepESN. The particular connections between these models are illustrated in Fig.11.



(a) Comparison of forecast errors.



(b) Comparison of projected time consumption.

Fig. 11. Comparison of urban water resources prediction error and time-consuming results of different algorithms.

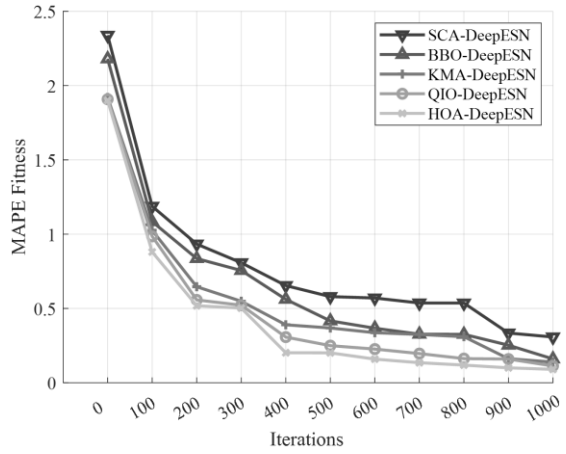
Fig. 11 presents the prediction error and time consumed for urban water allocation for the four algorithms. From Fig. 11, it can be seen that KPCA-HOA-DeepESN has the lowest prediction error among the 12-month prediction errors of the test set; KPCA-DeepESN is compared with PCA-DeepESN, which indicates that the principal component analysis method of KPCA is more effective; and the prediction time consumed by KPCA-HOA- DeepESN is the lowest.

B. Analysis of the Effectiveness of the Water Resources Optimization Model

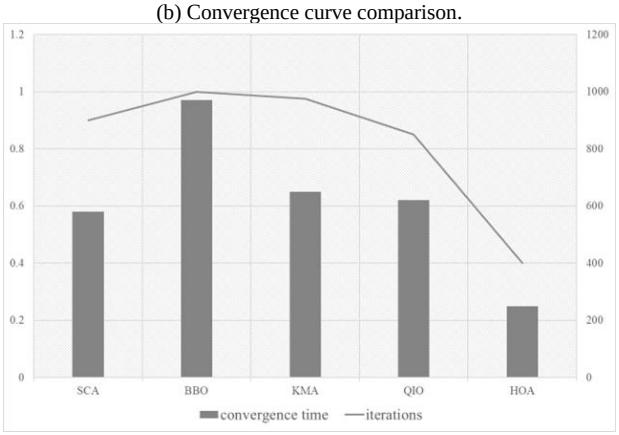
The water resources optimization configuration data is used as input to optimize the DeepESN network parameters using SCA, BBO, KMA, QIO, and HOA algorithms. The optimization results, convergence curves, and speeds are obtained and shown in Fig. 12(a)-(c). According to the Fig. 12, it is evident that the HOA algorithm enhances the optimization of DeepESN network parameters by achieving quicker convergence speed and greater convergence accuracy. The resulting optimized parameters are Nr=140, SR=0.3, IS=0.22, and SD=0.72.

No.	Parameters	SCA-DeepESN	BBO-DeepESN	KMA-DeepESN	QIO-DeepESN	HOA-DeepESN
1	Nr	103	120	145	120	140
2	SR	0.19	0.27	0.33	0.3	0.3
3	IS	0.21	0.26	0.29	0.24	0.22
4	SD	0.79	0.7	0.65	0.7	0.72

(a) Comparison of Optimal DeepESN Network Parameters.



(b) Convergence curve comparison.



(c) Convergence time vs. number of iterations.

Fig. 12. Comparison of optimization results of different algorithms.

V. Conclusion and Future Work

The HOA-DeepESN method, which integrates KPCA and deep learning techniques, effectively addresses the urban water balance resource allocation problem and enhances the efficiency of the allocation model. This paper begins by examining the optimal allocation problem, taking into account the equilibrium between the supply and demand of water resources. We then use the optimal allocation model to establish a method for urban water resources allocation based on the HOA-DeepESN network. The objective function is defined as the minimum of MAPE, and the optimization decision vector consists of the DeepESN network structure parameters. The proposed method is simulated and analyzed using urban water environment resource data from January 2010 to December 2023. The following conclusions are drawn: (1) The use of the KPCA technique improves the model training, testing, and prediction time. (2) Optimizing the parameters of the DeepESN network using the HOA algorithm enhances the prediction accuracy of the optimal allocation model. (3) The optimal values for the storage pool size, spectral radius, input scale factor, and storage pool sparsity are 140, 0.3, 0.22, and 0.72, respectively.

The study also has several limitations: The model is tested on urban water resource data from a specific period and location. Its performance may vary across different regions or under different environmental conditions. The choice of water resource indicators, though based on widely accepted criteria, may not capture all relevant factors, especially in more complex ecosystems.

Based on the above analysis, we look forward to future research directions, which can be started from the following three aspects: 1), Future studies could apply the KPCA-HOA-DeepESN approach to other geographic locations or sectors to validate its generalizability. 2), Integrating real-time data streams, such as satellite observations or sensor data, could further enhance the precision of the model in dynamic environments. 3), exploring other meta-heuristic optimization algorithms or combining HOA with other methods, like genetic algorithms or particle swarm optimization, could lead to even more robust models for resource allocation.

Acknowledgment

This work is supported by Precision Teaching and Students' Innovative Ability Driven by Data. Teaching Reform Research Project of Hunan General Higher Education Institutions Grant No.HNJG-2231216.

References

[1] Nematian J .A Two-Stage Stochastic Fuzzy Mixed-Integer Linear Programming Approach for Water Resource Allocation under Uncertainty in Ajabshir Qaleh Chay Dam[J].*Journal of Environmental Informatics*, 2023. https://doi.org/10.3808/jei.202300495

[2] AbdollahDoosti-Aref,HuseyinArslan.Resource allocation optimization in multiuser OFDM relay-assisted underwater acoustic sensor networks[J].Vehicular Communications, 2023, 42(8):100625.1-100625.21. https://doi.org/10.1016/j.vehcom.2023.100625

[3] Cansino-Loeza B ,Aurora del Carmen Munguía-López,José María Ponce-Ortega.A water-energy-food security nexus framework based on optimal resource allocation[J].*Environmental Science & Policy*, 2022, 133:1-16. https://doi.org/10.1016/j.envsci.2022.03.010

[4] Bushnaq O. M., Zhilin I., Masi G., Natalizio E., Akyidiz I. Automatic Network Slicing for Admission Control, Routing, and Resource Allocation in Underwater Acoustic Communication Systems[J].*IEEE Access*, 2022, 10:134440-134454. https://doi.org/10.1109/ACCESS.2022.3215029

[5] Bao K., Thrn D., Schrter B..Land Resource Allocation between Biomass and Ground-Mounted Pv Under Consideration of the Food-Water-Energy Nexus Framework at Regional Scale[J].*SSRN Electronic Journal*, 2022

[6] Aghu K., Reddy P. C. S.Energy-efficient resource allocation for NOMA heterogeneous networks using feedback water cycle algorithm[J].*International Journal of Modeling, Simulation, and Scientific Computing*, 2022.

[7] Timothy.Páez-Watson, Loosdrecht M C M V , Wahl S A .Predicting the impact of temperature on metabolic fluxes using resource allocation modelling. Application to polyphosphate accumulating organisms[J].*Water research*, 2023, 228(Pt A):119365.

[8] Wu D , Liu M .Assessing adaptability of the water resource system to social-ecological systems in the Beijing-Tianjin-Hebei region:Based on the DPSIR-TOPSIS framework[J]. *China Population-Resources and Environment*:English Edition, 2022, 20(3):261-269.

[9] Lv Y., Yu N., Sun H , Li H., Yang J. Optimal allocation of urban and rural water supply in coastal water shortage cities: the case of Yingkou City[J]. *Irrigation and Drainage*, 2024(1):73.

[10] Li C., Wan T., Han J., Jiang W. Towards Distributed Lexicographically Fair Resource Allocation with an Indivisible Constraint[J].*Mathematics*, 2022,. 10.

[11] Mangal R , Desai A , Treger D , Gomples M, Thaller S. Craniofacial Injuries in Swimming and Water Sports: Implications for Prevention[J]. *Journal of Craniofacial Surgery*, 2024, 35(2):452-455.

[12] Nasiriasayesh H., Yari A., Nazemi E.Adaptive IWD-based algorithm for deployment of business processes into cloud federations[J].*International Journal of Pervasive Computing and Communications*, 2023, 19(1):54-73.

[13] Fan Y., Chen H., Gao Z., Fang B., Liu X., Tsakiris G. A Model Coupling Water Resource Allocation and Canal Optimization for Water Distribution[J].*Water resources management*, 2023. https://doi.org/10.1007/s11269-023-03402-1

[14] Dai B , Yang X , Liu X .Shapley Value of Uncertain Coalitional Game based on Hurwicz Criterion with Application to Water Resource Allocation [J].*Group Decision and Negotiation*, 2022, 31. https://doi.org/10.1007/s10726-021-09776-w

[15] Zhang H., Chen M., Sun B., Zhao C.B.. Research on line loss calculation method of distribution network by fusion of kernel principal components and random forest[J]. *Energy and Environmental Protection*, 2022,44(08):246-250. https://doi.org/10.1016/j.enep.2022.06.015

[16] Bai Xiaoping,Liu Yuhang. Rolling bearing life analysis based on K-means degradation identification and random forest[J]. *Combined machine tools and automatic machining technology*,2024,(07):150-155+160. https://doi.org/10.1016/j.cmamt.2023.07.024

[17] Sunday O O, Stephen O E, Seyedali M. The Hiking Optimization Algorithm: a novel human-based metaheuristic approach[J]. *Knowledge-Based Systems*, 2024, 296:111880. https://doi.org/10.1016/j.knosys.2024.111880

[18] Zheng Wei-Nan,Yu Zhi-Yong,Huang Fang-Ivana. Time series complementation and single-step prediction based on two-channel echo state network[J]. Computer Science,2024,51(03):128-134. (in Chinese)

[19] Zhang Z. Z., Zhu Y. Q.,Yu W. Dynamic error-compensated echo state network with dual reservoir structure[J]. *Control Theory and Applications*,2024,41(03):385-395. (in Chinese)

[20] Bendali W , Saber I , Boussetta M , Bourachdi B, Mourad Y. Optimization of Deep Reservoir Computing with Binary Genetic Algorithm for Multi-Time Horizon Forecasting of Power Consumption[J].*Journal Européen des Systèmes Automatisés*, 2022. https://doi.org/10.18280/jesa.550402

[21] Soltani R , Benmohamed E , Ltifi H .Newman-Watts-Strogatz topology in deep echo state networks for speech emotion recognition[J].*Engineering Applications of Artificial Intelligence*, 2024, 133. https://doi.org/10.1108/IJPCC-08-2021-0156

[22] Mustaqeem, Ishaq M , Kwon S .A CNN-Assisted deep echo state network using multiple Time-Scale dynamic learning reservoirs for generating Short- Term solar energy forecasting[J].*Sustainable energy technologies and assessments*, 2022, 52(Aug. Pt. C):102275.1-102275.9. https://doi.org/10.1016/j.seta.2022.102275

[23] Rajamoorthy R , Saraswathi H V , Devaraj J , Kasinathan P, Elavarasan R M, Arunachalam G. A Hybrid Sailfish Whale Optimization and Deep Long Short-Term Memory (SWO-DLSTM) Model for Energy Efficient Autonomy in India by 2048[J].*Sustainability*, 2022, 14. https://doi.org/10.3390/su14148680

[24] Yue W. Q. DeepESN dynamic soft measurement modeling method and application based on RLS online learning algorithm[J]. *Chemical Automation and Instrumentation*,2021,48(05):491-496.(in Chinese)

[25] Li X., Bi F., Zhang L., Yang X., Zhang G. An Engine Fault Detection Method Based on the Deep Echo State Network and Improved Multi-Verse Optimizer[J]. *Energies*, 2022, 15. https://doi.org/10.3390/en15155677

Road Surface Crack Detection Based on Improved YOLOv9 Image Processing

Quanwu Li*, Shaopeng Duan
School of Information Engineering and Artificial Intelligence, Zhengzhou Vocational University of Information and Technology, Zhengzhou 450008, China

***Abstract*—Road surface crack detection is a critical task in road maintenance and safety management. Cracks in road surfaces are often the early indicators of larger structural issues, and if not detected and repaired in time, they can lead to more severe deterioration and increased maintenance costs. Effective and timely crack detection is essential to prolong road lifespan and ensure the safety of road users. This paper introduces CrackNet, an advanced crack detection model built upon the YOLOv9 architecture, which integrates a fusion attention module and task space disentanglement to enhance the accuracy and efficiency of road surface crack detection. Traditional methods often struggle with the complex and irregular nature of road cracks, as well as the challenge of distinguishing cracks from their backgrounds. CrackNet overcomes these challenges by leveraging an attention mechanism that highlights relevant features in both the channel and spatial dimensions while separating the tasks of classification and regression. This approach significantly reduces false negatives and improves localization accuracy. The effectiveness of CrackNet is validated through comparative analysis with other segmentation models, including Unet, SOLO v2, Mask R-CNN, and Deeplab v3+. CrackNet consistently outperforms these models in terms of F1 and Jaccard coefficients. This study highlights the critical role of accurate crack detection in minimizing maintenance costs and enhancing road safety.**

***Keywords*—Road crack; YOLOv9; deep learning; surveillance**

I. Introduction

Road surface damage refers to the occurrence of deterioration, cracks, and potholes in the road surface layer, which are major factors affecting road performance. Therefore, timely and accurate detection of road surface damage is a crucial aspect of road maintenance. Cracks are the initial manifestation of various types of road surface diseases, making the detection and repair of road cracks particularly important [1-3]. Not only do road surface cracks affect the appearance and comfort of driving, but if they are not repaired promptly, they can widen and worsen, leading to structural damage and reducing the overall performance and lifespan of the road. Thus, early detection and timely repair of cracked roads not only reduce the economic cost of road repairs but also ensure the safety of vehicles and drivers on the road. Moreover, with the increasing number of traffic accidents, road safety has become a global challenge. Therefore, the detection and repair of road surface cracks should be prioritized to ensure road safety and longevity [4-6].

Historically, road surface detection and maintenance primarily relied on manual inspection, which was not only time-consuming and labor-intensive but also low in accuracy and fraught with risks. Scholars around the world have utilized the latest scientific and technological advancements to conduct extensive and in-depth studies to accurately and effectively extract crack information from images. In 2014, Wang et al. [7] proposed a crack extraction method based on the valley boundary, employing a series of image processing algorithms to achieve crack detection results. In 2015, Liang et al. [8] introduced a road crack connection algorithm based on Prim's minimum spanning tree, which involves filling cracks to create a structured crack map.

However, these traditional methods of crack detection have obvious disadvantages. Each method is designed for specific databases or scenarios, and the crack detectors fail if there are changes in the dataset or scenario. This highlights a significant gap between conventional methods and current demands in real-world applications, where crack patterns, lighting conditions, and environmental variations pose challenges for traditional models. In particular, many existing models struggle with detecting fine or irregular cracks under diverse conditions, which leads to false positives or missed detections. This gap emphasizes the need for more robust, adaptable models that can address these challenges and ensure accurate detection in real-world settings.

In recent years, deep learning methods have been increasingly applied to road crack detection and segmentation, integrating deep learning techniques with road crack detection technologies, significantly enhancing the efficiency and accuracy of road crack detection. Lee et al. [9] researched a CNN-based road-surface crack detection model that responds to changes in brightness. They discovered that a preprocessing model, which adjusts the image brightness before inputting it into the crack detection model, enhances the consistency of road-surface crack detection, maintaining stable performance under varying brightness conditions.

Hammouch et al. [10] and colleagues studied an automated methodology for crack detection and classification in Moroccan flexible pavements using Convolutional Neural Networks (CNN). They found that good crack detection and classification are achieved on the dataset using both the CNN and a pre-trained Visual Geometry Group 19 (VGG-19) model. However, the accurate identification of road cracks remains a challenging issue due to their high similarity to the background, small size, and irregular shape in real-world scenarios. Enhancing the precision and timeliness of image-based crack extraction has become a focal point of current research. Originally utilized in

*Corresponding Author

the medical field for cell segmentation, YOLO networks handle complex noise interference better than road surface cracks and can extract both high and low-level features from objects. Despite their simplicity and high accuracy in cell segmentation, these networks have limitations in shallow feature extraction layers and the introduction of irrelevant features through the fusion of different feature levels. Consequently, this paper proposes an improved YOLO method for crack detection. During the feature extraction phase, a Fusion Attention Module (FAM) is embedded, which applies non-uniform weighting across channel and spatial dimensions to highlight useful information. Additionally, a Task-Aware Spatial Disentanglement Head (TSDHead) decouples classification and regression tasks, effectively addressing issues of crack misdetection and inaccurate localization, thus ensuring real-time detection while enhancing the accuracy of road crack detection.

At the end of this introduction, the structure of the paper is outlined as follows: Section II provides a detailed explanation of the improved YOLOv9 architecture and the modifications made to enhance crack detection accuracy. Section III describes the experimental setup, including the dataset used and the evaluation metrics employed to assess the model's performance. Section IV presents the results and a comparative analysis with other segmentation models, highlighting the strengths of CrackNet. Finally, Section V concludes the paper with a discussion on the potential applications of the model in real-world road maintenance systems and suggestions for future research directions. This structure is designed to guide readers through the study and provide a clear understanding of the proposed methodology and its practical implications.

II. Improved YOLOv9 Model

In this study, we conducted a comparative analysis of several segmentation models (including Unet, SOLO v2, Mask R-CNN, and Deeplab v3+) in the context of road crack detection tasks. The strengths and weaknesses of each model are summarized as follows:

Unet: The U-shaped architecture of Unet allows it to perform well on smaller datasets and enables end-to-end training, making it suitable for crack detection tasks. However, due to its reliance on a symmetrical encoder-decoder structure, Unet may suffer from over-segmentation or under-segmentation when detecting complex crack patterns, particularly in cases where crack boundaries are unclear.

SOLO v2: As an instance segmentation model, SOLO v2 transforms the segmentation task into a pixel classification problem, eliminating the need for proposal generation. As a result, it can deliver good segmentation results in crack detection, especially in complex background scenarios. However, SOLO v2 still struggles with accurately detecting fine and low-contrast cracks.

Mask R-CNN: Mask R-CNN uses a Region Proposal Network (RPN) to precisely localize crack regions and generate instance masks. This makes it highly accurate for detecting wide cracks. However, it comes with a high computational cost and tends to over-segment or miss finer cracks during detection.

Deeplab v3+: Combining atrous convolution with an encoder-decoder structure, Deeplab v3+ is well-suited for extracting features at large scales and handling crack images with complex backgrounds. However, its ability to recover fine details is limited, resulting in less effective performance when detecting small cracks compared to other models.

In contrast, CrackNet introduces a Fusion Attention Module and Task Space Disentanglement mechanism, which effectively enhances crack feature extraction, reduces false detections, and improves the localization of cracks. This is especially true when handling fine and irregular cracks. Therefore, CrackNet consistently outperforms the aforementioned models in terms of F1 and Jaccard coefficients, demonstrating superior overall performance [11-13].

A. YOLOv9 Model

The YOLO network has undergone multiple iterations to overcome the limitations of previous versions and enhance performance, achieving a good balance between speed and accuracy. The latest version, YOLOv9-Seg, comprises three components: Backbone, Neck, and Head, as illustrated in Fig. 1. The Backbone extracts features from the input image, while the Neck further processes these features and integrates information across different levels. Finally, the Head layer and subsequent post-processing steps generate the classification, location, and pixel segmentation results of detected objects.

The Backbone of YOLOv9-Seg is composed of three key modules: Conv, ADown, and RepNCSPELAN4. The Conv module, a standard component in convolutional neural networks (CNNs), utilizes convolution, batch normalization, and activation functions to extract features from the input image. The ADown module applies pooling operations to downsample the feature matrix. The RepNCSPELAN4 module plays a critical role in the YOLOv9-Seg network by segmenting and merging the feature matrix through layer aggregation, thereby reducing redundant computations and enhancing feature extraction efficiency.

The Neck component consists of a feature pyramid structure that integrates a Feature Pyramid Network (FPN) and a Path Aggregation Network (PAN). Lower-level convolutional features, despite having less semantic information and more noise, offer higher resolution and more detailed location data. On the other hand, higher-level features provide richer semantic information but compromise resolution and detail. FPN combines high-level and low-level features through a top-down upsampling approach, creating feature maps that are rich in semantic information. PAN further enhances the location accuracy across levels by propagating location information from the bottom to the top, strengthening the overall feature pyramid based on FPN.

SPPELAN combines the advantages of Spatial Pyramid Pooling Fast (SPPF) and Efficient Local Aggregation Network (ELAN). SPPF captures spatial information across multiple scales, improving the model's robustness, while ELAN is a lightweight network structure that enhances feature extraction through local aggregation and global integration. The combination of SPPF and ELAN further boosts feature extraction capabilities.

The head network includes three segment detectors, each operating on feature matrices at different scales to locate and

segment target objects, improving detection performance through multi-scale integration. In our implementation, we utilized pre-trained weights on a large dataset for transfer learning. Furthermore, we incorporated Programmable Gradient Information (PGI) and Generalized Efficient Layer Aggregation Network (GELAN) architectures to optimize both the model's performance and efficiency, as shown in Fig. 1.

B. Fusion Attention Module

Drawing from the design concepts of FcaNet (Frequency Channel Attention Networks) and CBAM (Convolutional Block Attention Module), this paper introduces the Fusion Attention Module (FAM). This module comprises a multispectral channel attention module and a spatial attention module, as illustrated in Fig. 2. The multispectral channel attention module, based on the multispectral frequency information of feature maps, adaptively models the importance of each channel, highlighting significant channel features. The spatial attention module focuses on areas within the feature map rich in detail, addressing the loss of some spatial information in the multispectral channel attention module [14, 15]. By chaining these two modules, the design retains both critical channel features and detailed features around the cracks.

1) Multispectral channel attention module: As shown in Fig. 2, the multispectral channel attention module utilizes the Discrete Cosine Transform (DCT) to extract multispectral frequency features from the feature maps. These features are used to model the importance of each channel, and subsequently, different weights are assigned to these channels to implement an attention mechanism along the channel dimensions. This paper employs 2D-DCT technology to transform the feature extraction process for different channels into a feature compression process using multispectral frequency components. Specifically, 2D-DCT maps time-domain signals from the spatial domain to the frequency domain, transforming energy dispersion in the time domain into relatively concentrated energy forms in the frequency domain.

The specific data processing flow of the multispectral channel attention module is as follows:

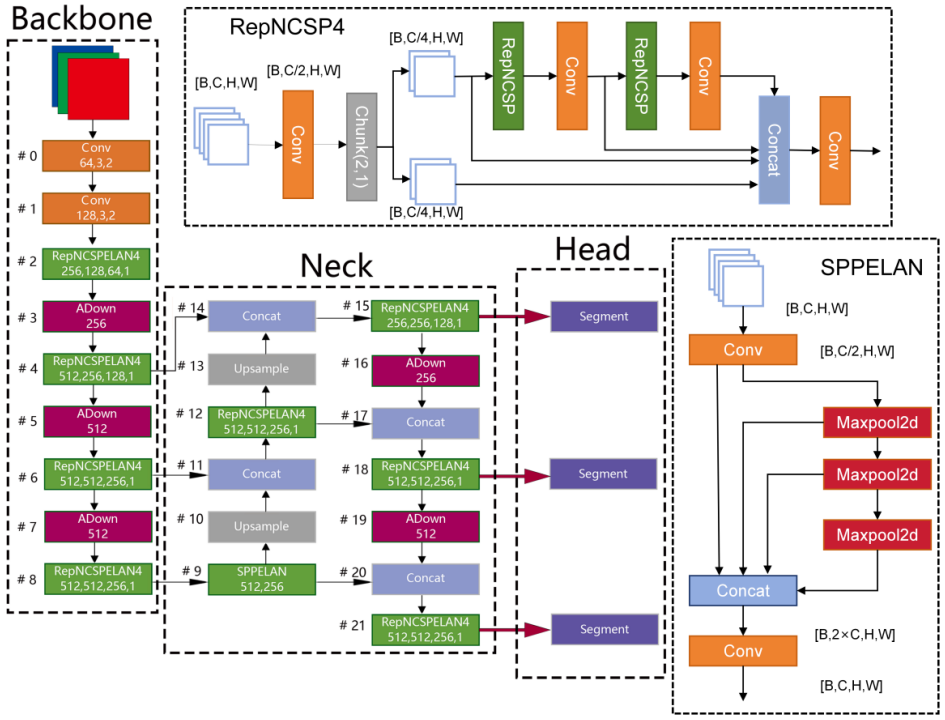


Fig. 1. Architecture of YOLOv9.

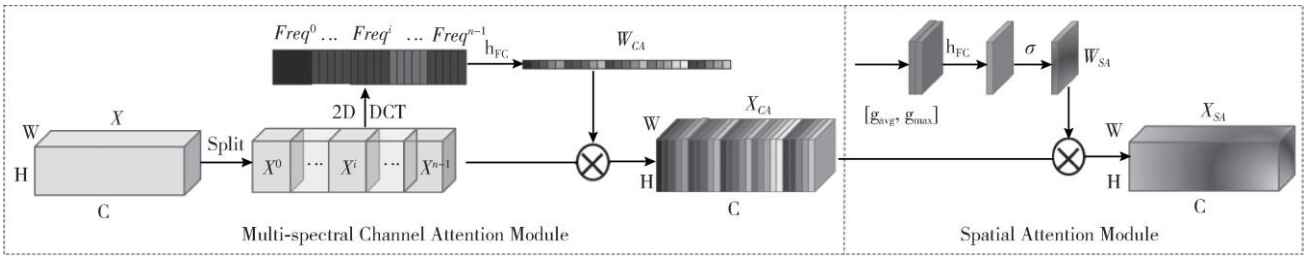


Fig. 2. Structure of the fusion attention module.

Step 1: As shown in Fig. 2, the input feature map $X \in R^{C\times H\times W}$ is split along the channel dimension into n feature map blocks $X^i \in R^{\frac{C}{n}\times H\times W}$.

Step 2: For each feature map block Xi, utilize the two-dimensional Discrete Cosine Transform (2D-DCT) to extract the corresponding multispectral frequency information, obtaining the feature vector $\mathrm{Freq}^i \in R^{\frac{\mathrm{C}}{\mathrm{n}}\times 16}$ as described by Eq. (1) and Eq. (2). Here, H and W represent the height and width of the feature map, respectively, and u, v are the two-dimensional indices for the feature map block Xi.

$$\mathrm{Freq}^i = 2DDCT^{\mathrm{u,v}}\left(X^i\right) = \sum_{h=0}^{\mathrm{H}-1}\sum_{w=0}^{\mathrm{W}-1} X^i_{:,h,w} B^{\mathrm{u,v}}_{h,w} \tag{1}$$

$$\mathrm{B}^{u,v}_{h,w} = \cos\left(\frac{h}{\mathrm{H}}\left(\mathrm{u}+\frac{1}{2}\right)\right)\cos\left(\frac{w}{\mathrm{W}}\left(\mathrm{v}+\frac{1}{2}\right)\right) \tag{2}$$

Step 3: Concatenate the feature vector Freqi along the channel dimension to form the multispectral frequency information Freq∈R C×16. As indicated in Eq. (3), after a fully connected and Sigmoid operation, the channel weight matrix WCA∈R 1×1×C is obtained. This matrix is then multiplied by the input feature map to produce the channel-attention-weighted feature map XCA.

$$W_{CA} = \sigma\left(h_{\mathrm{RC}}(\mathrm{Freq})\right) \tag{3}$$

Eq. (3) where σ represents the Sigmoid function and hRC denotes the fully connected operation.

2) Spatial attention module: As depicted on the right side of Fig. 2, the spatial attention module focuses on the cracks and their surrounding areas within the image based on the input feature map. Specifically, according to Eq. (4), the feature map XCA undergoes both max pooling and average pooling. Subsequently, these pooled features are concatenated along the channel dimension, and a fully connected operation is used to generate the spatial weight matrix WSA ∈ RH×W×1. This matrix is then multiplied by the feature map XCA to produce the output feature map XSA.

$$W_{SA} = \sigma\left(h_{\mathrm{FC}}\left(\left[\mathrm{g}_{\mathrm{avg}}\left(X_{CA}\right), \mathrm{g}_{\mathrm{max}}\left(X_{CA}\right)\right]\right)\right) \tag{4}$$

Eq. (4) where hFC represents the fully connected operation, gavg and gmax denote average pooling and max pooling, respectively, and σ is the Sigmoid function.

C. Task Space

In deep learning, classification tasks focus on capturing the overall information of the target, while regression tasks are more dependent on the edges and finer details of the object. Drawing inspiration from TSD and RetinaNet, this paper introduces a Task-Space Disentanglement Head (TSDHead), which separates the classification and regression tasks during the multi-dimensional prediction phase. This decoupling allows the model to optimize each task independently, without the need to balance between them. The classification branch optimizes weights by following the steepest descent of the classification loss gradient, while the regression branch optimizes in a similar manner for its own specific task.

As shown in Fig. 3, the TSDHead processes the fused feature map to perform classification and regression predictions, and then inputs the results into the Non-Maximum Suppression (NMS) module for further processing. Specifically, the TSDHead comprises both a classification and a regression branch. The classification branch, used for predicting object categories, includes four structurally identical depthwise separable convolutional layers and one category prediction layer. Each depthwise separable convolution layer consists of a depthwise convolution layer (kernel size of 3×3 and the same number of channels as the input feature map) and a pointwise convolution layer (kernel size of 1×1, with 256 channels). The category prediction layer uses a kernel size of 3×3 and a channel count of K×A, where K represents the number of categories (set to 5 in this paper, including four types of cracks and background) and A represents the number of preset anchor boxes per spatial position on the feature map, set to 3. The structure of the regression branch mirrors the classification branch, except that the K in the prediction layer of the regression branch is 4, indicating the offsets for the center position and dimensions of the bounding boxes. After processing through the TSDHead, the feature map yields the crack categories and bounding box coordinates, which are refined by the NMS module to produce the final prediction results.

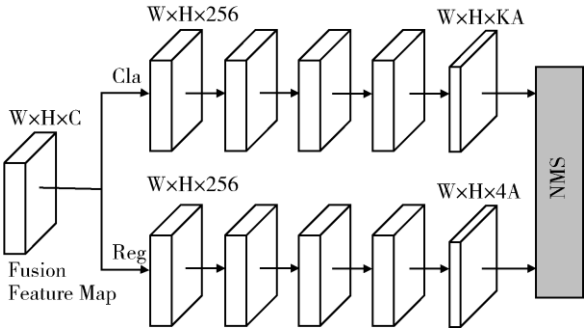


Fig. 3. Structure of the task-space disentanglement head.

1) K-means clustering of crack anchor box sizes: To address the diversity of road crack shapes and extreme aspect ratios, this paper employs the K-means clustering algorithm to cluster the sizes of bounding boxes in a constructed road crack dataset. Following the design philosophy of YOLOv5, the paper clusters large, medium, and small target sizes at three down sampling scales (8x, 16x, and 32x). Each down sampling scale is preset with three anchor boxes, with the clustering results presented in Table I.

TABLE I. CLUSTERING SIZES OF ANCHOR BOXES

	Scale_D32	**Scale_D16**	**Scale_D8**
Anchor_1	23,11	57,40	335,25
Anchor_2	76,8	212,13	115,89
Anchor_3	24,46	46,78	216,86

III. Experiments and Analysis

A Model Training and Testing Trials

1) Experimental data: The research dataset was constructed in two parts. The first part originated from the Crack500 dataset [11], where Yang and colleagues [11] used smart digital devices to capture 500 images of road surface cracks at Temple University with a resolution of 2000×1500, 24-bit RGB, creating the Crack500 dataset for crack detection. To enrich the experimental data, a photographic collection platform was established using smart digital devices to capture an additional 300 images of road surface cracks at a resolution of 1920×1080, 24-bit RGB, forming the second part. The digital devices used were equipped with three cameras, capable of capturing images up to 48 million pixels.

For ease of model training, a total of 800 images from both parts were cropped and filtered to produce 1600 images with a resolution of 320×320, 24-bit RGB. Of these, 1350 images were used as the training and validation set, which was randomly divided in a 9:1 ratio, and 250 images served as the test set. The test set was used solely for testing and did not participate in network training. Each collection was divided into two categories: fine narrow cracks and clearly visible wide cracks. Table I presents the number of each type of crack, and Fig. 4 provides examples of the crack images. The crack images were annotated using the LabelMe tool and further formatted into the VOC dataset structure.

TABLE II. Experimental Data

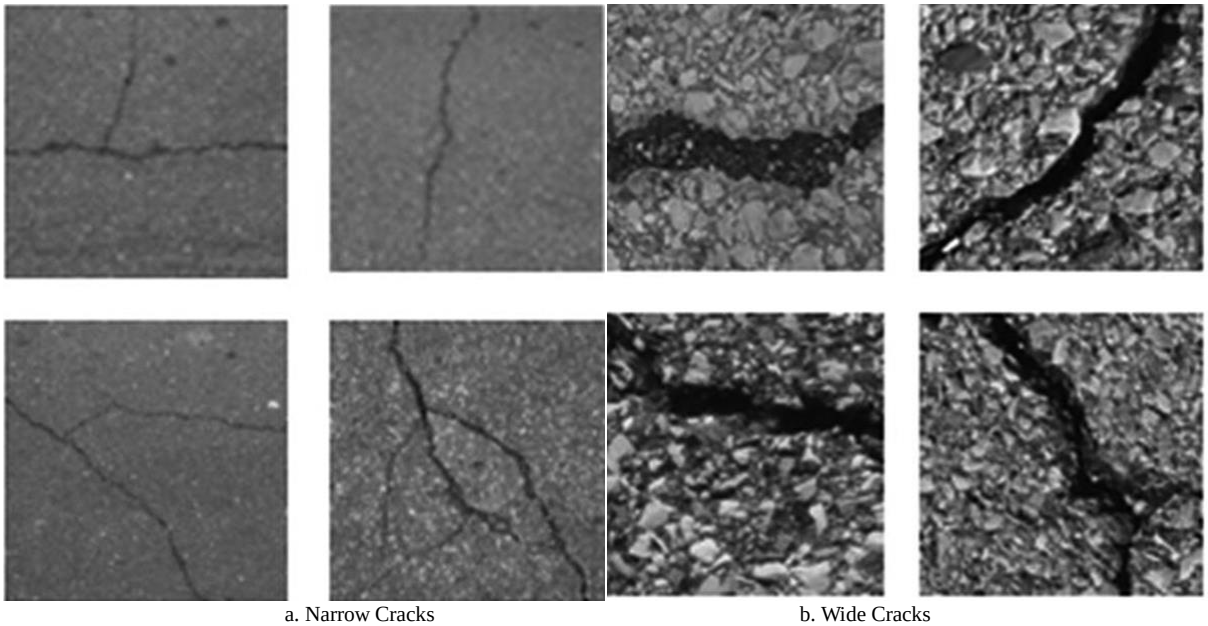
Training	Number of Images	Validation Set	Number of Images
Narrow Cracks	498	Narrow Cracks	91
Wide Cracks	852	Wide Cracks	159

2) Comparison of segmentation network models: This study compares the Improved YOLOv9 with Unet, SOLO v2 [12], Mask R-CNN (Mask Recycle Convolutional Neural Network), and Deeplab v3+ (Deep Convolutional Neural Networks v3 Plus) [13]. SOLO v2 and Mask R-CNN are instance segmentation algorithms, whereas Improved YOLOv9, Unet, and Deeplab v3+ are semantic segmentation models.

a) Unet: This network architecture features a clear U-shaped structure with symmetrical encoding on the left and decoding structures on the right, enhancing the extraction of feature map information. The Unet structure has low dependency on the number of images and can complete end-to-end training with only a small set of images, making it suitable for medical image segmentation.

b) Mask R-CNN: This network builds on the Faster Recycle Convolutional Neural Network (Faster R-CNN), adding a mask branch that runs in parallel with the classification and bounding box regression branches to predict segmentation masks. It employs a top-down, detection-based method that detects regions of each instance first and then segments the instance masks within these areas. Detection-based methods are generally highly accurate and rely on precise bounding box detection, which requires substantial computational resources [14].

c) SOLO v2: Unlike Mask R-CNN, this network transforms the segmentation task into a pixel classification problem, eliminating the need for proposal generation. The network has two branches: a category prediction branch that predicts the semantic category of the target, and a mask branch that predicts the instance mask of the target [15].



a. Narrow Cracks b. Wide Cracks

Fig. 4. Crack image of pavement.

d) Deeplab v3+: This network represents the latest generation of Deeplab models, using Deeplab v3 as the encoding structure and incorporating a decoder to address the loss of fine detail information caused by direct up-sampling of feature maps in Deeplab v3, thereby achieving advanced semantic segmentation performance.

3) Testing trial setup: After training, the models load the optimally saved weights from the training process to predict the test set, which consists of 250 images with a resolution of 320×320, 24-bit RGB. The test hardware platform includes an AMD Ryden 5 3600 CPU and NVIDIA GeForce GTX 2060 GPU, running on Windows 10 with Python version 3.6. Except for Mask R-CNN, which is tested using TensorFlow version 1.13, the other models are tested using PyTorch version 1.4. The test results are RGB three-channel images, which are then binarized and compared with the true images of the test set to compute evaluation metrics.

4) Evaluation metrics: To assess the segmentation performance of Improved YOLOv9 and the comparison models, this study employs the Jaccard coefficient and F1 score as evaluation metrics. Precision and recall are crucial parameters for binary classification problems and are important indicators of model segmentation performance. Calculations for precision and recall are provided in Eq. (5) and Eq. (6).

$$P = \frac{n_{\mathrm{TP}}}{n_{\mathrm{TP}} + n_{\mathrm{FP}}} \tag{5}$$

$$R = \frac{n_{\mathrm{TP}}}{n_{\mathrm{TP}} + n_{\mathrm{FN}}} \tag{6}$$

For a single image, segmenting the crack regions essentially means performing binary classification for each pixel, where nTP (true positives) represents pixels correctly identified as cracks, nFP (false positives) represents non-crack pixels predicted as cracks, nFN (false negatives) represents crack pixels predicted as non-cracks, and nTN (true negatives) represents non-crack pixels correctly identified as non-cracks.

A higher precision indicates a larger number of correctly identified crack pixels among those predicted as cracks by the model. Relying solely on either precision or recall to evaluate model performance is not advisable. For example, if all pixels in a test image are predicted as cracks, the recall would be 1, but the precision might be low.

Therefore, the harmonic mean of precision and recall, known as the F1 score, is used to measure model performance. The F1 score reflects the similarity between the predicted crack pixel set and the true crack pixel set. The F1 score ranges from 0 to 1, with higher values indicating better crack segmentation effectiveness. The calculation is shown in Eq. (7).

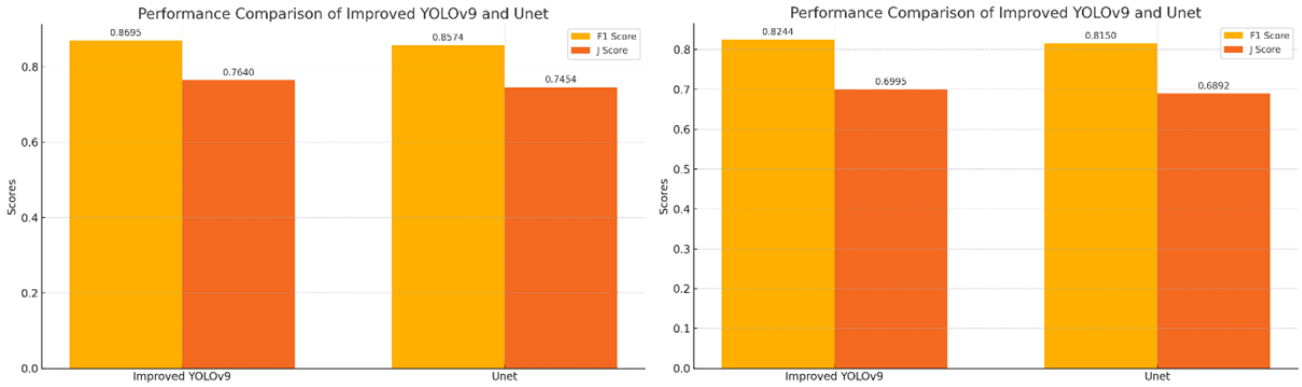
$$F_1 = \frac{2PR}{P + R} \tag{7}$$

The Jaccard coefficient measures the similarity between the predicted crack region and the actual crack region. It is calculated as the percentage of the intersection of the predicted and actual regions relative to the union of these regions. The value of the Jaccard coefficient ranges from 0 to 1, with higher values indicating a greater overlap between the predicted and actual areas, meaning that the predicted crack regions more closely match the actual regions. The calculation of the Jaccard coefficient is shown in Eq. (8).

$$J = \frac{n_{TP}}{n_{TP} + n_{FP} + n_{FN}} \tag{8}$$

B Experimental Results

1) Comparison of evaluation metrics between improved YOLOv9 and Unet models: This study first analyzes the enhancements made in Improved YOLOv9. The road surface crack test dataset includes two types of images: (1) fine narrow cracks with low contrast and narrow width, and (2) clear images of wider cracks. The F1 and Jaccard coefficients for Improved YOLOv9 and Unet under these two categories are shown in Fig. 5. As seen from Fig. 5, the metrics for Improved YOLOv9 are higher than those for Unet in both types of cracks, indicating that Improved YOLOv9 performs better in segmenting both narrow and wide cracks. Specifically, the F1 and Jaccard coefficients for narrow cracks are 4% to 6% lower than those for wide cracks, suggesting that crack width impacts the segmentation performance of the models.



a. Wide cracks b. Narrow cracks

Fig. 5. F1 and Jaccard coefficients of YOLOv9 and Unet.

Fig. 6 and Fig. 7 show the real and predicted segmentation results for narrow and wide cracks using Improved YOLOv9 and Unet models. The first column is the original image, the second column is the ground truth, and the third and fourth columns are the predictions from Unet and Improved YOLOv9, respectively, with white areas representing the crack regions.

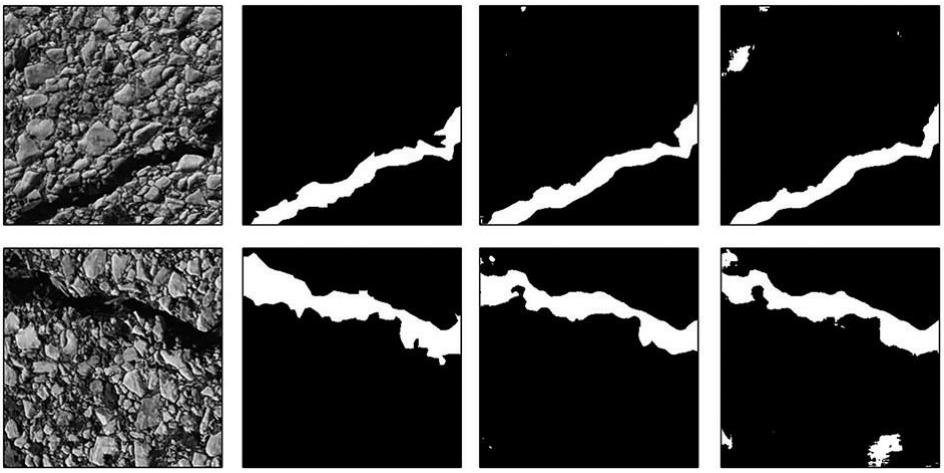


Fig. 6. Long and narrow crack segmentation result.

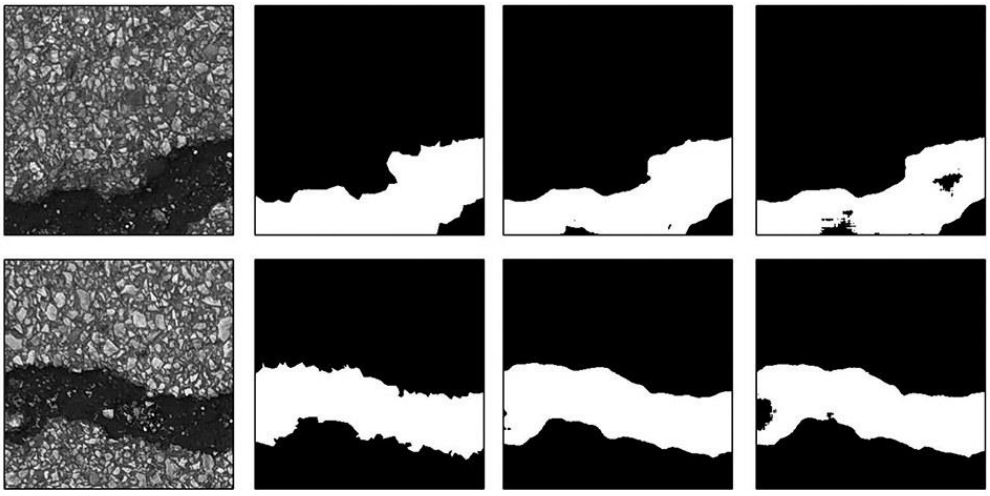


Fig. 7. Non-narrow crack segmentation result.

From the Figures, it is evident that Unet suffers from issues of over-segmentation and under-segmentation, particularly severe over-segmentation for narrow cracks (as shown in column 3 of Fig. 7) and under-segmentation for wide cracks (column 3 of Fig. 8). Compared to Unet, the Improved YOLOv9 proposed in this paper demonstrates better segmentation performance, with enhancements in feature extraction and the application of crack attention units contributing to more accurate crack image segmentation.

2) Real-time analysis of improved YOLOv9 and comparative models: This section of the study focuses on analyzing both the real-time performance and computational costs of the Improved YOLOv9 model compared to other segmentation models (Unet, SOLO v2, Mask R-CNN, and Deeplab v3+). The key metrics evaluated include single-frame image inference times, model complexity, and the balance between speed and accuracy.

As illustrated in Fig. 8, the inference time comparison shows that Improved YOLOv9 has a slightly longer inference time per frame (0.089 seconds) compared to Unet (0.084 seconds), but it offers significantly higher segmentation accuracy. This indicates that Improved YOLOv9 strikes an effective balance between speed and precision, which is essential for tasks requiring both real-time performance and high reliability, such as crack detection in road surfaces.

Other comparative models, such as SOLO v2 and Mask R-CNN, have considerably longer inference times (0.130 and 0.162 seconds per frame, respectively), making them less suitable for real-time applications where quick response is crucial. These models, while offering strong segmentation capabilities, suffer from higher computational costs and slower processing times, which could be a disadvantage in large-scale, real-time crack detection tasks.

Deeplab v3+ performs more closely to Improved YOLOv9, with an inference time of 0.093 seconds per frame. While this

model is competitive in terms of speed, it does not match the segmentation accuracy of Improved YOLOv9, especially in detecting fine and irregular cracks. Thus, for applications requiring both high accuracy and efficient real-time performance, Improved YOLOv9 proves to be the more optimal choice.

In terms of model complexity, the architectural advancements in Improved YOLOv9, such as the Fusion Attention Module and Task Space Disentanglement, contribute to its slight increase in computational cost compared to Unet. However, these enhancements also lead to more accurate feature extraction and better localization, particularly in complex road conditions. As a result, the minimal trade-off in processing time is justified by the superior detection performance in real-world applications.

This analysis highlights the strengths and weaknesses of each model regarding both real-time performance and computational efficiency. While Improved YOLOv9 may have a slightly higher computational cost compared to Unet, its improved accuracy and relatively low inference time make it the best choice for practical road maintenance operations where detection quality and speed are both critical. In contrast, models such as SOLO v2 and Mask R-CNN, despite their strong segmentation capabilities, exhibit slower processing times, making them less suitable for real-time deployments in large-scale applications.

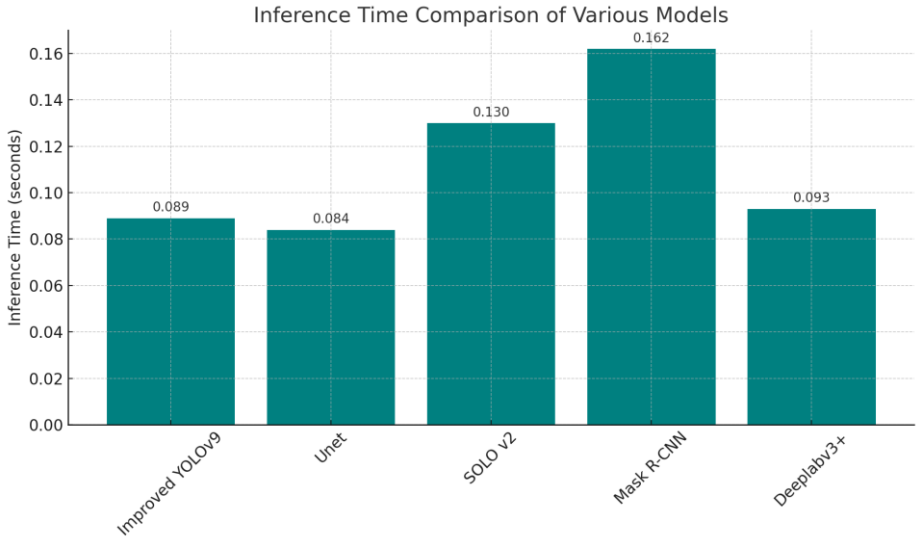


Fig. 8. Inference time of different models.

3) F1 and Jaccard indices of improved YOLOv9 and comparative models: In order to evaluate the segmentation performance of the Improved YOLOv9 model in detail, this research compares its results against those of Unet, SOLO v2, Mask R-CNN, and Deeplab v3+ on a test set consisting of 250 images. These images include two distinct types of cracks, providing a diverse basis for assessment. The average F1 and Jaccard coefficients obtained from the testing are graphically represented in Fig. 9.

The analysis of the results demonstrates that Mask R-CNN and Deeplab v3+ score significantly lower on both F1 and Jaccard indices compared to Improved YOLOv9 and Unet. This lower performance highlights the challenges these models face in accurately segmenting fine and narrow cracks, as well as broad and distinct cracks, under the testing conditions. Specifically, the metrics for Improved YOLOv9 are slightly higher than those for Unet, marking it as the superior model among the four evaluated. With F1 and Jaccard coefficients of 0.8403 and 0.7221, respectively, Improved YOLOv9 demonstrates the highest performance in terms of set evaluation metrics, indicating its enhanced capability in image segmentation and crack detection accuracy across diverse road surfaces.

These findings underscore the effectiveness of Improved YOLOv9 in handling varying crack types and conditions, potentially leading to more reliable and robust road maintenance and safety protocols. The integration of advanced feature extraction and attention mechanisms within Improved YOLOv9 likely contributes to its elevated performance, suggesting avenues for future enhancements in similar segmentation models.

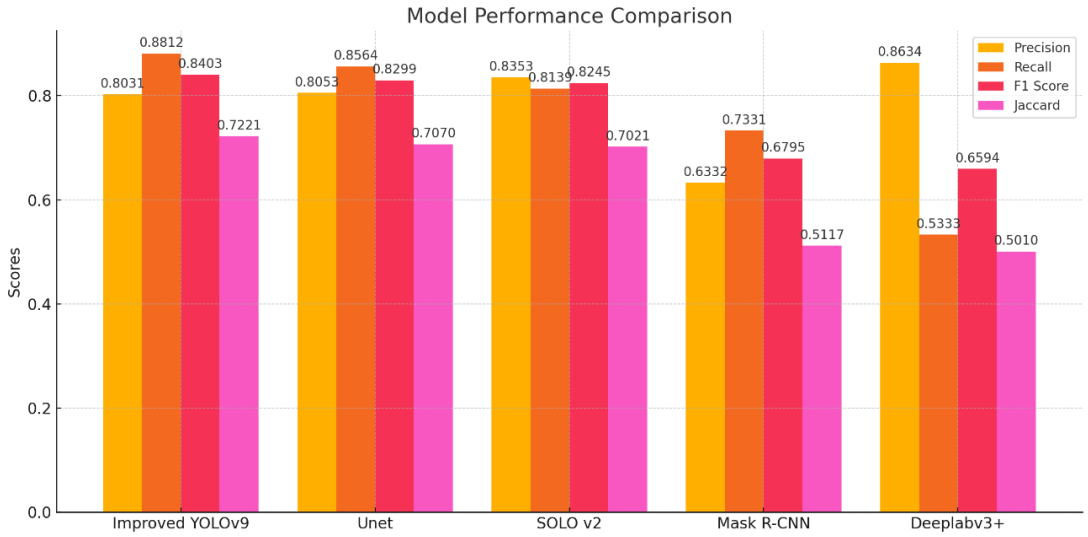


Fig. 9. F1 and Jaccard coefficients of different models.

4) Segmentation results on test data of improved YOLOv9 and comparative models: This study further analyzes the segmentation capabilities of the four models using the road surface crack test set. Three images of wide cracks with significant differences between the crack and the background were randomly selected from the test set for comparative analysis of predictions from the four models, as shown in Fig. 10. The segmentation results and evaluation metrics are consistent, with the Deeplab v3+ model performing poorly in actual segmentation, exhibiting issues such as excessive segmentation area and discontinuity. This indicates that Deeplab v3+ struggles with accurate crack image segmentation under conditions of limited image quantity. SOLO v2 and Mask R-CNN perform better than Deeplab v3+ but still show noticeable issues with crack misdetection. Improved YOLOv9 and Unet perform well in crack detection, with Improved YOLOv9 showing more precise crack segmentation, fewer misdetections, and better continuity.

To further investigate the performance of each model in segmenting fine narrow cracks with low contrast and narrow width, several such cracks were selected for comparison. Fig. 11 displays the segmentation results under conditions of narrow crack width and low contrast, where Mask R-CNN shows imprecise edge detection and misdetection issues (from left to right: original image, ground truth, Improved YOLOv9, Unet, SPLOv2, Mask R-CNN, Deeplabv3+). Deeplab v3+ not only has misdetection issues but also incorrectly identifies non-crack areas as cracks, particularly in cases of narrow longitudinal cracks, where misdetection is especially evident. Unet generally performs better than Mask R-CNN and Deeplabv3+ but also shows some misdetection. Improved YOLOv9, under conditions of narrow and low-contrast cracks, still clearly segments crack edges without misdetection or false detection, achieving the best segmentation results.

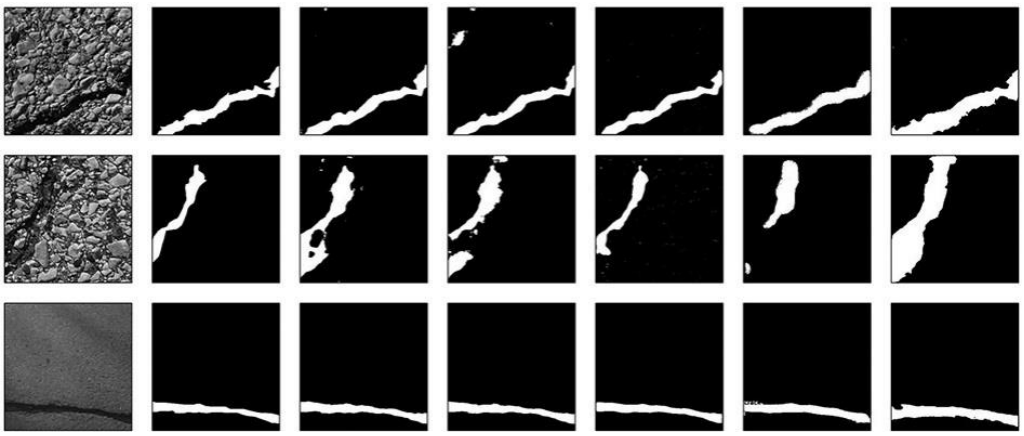


Fig. 10. Test results of pavement cracks under multiple models.

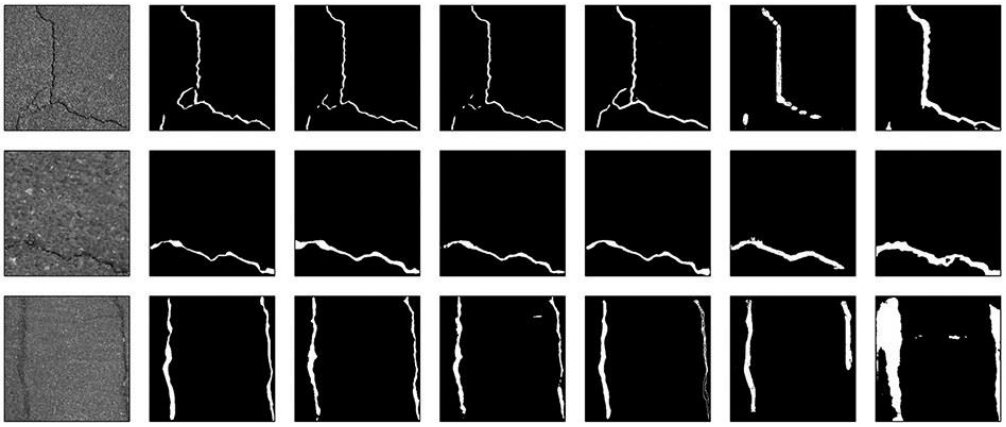


Fig. 11. Segmentation results of multiple models in the case of narrow crack width and low contrast.

IV. Discussion

To ensure the applicability of CrackNet in real-world road maintenance systems, deployment optimizations such as model pruning and quantization can be considered in the future.

Model Pruning: By removing less important connections or neurons, pruning can significantly reduce the model size and inference time without sacrificing much accuracy. This is particularly useful for deployment on mobile or edge devices with limited computational resources. Pruning can make CrackNet more efficient and suitable for resource-constrained platforms (such as drones or vehicle-mounted systems), enabling real-time crack detection in large-scale road inspections.

Quantization: Another potential optimization is model quantization, which converts high-precision weights (e.g., 32-bit floats) into lower precision (e.g., 8-bit integers). Quantization helps reduce the model size and speeds up inference, allowing faster computations while maintaining acceptable accuracy. This will make CrackNet more suitable for deployment in embedded systems and mobile devices, where memory and energy efficiency are critical.

V. Conclusion

Addressing the issues of imprecise edge segmentation and slow detection speed in traditional crack detection algorithms, this paper proposes a road crack detection method based on improved YOLOv9. By suppressing useless features extracted during high-low order feature fusion and enhancing the model's ability to extract crack features, the method achieves segmentation of both narrow and wide crack images.

F1 score and Jaccard coefficient are selected as evaluation metrics. A comparison between improved YOLOv9 and the basic Unet model in segmenting narrow and wide cracks demonstrates the superiority of the proposed method over the basic Unet algorithm, both quantitatively and qualitatively.

The real-time performance of the model is evaluated based on the inference time of a single-frame image. While the improved YOLOv9 outperforms Unet in segmentation performance, its inference speed is 0.089 seconds per frame, only 0.005 seconds slower than Unet, striking a balance between real-time performance and segmentation accuracy.

Further comparisons are made with three other classic segmentation networks. The results show that the evaluation metrics of the improved YOLOv9, with an F1 score of 0.8403 and a Jaccard coefficient of 0.7221, surpass those of classic segmentation models such as SOLO v2, Mask R-CNN, and Deeplabv3+. Compared to other models, the improved YOLOv9 achieves the highest evaluation metrics and the best segmentation performance, effectively extracting road cracks.

While the proposed model's segmentation performance on subtle narrow cracks is inferior to that on clear wide cracks, it does not account for the interference caused by different lighting conditions at different times. Future research will focus on adjusting the network structure to improve the segmentation performance on subtle narrow cracks and preprocessing images using image enhancement algorithms to eliminate the influence of lighting conditions, enabling high-precision crack detection under various lighting conditions. The proposed CrackNet model has significant potential for real-world applications in road maintenance systems. Its ability to accurately detect cracks in road surfaces, including fine and irregular cracks, positions it as a valuable tool for improving the efficiency and precision of road maintenance operations. By incorporating the CrackNet model into automated inspection systems, road maintenance departments can significantly reduce the time and labor costs associated with manual inspections, while ensuring more timely repairs, which are critical for preventing further road deterioration. Moreover, the model's real-time detection capability allows for continuous monitoring of road conditions, enhancing the safety of drivers and reducing the risks of accidents caused by undetected surface damage.

Funding

Key R&D and Promotion Special Project (Science and Technology Research) in Henan Province: Research on key technologies of road damage detection based on deep learning (232102210108).

Statement of Interest

The author declares that there is no conflict of interest in the manuscript.

REFERENCES

[1] Praticò F G, Fedele R, Naumov V, et al. Detection and monitoring of bottom-up cracks in road pavement using a machine-learning approach[J]. Algorithms, 2020, 13(4): 81.

[2] Ha J, Kim D, Kim M. Assessing severity of road cracks using deep learning-based segmentation and detection[J]. The Journal of Supercomputing, 2022, 78(16): 17721-17735.

[3] Feng X, Xiao L, Li W, et al. Pavement crack detection and segmentation method based on improved deep learning fusion model. Mathematical Problems in Engineering, 2020, 2020: 1-22.

[4] Wang S J, Zhang J K, Lu X Q. Research on Real-Time Detection Algorithm for Pavement Cracks Based on SparseInst-CDSM. Mathematics, 2023, 11(15): 3277.

[5] Bhat S, Naik S, Gaonkar M, et al. A survey on road crack detection techniques. 2020 international conference on emerging trends in information technology and engineering (ic-ETITE). IEEE, 2020: 1-6.

[6] Gavilán M, Balcones D, Marcos O, et al. Adaptive Road crack detection system by pavement classification. Sensors, 2011, 11(10): 9628-9657.

[7] Zhang L, Yang F, Zhang Y D, et al. Road crack detection using deep convolutional neural network. 2016 IEEE international conference on image processing (ICIP). IEEE, 2016: 3708-3712.

[8] Wang W, Wu L. Pavement crack extraction based on fractional integral valley bottom boundary detection. Journal of South China University of Technology (Natural Science Edition), 2014, 42(1): 117-122.

[9] Lee T, Yoon Y, Chun C, et al. Cnn-based road-surface crack detection model that responds to brightness changes. Electronics, 2021, 10(12): 1402.

[10] Hammouch W, Chouiekh C, Khaissidi G, et al. Crack detection and classification in moroccan pavement using convolutional neural network. Infrastructures, 2022, 7(11): 152.

[11] Fan R, Bocus M J, Zhu Y, et al. Road crack detection using deep convolutional neural network and adaptive thresholding. 2019 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2019: 474-479.

[12] Zhang L, Yang F, Zhang Y D, et al. Road crack detection using deep convolutional neural network. 2016 IEEE international conference on image processing (ICIP). IEEE, 2016: 3708-3712.

[13] Carr T A, Jenkins M D, Iglesias M I, et al. Road crack detection using a single stage detector based deep neural network. IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems. IEEE, 2018: 1-5.

[14] Siriborvornratanakul T. Pixel-level thin crack detection on road surface using convolutional neural network for severely imbalanced data. Computer-Aided Civil and Infrastructure Engineering, 2023, 38(16): 2300-2316.

[15] Sy N T, Avila M, Begot S, et al. Detection of defects in road surface by a vision system. MELECON 2008-The 14th IEEE Mediterranean Electrotechnical Conference. IEEE, 2008: 847-851.

DBN-GRU Fusion and Decomposition-Optimisation-Reconstruction Algorithm in Advertising Traffic Prediction

Ronghua Zhang
College of Media and Design, Xi'an Peihua University, Xi'an 710125, Shaanxi, China

***Abstract*—As the premise and foundation of advertisement traffic selling and distribution, effective IPTV advertisement traffic prediction not only reduces the operation cost, but also improves the intelligent level of new media advertisement traffic management. In order to further improve the accuracy of new media advertisement traffic prediction, this paper proposes a new media advertisement traffic prediction method based on the hybrid prediction framework of decomposition-optimisation-integration, which is a hybrid model of gated recurrent unit neural network and deep confidence network improved by capsule swarm optimisation algorithm. Firstly, according to the principle of system construction, paper analyses the influencing factors and construct a complete new media advertisement traffic prediction index system; secondly, paper improves the optimisation process of the parameters of the deep confidence network and the gated recurrent unit network by using the quilt group optimisation algorithm, and put forward a new media advertisement traffic prediction method based on the decomposition-optimisation-integration framework; Finally, the proposed method is analysed using new media advertisement traffic data. The results show that the proposed method improves the accuracy of the prediction model and solves the problem of large prediction error in new media advertisement traffic prediction methods.**

Keywords*—New media advertising traffic prediction; kernel principal component analysis; variational modal decomposition; quilt group algorithm; deep learning; decomposition-optimisation-reconstruction algorithm

I. INTRODUCTION

With the development of Internet technology, network-based IPTV (Internet Protocol Television) [1] enters people's vision and life, ware using the programme resources provided by the broadcasting network, and adopting the broadband communication network with higher data transmission rate, wider coverage, and better operation condition as the basic network facilities [2].The introduction of IPTV makes people enjoy the personalised, interactive and customisable audiovisual services [3]. IPTV service adopts the model of cooperation between broadcasters and telecommunication, the user data is not peer-to-peer sharing, and the user behaviour data cannot be accurately managed, which leads to the increase in the cost of bidding and targeting advertisement, the decrease in the efficiency, and the lack of obvious effect [4]. Effective IPTV advertisement traffic prediction, as the premise and foundation of advertisement traffic selling and distribution, not only reduces the operation cost, but also improves the intelligent level of new media advertisement traffic management [5]. Currently, new media advertising traffic prediction using time series prediction model [6], from the time series smoothness, linearity or not, the prediction method is divided into Autoregressive integrated moving average model (ARIMA) [7], BP neural network model [8], support vector machine [9], fuzzy theory [10], Elman recurrent neural network [11] and other methods. The study in [12] used ARIMA model to construct the energy demand forecasting problem in Turkey, and analysed the mapping relationship between energy influencing factors and energy demand; study in [13] analysed the multivariate data structure characteristics, combined with neural networks, and carried out the forecasting analysis of power energy consumption; literature [14] constructed the risk function based on the empirical error and the canonical term, and used SVM algorithm to construct the stock price index for the prediction; study in [15] combines K-means clustering algorithm and fuzzy neural network to construct the market sales trend prediction model; study in [16] uses Elman neural network and SVM algorithm to construct the cat catch quantity prediction model. In response to the analysis of the above literature, the existing new media advertising traffic prediction method indicator system selection lacks objectivity and the prediction accuracy is not high [17-19]. The factors affecting advertisement traffic prediction include not only statistical variables, but also time series data. In order to improve the accuracy of advertising traffic prediction, this paper adopts different prediction models for different variables. The single prediction model and simple combination prediction model can no longer adapt to the significant volatility and nonlinearity of advertising traffic data, and the prediction accuracy requirements are increasing, the hybrid prediction model based on Decomposition-optimization-ensemble (DOE) [20] is applied to the new media advertising traffic prediction problem. The study in [21] combines EMD, LSTM and SVR to solve the prediction problem; study in [22] uses complementary integration of empirical modal decomposition, singular spectrum analysis, and ELM to construct a time series prediction model. Deep learning, as a prediction method based on intelligent algorithms, has been widely used in all kinds of prediction problems, and the prediction effect is relatively excellent. With the advertisement traffic fluctuation showing randomness and non-stationarity, the advertisement traffic prediction faces the influence of complex and variable factors, and a single deep learning model can no longer meet the requirements of advertisement traffic prediction.

In order to further improve the new media advertisement traffic prediction accuracy, this paper adopts the hybrid

prediction framework of decomposition-optimisation-integration.

- Analyse the influencing factors of the new media advertisement traffic prediction model and construct the input vector of new media advertisement traffic prediction;
- Decompose the original new media advertisement traffic data using the variational modal decomposition algorithm to obtain more detailed information features of the new media advertisement traffic sequence;
- Improve the GRU and DBN network by combining with the quilt swarm algorithm, and at the same time, put forward a new media advertisement traffic prediction method based on the quilt optimization algorithm improving the DBN-GRU hybrid model for new media advertisement traffic prediction;
- The new media advertisement traffic data verifies that this paper's method has higher prediction accuracy.

II. Analysis of the Problem of Predicting Advertising Traffic in New Media

In order to construct an objective, scientific and reasonable system of influencing factors for new media advertising traffic prediction, this section analyses the influencing factors and constructs a completely new media advertising traffic prediction index system according to the principle of system construction.

Scientific, objective and comprehensive new media advertising traffic prediction influencing factors system construction index selection should be in line with the following principles [23]: 1) independent and comprehensive; 2) operable; 3) temporal; 4) comparable. Influence factors can be compared not only in the time dimension, but also vertically over a number of cycles. The principles of impact factor selection are shown in Fig. 1.

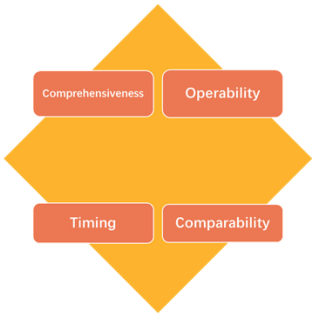


Fig. 1. Schematic diagram of the principle analysis.

According to the principled analysis of the selection of influencing variables for new media advertisement traffic prediction, the factors affecting the prediction should include the following dependent variables [24]: 1) daily click peak X1; 2) daily click peak X2; 3) platform code X3, the value of X3 is 1 means that the platform code is Inmobi, 2 means Zplay, 3 means Baidu, and 4 means Iflytek; 4) bidding reserve price X4; 5) Full insertion screen advert X5, the value of X5 is 0 for No and 1 for Yes; 6) Ad placement location information X6; 7) Ad provider X7; 8) Peak click time X8, Table I.

TABLE I. Influencing Variables of New Media Advertisement Flow

No.	Descriptions	Variables
1	The highest peak of daily clicks	X1
2	The lowest peak of daily clicks	X2
3	The platform code	X3
4	The reserve price of the auction	X4
5	Full interstitial ads	X5
6	The location information of the ad	X6
7	The value of the advertising provider	X7
8	The peak time of the click	X8

The new media advertisement traffic prediction impact variable system takes the key elements such as daily click peak X1, daily click minimum peak X2, platform code X3, bidding reserve price X4, full insertion screen advertisement X5, advertisement placement location information X6, advertisement provider X7, click peak time X8 as indicators, which fully embodies the whole elements of new media advertisement traffic prediction, and builds a scientific, objective, comprehensive and reasonable new media advertising traffic prediction impact vector system.

III. Related Technologies

A. KPCA

In order to extract the indicators with high contribution of the influence variables of new media advertisement traffic prediction, this paper adopts the Kernel Principal Component Analysis (KPCA) [25] method for feature extraction and dimensionality reduction of the influence variables. The principle of KPCA is shown in Fig. 2.

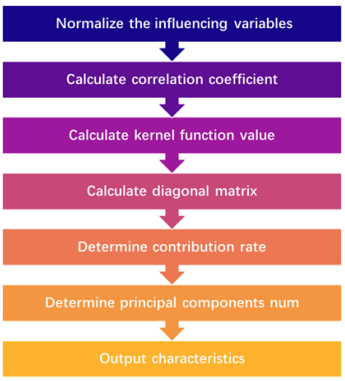


Fig. 2. The principle of kernel principal component analysis.

B. VMD

In order to better find the regularity of the time series of new media advertising traffic, this paper adopts the variational modal decomposition method to preprocess the predicted time series.

The main process of Variational mode decomposition (VMD) [26] is as follows:

1) Decompose $f(t)$ into k modal components with centre frequency and finite bandwidth, so that each mode satisfies the relevant conditions;

2) Obtain the optimal solution by obtaining the extreme points, update each modal component u_k with centre frequency ω_k;

3) Update λ with the value; 4) Judge whether the iteration stop condition is satisfied. satisfy the iteration stop condition. Repeat steps 2)-4) until the following iteration conditions are satisfied:

$$\frac{\sum_k \left\| \hat{u}_k^{n+1} - \hat{u}_k^n \right\|_2^2}{\left\| \hat{u}_k^n \right\|_2^2} < \varepsilon \tag{1}$$

In Eq. (1), $\varepsilon > 0$ is the determination accuracy.

C. Encapsulated Swarm Algorithm

Tunicate Swarm Algorithm (TSA) [27] is an intelligent swarm algorithm proposed to simulate the foraging behaviour of marine tunicate swarms, whose foraging process includes jet propulsion and swarm behaviour. The jet propulsion behaviour avoids conflicts between searching individuals and moves towards the optimal individual by means of the individual's own gravity, seawater current dynamics, and the interaction force between groups. The group determines the location of its companions through neural sensing of the current changes around itself and the light source of its companions, and gathers towards the food location to achieve group foraging (see Fig. 3).

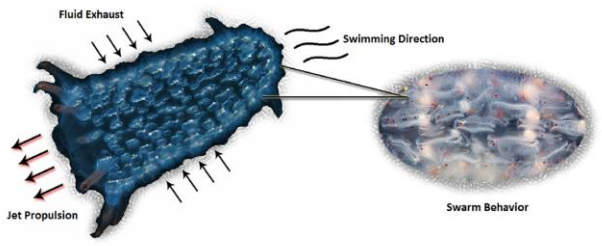


Fig. 3. Foraging behaviour of the periphyton

1) Jet propulsion: The quilt of the quilt swarm algorithm needs to avoid conflicts between individuals during jet propulsion. To avoid conflicts, new individuals are represented as follows:

$$A = \frac{G}{M} \tag{2}$$

In Eq. (2), G denotes the individual pendant force of the vesicle and M denotes the interaction force between the vesicle individuals, the calculation formula is as follows:

$$M = P_{\min} + c \cdot \left(P_{\max} - P_{\min} \right) \tag{3}$$

In Eq. (3), $P_{\max}, P_{\min}$ refers to the maximum and minimum values of the initial interaction velocity of individuals, respectively, which are usually set to $P_{\max} = 4, P_{\min} = 1$, and c is a random number.

After avoiding conflicts, the individual completes the search direction calculation using the distance between the optimal position and the current individual:

$$PD_i^t = \left| x_{best}^t - rand \cdot x_i^t \right| \tag{4}$$

In Eq. (4), x_{best}^t denotes the optimal individual, x_i^t denotes the current individual position, and $rand$ denotes a uniformly distributed random number.

Combining the distance between the optimal position and the current individual as well as the conflict avoidance strategy, the optimal individual drive-in formula for each vesicle individual term is as follows Eq. (5):

$$x_i^t = \begin{cases} x_{best}^t + A \cdot PD_i^t & rand \geq 0.5 \\ x_{best}^t - A \cdot PD_i^t & rand < 0.5 \end{cases} \tag{5}$$

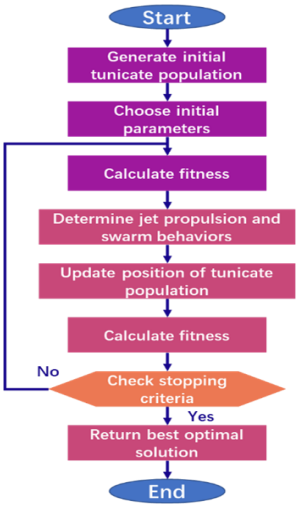


Fig. 4. Flowchart of TSA algorithm.

2) Group behaviour: The model for calculating the group behaviour of the quilt group is as follows:

$$x_i^{t+1} = \frac{x_i^t + x_i^{t-1}}{2 + c} \tag{6}$$

In Eq. (6), x_i^{t-1} denotes the updated position of the previous generation of vesicles relative to the most available individual, and c denotes a random value between 0 and 1.

3) TSA algorithm process and steps: According to the principle of TSA algorithm, the flowchart is shown in Fig. 4. During each iteration of the TSA algorithm, the location information of the encapsulated group is continuously evaluated and selected by the evaluation and selection strategy to obtain the final optimal solution.

This paper analyses the iterative optimization process of the TSA algorithm (see Fig. 5). From Fig. 5, the number of iterations increases and the population gradually converges to a centralised position.

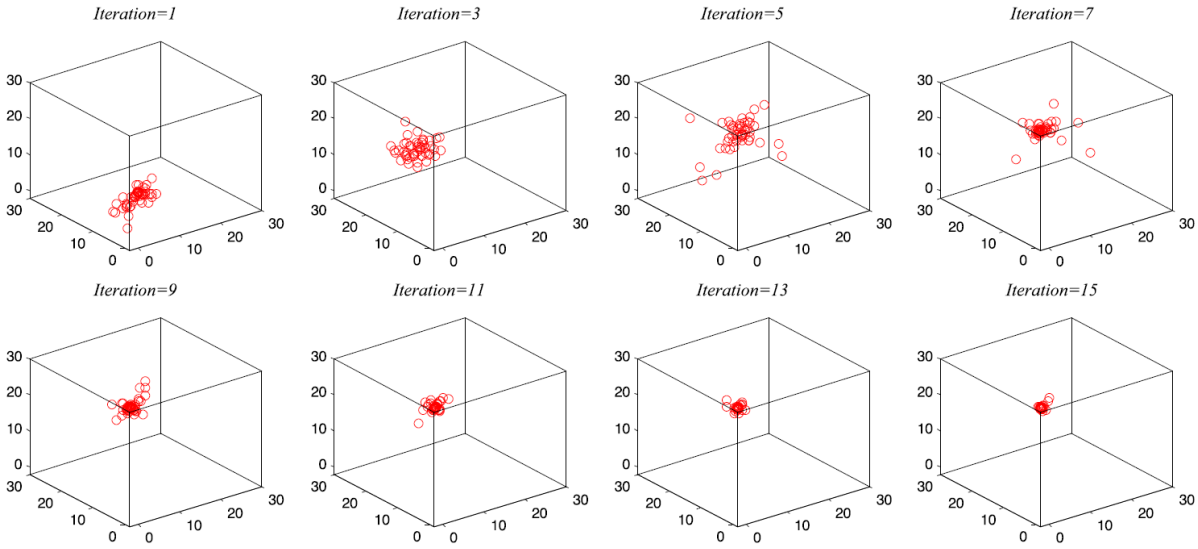


Fig. 5. Iterative optimisation process of the TSA algorithm.

D. Deep Confidence Networks

In order to analyse the mapping relationship between the influence variables of new media advertisement traffic prediction and the predicted value of traffic, this paper adopts deep confidence network as the prediction model construction algorithm, which solves the problem of constructing the model of influence variables and predicted value of traffic.

Deep Belief Networks (DBN) [28] consists of multiple layers of Restricted Boltzmann Machines (RBM), and the specific structure is shown in Fig. 6. The input layers v and h^1 constitute the first layer of Restricted Boltzmann Machines, and the input data is mapped through the activation function h_1, which is input to the second layer of Restricted Boltzmann Machines, and passes to reach the output layer in turn.

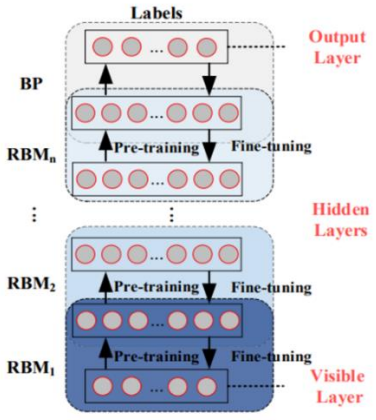


Fig. 6. Structure of deep confidence network.

1) Assuming that $\theta=(\omega,a,b)$ is a DBN network parameter, the energy function of RBM is expressed as:

$$E(v,h|\theta)=-\sum_{i=1}^{n}a_i v_i-\sum_{j=1}^{m}b_j h_j-\sum_{i=1}^{n}\sum_{j=1}^{m}v_i\omega_{ij}h_j \tag{7}$$

In Eq. (7) (v,h) is the state value, ω is the connection weight, and a and b are the biases.

2) Solve for θ^* by solving for the maximum value of the log-likelihood function:

$$\theta^*=\arg_\theta\max L(\theta)=\arg_\theta\max\sum_{k=1}^{K}\ln p\left(v^k|\theta\right) \tag{8}$$

In Eq. (8) *K* is the number of training samples.

3) Calculate the joint probability distribution function, Eq. (8) and Eq. (9):

$$p(v,h|\theta)=\frac{e^{-E(v,h|\theta)}}{Z(\theta)} \tag{9}$$

$$Z(\theta)=\sum_{v}\sum_{h}e^{-E(v,h|\theta)} \tag{10}$$

4) Calculate the activation probability of hidden layer nodes to determine the visible layer state, Eq. (11):

$$p\left(h_j=1|v,\theta\right)=sigmoid\left(b_j+\sum_{i=1}^{n}v_i\omega_{ij}\right) \tag{11}$$

5) Calculate the activation probability of the visual layer node as Eq. (12)

$$p\left(v_i=1|h,\theta\right)=sigmoid\left(a_i+\sum_{i=1}^{n}h_j\omega_{ij}\right) \tag{12}$$

(6) Update the RBM parameter θ, Eq. (13) to Eq. (15):

$$\Delta\omega_{ij}=\frac{\partial\log p(v)}{\partial\omega_{ij}}=\varepsilon\left(\left\langle v_i h_j\right\rangle_{data}-\left\langle v_i h_j\right\rangle_{predict}\right) \tag{13}$$

$$\Delta a_i = \frac{\partial \log p(v)}{\partial a_i} = \varepsilon\left(\langle v_i \rangle_{data} - \langle v_i \rangle_{predict}\right) \tag{14}$$

$$\Delta b_j = \frac{\partial \log p(v)}{\partial b_j} = \varepsilon\left(\langle h_j \rangle_{data} - \langle h_j \rangle_{predict}\right) \tag{15}$$

where ε denotes the learning rate, $\langle \square \rangle_{data}$ is the expectation of training after input data, and $\langle \square \rangle_{predict}$ is the expectation of the model itself.

E. Neural Network of Gated Recurrent Units

Compared with LSTM and RNN, GRU has a simple structure with fewer parameters and uses update gates and reset gates to control the network [29], and the structure is shown schematically in Fig. 7.

$$r_t = \sigma(W_{hr} h_{t-1} + W_{xr} x_t + b_r) \tag{16}$$

$$\tilde{h}_t = \tanh(W_{\tilde{r}h}(r_t * h_{t-1}) + W_{\tilde{x}h} x_t + b_{\tilde{h}}) \tag{17}$$

In Eq. (16) and Eq. (17), r_t is the reset gate which determines the amount of historical memory of h_{t-1}. $\tilde{h}_t$ is the latest information of the node at the current moment. h_{t-1}, h_t is the hidden layer information of the cell state at the moment of $t-1$ and t respectively, $W_{\tilde{r}h}$, $W_{\tilde{x}h}$, W_{xr}, W_{hr} are the weights, b_r, $b_{\tilde{h}}$ are the biases.

$$z_t = \sigma(W_{hz} h_{t-1} + W_{xz} x_t + b_z) \tag{18}$$

$$h_t = (1 - z_t) * h_{t-1} + z_t * \tilde{h}_t \tag{19}$$

In Eq. (18) and Eq. (19), W_{hz}, W_{xz} are weights and b_z is bias. z_t is the forgetting gate.

$$y_t = \sigma(W_{yt} h_t) \tag{20}$$

In Eq. (20), W_{yt} denotes the weights between the current hidden layer output h_t and the final output layer.

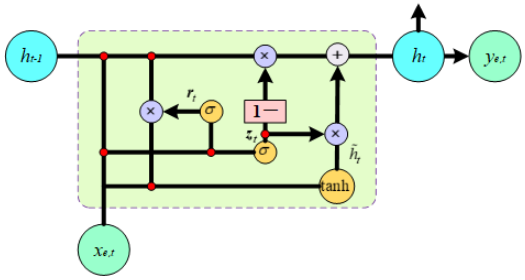


Fig. 7. GRU network.

F. Evaluation Indicators

This paper uses three evaluation indexes testing models such as Mean Absolute Error (MAE), Root Mean Square Five Error (RMSE), and Mean Absolute Percentage Error (MAPE), which are calculated by the following formulas:

$$RMSE = \sqrt{\left(\sum_{i=1}^{M}(\hat{y}_i - y_i)^2\right)/M} \tag{21}$$

$$MAE = \frac{1}{M}\sum_{i=1}^{M}|\hat{y}_i - y_i| \tag{22}$$

$$MAPE = \frac{1}{M}\sum_{i=1}^{M}\left|\frac{\hat{y}_i - y_i}{y_i}\right| \tag{23}$$

In Eq. (21) – Eq. (23), $\hat{y}_i$ denotes the predicted value based on the proposed algorithm, y_i denotes the true value and M is the number of test samples.

IV. A Methodological Process of New Media Advertisement Traffic Prediction Based on TSA-DBN-GRU Algorithm Under Decomposition-Optimisation-Reconfiguration Framework

A. DBN-GRU Prediction Model Based on TSA Algorithm

The combined DBN-GRU prediction model based on the TSA algorithm uses the TSA algorithm to optimise the DBN and GRU bias and weight values, and adopts the RMSE as the fitness function. The specific steps are as follows:

- Step 1: The Z-Score method was used to pre-process the raw data and divide the data set;
- Step 2: The TSA algorithm encodes the initial parameters of the DBN-GRU and calculates the value of the fitness function;
- Step 3: Using jet advancement and group behaviour, the DBN-GRU bias and weight value information is updated with the global optimal bias and weight values;
- Step 4: If the number of iterations satisfies the maximum number of iterations, output the bias and weight values and perform step (5), otherwise continue with step (3);
- Step 5: Decoding to obtain DBN-GRU bias and weight value training parameters;
- Step 6: Training to construct the TSA-DBN-GRU prediction model and analysing the prediction model using the test set.

B. Steps of the New Media Advertisement Traffic Prediction Process based on the Decomposition-Optimisation-Reconfiguration Framework

Combining VMD and KPCA, the TSA-DBN-GRU prediction method proposed in this paper is applied to the new media advertisement traffic prediction problem, and the flow chart is shown in Fig. 8, with the main steps:

- Step 1: Decompose the original new media advertisement flow time series by using Variable Modal Decomposition (VMD) to obtain $n+1$ components $\{VMF_1,\cdots,VMF_i,\cdots,VMF_k,Res_{vmd}\}$; use KPCA to perform principal component analysis and dimensionality reduction on the influencing variables of new media advertisement flow to obtain the transformed set of main influencing variables of new media advertisement flow;
- Step 2: For the eigenmode component VMF, GRU constructs the prediction model; for the main influencing variable of new media advertisement flow, DBN constructs the prediction model. In order to improve the accuracy of the prediction model, the TSA algorithm is used to optimise the bias and weight values of DBN-GRU, and select the optimal parameter values of bias and weight values;
- Step 3: Input each component and the influence factor data after dimensionality reduction into the component prediction model, and the output is superimposed and reconstructed to obtain the final prediction results.
- Step 4: Analyse the predictive model performance results.

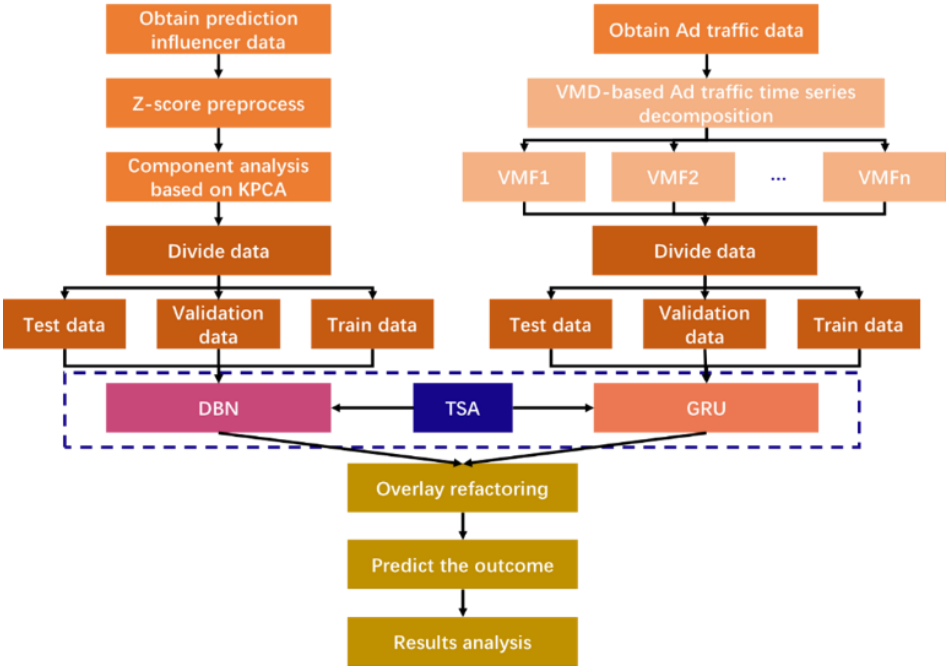


Fig. 8. New media advertisement traffic prediction.

V. Experiments and Analysis of Results

A. Algorithm Setup

The parameters of the new media advertising traffic prediction comparison algorithm are set in Table II.

B. Data Description

The data used in this paper comes from real data from a new media company's IPTV business. The data describes the number of viewing clicks of viewers 24 hours a day for almost three months. 70% of the data is selected as training set, 10% validation set and 20% as test set.

TABLE II. Parameter Settings of New Media Advertising Traffic Prediction Methods

Serial number	Arithmetic	Parameterisation
1	DBN-GRU	The number of DBN hidden nodes is 100, the number of GRU hidden nodes is 50, the activation function is the Relu function, and Adam's optimisation adjusts the weights
2	TSA-DBN-GRU	The number of DBN hidden nodes is 100, the number of GRU hidden nodes is 50, the activation function is Relu function and the number of TSA populations is 100
3	vmd-tsa-dbn-gru	The number of DBN hidden nodes is 100, the number of GRU hidden nodes is 50, the activation function is Relu function, the number of TSA populations is 100, and the VMD parameter settings refer to literature [30].
4	kpca-tsa-dbn-gru	The number of DBN hidden nodes is 100, the number of GRU hidden nodes is 50, the activation function is the Relu function, the number of TSA populations is 100, and the KPCA uses the Gaussian kernel function as the kernel function
5	vmd-kpca-tsa-dbn-gru	The number of DBN hidden layer nodes, the number of GRU hidden layer nodes, and the GRU network activation function is the Relu function

C. Correlation Analysis

In order to analyse the redundancy of the feature vectors of the new media advertising traffic prediction impact, this section uses Person correlation analysis method to analyse the feature vectors and advertising traffic. In Fig. 9, the new media advertising traffic is correlated with other variables, and all of them show positive correlation.

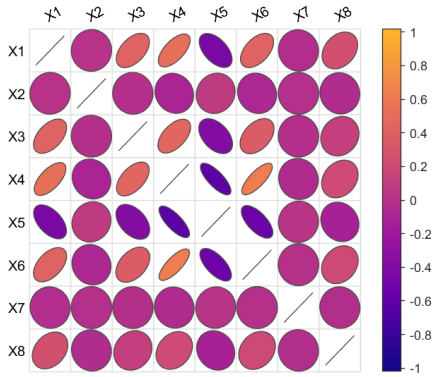
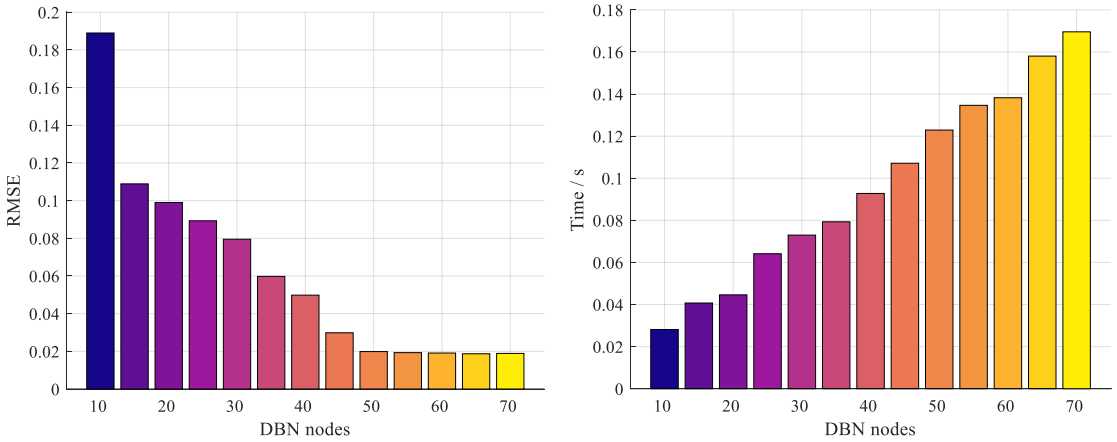


Fig. 9. Correlation analysis of factors influencing new media advertisement traffic prediction.

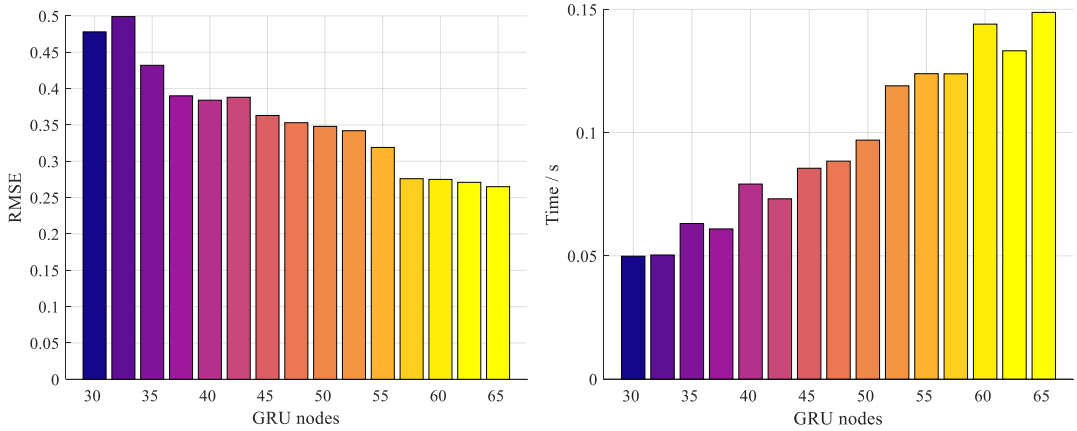
D. Parametric Analysis

In order to determine the optimal parameters, this paper analyses the results of choosing the parameters with higher prediction accuracy and less time-consuming by analysing different DBN hidden layer node number, GRU hidden layer node number, and population number conditions as shown in Fig. 10, 11, and 12. From Fig. 10, with the increase of the number of DBN hidden layer nodes, the prediction accuracy of the VMD-KPCA-TSA-DBN-GRU model increases, the time consumed increases, and the prediction accuracy tends to be stable when the number of DBN hidden layer nodes is 50; from Fig. 11, with the increase of the number of GRU hidden layer nodes, the prediction error of the VMD-KPCA-TSA-DBN-GRU model decreases, and the time consumed increases, and the prediction accuracy tends to be stable when the number of GRU hidden layer nodes is 60; from Fig. 12, the model prediction error decreases and the time-consuming time increases with the increase of the population. In summary, the VMD-KPCA-TSA-DBN-GRU model has a DBN hidden layer node number of 50, a GRU hidden layer node number of 60 and a population size of 80.



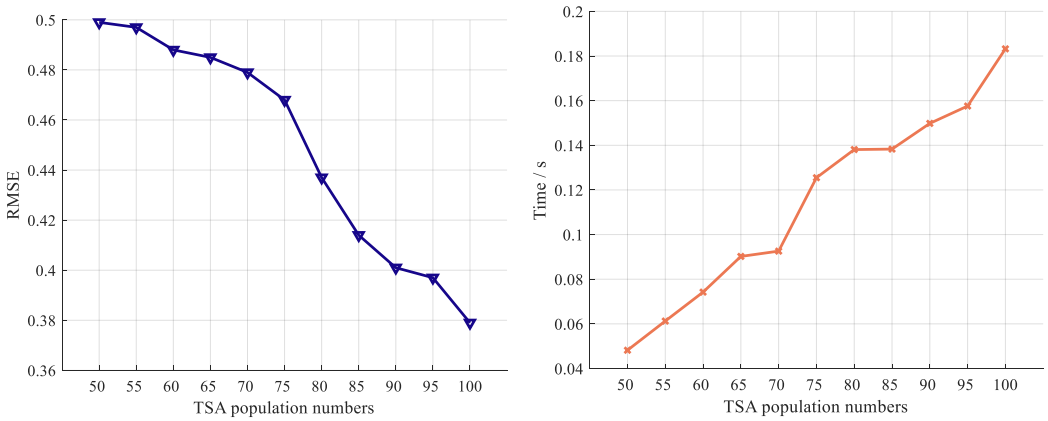
(a) Forecasting accuracy (b) Forecasting time

Fig. 10. Analysis of the impact of different number of DBN hidden layer nodes on prediction performance.



(a) Forecasting accuracy (b) Forecasting time

Fig. 11. Analysis of the impact of different number of GRU hidden layer nodes on the prediction performance.



(a) Forecasting accuracy (b) Forecasting time

Fig. 12. Analysis of the impact of different TSA population sizes on prediction performance.

E. Performance Analysis

1) Flow breakdown analysis: The result of decomposing the original new media advertisement traffic sequence using VMD decomposition algorithm is shown in Fig. 13. From Fig. 13, the detailed features of the new media advertisement traffic sequence data are better decomposed by using the VMD decomposition algorithm for decomposition.

2) Performance comparison: In order to verify the effectiveness and superiority of the new media advertising traffic prediction method based on the VMD-KPCA-TSA-DBN-GRU algorithm, VMD-KPCA-TSA-DBN-GRU is compared with four other models, and the prediction results of each model are shown in Fig. 14 and 15. The prediction results of different algorithms with relative error results are given in Fig. 14 and 15, respectively. The new media advertising traffic prediction based on the VMD-KPCA-TSA-DBN-GRU algorithm has the smallest error and the highest prediction accuracy, and the rest of the algorithms ranked as KPCA-TSA-DBN-GRU, VMD-TSA-DBN-GRU, TSA-DBN-GRU, and DBN-GRU, respectively.

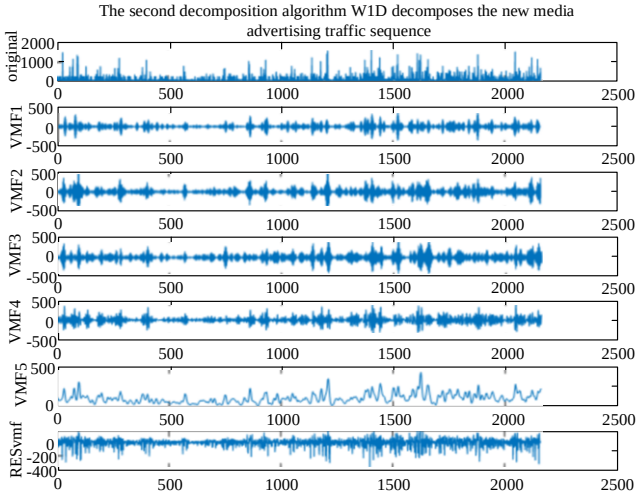


Fig. 13. Decomposition analysis of new media advertising traffic sequence.

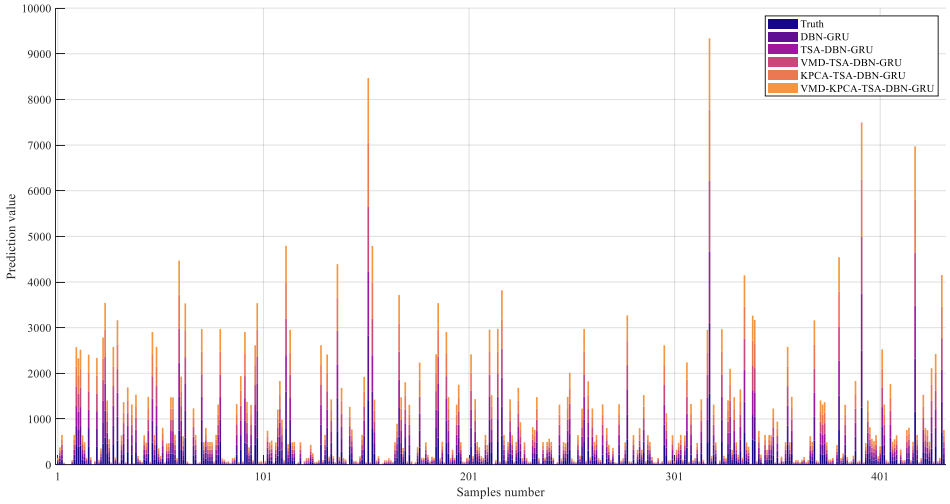


Fig. 14. Prediction results of different algorithms.

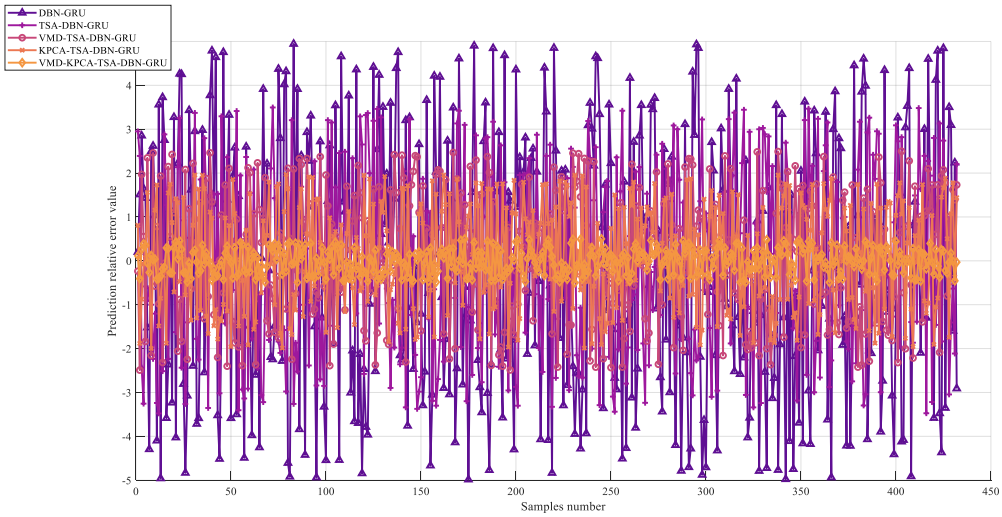


Fig. 15. Relative error results of different algorithms for prediction.

VI. Conclusion

In order to further improve the accuracy of new media advertisement traffic prediction, this paper proposes a new media advertisement traffic prediction method based on the optimisation of improved DBN-GRU network by the saccade swarm algorithm using the hybrid prediction framework of decomposition-optimisation-integration. The method analyses the new media advertisement traffic prediction problem, constructs a system of influence feature vectors, and adopts the nuclear principal component analysis method to analyse the principal components of the influence feature vectors; decomposes the original new media advertisement traffic time series using the variational modal decomposition method; and constructs a new media advertisement traffic prediction method by using the optimization of DBN-GRU network with the use of the quilt swarm algorithm. The specific conclusions are as follows:

- Kernel Principal Component Analysis (KPCA)-based methods were used to analyse the principal components of the eigenvectors of advertising traffic influence, and by comparing the prediction models that did not use KPCA, it was verified that KPCA analysis could improve the efficiency of the prediction models;
- The time series of new media advertisement flow is decomposed based on the VMD decomposition method, and by comparing the prediction model without the decomposition algorithm, it is verified that the VMD decomposition algorithm is able to improve the accuracy of the prediction model;
- The prediction accuracy of VMD-KPCA-TSA-DBN-GRU network prediction model is better than other models;
- The robustness of the prediction model proposed in this paper does not perform well, and further improving the VMD-KPCA-TSA-DBN-GRU prediction stability is the next research focus.

References

[1] Zhao J , Liu Z , Sun Q , Li Q, Jia X, Zhang R. Attention-based dynamic spatial-temporal graph convolutional networks for traffic speed forecasting[J]. Expert Systems with Application, 2022.

[2] Dangi R , Lalwani P .A novel hybrid deep learning approach for 5G network traffic control and forecasting[J].Concurrency and computation: practice and experience, 2023.

[3] Kish Z , Peters B , Nansen B , Gould H, Arnold M, Gibbs M. Media, mortality and necro-technologies: Eulogies for dead media:[J].New Media & Society,. 2023, 25(8):2163-2182.

[4] Lee M H , Nor M E ,Suhartono, Sadaei H J, Rahman N H A, Kamisan N A B. Fuzzy Time Series: an Application to Tourism Demand Forecasting[J].American journal of applied sciences, 2012, 9(1):132-140.

[5] Hechavarria A A , Shafiq M O .A modified attention mechanism powered by Bayesian Network for user activity analysis and prediction[J].Data & knowledge engineering, 2022.

[6] Gluhovsky I .Forecasting Click-Through Rates Based on Sponsored Search Advertiser Bids and Intermediate Variable Regression[J].Acm Transactions on Internet Technology, 2010, 10(3):1-28.

[7] Hands J , Coughlin T .New IEEE Media Sanitization Specification Enables Circular Economy for Storage[J].Computer, 2023.

[8] MAGNA. Global advertising market reaches new highs, surpasses pre-epidemic levels - MAGNA Global Advertising Forecast, December 2021 Edition[J]. China Advertising, 2022(2):6.

[9] Wang Z , Ding D , Liang X .TYRE: A dynamic graph model for traffic prediction[J].Expert Systems with Application, 2023.

[10] Fang W , Zhuo W , Yan J , Zhou T, Song Y, Qin J. Δfree-LSTM: An error distribution free deep learning for short-term traffic flow forecasting[J]. Neurocomputing, 2023.

[11] Zhang H , Kan S , Cao J , Chen L, Zhao T. A traffic flow-forecasting model based on multi-head spatio-temporal attention and adaptive graph convolutional networks[J].International Journal of Modern Physics, C. Physics and Computers, 2022.

[12] Ediger V, Akar S. ARIMA forecasting of primary energy demand by fuel in Turkey[J]. Energy Policy, 2007,35(3):1701-1708.

[13] Hamzaçebi C. Forecasting of Turkey's net electricity energy consumption on sectoral bases[J]. Energy Policy, 2007,35(3):2009-2016.

[14] Sareminia S. A Support Vector Based Hybrid Forecasting Model for Chaotic Time Series: Spare Part Consumption Prediction[J].Neural processing letters, 2023.

[15] Lee Y, Tong L. Forecasting time series using a methodology based on autoregressive integrated moving average and genetic programming[J]. Knowledge-Based Systems, 2011,24(1):66-72.

[16] Egrioglu E , Bas E .A new hybrid recurrent artificial neural network for time series forecasting[J].Neural computing & applications, 2023.

[17] Li Z , Ren Q , Chen L , Li J, Li X. Multi-scale convolutional networks for traffic forecasting with spatial-temporal attention[J].Pattern recognition letters, 2022.

[18] Zhiyu Lai,Xuhong Li. Analysing the development and trend of infomercials[J]. East China Science and Technology, 2022(3):81-83.

[19] Ma D , Zhu J , Song X B , Wang X. Traffic flow and speed forecasting through a Bayesian deep multi-linear relationship network[J].Expert Systems with Application, 2023.

[20] Weiguo Z , Yongqi S , Zhen Y L .A correlation information-based spatiotemporal network for traffic flow forecasting[J].Neural computing & applications, 2023, 35(28):21181-21199.

[21] Xue Xuan, Xiao Xianyong, Short-term electricity price prediction model based on empirical pattern decomposition and LSTM neural network[J]. Journal of Xi'an University of Technology, 2020, 36(1) :129-134.

[22] Ruili Ye, Zhizhong Guo, Ruiye Liu. Wind speed and wind power prediction for wind farms based on wavelet packet decomposition and improved Elman[J]. Journal of Electrotechnology, 2017, 32(21) :103-111.

[23] Cronin S .Trends: aaa forecasting hike in memorial day weekend traffic[J].Oil express, 2022(21):45.

[24] Yi X , Yun X , Jiawei Z , Chao C, Yao Z, Jie Z. Temporal super-resolution traffic flow forecasting via continuous-time network dynamics[J].Knowledge and information systems, 2023(11):65.

[25] Pascual H , Yee X C .Least squares regression principal component analysis: a supervised dimensionality reduction method[J].Numerical linear algebra with applications, 2022(1):29.

[26] Zhou L Z L .Fault feature extraction for rolling bearings based on parameter-adaptive variational mode decomposition and multi-point optimal minimum entropy deconvolution[J].Measurement, 2021, 173(1).

[27] Kaur S,Awasthi L K,Sangal A L,et al.Tunicate swarm algorithm:a new bio-inspired based metaheuristic paradigm for global optimisation[J]. Engineering Applications of Artificial Intelligence, 2020,90:103541.

[28] Sun J , Wang L , Razmjooy N .Anterior cruciate ligament tear detection based on deep belief networks and improved honey badger algorithm[J].Biomed. Signal Process. control. 2023, 84:105019.

[29] FANG Na, LI Junxiao, CHEN Hao, YU Junjie. Short-term power load forecasting based on CNN-GRU-MLR with multi-frequency combination[J]. Computer Simulation, 2023, 40(1):118-124.

[30] PU Wei, YANG Yiqiang, ZHANG Yuanbo, FU Jiangtao, SONG Hong. Power load combination forecasting model based on NGO-VMD-FCBF-Informer[J]. Intelligent Computers and Applications, 2023(011):013.

Applying Data-Driven APO Algorithms for Formative Assessment in English Language Teaching

Guojun Zhou*
Nanyang Medical College, Nanyang 473004, Henan, China

***Abstract*—This study proposes an innovative approach for improving the accuracy and efficiency of formative assessment in English language teaching. The method integrates the Artificial Protozoa Optimization (APO) algorithm with the Kernel Extreme Learning Machine (KELM) to overcome limitations such as local optima in traditional models. The study utilizes data from five university-level English courses, consisting of 327 samples divided into a training set (70%), validation set (15%), and test set (15%). The APO-KELM model is constructed by optimizing the KELM parameters using the APO algorithm. Comparative analysis is conducted against other models, including ELM, KELM, WOA-KELM, PPE-KELM, and AOA-KELM, in terms of accuracy (RMSE), MAPE (Mean Absolute Percentage Error), and convergence speed. The result shows that the APO-KELM model demonstrates superior performance with a Root Mean Square Error (RMSE) of 0.6204, compared to KELM (0.7210), WOA-KELM (0.6934), PPE-KELM (0.6762), and AOA-KELM (0.6451). In terms of MAPE, APO-KELM achieves 0.48, outperforming KELM (0.55), WOA-KELM (0.52), PPE-KELM (0.51), and AOA-KELM (0.49). Additionally, the APO-KELM model converged within 300 iterations, showing faster convergence compared to other models. The integration of the APO algorithm with the KELM significantly enhances the accuracy and efficiency of formative assessment in English language teaching. The APO-KELM model is more accurate and faster than traditional models, making it a valuable tool for improving assessment systems. Future research should focus on refining the APO algorithm for broader applications in educational assessments.**

Keywords*—Big data technology; APO algorithm; formative assessment in English language teaching; nuclear limit learning machine

I. INTRODUCTION

The implementation of education evaluation reform in China is increasingly gaining support from scholars and frontline teachers. This reform aims to achieve a comprehensive integration and effective connection between teaching evaluation and disciplinary parenting. It also seeks to establish a teaching evaluation index system that promotes students' physical and mental well-being, as well as their all-round development [1]. The development of a rigorous and efficient teaching evaluation index system is essential for conducting high-quality teaching evaluations. Additionally, the establishment of a comprehensive and systematic English teaching evaluation model not only facilitates the improvement of teaching evaluation practices and enhances disciplinary education outcomes, but also aligns with the contemporary goal of fostering moral values and educating individuals in the new era [2]. The use of big data technology to extract crucial information for the development of assessment methodologies has emerged as a future trend in teaching evaluation, owing to the growing volume of data generated by students and instructors throughout the teaching and learning process [3].

Currently, the study on formative assessment of English teaching using big data technology focuses mostly on two areas: the development of a teaching evaluation system and the creation of a teaching evaluation model. The objective of studying the English teaching evaluation system is to create an index system by analyzing the English teaching process, identifying the elements that influence the quality of teaching, and using appropriate algorithms to determine the final evaluation indexes [4]. Huang [5] develops teaching evaluation criteria based on the principles of effectiveness, differentiation, acceptability, and practicality. Assia and Samira [6] identify primary criteria from five aspects, including teachers, students, teaching content, teaching resources, and teaching media, to establish an English teaching evaluation system. Khodamoradi et al [7] divide the evaluation criteria for cultural teaching in senior high school English classrooms and constructs dimensions for the framework of the evaluation system. Chen and Yi [8] construct an evaluation system for secondary school English classrooms by examining and analyzing teaching plans, teaching methods, teaching attitudes, and classroom performance. The study on English teaching evaluation model mostly uses data-driven algorithms to develop the mapping link between English teaching evaluation indicators and evaluation scores [9]. The primary approaches used for teaching assessment include comprehensive fuzzy analysis [10], random forest [11], decision tree [12], extreme learning machine [13], neural network [14], and other similar techniques. The literature presents various approaches for evaluating English teaching. One study [10] suggests using an integrated fuzzy logic method, while another [11] utilizes random forest to establish the relationship between evaluation values and factors. Additionally, a high school English evaluation model is proposed [13], which is based on the extreme learning machine and tested using different datasets. Lastly, Shehu and Henay [14] propose a college English teaching evaluation model using a neural network. As the amount of data and the complexity of evaluation indexes increase, traditional machine learning algorithms may get stuck in local optima and fail to find the optimal evaluation model. To address this issue, intelligent optimization algorithms are employed to enhance the training process and improve the accuracy of the evaluation model. Furthermore, the English evaluation process lacks depth, resulting in an incomplete evaluation system and reduced efficiency. To overcome this

*Corresponding Author.

limitation, a more comprehensive evaluation system is utilized to enhance the accuracy of the evaluation model [15].

This paper addresses the limitations of the current English teaching evaluation method, which uses the Extreme Learning Machine algorithm [13]. These limitations include getting stuck in local optimal solutions, low evaluation accuracy, and time-consuming evaluations. To overcome these challenges, the paper proposes a formative assessment method for English teaching based on the APO-KELM model, which combines the Intelligent Optimization Algorithm with the Nuclear Extreme Learning Machine [16]. The primary contributions of this paper include: (1) analyzing the issue of formative assessment in English teaching using big data, and identifying comprehensive, scientific, effective, and quantifiable evaluation criteria for English teaching; (2) integrating the Artificial Protozoan Optimizer algorithm and the Kernel-Limit Learning Machine to develop a formative assessment approach based on an efficient data-driven algorithm for English teaching; (3) validating the effectiveness and robustness of the proposed method by utilizing formative data from English teaching in various colleges and universities.

II. Analysis of Formative Assessment Issues

A. Research Ideas on Formative Assessment in English Teaching

This work utilizes the research approach of problem identification, problem analysis, solution proposal, solution implementation, and solution validation [17] to investigate the issue of formative assessment in English education. The particular research concept is shown in Fig. 1.

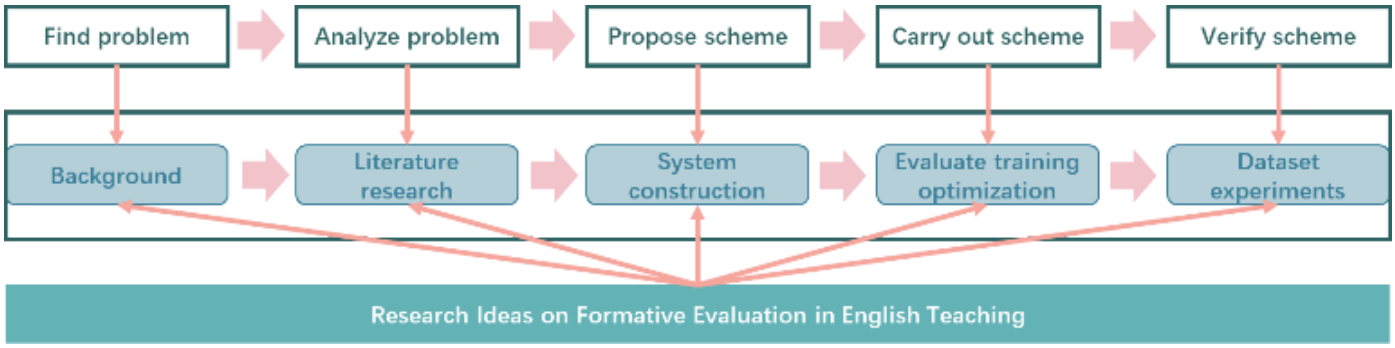


Fig. 1. Schematic diagram of the research idea.

The research ideas of this paper, as shown in Fig. 1, are as follows: 1) Identify the problem of formative assessment in English teaching by examining the background of formative assessment in English teaching; 2) Analyze the formative process of English teaching and identify the formative assessment indicators through literature research; 3) Develop the formative assessment indicator system for English teaching using data preprocessing and correlation analysis, while also proposing 4) Constructing a formative assessment model for English teaching by combining various machine learning algorithms and optimizing training for formative assessment of English teaching; 5) Validate the effectiveness and reliability of the proposed evaluation method using different datasets and data extraction methods.

Based on the analysis provided above, this paper conducts research on the problem of formative assessment in English teaching. The research includes the discovery and analysis of the problem, the establishment of an index system for formative assessment, the construction of a formative assessment model for English teaching, and the validation of the model's application. The specific key technologies are illustrated in Fig. 2.

B. Analysis of the Problem

The teaching evaluation issue revolves on the teaching evaluation index system, which involves examining and extracting the value of teaching evaluation indices. Machine learning techniques are then used to establish the mapping relationship between the index value and the evaluation value [18]. The issue of formative assessment in English teaching involves determining the teaching process by examining relevant literature, conducting analysis, and integrating the English curriculum, student development requirements, and English teaching evaluation practices. This process leads to the extraction of a formative assessment index system for English teaching. Furthermore, a data-driven algorithm is employed to construct a formative assessment model for English teaching. The specific problem analysis is illustrated in Fig. 3.

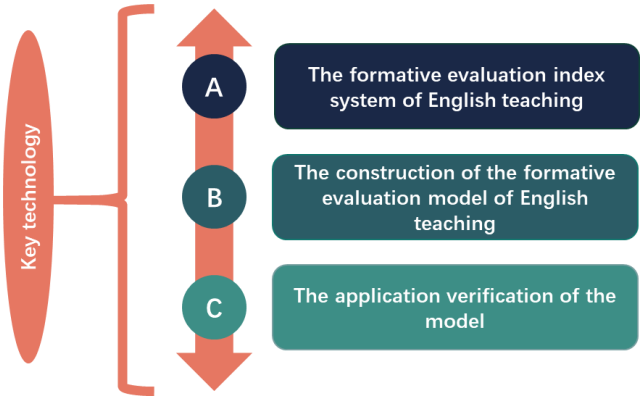


Fig. 2. Key technology content.

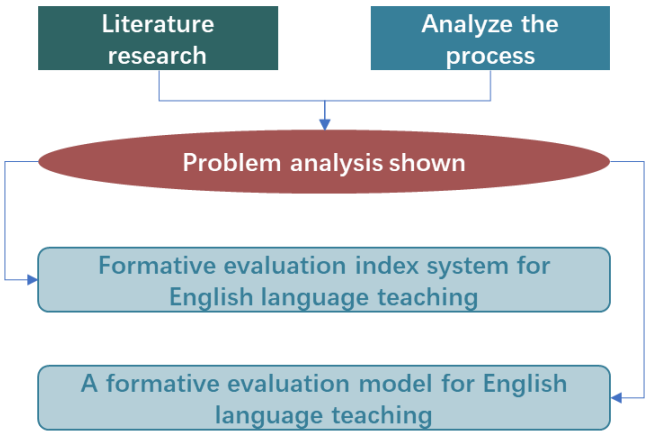


Fig. 3. Schematic diagram of the problem analysis.

C. Evaluation System Construction

The formative assessment problems in English teaching were analyzed to develop students' comprehensive language application ability. The focus was on the leading role of students' teaching evaluation and the diversity of evaluation methods and system construction. The teaching objectives, contents, methods, and effects were set as the first-level indicators, following the principles of human nature, scientific approach, developmental approach, systematic approach, and operability. The formative indicator system of English teaching was obtained through the use of the Delphi method questionnaire survey, deletion, and adjustment [19], as shown in Table I.

D. Analysis of Evaluation Models

The essence of the formative assessment problem of English teaching is a complex regression prediction problem, with the index value in the formative index system of English teaching as the input and the evaluation score as the output, the specific evaluation model is constructed as follows:

$$Y_{score} = F_{eval}\left(X_{index}\right) \quad (1)$$

Where Y_{score} is the evaluation score; F_{eval} is the evaluation model; X_{index} is the index value. In this paper, a data-driven algorithm is used to construct the formative assessment model of English teaching, as shown in Fig. 4.

TABLE I. EVALUATION INDICATOR SYSTEM

No.	Data set	Goal
1	A Teaching and Learning Objectives	A1 Developing students' language skills
		A2 Expanding Students' Cultural Awareness
		A3 Developing the quality of students' thinking
		A4 Improving Student Learning
2	B Teaching content	B1 English Language Knowledge
		B2 English Language Skills
		B3 Knowledge of English Culture
		B4 English Learning Strategies
3	C Teaching methods	C1 Inquiry-based teaching
		C2 Contextualised Teaching
		C3 Thematised Teaching
4	D Teaching Effectiveness	D1 Teaching effectiveness of teachers
		D2 Student Learning Outcomes

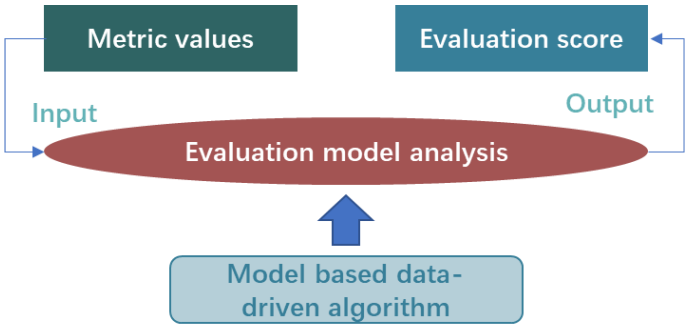


Fig. 4. Evaluation model analysis.

III. APO-KELM ALGORITHM

In order to solve the problem of formative assessment in English language teaching, this section uses the artificial protozoan optimiser algorithm to improve the kernel-limit learning machine for the construction of formative assessment model in English language teaching.

A. APO Algorithm

1) Principle of APO algorithm: Swarm intelligence optimization system Artificial Protozoa Optimizer (APO) [20] is inspired by natural phenomena. The method introduces a new Artificial Protozoa Optimizer (APO) that is inspired by protozoa. APO imitates the foraging, quiescent, and reproductive behaviors of protozoa in order to replicate their survival strategies. From a practical perspective, the method is employed to resolve five common engineering design challenges in continuous environments with constraints. Moreover, the method is employed to perform multilevel picture segmentation in a discrete space while adhering to specific constraints.

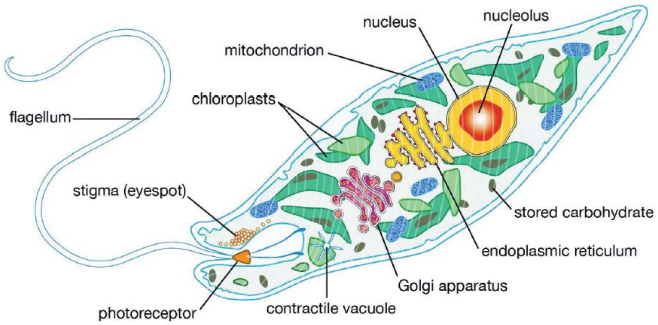


Fig. 5. Representation of protozoan behaviour.

Microorganisms have a unique advantage, as evidenced by research on a variety of biological processes. As microorganisms, bacteria, algae, and protozoa execute functions that are comparable to those of organelles in higher plants and animals. Specialized structures known as "organelles" execute these functions. Metabolism, reproduction, genetic continuity, adaptability to environmental stimuli, and variability are fundamental life features of microorganisms. Because of their simple and low-complexity structure, microbial beings are often more successful than larger organisms. Researching the principles of behavioral processes such as reproduction, dormancy, and foraging, the APO algorithm is employed. Fig. 5 shows representation of protozoan behavior.

a) Foraging

i) Self-supporting model: By generating carbohydrates via their chloroplasts, protozoa may provide nourishment. The protozoan will migrate away from its current location and towards a specific spot if it is subjected to extreme light intensity. When the light intensity around the protozoan is low, the protozoan relocates to a different position (Fig. 7). The autotrophic model may be described by the following particular model:

$$X_i^{new} = X_i + f \cdot \left(X_j - X_i + \frac{1}{np} \cdot \sum_{k=1}^{np} \omega_a \cdot \left(X_{k-} - X_{k+} \right) \right) \square\ M_f \tag{2}$$

$$X_i = \left[x_i^1, x_i^2, \cdots, x_i^{\dim} \right]$$
$$X_i = sort\left(X_i \right) \tag{3}$$

$$f = rand \cdot \left(1 + \cos\left(\frac{iter}{iter_{\max}} \cdot \pi \right) \right) \tag{4}$$

$$np_{\max} = \left\lfloor \frac{ps-1}{2} \right\rfloor \tag{5}$$

$$\omega_a = e^{-\left| \frac{f(X_{k-})}{f(X_{k+}) + eps} \right|} \tag{6}$$

$$M_f\left[di \right] = \begin{cases} 1 & randperm\left(\dim, \left\lceil \dim \cdot \frac{i}{ps} \right\rceil \right) \\ 0 & otherwise \end{cases} \tag{7}$$

where X_i^{new} denotes the updated protozoan position; X_i denotes the current protozoan position; X_{k-} denotes the randomly selected neighbourhood-1 protozoan; X_{k+} denotes the randomly selected neighbourhood+1 protozoan; f denotes the foraging factor; np denotes the individual of the neighbourhood pairs; $x_i^{\dim}$ denotes the dimensional position of the ith protozoan; $iter$ denotes the number of iterations; $iter_{\max}$ denotes the maximum number of iterations; ps denotes the population size; $f(\cdot)$ denotes the formula for calculating the fitness value; eps denotes the minimal value, which is generally taken as 2.2204e16; denotes the dimension index; denotes the fitness value; and denotes the mapping vector. The general value is 2.2204e-16; M_f is the mapping vector; di is the dimension index (see Fig. 6).

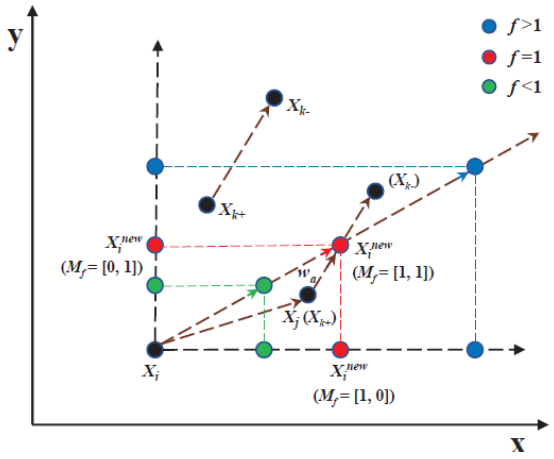


Fig. 6. Self-supporting model.

ii) Heterotrophic model: Protozoa are able to acquire nourishment by absorbing organic substances from their environment while under darkness. If X is a nearby location with abundant food, protozoa will travel towards it. The precise model of the heterotrophic model is as follows:

$$X_i^{new} = X_i + f \cdot \left(X_{near} - X_i + \frac{1}{np} \cdot \sum_{k=1}^{np} \omega_h \cdot \left(X_{i-k} - X_{i+k} \right) \right) \square\ M_f \tag{8}$$

$$X_{near} = \left(1 \pm Rand \cdot \left(1 - \frac{iter}{iter_{\max}} \right) \right) \square\ X_i \tag{9}$$

$$\omega_h = e^{-\left| \frac{f(X_{i-k})}{f(X_{i+k}) + eps} \right|} \tag{10}$$

$$Rand = [rand_1, rand_2, \cdots, rand_{\dim}] \quad (11)$$

where X_{near} denotes the neighbourhood position; X_{i-k} and X_{i+k} are the i-kth and i+kth neighbourhood positions, respectively; ω_h is the weight of the heterotrophic pattern; and $Rand$ is a random vector.

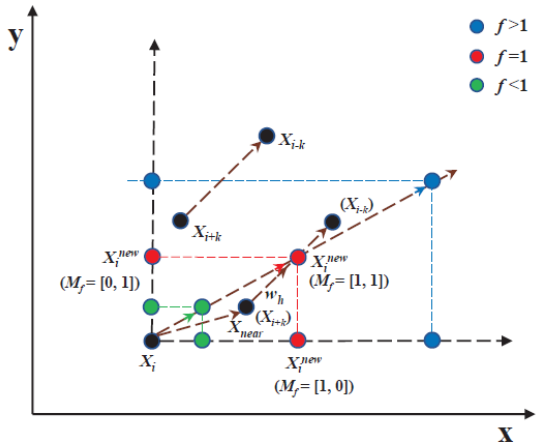


Fig. 7. Self-supporting model.

b) Dormancy: Every element of a single solution vector is multiplied by a random value selected from a Gaussian distribution to create a new offspring. The Gaussian random variable influences the number of interruptions introduced to the parent vector, aiding the algorithm in eliminating local optima. The offspring produced by the Gaussian variation at generation *m* is defined for every parent solution vector:

$$X_i^{new} = X_{\min} + Rand \square \left(X_{\max} - X_{\min}\right) \quad (12)$$

$$\begin{aligned} X_{\min} &= [lb_1, lb_2, \cdots, lb_{\dim}] \\ X_{\max} &= [ub_1, ub_2, \cdots, ub_{\dim}] \end{aligned} \quad (13)$$

where $X_{\min}$ and $X_{\max}$ denote the lower and upper bound vectors, respectively, and lb and ub denote the lower and upper bound variables, respectively (Fig. 8).

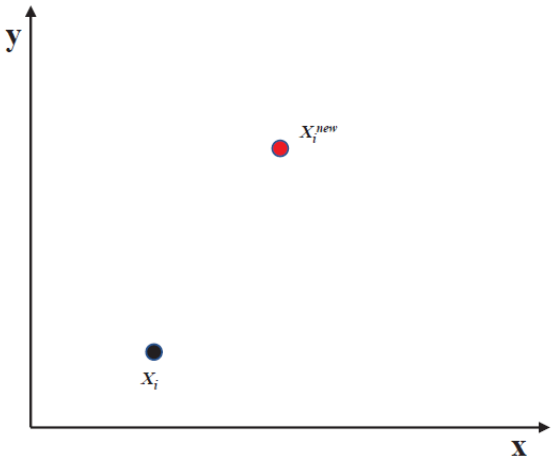


Fig. 8. Diagram of hibernation.

c) Reproduction: Protozoa are capable of asexual reproduction when they reach the appropriate age and are in good condition. In theory, this process of reproduction results in the protozoan dividing into two identical progeny. This behavior is simulated by creating a duplicate protozoan and analyzing a perturbation. The mathematical representation of reproduction is as follows:

$$X_i^{new} = X_i \pm rand \cdot \left(X_{\min} + Rand \square \left(X_{\max} - X_{\min}\right)\right) \square M_r \quad (14)$$

$$M_r[di] = \begin{cases} 1 & randperm\left(\dim, \lceil \dim \cdot rand \rceil\right) \\ 0 & otherwise \end{cases} \quad (15)$$

where $\pm$ denotes interference forward or backward, and M_r denotes reproduction mapping relationships (see Fig. 9).

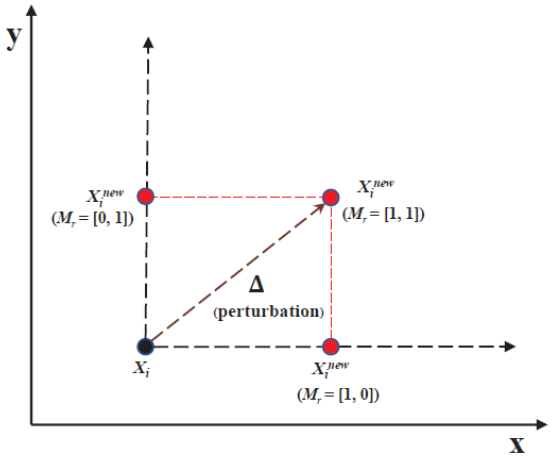


Fig. 9. Diagram of reproduction.

d) Other parameter settings: The other parameters of the APO algorithm are set as follows:

$$pf = pf_{\max} \cdot rand \quad (16)$$

$$p_{ah} = \frac{1}{2} \cdot \left(1 + \cos\left(\frac{iter}{iter_{\max}} \cdot \pi \right) \right) \quad (17)$$

$$p_{dr} = \frac{1}{2} \cdot \left(1 + \cos\left(\left(1 - \frac{i}{ps} \right) \cdot \pi \right) \right) \quad (18)$$

Where pf denotes the dormancy ratio parameter, $pf_{\max}$ is the maximum ratio parameter, p_{ah} is the conversion probability between autotrophic and heterotrophic modes, and p_{dr} is the conversion probability between dormancy and reproduction. The conversion probability is mainly used to balance the conversion of exploration and exploitation operators, as shown in Fig. 10.

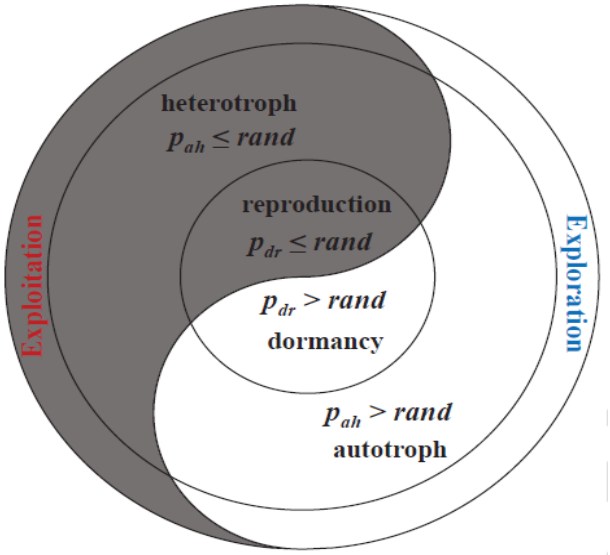


Fig. 10. Schematic diagram of the behavioural transition between development and exploration.

2) APO algorithm pseudo-code: According to the optimisation strategy of APO algorithm, the pseudo-code of APO algorithm is shown in Table II.

TABLE II. APO ALGORITHM PSEUDO-CODE

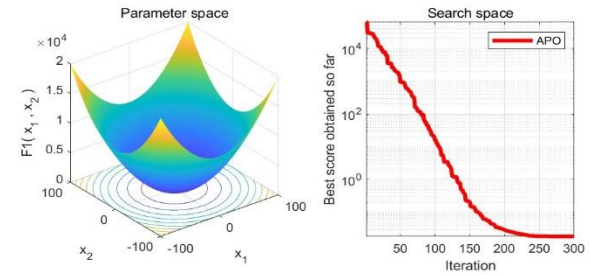
Algorithm 1: Artificial Protozoa Optimisation Algorithm (APO)
Initialise the parameters ps, dim, np, pfmax and MaxFEs;
Protozoan populations were randomly generated and fitness values were calculated;
While FEs<MaxFEs
Sort(Xi), calculating the scaling parameter, calculating the conversion probability
For i=1:ps do
If i in Drindex do
Individual positions are updated using either the dormant behaviour operator or the reproduction behaviour operator;
Else
Individual positions were updated using either the autotrophic behaviour operator or the heterotrophic behaviour operator;
End if
Calculate fitness values and compare updated populations;
End for
Output optimal protozoan individuals;
FEs = FEs + ps;
End while

3) Performance analysis of APO algorithm optimisation: In order to verify the convergence of the APO algorithm, this paper chooses F1-F8 test functions (see Table III) [21] to analyse the performance of APO, and the specific results are shown in Fig. 11.

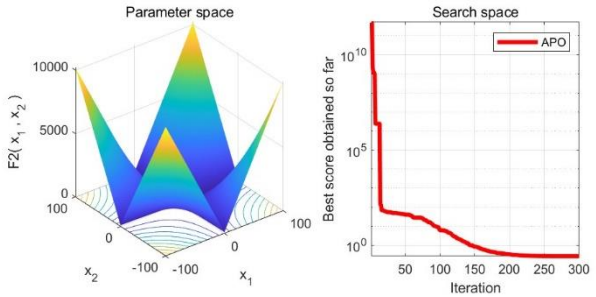
TABLE III. TEST FUNCTION SETTINGS

serial number	name (of a thing)	n	realm
1	F1	30	[-100,100]
2	F2	30	[-10,10]
3	F3	30	[-100,100]
4	F4	30	[-100,100]
5	F5	30	[-30,30]
6	F6	30	[-100,100]
7	F7	30	[-1.28,1.28]
8	F8	30	[-500,500]

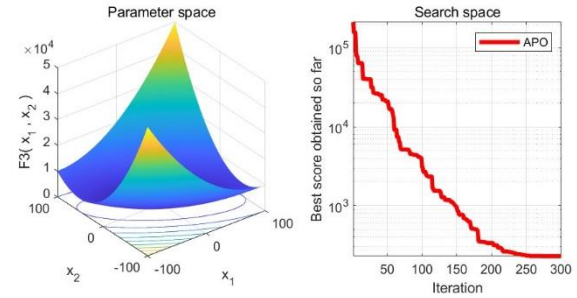
As can be seen from Fig. 11, the APO algorithm can converge to a certain accuracy and achieve a better optimal solution in the F1 to F8 function tests.



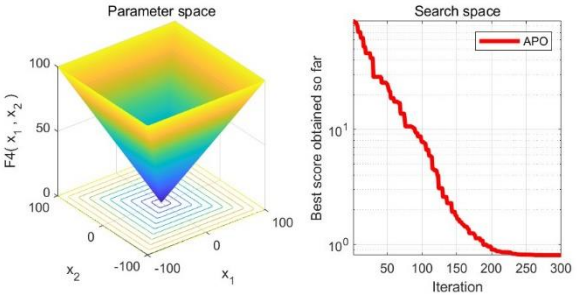
(a) F1



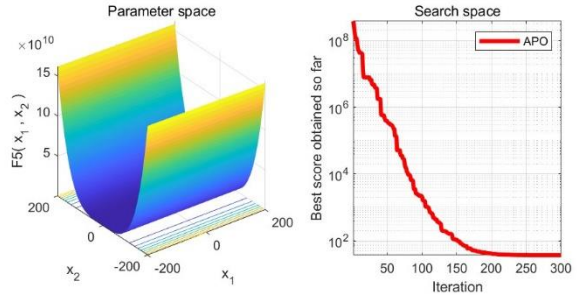
(b) F2



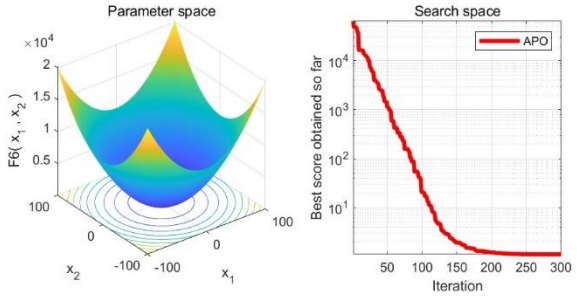
(c) F3



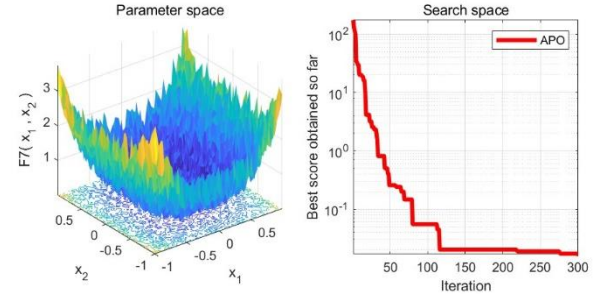
(d) F4



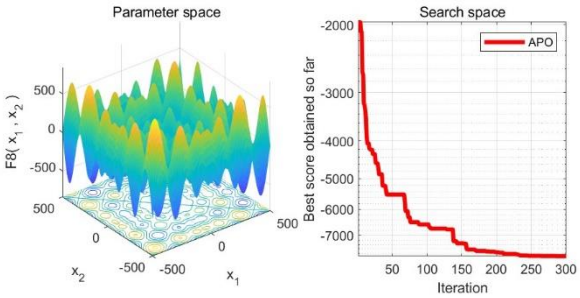
(e) F5



(f) F6



(g) F7



(h) F8

Fig. 11. APO optimisation performance test results.

B. The KELM Model

Kernel Based Extreme Learning Machine (KELM) [22] is an extreme learning machine algorithm based on kernel functions, which achieves high-dimensional mapping of data through kernel functions, thus improving the performance of the model.KELM has better stability and generalisation capabilities when dealing with classification and regression problems compared to traditional Support Vector Machines (SVMs) and Extreme Learning Machines (ELMs) [23], which usually have better stability and generalisation capabilities. A key advantage of KELM is that it can directly handle multi-class classification problems and usually does not require complex weight adjustments as in traditional neural networks (see Fig. 12).

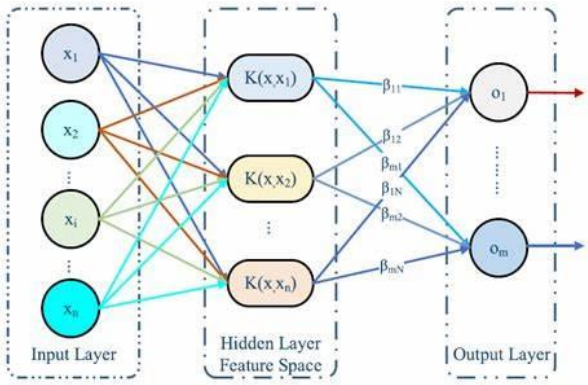


Fig. 12. KELM structure.

The KELM model is calculated as follows:

$$F(X)=\left[K(X,X_1);\cdots;K(X,X_n)\right]\left(\frac{I}{C}+\Omega_{ELM}\right)^{-1}L \tag{19}$$

Where, $(X_1, X_2, \cdots, X_n)$ is the given training sample, n is the number of samples, K is the kernel function, Ω_{ELM} is the kernel matrix and $F(X)$ is the learning objective function.

The steps of KELM are shown in Fig. 13 and described below:

- Determine the number of neurons in the hidden layer, randomly set the connection weights between the input layer and the hidden layer w and the bias of the hidden layer neurons b ;

- Choose an infinitely differentiable function as the activation function of the neurons in the hidden layer, and then calculate the hidden layer output matrix H ;
- Calculate the output layer weights.

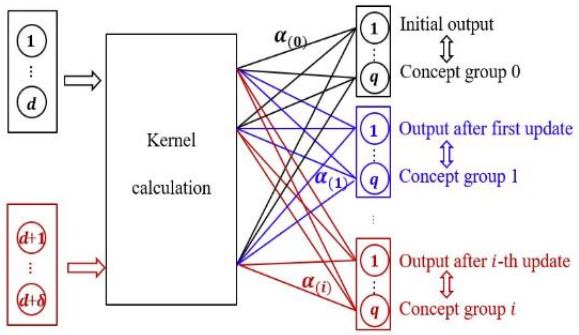


Fig. 13. KELM learning training steps.

The KELM model is mainly applied in the fields of data regression prediction, fault early warning, online data prediction, feature selection and parameter tuning, dealing with nonlinear and non-smooth data, and time series analysis [24], and the application schematic is shown in Fig. 14.

Fig. 14. KELM application.

C. APO-KELM Structural Steps

This paper utilizes the APO algorithm to optimize the parameters of the Kernel Extreme Learning Machine (KELM) model for constructing the formative assessment model of English language teaching. The objective is to enhance the evaluation accuracy and generalization of KELM. The specific optimization schematic can be seen in Fig.15. The APO method divides the decision variables into two parts [25] (Fig. 15): the first part consists of the weights and bias, and the second portion consists of the parameters of the activation function. The APO algorithm uses the RMSE function as the fitness function. Fig.16 displays the structure of the APO-KELM model, while Table IV presents the pseudo code.

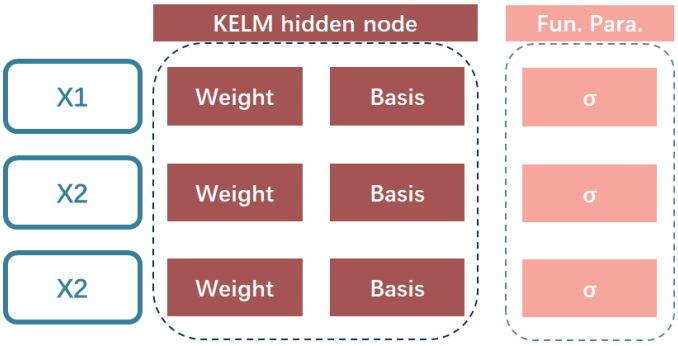


Fig. 15. Schematic diagram of APO-KELM optimisation variables.

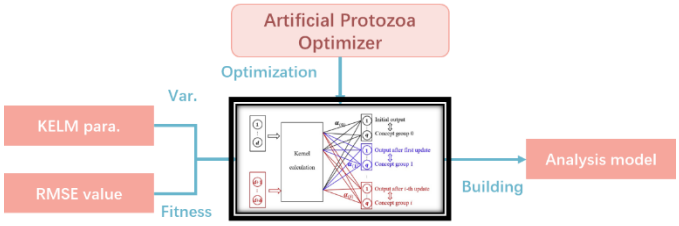


Fig. 16. Schematic diagram of APO-KELM structure.

TABLE IV. APO-KELM ALGORITHM PSEUDO-CODE

Algorithm 2: APO-KELM algorithm pseudo-code
Initialisation of the APO algorithm parameters, using real number encoding for the KELM model decision optimisation variables;
The RMSE was calculated as the fitness value to update the optimal KELM model parameters;
Whether the While iteration condition is satisfied
Behavioural stage transition probabilities were calculated and populations were updated using autotrophic, heterotrophic, dormant or reproducing behavioural operators;
Calculate the fitness value;
Updating Optimal KELM Network Parameters Individual;
End while
Output optimal KELM network parameters;
Construction of the APO-KELM evaluation model.

IV. MODEL APPLICATION

In this paper, the APO-KELM model is applied to the problem of formative assessment of English teaching, which mainly solves the problem of constructing the formative assessment model of English teaching, i.e., the APO-KELM model is used to learn to optimise the mapping relationship between the values of the formative assessment indexes and the evaluation scores of English teaching, so as to obtain the formative assessment model of English teaching based on the APO-KELM algorithm, and the method of its application is shown in Fig. 17, and the specific steps are shown in Table V.

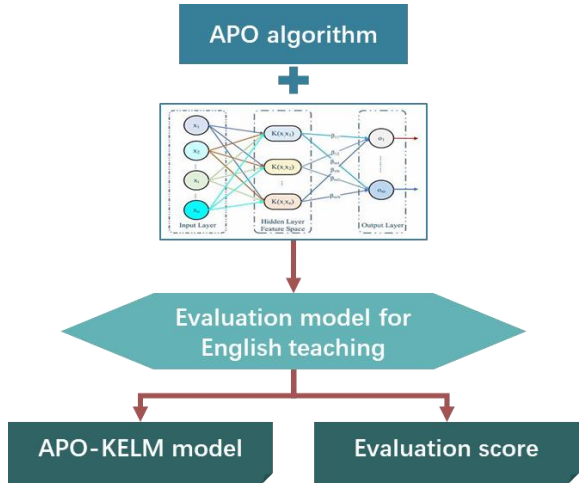


Fig. 17. APO-KELM applied in the formative assessment model of English language teaching.

TABLE V. APO-KELM ALGORITHM PSEUDO-CODE

Algorithm 3: Formative assessment Model Construction for English Language Teaching Based on APO-KELM Algorithm
Analysing evaluation problems in English language teaching and designing evaluation programmes;
Describe the process of English teaching, extract the evaluation indexes and construct the evaluation index system;
Data preprocessing and correlation analysis to construct a learning training set for formative assessment model of English language teaching;
Initialise the APO-KELM model;
The KELM model parameters were optimised iteratively using the APO algorithm optimisation strategy;
Obtain optimal KELM model parameters;
The APO-KELM model was retrained using the training set to obtain a formative assessment model for English language teaching;
Data validation analysis of the model.

V. VALIDATION ANALYSIS

A. Experimental Setup

1) Data setting: The research in this paper investigated five university English classes for questionnaires and obtained relevant data, which were divided into training set, validation set, and test set (as shown in Fig. 18), in which the ratio was 7:1.5:1.5, and the total number of sample sets was 327 groups, and only then did the questionnaire data were analysed with the SPSS 22.0 statistical software to obtain the final standardised data.

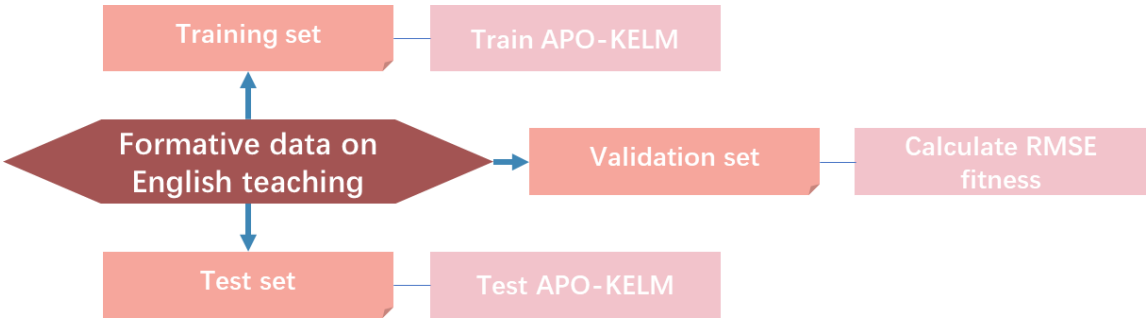


Fig. 18. Purpose of data set segmentation.

2) Algorithm parameter setting: In order to verify the superiority of comparing APO-KELM algorithms, ELM, KELM, WOA-KELM [26], PPE-KELM [27], and AOA-KELM [28] are used in this paper, and the specific parameter settings of each algorithm are shown in Table VI.

TABLE VI. COMPARISON ALGORITHM PARAMETER SETTINGS

No.	Arithmetic	Parameter settings	ELM/KELM Parameter Setting
1	ELM	No	The number of hidden layer nodes is 80
2	KELM	No	Hidden_node=80, kernel function is radial basis function
3	WOA-KELM	a=[2,0]	Refer to section 5.2 Analysis
4	PPE-KELM	a=1.1, c=0.2	Same settings as WOA-KELM
5	AOA-KELM	a=5, μ=0.5	Same settings as AOA-KELM
6	APO-KELM	np=1, pfmax=0.1	Refer to section 5.2 Analysis

3) Environmental settings: The simulation experiments in this paper are mainly executed on a laptop computer configured with Windows 11 operating system having 16GB RAM with Intel(R) Core(TM) i7-8750H CPU @2.20GHz 2.21GHz.The execution of each algorithm is analysed using Matlab2021a.

B. Analysis of Results

1) Parametric analysis: The CEC2022 standard function is used to analyze the size change of the APO algorithm's foraging factor in order to examine the influence of the foraging behavior factor with the number of iterations. The precise findings are shown in Fig. 19. The foraging factor diminishes as the number of iterations increases, causing the APO algorithm to choose exploration over exploitation.

This work examines the English evaluation accuracy under the APO algorithm population of 40, 50, 60, 70, 80, 90, 100, 110, 120, and 130 in order to investigate the effect of APO algorithm population on the evaluation performance of APO-KELM model. The precise findings are shown in Fig. 20.

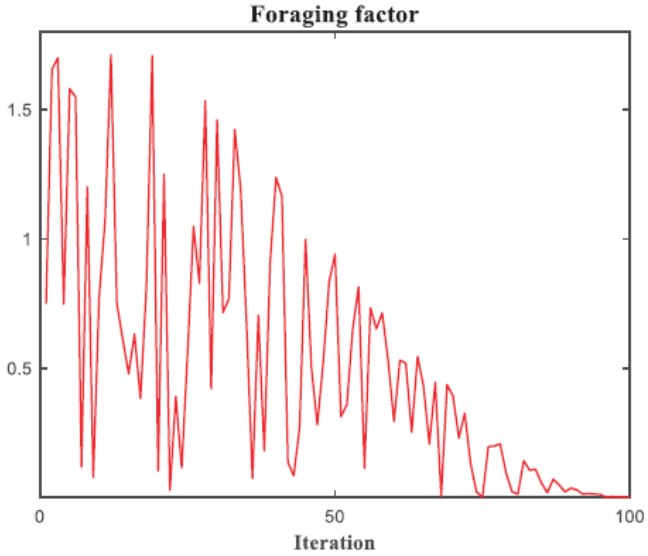


Fig. 19. Results of APO algorithm foraging factor change with increasing number of iterations.

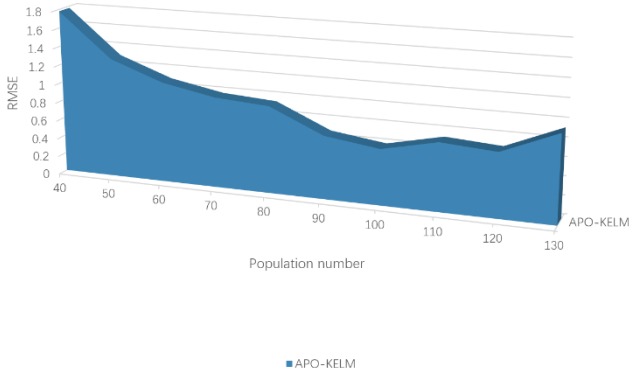


Fig. 20. Results of the effect of the number of populations of the APO algorithm on the performance of the APO-KELM model.

In order to explore the impact of the number of hidden layer nodes of KELM algorithm on the evaluation performance of APO-KELM model, this paper analyses the evaluation accuracy of English under the number of hidden layer nodes of KELM algorithm of 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, and 150, and the specific results are shown in Fig. 21.

2) Comparative algorithm analysis: This study utilizes ELM, KELM, WOA-KELM, PPE-KELM, AOA-KELM, and APO-KELM to develop the formative assessment model for English instruction. The performance results of these algorithms are compared and shown in Fig. 22 and Fig. 23.

Fig. 22 displays the convergence outcomes of WOA-KELM, PPE-KELM, AOA-KELM, and APO-KELM in ELT formative data. Fig. 22 shows that as the number of iterations increases, the WOA-KELM, PPE-KELM, AOA-KELM, and APO-KELM models converge with a decrease in fitness value. In terms of convergence accuracy, the KELM model based on the APO algorithm has the lowest convergence fitness value. In terms of convergence speed, APO-KELM converges the fastest, starting to converge within the first 300 iterations.

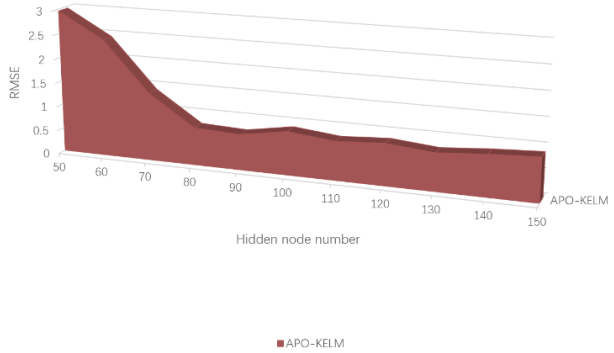


Fig. 21. Results of the effect of the number of KELM hidden layer nodes on the performance of the APO-KELM model.

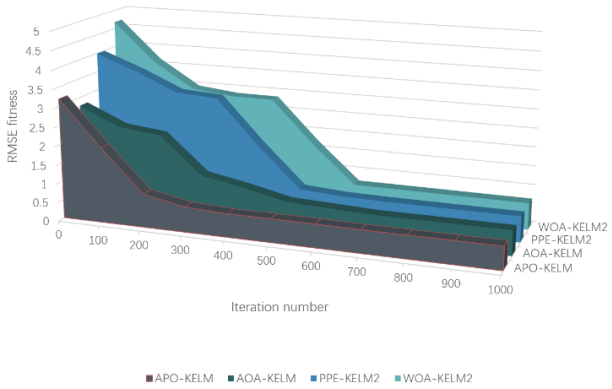
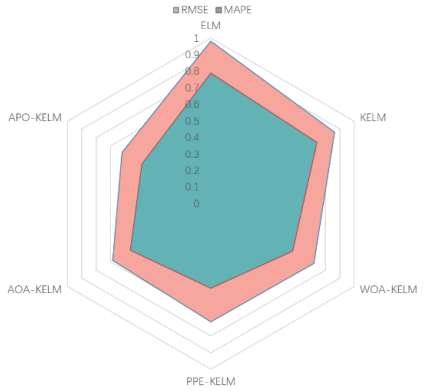
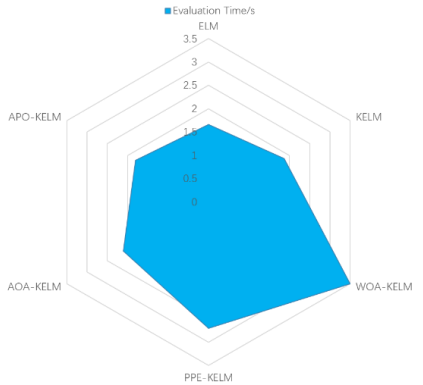


Fig. 22. Optimisation iteration process of KELM model with different optimisation algorithms.

Fig. 23 displays the performance comparison findings of ELM, KELM, WOA-KELM, PPE-KELM, AOA-KELM, and APO-KELM algorithms. The comparison is based on the performance of formative assessment models used in English language teaching and learning. The performance metrics considered are RMSE, MAPE, and elapsed time. Fig. 23 clearly demonstrates that the APO-KELM model outperforms the other models in terms of RMSE, with a value of 0.6204. Additionally, in terms of MAPE, the APO-KELM model is superior to the other models, with a value of 0.48. The ELM model outperforms other algorithms, including the KELM, APO-KELM, APOA-KELM, PPE-KELM, and WOA-KELM models, in terms of time efficiency.



(a) RMSE and MAPE.



(b) Time consuming.

Fig. 23. RMSE, MAPE, and elapsed time results for the comparison algorithm model.

VI. CONCLUSION

This research use the APO algorithm and Nuclear Limit Learning Machine to analyze and simulate trials related to the issue of formative assessment in English instruction. Firstly, it examines the issue of formative assessment of English teaching in the context of big data technology. It identifies evaluation criteria and establishes an index system for formative assessment of English teaching. Secondly, to address the challenge of constructing a formative assessment model for English teaching, it enhances the KELM using the APO algorithm. It introduces the method of formative assessment of English teaching based on the APO-KELM model. Lastly, it applies the APO-KELM model to multiple sets of data for formative assessment of English teaching. The simulation studies demonstrate that the screening approach suggested in this research has superior stability, merit-seeking ability, and convergence accuracy.

Future study should focus on enhancing the precision and speed of convergence of the APO algorithm, as well as expanding its application to a wider range of teaching assessment challenges.

REFERENCES

[1] Yazidi R E .Investigating the influence of formative assessment on the learning process in the English language classroom[J]. Education and Training, 2023.

[2] Zhang H , Ge S , Saad M R B M .Formative assessment in K-12 English as a foreign language education: a systematic review[J].Heliyon, 2024, 10(10):e31367 .

[3] Sar H R S K .The role of clandestine assessment in Iranian EFL context: a teacher's perceptions about the impact of educational digital-based games on teaching and learning English[J].Education and Information Technologies, 2024, 29(8):10127-10151.

[4] Zhang L , Li Q .Improved Collaborative Filtering Automatic Assessment System for Teaching English Writing in College[J].Advances in multimedia,. 2022, 2022(5):1.1-1.9.

[5] Huang Q .Influence of EFL Teachers' Self-Assessment on Their Self-Regulation and Self-Efficacy[J].Frontiers in psychology, 2022, 13:891839.

[6] Assia Z , Samira A .Practices, validity and challenges of online formative assessment in Algerian higher education[J].Contemporary Educational Researches Journal, 2023.

[7] Khodamoradi A , Maghsoudi M , Saidi M .Investigating the Washback Effect of Online Formative Assessment (OFA) During the COVID-19 Pandemic: A Case of Perceptual Mismatches Between Prospective Teachers and Teacher Educators[J].Practical Assessment, Research and Evaluation, 2022, 27.

[8] Chen L , Yi P .A Review of the Research on the Evaluation of High School English Writing Portfolio[J].IRA International Journal of Education and Multidisciplinary Studies, 2022.

[9] Upa R , Damayanti S .Incorporating Internet-Based Application in Teaching and Assessing English for Agriculture Students[J].IDEAS: Journal on English Language Teaching and Learning, Linguistics and Literature, 2022.

[10] Effendi T , Mayuni I .Examining teacher-made English test in a language school[J].LADU: Journal of Languages and Education, 2022.

[11] Malik S , Asif S I .Evaluation of Phonics Content in PTB Primary Grade Text Books and Assessment Schemes: Scope for Technology-Enhanced Language Learning (TELL) and Assessment Tools[J].International Journal of Linguistics and Culture, 2022.

[12] Baharom N , Aziz M S A , Ismail K .Portfolio Based Assessment in a Culturally Diverse ESL Classroom: Understanding Learners€ Autonomous Learning Practices[J].World Journal of English Language, 2022, 12.

[13] Esfandiari R , Arefian M H .Developing collective eyes for Iranian EFL teachers' computer-assisted language assessment literacy through internet -based collaborative reflection[J].Education and Information Technologies, 2024, 29(8):9473-9494.

[14] Shehu A O , Henay E N .Secondary English Teaching Programs in Turkey and Kosovo: a Comparison in Terms of the Items of the Curriculum[J].Prizren Social Science Journal, 2022, 6.

[15] Pawar P N , Yadav S , Lohar R .Computer-Aided Teaching and Assessment of Reading Skills in English as a Second Language[J]. Education Transformations, 2023.

[16] WANG Si, ZHANG Guohao, CHEN Yi'an. Prediction of anti-breast cancer drug properties based on GWO-KELM and GBDT[J]. Journal of Chongqing Gongshang University (Natural Science Edition), 2023, 40(6):93-104.

[17] Derakhshan A , Ghiasvand F .Demystifying Iranian EFL teachers' perceptions and practices of learning-oriented assessment (LOA): challenges and prospects in focus[J].Language Testing in Asia, 2022, 12(1):1-18.

[18] Wolterinck-Broekhuis C H D , Poortman C L , Schildkamp K , Visscher A J. Key stakeholder voices: investigating student perceptions of teachers' use of assessment for learning[J].Educational Assessment, Evaluation and Accountability, 2024, 36(2):257-275.

[19] ZHANG Yu-Hui, XUE Dan, WANG Du-Yao, JIA Rui-Ting, SONG Zhu-Zhen, HU Wu-Min. Evaluation of an animal model of spleen qi deficiency and analysis of medication characteristics based on data mining and Delphi method[J]. Chinese Herbal Medicine, 2023, 54(14):4590-4598.

[20] Wang X, Snášel V, Mirjalili S, Pan J, Kong L, Hisham A S. Artificial Protozoa Optimizer (APO): a novel bio-inspired metaheuristic algorithm for engineering optimisation[J]. Knowledge-Based Systems, 2024: 111737.

[21] Liu C.H.,He Q. A golden sine chimpanzee optimisation algorithm incorporating multiple strategies[J]. Journal of Automation, 2023, 49(11):2360-2373.

[22] AN Liuming, SHA Desheng, ZHANG Qing, LI Qian, LIU Xiaobo, ZHANG Xinyun. Research on intelligent fault diagnosis of wind turbine based on WOA-KELM algorithm[J]. Thermal Power Generation, 2023, 52(12):131-139.

[23] Wu Y , Guo G , Gao H .ELM: a novel ensemble learning method for multi-target regression and multi-label classification problems[J].Applied Intelligence, 2024, 54(17-18):7674-7695.

[24] WANG Lifu,WEI Yuqi,LIU Yijiangze. Transformer fault identification method based on KPCA and IPFA-KELM[J]. Control Engineering, 2023, 30(7):1180-1189.

[25] CHEN Zheng, GUO Yalin, GUO Chun. Greenhouse gas prediction of Chengdu metro construction phase based on WOA-DELM[J]. Tunnel Construction (in Chinese and English), 2022, 42(12):2048-2063.

[26] Narwal A .Resource Utilization Based on Hybrid WOA-LOA Optimization with Credit Based Resource Aware Load Balancing and Scheduling Algorithm for Cloud Computing[J].Journal of Grid Computing, 2024, 22(3).

[27] Song P C , Chu S C , Pan J S H .Simplified Phasmatodea population evolution algorithm for optimisation[J].complex & intelligent systems, 2022, 8(4):2749-2767.

[28] Aslan S , Kzloluk S , Sert E .TSA-CNN-AOA: Twitter sentiment analysis using CNN optimized via arithmetic optimisation algorithm[J].Neural computing & applications, 2023:1-18.

Enhancing Diabetic Retinopathy Classification Using Geometric Augmentation and MobileNetV2 on Retinal Fundus Images

Helmi Imaduddin[1], Adnan Faris Naufal[2], Fiddin Yusfida A'la[3], Firmansyah[4]
Department of Informatics Engineering, Universitas Muhammadiyah Surakarta, Surakarta, Indonesia[1]
Department of Physiotherapy, Universitas Muhammadiyah Surakarta, Surakarta, Indonesia[2]
Department of Informatics Engineering, Sebelas Maret University, Surakarta, Indonesia[3]
Department of Nutrition Science, Universitas Muhammadiyah Surakarta, Surakarta, Indonesia[4]

***Abstract*—Diabetic retinopathy (DR) ranks among the foremost contributors to blindness worldwide, particularly affecting the adult demographic. Detecting DR at an early stage is crucial for preventing vision loss; however, conventional approaches like fundus examinations are often lengthy and reliant on specialized expertise. Recent developments in machine learning, especially the application of deep learning models, provide a highly effective option for classifying diabetic retinopathy through retinal fundus images. This investigation examines the efficacy of geometric data augmentation methods alongside MobileNetV2 for the classification of diabetic retinopathy. Utilizing augmentation techniques like image resizing, zooming, shearing, and flipping enhances the model's ability to generalize. MobileNetV2 is selected for its impressive inference speed and computational efficiency. This analysis evaluates the effectiveness of MobileNetV2 in relation to InceptionV3, emphasizing metrics such as accuracy, precision, sensitivity, and specificity. The findings show that MobileNetV2 attains exceptional performance, achieving an accuracy of 97%. These findings highlight the promise of employing efficient models and augmentation strategies in clinical settings for the early identification of DR. The findings highlight the critical need to incorporate advanced machine learning methods to enhance healthcare results and avert blindness caused by diabetic retinopathy.**

***Keywords*—Diabetic retinopathy; data augmentation; InceptionV3; MobileNetV2; transfer learning**

I. INTRODUCTION

Diabetic retinopathy is a significant complication linked to diabetes mellitus, contributing significantly to the global incidence of blindness. The International Diabetes Federation (IDF) indicated that in 2019, around 463 million individuals globally were diagnosed with diabetes mellitus (DM), with projections suggesting a significant increase to about 700 million by 2045. Diabetic retinopathy (DR) remains a prevalent complication linked to diabetes, posing a significant health issue as it stands as a primary cause of preventable blindness, especially within the adult working-age demographic worldwide [1]. The condition is characterized by impairment of the retinal blood vessels, leading to potential leakage, bleeding, and the development of scar tissue. These alterations may ultimately result in diminished visual acuity or potentially irreversible blindness [2], [3]. It is essential to achieve a more profound understanding of the fundamental mechanisms of diabetic retinopathy and to create more effective approaches for its early detection to avert more severe outcomes.

Identifying diabetic retinopathy at an early stage is essential to prevent additional harm to the eyes. The application of early interventions, including the management of blood glucose levels and the arrangement of routine eye examinations, has been shown to decrease the likelihood of blindness [4]. This research suggests that through prompt identification and effective management, individuals with diabetes can preserve their ocular health and hinder the advancement of the condition. Nonetheless, a considerable obstacle remains, as numerous patients do not recognize the existence of diabetic retinopathy until symptoms become evident [5]. This research highlights the necessity for creating more effective approaches for the classification and detection of the disease.

Technological developments in retinal imaging and deep learning have pioneered new avenues for boosting the precision of diabetic retinopathy diagnoses. Conventional diagnostic techniques for identifying diabetic retinopathy, such as eye examinations by an ophthalmologist, are regularly laborious and rely on a physician's experience and acumen. Machine learning algorithms and imaging processing methods can heighten the effectiveness and exactitude of the categorization process. Convolutional neural networks (CNNs) are inspired by the structure and function of brain neurons with image input [6], [7]. The use of CNN has evidenced proficiency in detecting diverse medical conditions from medical visuals [8], [9],[10].

Numerous previous studies have attempted to classify diabetic retinopathy using Convolutional Neural Networks (CNN). State-of-the-art CNN architectures, such as VGG, ResNet, and Inception, have been applied for feature extraction, significantly improving the sorting process [11]. Additionally, investigations combining CNNs with preprocessing strategies like Contrast Limited Adaptive Histogram Equalization (CLAHE) have indicated enhanced model productivity and accuracy [12]. Furthermore, examination by [13] has proposed hybrid approaches that integrate machine learning and deep learning methods, for example, merging Support Vector Machines (SVM) and Random Forests with CNNs to further optimize categorization

performance. Moreover, transfer learning has been employed to utilize pre-trained models, minimizing the need for large data sets and reducing computational demands [14].

The use of augmentation techniques in image classification has been shown to impact model accuracy [15] significantly. In the realm of diabetic retinopathy classification, augmentation plays a crucial role in enhancing the model's ability to identify significant patterns and features that might be overlooked in the original dataset. In the realm of image data classification, geometric augmentation serves as an essential method for improving both the quality and quantity of training data utilized in machine learning models. Geometric augmentation includes various transformations such as rotation, cropping, and rescaling, which can enhance the learning process by presenting the model with the natural variations found in the data. Augmenting the training data allows us to reduce overfitting and improve the model's generalization, which in turn enhances classification accuracy [16],[17],[18].

Moreover, utilizing transfer learning model architectures like MobileNetV2 and InceptionV3, designed for enhanced efficiency and accuracy in image recognition, can significantly improve the classification ability for diabetic retinopathy [19], [20], [21], [22]. MobileNetV2 provides benefits regarding efficiency and inference speed [23], [24], [25], [26]. In a clinical setting, where the speed of diagnosis is essential, more efficient models can offer considerable benefits. MobileNetV2 demonstrates enhanced inference speed while maintaining a high level of accuracy, positioning it as a compelling choice for practical applications. In scenarios with constrained computing resources, MobileNetV2 emerges as a more viable option.

The comparative analysis and performance evaluation of MobileNetV2 and InceptionV3 in diabetic retinopathy classification reveals that each model has its unique strengths and weaknesses. Choosing the best model necessitates careful consideration of the unique needs of the clinical application, such as accuracy, efficiency, interpretability, and generalizability. Additional investigation is essential to explore the integration of the two models or to create a new model that harnesses the advantages of both.

It is crucial to highlight the importance of early detection and precise classification in diabetic retinopathy. Utilizing the most recent technological innovations in image processing and machine learning presents a significant opportunity to improve diagnosis and treatment results for individuals with diabetes. This study seeks to significantly enhance the prevention of blindness caused by diabetic retinopathy by refining classification accuracy through the application of geometric augmentation techniques and transfer learning models.

II. METHODOLOGY

The study was carried out in multiple phases, starting with the collection of datasets from Dr Sardjito and the APTOS 2019 dataset. The datasets were subsequently partitioned into three separate subsets: training sets, testing sets, and validation sets. The next step in the process involves enhancing the training data and training the model using the MobileNetV2 and InceptionV3 architectures. The last phase consists of assessing the model through a confusion matrix to derive the metrics for accuracy, precision, sensitivity, and specificity. Fig. 1 illustrates the research flow.

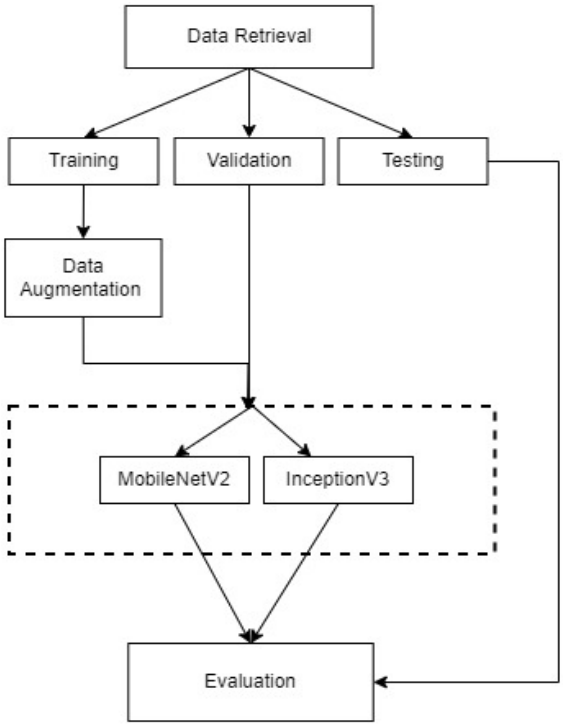


Fig. 1. Research flow.

A. Data Retrieval

The acquisition of data was crucial in this study, especially regarding the classification of diabetic retinopathy. The data for the retinal fundus images was sourced from two main origins. The data were collected from Dr Sardjito Hospital in Yogyakarta and the APTOS 2019 dataset. Dr. Sardjito Hospital stands out as a leading medical institution in Indonesia, featuring an extensive collection of retinal fundus images that covers a wide range of diabetic retinopathy severity. The data holds considerable importance as it accurately represents the condition of patients treated at the hospital, thus improving the relevance and precision of the developed classification model. Fig. 2 presents the exemplar of the retinal fundus image dataset.

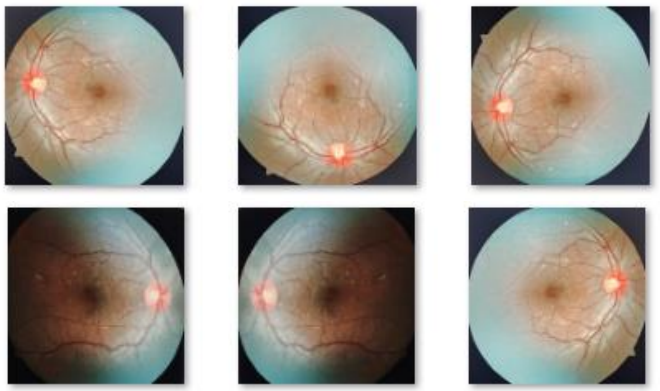


Fig. 2. Retina images dataset.

Additionally, the APTOS 2019 dataset, which is publicly available, was utilized in this study. This study employs a dataset consisting of 3,677 retinal fundus images, categorized into two groups: diabetic retinopathy positive (1,872 images) and average (1,805 images). The use of this dataset allows for model training with a larger volume of diverse data, which is essential for improving model generalization. For additional information concerning the datasets employed in this study, please consult Table I.

TABLE I. DATASET

No	Class	Data
1	Diabetic Retinopathy	1.872
2	Normal	1.805
	Total	**3.677**

Following the collection process, the data is divided into three separate sets: training data, validation data, and testing data. The dataset is segmented into three parts: 80% is allocated for training the model, 10% is designated for validation, and the final 10% is reserved for testing the model's accuracy. The proportional division plays a vital role in guaranteeing that the model learns from the available data while also being able to generalize to previously unseen data. This fact aligns with essential principles of machine learning that highlight the importance of validating models.

B. Data Augmentation

Subsequently, the geometric augmentation technique serves as a method to enhance both the quantity and diversity of training data through the modification of existing images. This study utilized various augmentation techniques, such as resizing images to a resolution of 224x224 pixels, adjusting the zoom by a factor of 0.2, applying shear transformations within a range of 0.2, and implementing both horizontal and vertical flip transformations. The application of these techniques is expected to enable the model to learn from a broader array of images, thus improving its ability to generalize in classification tasks.

Images were resized to (224x224) to maintain uniform resolution, an essential factor in training deep learning models. This size was chosen due to its status as a standard dimension commonly utilized in various neural network architectures, such as MobileNetV2 and InceptionV3. Maintaining a consistent size allows for more efficient and effective data processing by the model.

The utilization of a zoom range and shear range facilitates diversity in the viewing angle and perspective of the image. The model can learn to recognize important features of retinal fundus images at various scales through zooming. At the same time, the shear range allows for adaptation to distortions that may occur during image capture. This technique holds considerable importance due to the variability in the angles at which retinal fundus images are captured and the differing lighting conditions present during their acquisition. The implementation of horizontal and vertical flips serves as an essential technique in enhancing data through augmentation. The absence of a fixed orientation in retinal fundus images allows for the use of flip techniques, which helps the model learn from inverted images and improves its ability to recognize essential patterns. This study is especially relevant in the context of classifying diabetic retinopathy, as changes in image orientation can influence the precision of detection outcomes.

The choice of these geometric augmentation techniques is informed by the results of earlier studies that have shown that data augmentation can significantly improve model accuracy in image classification tasks [27], [28], [29]. Data augmentation plays a crucial role in reducing overfitting and improving model performance when working with limited data sets [30], [31]. The application of these techniques is expected to yield a model that demonstrates improved performance in classifying diabetic retinopathy.

C. Training Model

The model development process in this study involved training two well-known neural network architectures, specifically MobileNetV2 and InceptionV3. The selection of these two models is based on their proven effectiveness across various image recognition and classification tasks, along with their computational efficiency. MobileNetV2 is tailored for devices with constrained computational capabilities, whereas InceptionV3 provides enhanced depth and complexity, enabling a more thorough examination of the relevant features.

The model underwent training with the dataset that had been previously collected and prepared. The training parameters comprised a dropout rate of 0.2 to mitigate overfitting, a sigmoid activation function for binary classification, and the Adamax optimizer, known for its efficacy in tackling optimization challenges. The learning rate was established at 0.0001, a frequently utilized value to promote stable convergence throughout the training process. The training procedure was planned for 30 epochs, incorporating early stopping to halt the training if there was no enhancement in accuracy over five successive epochs.

Throughout the training process, evaluations of the model were conducted at consistent intervals to assess its performance. The evaluation described was carried out utilizing a validation data set that was separate from the training data set. This approach allows for the determination of whether the model is showing indications of overfitting. In this situation, the model becomes excessively dependent on the training data and needs to generalize to new data. Should this situation arise, adjustments might be made regarding the training parameters or the augmentation method utilized.

After training the model, the next step involves fine-tuning the chosen architecture. Fine-tuning involves adjusting a pre-trained model by utilizing a more specialized dataset. In this context, the MobileNetV2 and InceptionV3 models, previously trained on a substantial dataset, will be fine-tuned to the dataset of retinal fundus images that have been gathered. This process aims to improve the accuracy of models used for classifying diabetic retinopathy. By implementing a structured approach in model development, it is expected that both architectures will produce the best results in diabetic retinopathy classification. This study aims to enhance classification accuracy while

providing an in-depth understanding of the effectiveness of various techniques and architectures in the detection of diabetic retinopathy.

D. Evaluation

The evaluation of the model is a vital step in determining the effectiveness of the created classification system. This study utilized several evaluation metrics, such as accuracy, precision, specificity, and sensitivity. The chosen metrics offer unique insights into the model's effectiveness in classifying retinal fundus images according to the severity of diabetic retinopathy.

Accuracy serves as a crucial metric that reflects the ratio of correct predictions to the overall predictions generated by the model. This metric holds significant value, offering a comprehensive insight into the model's ability to identify images accurately. Nevertheless, depending solely on accuracy needs to be improved, especially in scenarios involving unbalanced datasets, where the quantity of images across different categories can differ significantly. As a result, further metrics, including precision and sensitivity, are also computed.

Precision measures the ratio of accurate positive predictions to all optimistic predictions, while sensitivity evaluates how effectively the model detects actual positive cases. In contrast, specificity measures the ability of the model to identify adverse conditions. The application of a combination of these metrics enables a more thorough understanding of the model's performance in diabetic retinopathy classification.

The testing process was carried out utilizing the previously segregated test data set. Following this, the outcomes of these tests undergo analysis aimed at pinpointing the model's strengths and weaknesses in classification. For example, when the model shows high accuracy yet low sensitivity, it may indicate that the model is more skilled at recognizing images without retinopathy than those that display signs of the condition.

The examination of these findings is essential for advancing model development. If the model shows less than ideal-performance, adjustments can be made to the architecture, training parameters, or augmentation techniques used. As a result, the evaluation of models serves not just as a final step but as a crucial part of the ongoing model development process.

III. Results and Discussion

Diabetic retinopathy is a significant contributor to global blindness, highlighting the critical need for precise classification to facilitate early intervention and effective disease management. This study presents a comparative analysis of two deep learning models, MobileNetV2 and InceptionV3, aimed at evaluating their performance in classifying retinal fundus images to detect diabetic retinopathy. The findings indicate that both models show acceptable performance, yet significant differences are apparent in the evaluation metrics.

MobileNetV2 exhibited higher accuracy than InceptionV3, achieving an accuracy rate of 97%. This result suggests that the model demonstrates enhanced capability in identifying relevant features within retinal fundus images. The accuracy of the MobileNetV2 model is particularly impressive, achieving 97%. This result suggests that the model is highly effective in reducing false positives. On the other hand, InceptionV3 demonstrates an accuracy of 94% and a precision of 97%. Although these values are noteworthy, they indicate that MobileNetV2 surpasses InceptionV3 in terms of overall accuracy. Fig. 3 presents the graph depicting the training accuracy of MobileNetV2.

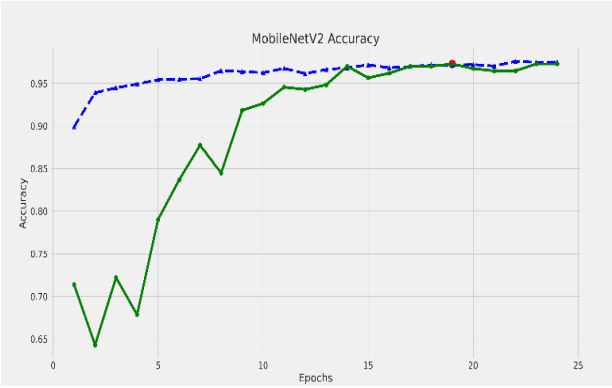


Fig. 3. MobileNetV2 training accuracy.

The model's sensitivity, characterized by its capacity to identify positive cases, produced some fascinating outcomes. MobileNetV2 showed a sensitivity of 96%, whereas InceptionV3 displayed a sensitivity of just 91%. This result suggests that MobileNetV2 demonstrates greater efficacy in recognizing patients with diabetic retinopathy, which holds considerable importance in a clinical environment where timely identification can avert more severe disease advancement.

The measure of specificity, reflecting the model's ability to identify negative cases correctly, showed similar results for both models, achieving a value of 97%. This result indicates that, even with differences in sensitivity and accuracy, both models demonstrate a similar ability to recognize individuals without diabetic retinopathy. The results indicate that InceptionV3 continues to be a dependable choice for clinical applications.

This study revealed that while InceptionV3 showed similar precision to MobileNetV2, the differences in sensitivity and accuracy suggested that MobileNetV2 performed better in detecting diabetic retinopathy. This results from the enhanced capability of MobileNetV2 to utilize augmentation data used during training, which improves the model's ability to generalize across variations in retinal fundus images.

Furthermore, both models underwent assessment using a varied dataset that included images of patients displaying different stages of diabetic retinopathy. The findings indicated that MobileNetV2 showed enhanced efficacy in detecting the early stages of the disease, which are frequently difficult to identify. This finding highlights the crucial influence that choosing the suitable model can exert on the precision of diagnosis and the management of patients after that. Fig. 4 illustrates the confusion matrix for the evaluation of MobileNetV2.

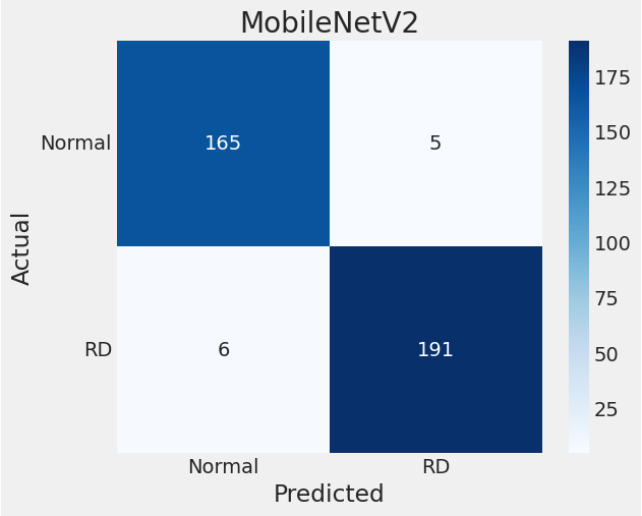


Fig. 4. Confusion matrix.

This study employs various methodologies that significantly diverge from those used in earlier investigations, enabling a more thorough analysis. A previous investigation by [32] utilized CNN to classify diabetic retinopathy, resulting in an accuracy of 75% and a sensitivity of 95%. A separate investigation conducted by [33] utilized ResNet50 to classify the APTOS 2019 dataset, achieving an accuracy of 91%. The findings from this study are thoroughly compared with those of several prior studies in Table II. The comparisons provide valuable insights into the progress and contributions of this study in relation to the current body of literature.

TABLE II. COMPARISON WITH OTHER STUDIES

No	Researchers	Method	Accuracy
1	Pratt	CNN	75%
2	Devi	ResNet50	91%
3	**Our Study**	**MobileNetV2**	**97%**

This study utilizes a range of methods that markedly diverge from those used in earlier investigations, facilitating a more thorough and detailed analysis. A comprehensive comparison of the findings from this study with those of several prior studies is outlined in Table I, emphasizing the differences in methodology, data processing techniques, and model performance across various experiments. The comparisons yield essential insights into the progress and contributions of this study in relation to the current body of literature.

IV. CONCLUSION

This study's findings demonstrate that MobileNetV2 and InceptionV3 serve as two effective models for classifying diabetic retinopathy through retinal fundus images. While both models showed commendable performance, MobileNetV2 revealed enhanced accuracy and sensitivity, positioning it as a more appropriate option for clinical applications. The implications of these findings are substantial for managing and preventing blindness caused by diabetic retinopathy, laying a groundwork for additional exploration in this area.

Future investigations should explore the potential advantages of integrating the MobileNetV2 and InceptionV3 models within an ensemble framework. This method enables the advantages of each model to be utilized, thus improving the overall accuracy and sensitivity. Moreover, it is essential to broaden the datasets employed for training and evaluating the models. Employing more extensive and varied datasets can improve model generalization and decrease the likelihood of overfitting. Additionally, gathering data from diverse geographical areas could improve our understanding of the differences in the clinical manifestations of diabetic retinopathy.

ACKNOWLEDGMENT

This study received full funding from the Ministry of Education, Culture, Research, and Technology, reference number 196.19/A.3-III/LRI/VI/2024. I would like to express my gratitude for the support which was instrumental in funding this work and facilitating the task at hand. This research would not have been possible without this generous funding.

REFERENCES

[1] Z. Teo, Y. Tham, M. Yu, M. Chee, T. Rim, N. Cheung, M. Bikbov, Y. Wang, Y. Tang, Y. Lu, I. Wong, D. Ting, G. Tan, J. Jonas, C. Sabanayagam, T. Wong, and C. Cheng, "Global Prevalence of Diabetic Retinopathy and Projection of Burden through 2045: Systematic Review and Meta-analysis," Ophthalmology, 2021. doi: 10.1016/j.ophtha.2021.04.027.

[2] J A. K. Morya, P. Ramesh, N. Prateek, K. Kaur, B. Gurnani, A. Heda, and S. Salodia, "Diabetic retinopathy: A review on its pathophysiology and novel treatment modalities," World Journal of Methodology, vol. 14, no. 4, 2024. doi: 10.5662/wjm.v14.i4.95881.

[3] J. C. Ferreira, J. D. Fernandes, A. C. C. Teodoro, G. Castro, D. D. Teixeira, L. F. R. Almeida, V. R. Queiroz, F. R. T. Dias, N. R. Queiroz, A. B. Dognani, I. G. Lima, and J. M. Silva, "Retinopatia diabética: principais aspectos da doença," Revista Ibero-Americana de Humanidades, Ciências e Educação, vol. 10, no. 8, pp. 961-967, 2024. Doi: 10.51891/rease.v10i8.15137.

[4] D. Poborowska, W. Kahan, K. Polańska, O. Najjar, M. Wojaczek, E. Bąk, W. Szafrańska, J. Fordymacki, and T. Gańko, "Physical activity as a prescription for diabetic retinopathy," Quality in Sport, 2024. doi: 10.12775/qs.2024.18.53313.

[5] S. Walia, "Prevalence of Diabetic Retinopathy among Self-reported Newly Diagnosed Diabetics," IgMin Res, vol. 2, no. 5, pp. 370-373, 2024. doi: 10.61927/igmin190.

[6] W. Supriyanti and D. A. Anggoro, "Classification of Pandavas Figure in Shadow Puppet Images using Convolutional Neural Networks," Khazanah Inform. J. Ilmu Komput. and Inform., vol. 7, no. 1, pp. 18–24, 2021, doi: 10.23917/khif.v7i1.12484.

[7] R. D. Nurfita, G. Ariyanto, "Implementasi Deep Learning berbasis Tensorflow untuk Pengenalan Sidik Jari," J. Emit., vol. 18, no. 01, pp. 22–27, 2018 , doi: 10.23917/emitor.v18i01.6236.

[8] H. Imaduddin and A. R. Sakina, "Eye disease detection using transfer learning based on retinal fundus image data," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 36, no. 1, p. 509, Jul. 2024, doi: 10.11591/ijeecs.v36.i1.pp509-516.

[9] L. F. C. Vilela, N. O. Cabral, A. C. Destefani, and V. C. Destefani, "Harnessing the power of artificial intelligence for early detection and management of diabetic retinopathy, age-related macular degeneration, and glaucoma: A narrative review of deep learning applications in ophthalmology," Revista Ibero-Americana de Humanidades, Ciências e Educação, vol. 10, no. 8, pp. 3311-3320, 2024. doi: 10.51891/rease.v10i8.15395.

[10] D. Aparna, N. Mahajan, and S. Mehandia, "Recent Development and Application in Deep Learning for Diabetic Retinopathy Image

Classification," Deleted Journal, vol. 6, no. 07, pp. 2398-2407, 2024. doi: 10.47392/irjaem.2024.0347.

[11] K. Kayathri and K. Kavitha, "CGSX Ensemble: An Integrative Machine Learning and Deep Learning Approach for Improved Diabetic Retinopathy Classification," International Journal of Electrical & Electronics Research, vol. 12, no. 2, pp. 669-681, 2024. doi: 10.37391/ijeer.120245.

[12] C. Wangweera and P. Zanini, "Comparison review of image classification techniques for early diagnosis of diabetic retinopathy," Biomedical Physics & Engineering Express, 2024. doi: 10.1088/2057-1976/ad7267.

[13] N. B. Madan and N. V. Bhandari, "Comparative Study of Diabetic Retinopathy Detection Using Machine Learning Methods," Deleted Journal, vol. 6, no. 07, pp. 2134–2139, Jul. 2024. doi: 10.47392/irjaem.2024.0312.

[14] N. S. J. Nagar, "A Comprehensive Review on Diabetic Retinopathy Detection Techniques using Neural Network Architectures," Deleted Journal, vol. 20, no. 10s, pp. 1401–1409, Jul. 2024. doi: 10.52783/jes.5309.

[15] U. Muñoz-Aseguinolaza, B. Sierra, and N. Aginako, "Rotational augmentation techniques: a new perspective on ensemble learning for image classification," ArXiv, abs/2306.07027, 2023. doi: 10.48550/arXiv.2306.07027.

[16] R. Zhang, B. Zhou, C. Lu, and M. Ma, "The performance research of the data augmentation method for image classification," Math. Probl. Eng., 2022. doi: 10.1155/2022/2964829.

[17] R. Alharbi, H. Alhichri, R. Ouni, Y. Bazi, and M. Alsabaan, "Improving remote sensing scene classification using quality-based data augmentation," Int. J. Remote Sens., vol. 44, pp. 1749–1765, 2023. doi: 10.1080/01431161.2023.2184213.

[18] I. Kandel, M. Castelli, and L. Manzoni, "Brightness as an augmentation technique for image classification," Emerg. Sci. J., vol. 6, no. 4, 2022. doi: 10.28991/esj-2022-06-04-015.

[19] M. S., B. B., and E. M., "Assessment of transfer learning models for grading of diabetic retinopathy," The Scientific Temper, 2023. doi: 10.58414/scientifictemper.2023.14.2.17.

[20] C. Bhardwaj, S. Jain, and M. Sood, "Transfer learning based robust automatic detection system for diabetic retinopathy grading," Neural Comput. Appl., vol. 33, pp. 13999–14019, 2021. doi: 10.1007/s00521-021-06042-2.

[21] Y. Brik, B. Attallah, I. Aiche, H. Lahmar, and Z. Zohra, "Deep learning-based framework for automatic diabetic retinopathy detection," in Proc. 32nd Int. Conf. Comput. Theory Appl. (ICCTA), 2022, pp. 129–134. doi: 10.1109/ICCTA58027.2022.10206262.

[22] M. Raiaan et al., "A lightweight robust deep learning model gained high accuracy in classifying a wide range of diabetic retinopathy images," IEEE Access, vol. 11, pp. 42361–42388, 2023. doi: 10.1109/ACCESS.2023.3272228.

[23] A. Mutawa, S. Alnajdi, and S. Sruthi, "Transfer learning for diabetic retinopathy detection: A study of dataset combination and model performance," Appl. Sci., vol. 13, no. 9, 2023. doi: 10.3390/app13095685.

[24] M. Mazumder, T. Hossain, F. Shamrat, N. Jahan, Z. Tasnim, and A. Khater, "Deep learning approaches for diabetic retinopathy detection by image classification," in Proc. 3rd Int. Conf. Smart Electron. Commun. (ICOSEC), 2022, pp. 1504–1510. doi: 10.1109/ICOSEC54921.2022.9952159.

[25] A. Pamadi, A. Ravishankar, P. Nithya, G. Jahnavi, and S. Kathavate, "Diabetic retinopathy detection using MobileNetV2 architecture," in Proc. Int. Conf. Smart Technol. Syst. Next Gen. Comput. (ICSTSN), 2022, pp. 1–5. doi: 10.1109/ICSTSN53084.2022.9761289.

[26] M. Mazumder, T. Hossain, F. Shamrat, N. Jahan, Z. Tasnim, and A. Khater, "Deep learning approaches for diabetic retinopathy detection by image classification," in Proc. 3rd Int. Conf. Smart Electron. Commun. (ICOSEC), 2022, pp. 1504–1510. doi: 10.1109/ICOSEC54921.2022.9952159.

[27] C. Khosla and B. Saini, "Enhancing performance of deep learning models with different data augmentation techniques: A survey," in Proc. Int. Conf. Intell. Eng. Manag. (ICIEM), 2020, pp. 79–85. doi: 10.1109/ICIEM48762.2020.9160048.

[28] R. Dabare, K. Wong, M. Shiratuddin, and P. Koutsakis, "A fuzzy data augmentation technique to improve regularisation," Int. J. Intell. Syst., vol. 37, pp. 4561–4585, 2021. doi: 10.1002/int.22731.

[29] Q. Mi, Y. Xiao, Z. Cai, and X. Jia, "The effectiveness of data augmentation in code readability classification," Inf. Softw. Technol., vol. 129, 2021. doi: 10.1016/j.infsof.2020.106378.

[30] N. Dvornik, J. Mairal, and C. Schmid, "On the importance of visual context for data augmentation in scene understanding," IEEE Trans. Pattern Anal. Mach. Intell., vol. 43, pp. 2014–2028, 2018. doi: 10.1109/TPAMI.2019.2961896.

[31] C. Shorten and T. Khoshgoftaar, "A survey on image data augmentation for deep learning," J. Big Data, vol. 6, no. 1, 2019. doi: 10.1186/s40537-019-0197-0.

[32] H. Pratt, F. Coenen, D. M. Broadbent, S. P. Harding, and Y. Zheng, "Convolutional neural networks for diabetic retinopathy," in Proc. Med. Imag. Understand. Anal. (MIUA), 2016, vol. 90, pp. 200–205. doi: 10.1016/j.procs.2016.07.014.

[33] Y. S. Devi and S. P. Kumar, "A deep transfer learning approach for identification of diabetic retinopathy using data augmentation," IAES Int. J. Artif. Intell., vol. 11, no. 4, pp. 1287–1296, 2022. doi: 10.11591/ijai.v11.i4.pp1287-1296.

New Method in SEM Analysis Using the Apriori Algorithm to Accelerate the Goodness of Fit Model

Dien Novita[1], Ermatita[2*], Samsuryadi[3], Dian Palupi Rini[4]
Doctoral Program in Engineering Science, Universitas Sriwijaya, Palembang, Indonesia[1]
Faculty of Computer Science, Universitas Sriwijaya, Palembang, Indonesia[2, 3, 4]
Faculty of Computer Science and Engineering, Universitas Multi Data Palembang, Palembang, Indonesia[1]

Abstract*—This research aims to develop a new method in Structural Equation Modelling (SEM) analysis using the Apriori algorithm to accelerate the achievement of Goodness of Fit models, focusing on traditional retail purchasing decision models in Indonesia, especially in Palembang. SEM will be used to model causal relationships between variables that influence purchasing decisions in traditional retail. However, the Goodness of Fit model testing process takes a long time due to the complexity of the model. Therefore, this research uses the Apriori algorithm to filter variables that have a significant relationship in traditional retail purchasing decision models to reduce model complexity and speed up Goodness of Fit calculations. There are two stages in the research. First, the Apriori algorithm identifies frequent item sets that frequently appear among variables influencing traditional retail consumer purchasing decisions, such as product, price, and location. This pattern becomes the basis for SEM modeling, focusing on selected variables and, in the second stage, measuring the Goodness of Fit of the SEM model, namely GFI, RMSEA, AGFI, NFI, and CFI, to evaluate the suitability of the model which explains the factors that support traditional retail purchasing decisions in Palembang. The practical implications of this research are significant, as it provides a more efficient and effective method for modeling and understanding consumer behavior in the context of traditional retail. Based on other studies, if this research uses a conventional SEM approach, it does not meet the cut-off value of Goodness of Fit. Meanwhile, the results of the proposed method, namely combining Apriori into SEM, called APR-SEM, obtained a significant Goodness of Fit evaluation. The model coefficient of determination value from APR-SEM is R^2 0.71, higher than the conventional model, R^2 0.52. This method effectively simplifies the SEM model by identifying the most relevant relationships, thereby providing a clearer understanding of the critical factors influencing purchasing decisions in traditional retail in Palembang City.

Keywords*—APR-SEM; method; goodness of fit; traditional retail

I. Introduction

The existence of retail in Indonesia is relatively fast. According to 2021, Global Retail Development Index (GRDI) data, Indonesia managed to rank fourth, up one place from 2019 [1]. Meanwhile, Indonesia's retail sales growth was reported to increase by 3% in September 2021 [2]. The Indonesia Retail Summit 2023, which carries the theme ASEAN Retail: Epicentrum of Growth, shows the enthusiasm and commitment to Indonesia's role in strengthening the ASEAN and even the global retail industry. Currently, the Indonesian retail industry is the largest in ASEAN; Indonesia is in the number one position for retail in ASEAN [3].

In Indonesia, there are two forms of retail business run by the community, namely traditional retail and modern retail [4]. In contrast to traditional retail, modern retail is a shop with a self-service system that sells various types of goods at retail in minimarkets, malls (supermarkets and hypermarkets), department stores, or wholesale shops in the form of wholesalers [5].

With modern management, service, quantity, quality, and prices, modern retail has a higher competitiveness than traditional retail. Many traditional retailers then lack visitors, and their turnover decreases until they finally close due to their inability to compete with the many modern retailers nearby [6][7]. However, quite a few traditional retailers can survive amidst the invasion of many modern minimarkets popping up around these traditional retailers. These retailers continue to survive, sell, and serve buyers and are still busy with buyers. Interestingly, traditional retail in Indonesia also dominates the retail sales business in Indonesia [8]. Retail sales activities in Indonesia are still dominated by traditional retail. This can be seen from the number of outlets and the sales value which is much higher than modern retail outlets. According to data compiled by Euromonitor [8], there are 3.57 million traditional retail outlets in Indonesia.

With the current conditions, where the Indonesian retail industry is the largest in ASEAN, and traditional retail dominates the retail sales business in Indonesia, the large number of studies that discuss the existence of retail, including traditional retail types, are the basis for this research. Traditional retail businesses aim to increase competitiveness to survive with unique products, services, and facilities according to traditional retail characteristics and, of course, to make a profit. Increasing competitiveness in traditional retail businesses must be distinct from the owner's ability to manage the business. Traditional retail ownership, which is more personal, requires managers to survive by relying on brilliant ideas to advance their business. The use of ideas or concepts known as tacit knowledge is part of knowledge management [9]. Some research models are based on converting tacit knowledge into individual knowledge [10]. The purchasing decision model in traditional retail has 3 variables, namely product, price, and place which influence purchasing decisions [11].

In various disciplines such as marketing, management, and information technology, analysis of relationships between

variables is critical to understanding the dynamics that influence research results. Structural Equation Modelling (SEM) is a powerful method for analyzing complex relationships between latent variables and their indicators. Meanwhile, the Apriori algorithm, which originates from the field of data mining, is well known for analyzing association patterns between items in large data sets. Although SEM is very effective for modelling structural relationships between variables, this method is not designed to handle the analysis of high-frequency association patterns in large data sets. SEM can be obtained through the partial least squares structural equation modelling technique [12]. On the other hand, the Apriori algorithm can identify significant association rules in the data but cannot explicitly model the hypothesized causal relationships as SEM does. Apriori can generate association rules on data sets, for example, transactional basket data, to produce variations in sets of items (baskets) that adequately represent consumer purchasing patterns [13].

Therefore, combining these two methods offers a more comprehensive approach to analyzing complex data. This research aims to produce a model related to purchasing decisions in traditional retail using SEM analysis. SEM analysis tests the model's suitability by examining various Goodness of Fit criteria. However, the model Goodness of Fit testing process often takes a long time due to the complexity of the model. Therefore, combining the Structural Equation Modelling(SEM) method with the Apriori algorithm will make it easy to analyze complex relationships between variables and identify significant association patterns in the data. This approach can provide more profound and comprehensive insight into the relationships between variables so that Goodness of Fit criteria are quickly achieved.

This paper consists of several parts. In Section II, this paper reviewing several concepts related to research involving Structural Equation Modeling techniques and the Apriori Algorithm; besides looking at the retail conditions in Indonesia. Section III, this paper provides a general overview of research methodology, including respondent demographics and research model. Section IV of this paper explains the proposed research method regarding the stages. Section V, this paper provides results and discussion, and finally, Section VI concludes this paper.

II. Literature Review

The existence of traditional retail has a significant influence on economic development in Indonesia with the number of traditional retailers surpassing modern retail. Based on type, traditional grocery stores are the most numerous retailers in Indonesia. The number was recorded at 3.57 million units. A total of 38,323 retailers are in the form of department stores. Then, there are 1,411 supermarket-type retailers. Then, forecourt retail and hypermarkets were 358 units and 285 units, respectively, as in Table I.

The dominant type of retail in Indonesia is the traditional grocery store, which is both wholesale and retail. The types of products sold in traditional grocery stores are shown in Table II below.

TABLE I. Types of Retail and Number in Indonesia in 2022 [14]

Retail Type	Total (unit)
Traditional Grocery	3,935,238
Department Store	41,453
Supermarket	1,544
Food/Beverage Specialist	5,455
Hypermarket	298

TABLE II. Types of Products in Traditional Grocery Stores

Types of Products	Source
Necessities, snacks, drinks, toiletries and washing supplies, household supplies, medicines, kitchen spices, instant food, LPG gas, and stationery supplies.	[15]
Household equipment and necessities.	[16]
A variety of daily household needs	[17]

State-of-the-art research [18][19][20][21][22][23] which formulates business strategies for retail businesses, especially small-scale retail, in the form of developing business strategy models using data mining, artificial neural networks, and structural equation modelling, no one has combined the tools between data mining and structural equation modelling. However, research in study [24] and [25] has used a combination of SEM and data mining methods with model validation between 54%-89%. The research model [26] is the Apriori + hybrid structural equation model (SEM) using a data-based Apriori algorithm that explores large-scale hidden relationships between variables. Meanwhile, the SEM model captures user behaviour and decision-making procedures, providing interpretable results. Additionally, association rules in Apriori facilitate the specification of complex SEM models, thereby substantially reducing modelling calibration. The Goodness of Fit results show that the SEM + Apriori hybrid model performs better than the conventional model, namely with an R^2 value of 0.82, which is greater than the conventional model, 0.69.

From the previous research above, this is the first time anyone has specifically proposed a combination of Apriori and SEM analysis in formulating research models. Although research [26] has used a hybrid SEM + Apriori model, it is limited to the automotive industry. So, this research proposes SEM analysis using the Apriori algorithm to model purchasing decisions in traditional retail. The following are several theories related to the proposed method in this research, namely Association Rule, Apriori Algorithm, and Structural Equation Modelling.

A. Association Rule

Association rule mining is a data mining technique that finds similar rules in an event [27]. An example of an association rule that is often encountered is the process of purchasing merchandise at a shopping centre. From historical data it is known that the purchase of bread mainly follows the purchase of milk, so shop owners can increase their profits by arranging the location of milk and bread close together and providing discounts that attract buyers. Commonly used association methods are FP-Growth, Coefficient of Correlation, Chi-Square, Apriori, and others.

B. Apriori Algorithm

The Apriori algorithm, a classic in data mining, is a powerful tool for uncovering association rules. Its main purpose is to delve deep into the complex network of associationrelationships between variables [26], thereby showcasing the depth of the topic.

- Support is the probability that items A and B appear simultaneously, representing the importance of the corresponding association rule in the dataset.

$$support(A \rightarrow B) = P(A \cup B)$$

- Confidence is the proportion of the number of times that A and B appear simultaneously over the number of times that A appears. This represents the credibility of the association rule.

$$confidence(A \rightarrow B) = \frac{support(A \rightarrow B)}{support(A)}$$

Key metrics in the Apriori algorithm are based on:

- Support: Percentage of transactions containing itemsets or rules. The higher the support, the more frequently the item or rule occurs.
- Confidence: The probability that the consequent occurs when the antecedent exists. A value close to 1 indicates the strength of the rule.
- Lift: It's the key that unlocks the door to understanding association. The ratio between actual support and expected support if the antecedent and consequent were independent. Values greater than 1 indicate a positive association, enriching our knowledge about the data.
- Conviction: Measuring the strength of a rule by considering the frequency of antecedents that are not followed by consequents. The infinity (inf) value indicates the rule is firm.

The steps in the Apriori Algorithm are:

1) Determine minimum support and confidence
2) Find items that appear frequently (frequent itemsets)
3) Remove items that don't appear frequently
4) Create association rules
5) Evaluate association rules

C. Structural Equation Modelling

Structural Equation Modelling (SEM) is a technique for observing the interdependence between various variables. It is a confirmatory method to check the suitability of data and conceptual models. This is especially true when drawing conclusions where variables cannot be measured. SEM is also called a combination of factor analysis and multiple regression. If completed on a software platform, it can be completed using IBM SPSS AMOS, LISREL, and R [28]. The stages in the SEM method are [18]:

1) Development of a theoretical model
2) Development of path diagrams
3) Convert the path diagram into an equation
4) Select input matrix and model estimation
5) Possible identification problems
6) Evaluate goodness of fit criteria

The minimum number of samples in SEM recommended is 100-150 data [29]. Five or fewer constructs exist, each with more than three items (observed variables) and high item communality (0.6 or higher). Table III shows the goodness of fit in step 6 for the model.

TABLE III. MODEL-OF-FIT INDICES

Model-of-fit indices	Full name/key concerns	Cut off value
RMSEA	Root Mean Square Error of Approximation	Value between 0.08 and 0.10 (mediocre fit), <0.08 (good fit)
GFI	Goodness of fit statistics Exhibits bias towards samples	Value >0.90 or >0.95 (use 0.95 if factor loading and number of sample are low)
AGFI	Adjusted goodness of fit statistics Needs to be accompanied by other indices	Value of >0.80
NFI	Normed fit index Sensitive to sample size	Value of >0.90
CFI	Comparative fit index Revised version of NFI Less affected by sample size	Value of ≥0.90

III. RESEARCH METHODOLOGY

Questionnaire data collection used Google Forms [29] to reach all areas of the city of Palembang as research objects. Table IV shows the demographics of a total of 213 respondents.

TABLE IV. RESPONDENT DEMOGRAPHICS

Sample Characteristic		Percent (%)
Gender	Male	57.75
	Female	42.25
Age	Lower than 20 years	39.91
	20-29	49.30
	30-39	5.16
	40-49	4.69
	50-59	0.94
Occupation	Not yet working	0.94
	BUMN	0.47
	Teacher/Lecturer	1.41
	Housewife	48.83
	Student	43.19
	PNS/TNI/Polri	1.41
	Private	3.76
Area	Alang-alang Lebar	8.45
	Bukit Kecil	0.94
	Gandus	1.41
	Ilir Barat I	8.92

	lir Barat II	8.45
	Ilir Timur I	7.98
	Ilir Timur II	14.55
	Ilir Timur III	6.57
	Jakabaring	2.82
	Kalidoni	10.80
	Kemuning	0.47
	Kertapati	0.94
	Plaju	1.41
	Sako	8.45
	Seberang Ulu I	1.41
	Seberang Ulu II	0.94
	Sematang Borang	7.51
	Sukarami	7.98

The object of this research is traditional retail consumers in Palembang City. Fig. 1 shows the methodology adopted for this study. First, the research focuses on reviewing journal literature related to traditional retail existence models, producing a research conceptual model, and compiling a questionnaire based on this conceptual model.

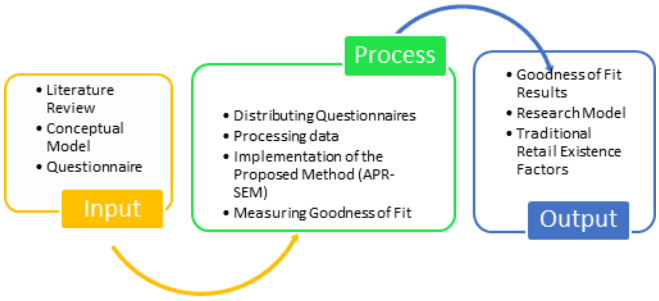


Fig. 1. Research methodology.

The conceptual model of purchasing decisions in traditional retail consists of four variables: exogenous variables: product, price, and place, and endogenous variables: purchasing decisions, as in Fig. 2.

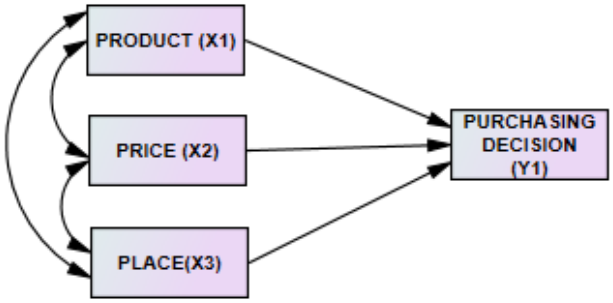


Fig. 2. Purchasing decision models in traditional retail.

Table V shows the indicators for each variable in this research.

TABLE V. INDICATORS OF EACH VARIABLE

Variable	Indicator	Code
Product (X1)	product availability	X11
	product variety	X12
	quality product	X13
	product packaging	X14
Price (X2)	price according to product quality	X21
	cheap price	X22
	discounts	X23
	bargaining price	X24
Place (X3)	comfortable and safe	X31
	clean	X32
	location	X33
	parking area	X34
Purchasing Decision (Y1)	self-interest	Y11
	make ends meet	Y12
	location near home	Y13
	time is not long	Y14
	social level	Y15

The questionnaires used Google Form media, and the data in this research used AMOS for SEM analysis and Jupyter Lab Python for the Apriori algorithm. The next step is to test the model's goodness of fit. One of the main challenges in SEM is a model's Goodness of Fit testing process, which evaluates how well a proposed model fits empirical data. These models, due to their complexity involving many variables and complex causal relationships, often take a long time to test, especially when they are highly complex.

IV. PROPOSED METHOD

This research proposes an APR-SEM method by integrating the Apriori algorithm in SEM analysis to overcome the challenges of this research model, which involves many variables, complex causal relationships, and testing processes. The Apriori algorithm is used in association analysis to find significant relationship patterns between variables. In the context of SEM, this algorithm can filter and identify variables with a significant relationship so that only relevant variables are included in the final model. So, Fig. 3 is a proposed method combining the Apriori algorithm into the SEM analysis technique with the following process.

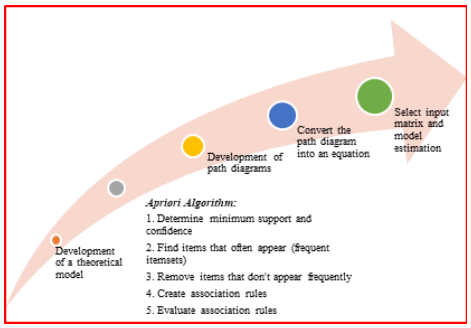


Fig. 3. Proposed method APR-SEM.

APR-SEM is an approach that combines the power of the Apriori algorithm to filter significant variables before use in an SEM model. This aims to:

1) Reduce the complexity of the SEM model by filtering out irrelevant variables.

2) Speed up achieving Goodness of Fit in the SEM model by looking for the strongest associations between variables.

Overall, this new method shows how the Apriori algorithm can be used upfront to filter out significant variables before inserting them into the SEM model, thereby speeding up and simplifying the SEM evaluation process.

V. Result and Discussion

A. Result

The stages in the SEM method are the development of a theoretical model. This stage builds a research model using an in-depth literature study related to research related to purchasing decisions in traditional retail. This stage produces consumer behaviour with the determining factors for purchasing decisions in traditional retail: price, product, and place variables. The next stage is the development of path diagrams. Before entering this stage, the Apriori algorithm will look for the strongest associations between the indicators in the research model. In this case, using Jupyter Lab Python, get the most robust association rule from the research variables. The results of the best rule association for each research variable are as in Table VI.

TABLE VI. Association Best Rule

Variable	Association Best Rule	Key Matric			
		Support	Confidence	Lift	Conviction
X1	X12→X11	98.4%	1.000	1.016	Inf.
	X11→X12	98.4%	1.000	1.016	Inf.
X2	X21→X22	59.8%	0.987	1.062	5.457
	X22→X21	59.8%	0.987	1.062	5.457
X3	X32→X31	98.4%	0.992	1.008	1.984
	X31→X32	98.4%	0.992	1.008	1.984
Y1	Y11→Y12	98.4%	1.000	1.008	Inf.
	Y12→Y11	98.4%	1.000	1.008	Inf.
	Y11→Y14	81.1%	0.824	1.016	1.073
	Y14→Y11	81.1%	0.824	1.016	1.073

The Apriori results will be compared between the conventional SEM results without Apriori and the proposed APR-SEM method for variable X1, as in Fig. 4.

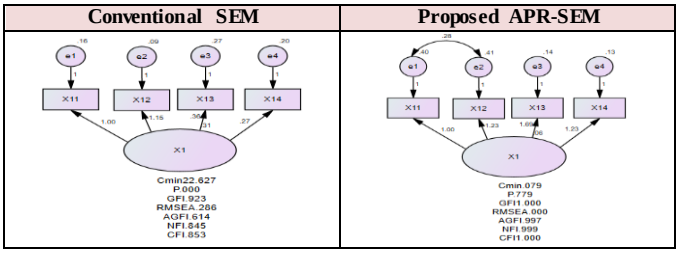


Fig. 4. The comparison of X1 results.

The goodness of fit results for variable X1, as in Table VII.

TABLE VII. Goodness of Fit Variable X1

Index	Cut off value	Conventional SEM	Proposed APR-SEM
GFI	> 0,90	0.923	1.000
RMSEA	< 0,08	0.286	0.000
AGFI	> 0,80	0.614	0.997
NFI	> 0,90	0.845	0.999
CFI	> 0,90	0.853	1.000

From the goodness of fit results of the product variable (X1), the goodness of fit results using the proposed Apriori-SEM method obtained results that all met the cut-off value.

The Apriori results will be compared between the conventional SEM results without Apriori and the proposed APR-SEM method for variable X2, as in Fig. 5.

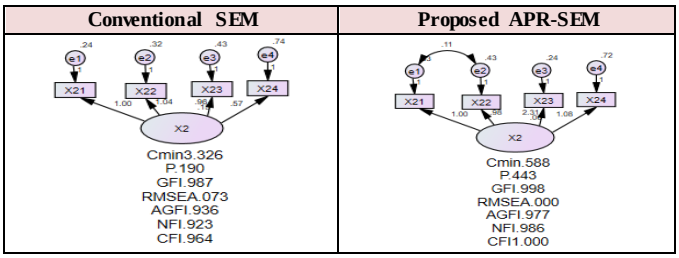


Fig. 5. The comparison of X2 results.

From the Apriori results, the best association rule is between variables X21 and X22, so there is a relationship between them in the path diagram. The goodness of fit results for variable X2, as in Table VIII.

TABLE VIII. Goodness of Fit Variable X2

Index	Cut off value	Conventional SEM	Proposed APR-SEM
GFI	> 0,90	0.987	0.998
RMSEA	< 0,08	0.073	0.000
AGFI	> 0,80	0.936	0.977
NFI	> 0,90	0.923	0.986
CFI	> 0,90	0.964	1.000

The goodness of fit results of the product variable (X2) using the proposed APR-SEM method obtained results that all met the cut-off value, the same as conventional SEM. But in this case, the P value in Fig. 5 is higher in the proposed APR-SEM model, namely 0.443, which shows that the model is better.

The Apriori results will be compared between the conventional SEM results without Apriori and the proposed APR-SEM method for variable X3, as in Fig. 6.

From the Apriori results, the best association rule is between variables X31 and X32, so there is a relationship between them in the path diagram. The goodness of fit results for variable X3, as in Table IX.

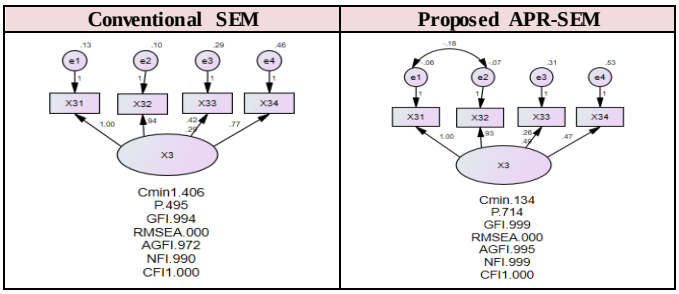


Fig. 6. The comparison of X3 results.

TABLE IX. GOODNESS OF FIT VARIABLE X3

Index	Cut off value	Conventional SEM	Proposed APR-SEM
GFI	> 0,90	0.994	0.999
RMSEA	< 0,08	0.000	0.000
AGFI	> 0,80	0.972	0.995
NFI	> 0,90	0.990	0.999
CFI	> 0,90	1.000	1.000

The goodness of fit results of the product variable (X3) using the proposed APR-SEM method obtained results that all met the cut-off value, the same as conventional SEM. But in this case, the P value in Fig. 6 is higher in the proposed APR-SEM model, namely 0.714, which shows that the model is better.

The Apriori results will be compared between the conventional SEM results without Apriori and the proposed APR-SEM method for variable Y1, as in Fig. 7. From the Apriori results, the best association rule is between variables Y11 and Y12 and also Y11 and Y14, so there is a relationship between them in the path diagram. The goodness of fit results for variable Y1, as in Table X.

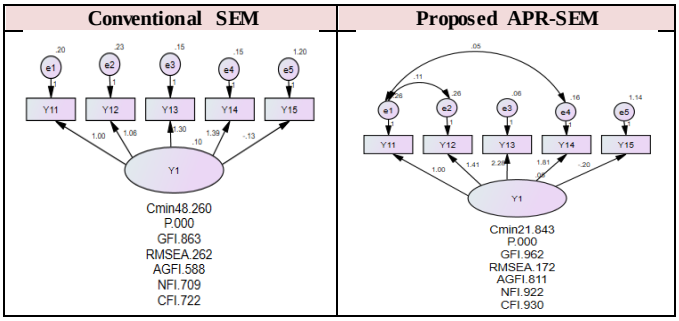


Fig. 7. The comparison of Y1 results.

TABLE X. GOODNESS OF FIT VARIABLE Y1

Index	Cut off value	Conventional SEM	Proposed APR-SEM
GFI	> 0,90	0.863	0.962
RMSEA	< 0,08	0.262	0.172
AGFI	> 0,80	0.588	0.811
NFI	> 0,90	0.709	0.922
CFI	> 0,90	0.722	0.930

The goodness of fit results of the purchasing decision variable (Y1) using the proposed Apriori-SEM method obtained results that all met the cut-off value except RMSEA, but this can be considered because the other indices have met. This is different from conventional SEM, which does not meet all requirements. This shows that the model is better.

Before describing the path diagram of the entire research model, it is necessary to convert it into equation form. The research model has latent variables (X1, X2, X3, and Y1) which are connected to several measurement variables such as X11, X12, X13, and X14 for X1 variable. X21, X22, X23, and X24 for X2 variable. X31, X32, X33, and X34 for X3 variable. Y11, Y12, Y13, Y14, and Y15 for Y1 variable. Convert the path diagram to an equation, namely:

1) Measurement model: X1 is determined by the indicators X11, X12, X13, and X14

$$X11 = \lambda_{11}X1 + e_1 \quad (1)$$

$$X12 = \lambda_{12}X1 + e_2 \quad (2)$$

$$X13 = \lambda_{13}X1 + e_3 \quad (3)$$

$$X14 = \lambda_{14}X1 + e_4 \quad (4)$$

X2 is determined by the indicators X21, X22, X23, and X24

$$X21 = \lambda_{21}X1 + e_5 \quad (5)$$

$$X22 = \lambda_{22}X1 + e_6 \quad (6)$$

$$X23 = \lambda_{23}X1 + e_7 \quad (7)$$

$$X24 = \lambda_{24}X1 + e_8 \quad (8)$$

X3 is determined by the indicators X31, X32, X33, and X34

$$X31 = \lambda_{31}X1 + e_9 \quad (9)$$

$$X32 = \lambda_{32}X1 + e_{10} \quad (10)$$

$$X33 = \lambda_{33}X1 + e_{11} \quad (11)$$

$$X34 = \lambda_{34}X1 + e_{12} \quad (12)$$

Y1 is determined by the indicators Y11, Y12, Y13, Y14, and Y15

$$Y11 = \lambda_{y11}Y1 + e_{13} \quad (13)$$

$$Y12 = \lambda_{y12}Y1 + e_{14} \quad (14)$$

$$Y13 = \lambda_{y13}Y1 + e_{15} \quad (15)$$

$$Y14 = \lambda_{y14}Y1 + e_{16} \quad (16)$$

$$Y15 = \lambda_{y15}Y1 + e_{17} \quad (17)$$

2) Structural model: Structural models explain the relationships between latent variables in the system. Y1 is influenced by X1, X2, and X3.

$$Y1 = \beta_{11}X1 + \beta_{12}X2 + \beta_{13}X3 + \xi_1 \quad (18)$$

3) Covariance between latent variables: The covariance between latent variables X1, X2, and X3 is written as the equation:

$$Cov(X1, X2) = \phi_{12} \quad (19)$$

$$Cov(X1, X3) = \phi_{13} \quad (20)$$

$$Cov(X1, X2) = \phi_{12} \quad (21)$$

So, the path diagram of the traditional retail purchasing decision research model is as in Fig. 8.

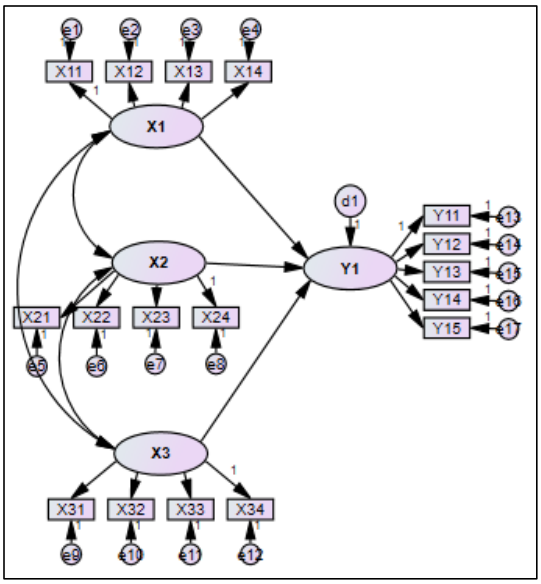


Fig. 8. Path diagram.

The next step is to choose the input matrix by selecting the Covariance Matrix or Correlation Matrix as the input data. After selecting the input matrix, determine the estimation method used. Maximum Likelihood (ML) is the default estimation method when using AMOS. After selecting the input matrix and estimation method, the next step is to run the analysis to obtain parameter estimates and model fit. The estimated calculation results from the research model using conventional SEM are shown in Fig. 9.

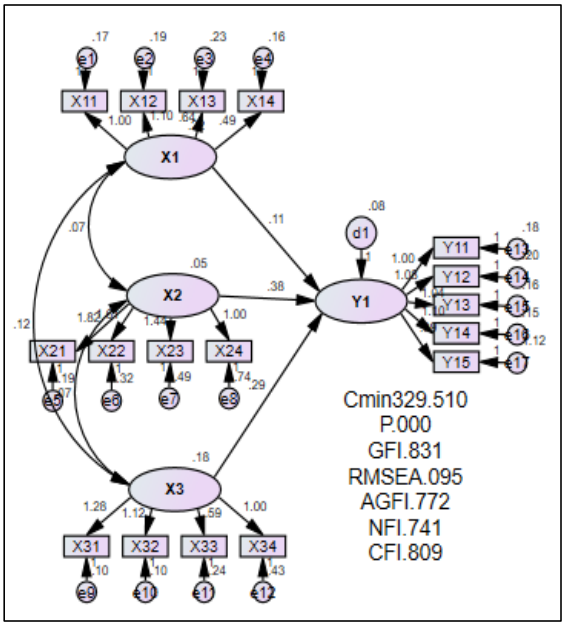


Fig. 9. The SEM conventional results.

From the Apriori results and modification of the path diagram model using AMOS, the calculated estimate results are in Fig. 10.

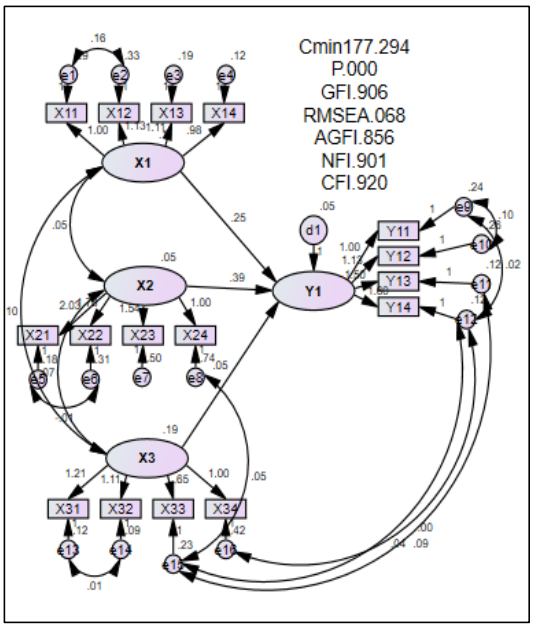


Fig. 10. The APR-SEM results.

From the Apriori results and the modification of the path diagram model using AMOS, the calculated estimate results meet the goodness of fit rules in conventional SEM and APR-SEM, as in Table XI.

TABLE XI. GOODNESS OF FIT FULL MODEL

Index	Cut off value	Conventional SEM	Proposed APR-SEM
GFI	> 0,90	0.831	0.906
RMSEA	< 0,08	0.095	0.068
AGFI	> 0,80	0.772	0.856
NFI	> 0,90	0.741	0.901
CFI	> 0,90	0.809	0.920

These results indicate that none of the measures of suitability when using conventional SEM are suitable. By adding the Apriori algorithm to find patterns or association rules between indicator variables and modifying the path diagram model using AMOS, the path diagram results for each variable X1, X2, X3, and Y1 obtained results that all met the cut-off value.

B. Discussion

From the results of research on the Goodness of Fit model using the APR-SEM method, it is stated that the purchasing decision model by traditional retail customers depends on three factors: product, price, and place. The model coefficient of determination value from APR-SEM is R^2 0.71, higher than the conventional model, R^2 0.52. Variable Y15, namely social level, has a value of 0 for the level of contribution to the model, so it is removed from the latent variable of the AMOS model. This is by the research results [30] and [31], which state that purchasing decisions at traditional retail are not based on a social level but

on consumer age, usually older, who is more likely to shop at traditional retailers.

This research also shows hidden relationships obtainedfrom association rules using the Apriori algorithm, namely the relationship between product availability and diversity, guaranteed product quality at low prices, and a comfortable, safe, clean place. Apart from that, there are four newcorrelations from the modification of the model from AMOS using Modification Indices. Namely, there is a relationship between the main tendencies of buyers in traditional retail because the retail location is close to home, and they can haggle over prices and not wait long for service. Besides that, there is a correlation between parking space availability for buyers who can be served quickly in traditional retail, such as shopping straight from their vehicle.

So, a clear agenda for future Structural Equation Modeling analysis to achieve the Goodness of Fit model (APR-SEM method) is to follow the following steps:

1) Development of a theoretical model
2) Evaluation of best association rules with the Apriori Algorithm
3) Development of path diagram
4) Convert the path diagram into an equation
5) Estimates goodness of fit model

VI. Conclusion

Combining the Apriori algorithm with the SEM method produces a more comprehensive analytical approach to understanding the relationships between variables and association patterns in the data. This can be seen from the purchasing decision model in traditional retail, which does not meet goodness of fit and becomes fit after adding the best association rules to the research model path diagram. The combination of SEM and Apriori allows the discovery of new insights that might have yet to be revealed if these two methods were used separately. For example, associations discovered by Apriori can lead to more in-depth modeling of structural relationships in SEM. This purchasing decision model in traditional retail will provide an analytical framework that helps in understanding the factors that influence the sustainability and competitiveness of traditional retail amidst market competition with modern retail and technological developments. This model will guide traditional retail owners in formulating appropriate strategies to increase their competitiveness, such as adaptingto consumer preferences, integrating technology, or improving service quality. However, combining these two methods, namely SEM and Apriori analysis, avoids including all associative patterns in SEM. Choose the most important relationships with strong theoretical or logical support. We cannot directly obtain goodness of fit in the model, but we must still modify the indices (MI) if necessary. However, be careful not to make modifications that violate the theory. Checkresidual correlations and eliminate non-significant relationships.

References

[1] AT Kerney, 'Global Retail Development Index', 2021. [Online]. Available: https://www.kearney.com/industry/consumer-retail/global-retail-development-index

[2] CEIC, 'Pertumbuhan Penjualan Ritel Indonesia', 2021. https://www.ceicdata.com/id/indicator/indonesia/retail-sales-growth

[3] PANRB, 'Indonesia Ritel Summit 2023 Dongkrak Pergerakan dan Tingkat Konsumsi Wisatawan', 2023. https://www.menpan.go.id/site/berita-terkini/berita-daerah/indonesia-ritel-summit-2023-dongkrak-pergerakan-dan-tingkat-konsumsi-wisatawan

[4] H. Chaniago, I. Mulyawan, T. Suhaeni, and R. Jumiyani, 'Faktor Kunci Keberhasilan Ritel Modern Di Indonesia', Jurnal Akuntansi, Ekonomi dan Manajemen Bisnis, vol. 7, no. 2, pp. 201–208, 2019, doi: 10.30871/jaemb.v7i2.1726.

[5] A. Tohri, M. Mastur, H. Habibuddin, H. Syamsiar, and L. Parhanuddin, 'Dampak Sosial dan Ekonomi Ritel Modern (Alfamart dan Indomaret) Terhadap UMKM di Lombok Timur', RESIPROKAL: Jurnal Riset Sosiologi Progresif Aktual, vol. 5, no. 1, pp. 45–56, 2023, doi: 10.29303/resiprokal.v5i1.280.

[6] P. S. Arimawa and F. Leasiwal, 'Dampak Keberadaan Pasar Modern Terhadap Eksistensi Pasar Tradisional Di Kota Tobelo Kabupaten Halmahera Utara', Jurnal Pundi, vol. 2, no. 3, pp. 287–292, 2018, doi: 10.31575/jp.v2i3.100.

[7] Z. Muhzinat and S. Achiria, 'Dampak Keberadaan Minimarket terhadap Toko Kelontong di Pasar Klampis Kabupaten Bangkalan Madura', IQTISHADIA Jurnal Ekonomi & Perbankan Syariah, vol. 6, no. 2, pp. 203–211, 2019, doi: 10.19105/iqtishadia.v6i2.2448.

[8] U. S. D. of Agriculture, 'Ritel Tradisional Dominasi Usaha Penjualan Eceran di Indonesia', 2022. [Online]. Available: https://databoks.katadata.co.id/datapublish/2022/07/12/ritel-tradisional-dominasi-usaha-penjualan-eceran-di-indonesia

[9] D. Novita and E. Ermatita, 'Implementation Knowledge Management for Knowing the Factors That Have Influenced Income for Traditional Retail', in Proceeding of International Conference of Health, Science and Technology, 2021, pp. 260–263. [Online]. Available: https://ojs.udb.ac.id/index.php/icohetech/article/view/1137/977

[10] C. Ronceros, J. Medina, P. León, A. Mendieta, J. Fernández, and Y. Martinez, 'Knowledge Management Model for the Generation of Innovative Capacities in Organizations that Provide Services', International Journal of Advanced Computer Science and Applications, vol. 14, no. 5, pp. 423–430, 2023, doi: 10.14569/IJACSA.2023.0140545.

[11] Muflihatul Fauza, 'Analisis Faktor Yang Mempengaruhi Eksistensi Ritel Tradisional Dalam Menghadapi Ritel Modern Di Kecamatan Medan Amplas', At-Tawassuth, vol. 2, no. 1, pp. 146–169, 2017.

[12] J. J. Rodríguez-Delgado, P. López-Casaperalta, M. G. Berrios-Espezúa, A. M. Acosta-Quelopana, and J. Sulla-Torres, 'Digital Learning Tools for Security Inductions in Mining Interns: A PLS-SEM Analysis', International Journal of Advanced Computer Science and Applications, vol. 13, no. 5, pp. 530–536, 2022, doi: 10.14569/IJACSA.2022.0130562.

[13] M. I. Akazue et al., 'Handling Transactional Data Features via Associative Rule Mining for Mobile Online Shopping Platforms', International Journal of Advanced Computer Science and Applications, vol. 15, no. 3, pp. 530–538, 2024, doi: 10.14569/IJACSA.2024.0150354.

[14] M. A. Rizaty, 'Jumlah Toko Retail Indonesia Mencapai 3,61 Juta pada 2021', dataindonesia.id, 2023. https://dataindonesia.id/industri-perdagangan/detail/jumlah-toko-retail-indonesia-mencapai-361-juta-pada-2021 (accessed Jul. 02, 2023).

[15] D. Januaji, 'Mau Buka Toko Kelontong? 10 Barang Ini Wajib Ada', ottopay.id, 2023.

[16] T. H. Putra, 'Toko Kelontong Tradisional Dalam Era Teknologi Bisnis Digital', vol. 2, no. 3, 2023.

[17] S. Lestari, B. A. Yani, and I. A. DPW, 'Analisis Perbedaan Persepsi Konsumen Minimarket Modern dan Toko Kelontong di Desa Kartonatan, Kartasura, Sukoharjo', Edunomika, vol. 5, no. 2, pp. 1032–1037, 2021, [Online]. Available: https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf

[18] S. T. Ha, M. C. Lo, M. K. Suaidi, A. A. Mohamad, and Z. Bin Razak, 'Knowledge management process, entrepreneurial orientation and performance in smes: Evidence from an emerging economy', Sustainability (Switzerland), vol. 13, no. 17, 2021, doi: 10.3390/su13179791.

[19] P. Pitakkornrat and P. Pongsiri, 'A Structural Equation Model of Knowledge Management Strategy to Develop Best Practice for Industrial Business in Thailand', Academy of Strategic Management Journal, vol. 19, no. 2, pp. 1–13, 2020.

[20] F. Ibrahim, B. S. Putra, F. H. Azhra, and N. Fadhlurrohman, 'Analysis of Marketing Strategy at Setia Stores Using AHP, Clustering, and AR-Mba Method', International Journal of Industrial Optimization, vol. 2, no. 2, p. 125, 2021, doi: 10.12928/ijio.v2i2.4369.

[21] B. Melović, M. Dabić, M. Vukčević, D. Ćirović, and T. Backović, 'Strategic Business Decision Making : The Use and Relevance of Marketing Metrics and Knowledge Management', Journal of Knowledge Management, vol. 25, no. 11, pp. 175–202, 2021, doi: 10.1108/JKM-10-2020-0764.

[22] A. R. Wibowo and A. Jananto, 'Implementasi Data Mining Metode Asosiasi Algoritma FP-Growth Pada Perusahaan Ritel', Inspiration: Jurnal Teknologi Informasi dan Komunikasi, vol. 10, no. 2, p. 200, 2020, doi: 10.35585/inspir.v10i2.2585.

[23] R. Takdirillah, 'Penerapan Data Mining Menggunakan Algoritma Apriori Terhadap Data Transaksi Sebagai Pendukung Informasi Strategi Penjualan', Edumatic : Jurnal Pendidikan Informatika, vol. 4, no. 1, pp. 37–46, 2020, doi: 10.29408/edumatic.v4i1.2081.

[24] C. L. Yang, C. Y. Huang, and Y. H. Hsiao, 'Using Social Media Mining and PLS-SEM to Examine The Causal Relationship Between Public Environmental Concerns and Adaptation Strategies', International Journal of Environmental Research and Public Health, vol. 18, no. 10, 2021, doi: 10.3390/ijerph18105270.

[25] J. T. Thorson et al., 'Identifying Direct and Indirect Associations Among Traits by Merging Phylogenetic Comparative Methods and Structural Equation Models', Methods in Ecology and Evolution, vol. 14, no. 5, pp. 1259–1275, 2023, doi: 10.1111/2041-210X.14076.

[26] X. Lai, S. Zhang, N. Mao, J. Liu, and Q. Chen, 'Kansei engineering for new energy vehicle exterior design: An internet big data mining approach', Computers and Industrial Engineering, vol. 165, no. June 2021, p. 107913, 2022, doi: 10.1016/j.cie.2021.107913.

[27] M. A. Muslim et al., Data Mining Algoritma C4.5, Cetakan Pe. Semarang, 2019.

[28] J. J. Thakkar, Structural equation modelling: Application for research and practice (with AMOS and R), vol. 285. 2020. doi: 10.1007/978-981-15-3793-6_1.

[29] T. L. Wiemken, S. P. Furmanek, W. A. Mattingly, J. Haas, J. A. Ramirez, and R. M. Carrico, 'Googling your hand hygiene data: Using Google Forms, Google Sheets, and R to collect and automate analysis of hand hygiene compliance monitoring', American Journal of Infection Control, vol. 46, no. 6, pp. 617–619, 2018, doi: 10.1016/j.ajic.2018.01.010.

[30] I. Rakasyifa and G. W. Mukti, 'Faktor-Faktor Yang Mempengaruhi Keputusan Pembelian Sayur dan Buah Di Ritel Online (Suatu Kasus Pada Konsumen Ritel Online Di Jakarta)', Jurnal Pemikiran Masyarakat Ilmiah Berwawasan Agribisnis, vol. 6, no. 1, pp. 275–289, 2020.

[31] S. I. Isnawati and A. Purwanto, 'Generation Z Buying Behaviour Analysis of Retail Business Opportunities', Ilmiah Bisnis, Manajemen dan Akuntansi, vol. 2, no. 2, pp. 11–21, 2022, doi: http://dx.doi.org/10.35.

Optimizing Energy Efficient Cloud Architectures for Edge Computing: A Comprehensive Review

TA Gamage*, Indika Perera
Department of Computer Science and Engineering, University of Moratuwa, Sri Lanka

***Abstract*—Now-a-days, edge computing and cloud computing are considered for collaborating together to produce computing solutions that are more effective, scalable and adaptable. The proliferation of cloud infrastructures has drastically increased energy consumption leading to the need for more research in optimizing energy efficiency for sustainable and efficient systems with reduced operational costs. In addition, the edge computing paradigm has gained wide attention during the last few decades due to the rise of the Internet of Things (IoT) devices, the emergence of applications that require low latency, and the widespread demand for environmentally friendly computing. Moreover, lowering cloud-edge systems' energy footprints is essential for fostering sustainability in light of growing concerns about environmental effects. This research presents a comprehensive review of strategies aimed at optimizing energy efficiency in cloud architectures designed for edge computing environments. Various strategies, including workload optimization, resource allocation, virtualization technologies, and adaptive scaling methods, have been identified as techniques that are widely utilized by contemporary research in reducing energy consumption while maintaining high performance. Furthermore, the paper investigates how advancements in machine learning and AI can be leveraged to dynamically manage resource distribution and energy-efficient enhancements in cloud-edge systems. In addition, challenges to the approaches for energy optimization have been discussed in detail to further provide insights for future research. The conducted comprehensive review provides valuable insights for future research in the edge computing paradigm, particularly emphasizing the critical importance of enhancing energy efficiency in these systems.**

Keywords*—*Cloud computing; edge computing; energy efficiency; sustainability

I. Introduction

Cloud computing is a concept for providing computer resources such as servers, storage, databases, networking, software, and analytics over the internet. Users can obtain physical infrastructure and data centers on-demand from cloud service providers, negating the need to own and manage them and providing more flexibility, scalability, and cost-efficiency. Without the upfront expenses and hassles of maintaining traditional IT systems, cloud computing allows businesses and individuals to scale their IT needs as needed, covering everything from data storage to sophisticated application development [1] [2] [3].

The adaptability of cloud technology is one of its most intriguing features. Businesses can simply reallocate their computer resources to meet changing demands, allowing for ongoing scaling in response to changing business requirements. Global accessibility is yet another fundamental benefit of cloud computing. Moreover, cloud services reduce geographical barriers, enabling real-time collaboration across several regions and supporting the delivery of services to a global clientele with less idle time [2].

Edge computing is a distributed computing paradigm that moves data storage and computation closer to the point of demand, which is generally at the network's edge, close to the data generating source. Edge computing reduces latency, bandwidth utilization, and reaction times by processing data locally on IoT sensors, gateways, or edge servers rather than depending on a centralized cloud [4], [5]. This method is more efficient for time-sensitive applications where rapid decisions are essential, like real-time analytics, industrial automation, and driverless cars. Edge computing improves performance, security, and dependability in a variety of applications with the use of decentralized computing [6], [7].

Cloud computing has revolutionized the way businesses and organizations operate, offering scalable, on-demand computing resources. Nevertheless, the growth of cloud infrastructures has increased their energy consumption that has been a major concern. Therefore, the demand for energy-efficient cloud architectures has become a critical area of research due to environmental concerns, operational costs, and the need for sustainability. In addition, the proliferation of edge computing where data is processed closer to the data source to reduce latency and bandwidth usage adds another dimension to cloud energy optimization [8], [9].

The rapid growth of energy consumption by edge cloud computing infrastructures has been a significant focus of contemporary research considering the operational costs and environmental concerns aiming at the sustainability of cloud computing architectures. Among the approaches for a sustainable edge computing paradigm, dynamic resource allocation, AI driven energy optimization, energy-aware scheduling and load balancing, green data centres, virtualizations and containerizations are acquiring significant focus by the researchers [10], [11], [12], [13].

Nevertheless, the exponential growth of cloud computing infrastructures has resulted in inflated demand for further research on optimizing energy efficient cloud architectures in order to move towards a sustainable edge computing paradigm. In addition, maintaining performance and scalability while reducing energy consumption has also been a controversial topic that is further researched [14] [15]. Therefore, further research that enhance the green cloud architectures for edge

The open-access publication fee of this paper is supported by the SRC publication fee scheme of the University of Moratuwa

computing are required for the improved sustainability of the cloud computing paradigm.

The rest of the paper is laid out as follows. Section II discusses approaches that have been widely concerned to achieve sustainability in the edge computing paradigm focusing on energy efficiency while Section III broadly explores recent related work that makes use of different strategies for energy efficiency in the edge computing paradigm. Section IV provides a discussion of the conducted review work along with challenges and further insights into the energy-efficient approaches in the edge computing domain. Finally, Section V concludes the research findings along with future directions for the conducted research work.

II. Strategies for Energy Optimization

The following strategies were identified as the main approaches that are widely focused in research that aim at energy optimizations in edge computing. Nevertheless, the techniques that are utilized for edge computing and even in the cloud computing paradigm in contemporary research are a combination of the below-discussed approaches.

A. Energy Aware Scheduling and Load balancing

Energy-aware scheduling and Load Balancing in edge computing aims to optimize resource allocation while reducing energy consumption. In the context of an edge environment, resources are distributed across a number of small, geographically separated devices, requiring efficient scheduling algorithms to manage tasks without overloading nodes or consuming excessive amounts of energy [16], [17]. Energy-aware scheduling approaches prioritize tasks based on their energy demands and resource requirements, ensuring that high-priority tasks are executed on energy-efficient nodes while low-priority tasks are deferred across less critical resources. By optimizing task scheduling, systems can minimize energy wastage, extend device lifespans, and ensure seamless service delivery [18] [19].

Load balancing complements energy-aware scheduling by distributing computational workloads evenly across available nodes to prevent resource overuse and reduce energy consumption. In edge computing, load balancing techniques must consider not only the computational capacity of each node but also its current energy state. Dynamic load balancing ensures that tasks are allocated to nodes with sufficient energy reserves, minimizing the risk of node failure due to energy depletion. These approaches improve the efficiency and sustainability of edge computing setups, enabling them to support more applications and services without overwhelming the energy resources of distributed nodes [20] [21].

B. AI-Driven Energy Optimization

AI-driven energy optimization approaches that are utilized in Edge computing incorporate artificial intelligence strategies to improve the energy efficiency of edge networks and devices, which are frequently decentralized and resource-constrained. AI algorithms, in particular deep learning and machine learning, are able to track and forecast edge device energy consumption and task trends [22]. AI systems are able to make decisions about how best to assign jobs to nodes, modify power settings, and dynamically manage resource utilization based on needs by evaluating real-time data. With this real-time optimization, energy conservation is guaranteed without compromising the necessary performance and service levels.

AI can also provide intelligent load balancing and scheduling, which will optimize the energy consumption of edge computing systems. AI models, for instance, can anticipate high load periods and move workloads to nodes that use less energy or have unused resources. AI algorithms can also allow edge devices to transition into low-power modes while they are inactive or when processing demands drop, which will cut down unnecessary energy consumption. AI-driven energy optimization may dramatically increase the lifespan of edge devices, slash operating costs, and lessen the environmental effect of edge computing infrastructures by continually learning from and reacting to the system [23] [24].

C. Virtualization and Containerization

Virtualization and Containerization in edge computing play a significant role in improving resource usage, flexibility, and scalability of edge networks. Several Virtual Machines (VMs) can operate on a single physical server owing to virtualization, which makes it possible to abstract hardware resources. This makes it possible to consolidate edge resources and execute various applications or services in separate environments, making the best use of the hardware that is available. Virtualization assists in the management of various workloads and offers the flexibility to dynamically scale resources in response to variations in demand in edge computing [25], [26]. In addition, it makes it possible to handle software upgrades and system maintenance effectively without interfering with ongoing services that in turn increase system reliability.

Nevertheless, containerization, which bundles apps and their dependencies into containers, is a less complex substitute for virtualization. Since containers share the host operating system kernel, containers are more efficient than VMs in terms of startup times and overhead. Moreover, containerization facilitates the quick deployment and scalability of applications among dispersed nodes in edge computing. Due to its great degree of mobility, moving apps between various edge devices or contexts is much simpler. This is especially critical in edge environments, which are dynamic and heterogeneous and have a wide range of device capabilities [27], [28], [29]. Therefore, it can be stated that containerization is a perfect solution for the changing needs of edge computing since it allows for quicker application development cycles, better system responsiveness, and more effective resource management.

D. Network Optimization

Network optimizations in edge computing primarily aims to reduce latency, enhance bandwidth efficiency, and improve overall performance by bringing data processing and storage closer to end devices, such as IoT sensors or mobile users. By decentralizing computing power, edge computing reduces the amount of data that needs to be sent to central cloud data centers, minimizing delays in data transmission [30], [31]. Techniques like adaptive routing allow the network to choose the optimal path for data, considering real-time conditions such as congestion, which improves response times [32].

Moreover, Dynamic Voltage and Frequency Scaling (DVFS) is another approach in network optimization for energy efficiency that reduces energy consumption when full performance is not needed by adjusting the power consumption of networking devices depending on real-time demands [33], [34]. Network Function Virtualization (NFV) is also widely researched as an efficient approach for network optimization for energy efficiency in edge computing as it enables the operation of several network services on a single physical server, which eliminates the need for specialized hardware [35]. Adaptive transmission power control [36], [37] and the application of energy-efficient communication protocols [38], such as the enhanced energy efficiency features of 5G [39] are other approaches that wireless networks can reduce overall power consumption. Therefore, these approaches can significantly lower the energy footprint of networks without sacrificing the performance by following the network optimization techniques discussed above.

E. Green Data Centers

Edge data centers are typically smaller and distributed, which makes traditional data center energy efficiency techniques less applicable. By utilizing sustainable methods like the usage of renewable energy sources, cutting-edge cooling systems, and energy-efficient hardware, green data center features aim to reduce their environmental impact for sustainable and green data centers [40], [41]. The transition towards greener operations decreases carbon footprints and operational expenses, making these data centers a crucial element of sustainable IT infrastructure.

In contemporary research, other than the shift towards renewable energy sources in data centers that assists in reducing dependency on the grid, automation techniques, low power consuming electric equipment, and devices with extended thermal limits have also been incorporated in order to improve sustainability and to move towards green data centers [42]. In addition, thermal energy harvesting, kinetic energy and hybrid systems have also been noted in data centers to improve the resilience, and contribute to more sustainable and energy efficient infrastructures.

III. RECENT WORK

The authors in study [43] have conducted a comprehensive analysis of energy consumption across various cloud-related architectures, including cloud, fog, and edge computing. It introduces a taxonomy that categorizes these architectures based on their characteristics, such as the number and role of data centers and their connectivity. The authors propose a generic energy model that accurately estimates and compares the energy consumption of these infrastructures, taking into account factors like cooling systems and network devices. The findings of this research work indicate that fully distributed architectures can consume significantly less energy between 14% and 25% compared to centralized and partly distributed architectures, highlighting the importance of energy efficiency in the design and deployment of modern computing solutions. In summary, the study aims to provide a foundational framework for future research in energy consumption analysis within the evolving landscape of cloud computing technologies. However, while the proposed model effectively highlights architectural differences and provides insights into energy efficiency, it may benefit from more consideration of real-world variables, such as the uneven distribution of end users and the impact of varying application workloads on energy consumption. In addition, the reliance on existing simulators, which have their limitations, could affect the accuracy of the results.

Another group of researchers in study [13] have presented a novel framework that employs Deep Reinforcement Learning (DRL) to optimize workflow scheduling in edge-cloud computing environments, specifically targeting the challenges introduced by the proliferation of IoT devices. Traditional cloud architectures often struggle with the demands of IoT applications due to issues like high latency and limited bandwidth. This study aims to address these challenges by balancing the conflicting objectives of minimizing energy consumption and execution time while ensuring that workflow deadlines are met. The proposed DRL technique demonstrates significant improvements over baseline algorithms, achieving 56% better energy efficiency and 46% faster execution times. Key innovations include a hierarchical action space that distinguishes between edge and cloud nodes, as well as a multi-actor framework that enhances the learning process by allowing separate networks to manage task allocation. The results indicate that this approach is particularly effective for latency-sensitive applications, such as video surveillance, where efficient resource management is critical. Overall, the research highlights the potential of DRL in optimizing resource allocation and scheduling in edge-cloud environments, providing valuable insights for future advancements in this rapidly evolving field.

The researchers of study [11] address the crucial issue of resource allocation in cloud computing, particularly in the context of increasing energy consumption and performance demands on data centers. The authors propose a hybrid model that combines Genetic Algorithms (GA) and Random Forest (RF) techniques to optimize the allocation of VMs to physical machines (PMs). The GA is employed to generate an optimized training dataset that maps VMs to PMs, which is then utilized by the RF for classification and allocation tasks. This approach aims to minimize power consumption while maximizing resource utilization and maintaining load balance across the data center. The effectiveness of the proposed model is evaluated using real-time workload traces from PlanetLab, showing significant improvements in energy efficiency and execution time compared to traditional methods. The study contributes to the existing body of knowledge by demonstrating the potential of hybrid optimization techniques in enhancing cloud infrastructure management. However, the authors acknowledge the need for further research to assess the model's adaptability to diverse workloads and its scalability in heterogeneous cloud environments.

The research in [10] introduces an Energy-Efficient Task Offloading Strategy (ETOS) aimed at enhancing energy efficiency in Mobile Edge Computing (MEC) environments for resource-intensive mobile applications. The study formulates the task offloading problem as a non-linear optimization challenge, proposing a hybrid approach that combines Particle Swarm Optimization (PSO) and Grey Wolf Optimizer (GWO)

to effectively allocate resources while considering capacity and latency constraints. The proposed ETOS leverages the collaborative capabilities of MEC servers to minimize energy consumption during task execution. Extensive simulations demonstrate that ETOS outperforms existing baseline methods in terms of energy utilization, response delay, and offloading utility, particularly under limited resource conditions. Despite its promising results, the research highlights the need for real-world validation and addresses the potential complexity of implementing the hybrid optimization approach in practical scenarios, suggesting directions for future work to enhance applicability and effectiveness in real-world MEC systems.

The research in study [12] focuses on developing a novel multi-classifier algorithm aimed at optimizing energy-efficient task offloading in Fog Computing environments for IoT applications. As the number of connected devices increases, efficient resource management becomes crucial to minimize energy consumption and enhance service quality. The proposed algorithm evaluates various attributes related to tasks, network conditions, and processing capabilities of Fog nodes to determine the most suitable node for task execution. By leveraging machine learning techniques, the algorithm aims to improve decision-making processes regarding task offloading, thereby reducing execution time and energy usage. The study emphasizes the importance of balancing energy efficiency with performance metrics, demonstrating that the multi-classifier approach can significantly enhance Quality of Service (QoS) parameters. In summary, this research contributes to the ongoing efforts to optimize Fog Computing frameworks, making them more effective in handling the computational demands of IoT applications while addressing energy constraints.

The authors of study [44] propose a novel framework to optimize energy consumption and computational efficiency in IoT environments. It introduces a three-layer architecture comprising sensor, edge, and cloud layers, facilitating effective task offloading and resource management. The study employs Long Short Term Memory (LSTM) networks for accurate workload prediction, enabling the system to adapt to dynamic conditions. Additionally, it utilizes Lyapunov optimization methods to address the non-convex nature of resource allocation problems. Simulation results demonstrate significant improvements in energy efficiency and processing rates. However, the research acknowledges limitations, including concerns about scalability, the assumptions made regarding user behavior, and a lack of focus on security aspects. Therefore, the paper contributes valuable insights into mobile edge computing, highlighting the potential for enhanced performance in IoT networks while suggesting areas for further exploration and refinement.

The research of [22] presents the Edge Intelligent Energy Consumption Model (ECMS) aimed at optimizing energy usage in MEC environments. As energy consumption in edge data centers becomes increasingly critical, the ECMS model provides a framework for predicting and managing energy needs based on varying workloads, including CPU-intensive, Web transactional, and I/O-intensive tasks. The authors validate the model through experimental results, demonstrating its superior performance in accuracy and training time compared to existing models like TW BP PM and FSDL. The study categorizes energy consumption modeling into two main approaches: system resource utilization and Performance Monitor Counter (PMC)-based modeling. The ECMS model leverages a simpler network topology and lower input dimensions, resulting in reduced training time and CPU workload during execution. The findings indicate a strong correlation between energy consumption and CPU utilization, emphasizing the need for precise energy models to inform optimization algorithms. The research concludes with future directions, suggesting the extension of the ECMS model to mixed workloads and integration with advanced AI/ML techniques, such as reinforcement learning, to further enhance energy efficiency in edge computing environments, ultimately contributing to sustainable practices in the industry.

A technical analysis on service placement approaches in the context of edge computing has been focused by the authors [45] with the aim of addressing energy efficiency in edge computing paradigm in IoT systems. The main objective of this research work has been to identify the effective and efficient strategies for service placement in IoT environments along with a taxonomy to categorize the studies in this field and in terms of cloud edge service placement approaches and algorithms that have been utilized. In addition to the technical analysis, a statistical analysis has also been provided by the authors along with evaluation factors to which the research findings provide further insights on future research in this paradigm. The results suggest that the server placement approaches fall under three types of categories, namely, decentralized, centralized and hierarchical while Genetic Algorithm has been widely utilized by researchers compared to other machine learning algorithms such as Greedy, Markov, BSAP, Topsis and Polynomial algorithms. Furthermore, time, cost, and latency evaluation metrics have been identified as the most concerned evaluation metrics in the context of service placement. Finally, the authors provide insights on to open issues and challenges in the context of service placement that is vital for future research focusing on service placement.

The research in study [19] presents a heterogeneous cluster-based wireless sensor network (WSN) model aimed at optimizing task allocation to minimize energy consumption and balance load. The network consists of clusters, each with a cluster center and several sensor nodes, where the cluster center collects data from the nodes and communicates with a central processor. The study establishes a task model where complex tasks are divided into independent subtasks, each requiring specific resources, data sizes, and computation times. To address the task allocation problem, the authors propose a Fusion Algorithm (FA) that integrates Genetic Algorithm (GA) and Ant Colony Optimization (ACO) techniques. This algorithm features a novel mutation operator and a new population initialization method, enhancing its effectiveness in reducing energy consumption and balancing the load across the network. Experimental results demonstrate that the FA outperforms traditional GA, achieving 8.1% lower energy consumption and significantly reducing the load on both sensor nodes and cluster centers. The proposed approach ensures all sensors remain operational throughout task execution, thereby increasing the reliability and longevity of the WSN. Therefore,

the research contributes valuable insights into efficient task allocation strategies in edge computing environments.

The researchers of study [46] investigate an RIS-assisted Non-Orthogonal Multiple Access (NOMA) Mobile Edge Computing (MEC) network, focusing on minimizing energy consumption for users. The authors propose a joint optimization approach that includes RIS phase shifts, data transmission rates, power control, and transmission time. Due to the non-convex nature of the problem, the authors decompose it into two sub-problems: firstly, utilizing a dual method for a closed-form solution with a fixed RIS phase vector, and the other employing a penalty method for suboptimal power control solutions. The optimization process alternates between these sub-problems until convergence is achieved. To demonstrate the effectiveness of their proposed NOMA-MEC scheme, the authors compare it against three benchmark schemes: TDMA-MEC partial offloading, full local computing, and full offloading. These researchers have also introduced an alternating 1-D search method for optimizing RIS phase shifts in the TDMA-MEC scheme. Numerical results indicate that the proposed scheme significantly reduces overall energy consumption and highlights the impact of user distance on performance. The paper concludes by acknowledging the potential for future work on robust transmission design to address channel state information estimation errors.

Another group of researchers in [47] have worked on a deep reinforcement learning (DRL) approach for delay-aware and energy-efficient computation offloading in dynamic MEC networks with multiple users and servers. The primary objective is to maximize the number of tasks completed before their deadlines while minimizing energy consumption. The proposed DRL model operates in an end-to-end manner, eliminating the need for post-action optimization functions, and can handle a large action space without relying on traditional optimization methods. The study formulates the offloading problem as a Markov Decision Process (MDP), capturing the complexity of the MEC system by incorporating time-varying channel conditions and various task profiles. Extensive simulations demonstrate that the proposed DRL model significantly outperforms existing DRL models and greedy algorithms in terms of task completion and energy efficiency. The results indicate that the DRL model learns optimal policies over time, effectively managing the trade-off between exploration and exploitation during training. The conducted research highlights the potential of DRL in enhancing the performance of MEC systems, making it a valuable contribution to the field of IoT and edge computing.

The research in [48] presents a novel approach to enhance task offloading in dynamic vehicular environments. It addresses the limitations of existing centralized and decentralized Deep Reinforcement Learning (DRL) algorithms, which often struggle with computational constraints and coordination issues. The proposed framework introduces a multi-layer Vehicular Edge Computing (VEC) architecture that optimizes task management across vehicles, edge servers, and cloud resources. Key contributions include the development of an energy-efficient VEC framework that considers the diverse computing capabilities of network entities and introduces a utility function to enhance energy efficiency. Additionally, a decentralized Multi-Agent Deep Reinforcement Learning (MADRL) algorithm is proposed, which effectively adapts to changing conditions while minimizing latency and maximizing task completion rates. The research also provides a comprehensive performance evaluation using simulations in a realistic environment, demonstrating the effectiveness of the proposed solution in managing varying traffic densities. The conducted research highlights the potential of decentralized approaches in improving the efficiency and responsiveness of vehicular networks, paving the way for advancements in autonomous vehicle applications and real-time data processing.

The research in [24] presents a novel cloud-edge cooperative content-delivery strategy aimed at minimizing network latency in asymmetrical Internet of Vehicles (IoV) environments. By leveraging Deep Reinforcement Learning (DRL), the authors propose a Deep Q Network (DQN) policy that optimizes content caching and request routing based on perceptive request history and current network states. The study formulates the joint allocation of heterogeneous resources as a queuing theory-based delay minimization objective, addressing the challenges of computation complexity and dynamic network conditions. Extensive simulations demonstrate that the proposed strategy significantly reduces network latency compared to existing solutions, showcasing its adaptability to varying user requirements and network states. The findings indicate that the DQN model achieves fast convergence and improved performance across different scenarios. The paper concludes with a discussion on future work, including the exploration of end-user mobility and deeper collaboration among mobile users, edge, and cloud networks to enhance overall Quality of Experience (QoE) while balancing network delay and energy consumption. This research contributes valuable insights into optimizing resource allocation in IoT-edge-cloud systems, particularly in the context of intelligent transportation systems.

Table I illustrates a summary of the recent work that were discussed in detail under objective, approach, key findings and remarks of the particular research work.

TABLE I. SUMMARY OF THE LITERATURE REVIEW

Reference	Objective	Approach	Findings	Remarks
[43]	To evaluate and compare energy consumption of Cloud, Fog, and Edge computing infrastructures	A taxonomy of different cloud architectures and a generic energy model	Fully distributed architectures consume 14%-25% less energy than centralized ones	Model may not account for real-world variables and simulator constraints
[13]	Energy-efficient resource scheduling in edge cloud environment	Deep Reinforcement Learning	• Energy consumption (56% of improvement) • Execution time (46% of improvement)	The proposed reinforcement learning framework is designed to operate in a centralized manner
[11]	Optimize virtual machine allocation in cloud infrastructure, aiming to minimize power consumption while maintaining load balance and maximizing resource utilization	Genetic Algorithm (GA) and Random Forest (RF) techniques	• Execution Time (37% of reduction) • Resource Utilization (11% Improvement)	Limited generalizability due to specific workload traces, complexity in real-world implementation, and potential oversight of other critical factors
[10]	Propose a task offloading scheme that minimizes the overall energy consumption along with satisfying capacity and delay requirements	Hybrid approach established based on Particle Swarm Optimization (PSO) and Grey Wolf Optimizer (GWO)	The proposed strategy considerably outperforms other baseline approaches, such as OEOS, ROA-DPH, ATO, and Local execution in terms of energy consumption, execution time, and offloading utility	Lacks real-world validation and may face implementation complexity in resource-constrained environments
[12]	Propose a novel energy-efficient task offloading method for IoT, Fog, and Cloud computing paradigms	Multi classifier-based approach	• Energy Consumption (11.36% of reduction) for Cloud-only • Energy Consumption (9.30% of reduction) for edge-ward • Network usage (67% of reduction) for Cloud-only • Network usage (96% of reduction) for edge-ward	Lacks extensive empirical validation and does not address decentralized approaches for dynamic environments
[44]	Propose a hierarchical communication and computation framework for jointly optimizing energy consumption and computation rate is proposed	The Long Short Term Memory (LSTM) network	The proposed method can greatly improve system performance by saving energy costs and achieving a high processing rate	Scalability concerns, assumptions about user behavior, limited security focus, and complexity in practical implementation
[22]	Predicting energy consumption and monitor edge servers	Intelligent energy modeling approach that combines Elman Neural Network (ENN)	The proposed ECMS outperforms the baseline power models (FSDL, CMP, TW_BP_PM, AEC, CUBIC, Power regression)	The research primarily focuses on specific workloads, limiting its applicability to broader, mixed workload scenarios in MEC environments
[45]	Identify studies related to service placement strategies to categorize the relevant studies as a knowledge source for further research	Perform a technical analysis on the cloud edge service placement approaches	• Methods and algorithms of the existing service placement approaches • Evaluation metrics for service placement approaches • Tools and environments developed for service placement approaches	Lacks any further implementation towards the service placement paradigm
[19]	Develop an efficient task allocation strategy for heterogeneous wireless sensor networks that minimizes energy consumption and balances load to extend network lifetime and enhance reliability	Fusion Algorithm combining Genetic Algorithm and Ant Colony Optimization for effective task allocation in WSNs	• Load on sensors was reduced by 58% with the FA, while the load on cluster centers decreased by 30.8%. • FA achieved an 8.1% reduction in energy consumption compared to the traditional GA.	The research may not address complex task dependencies and real-world scenarios requiring dynamic resource allocation and execution order
[46]	Minimize energy consumption in RIS-assisted NOMA-MEC networks	Jointly optimize RIS phase shifts, transmission rates, and power control	Significant energy savings compared to benchmark schemes.	Non-convex optimization and CSI estimation errors affect performance
[47]	Maximize task completion before deadlines while minimizing energy consumption in MEC systems	Deep Reinforcement Learning model	Proposed model outperforms existing methods in task completion and energy efficiency through extensive simulations	Model's performance may affect the complexity of real-world environments
[48]	Optimize task offloading and resource management in dynamic vehicular environments using a decentralized framework	A multi-layer edge computing architecture and a decentralized multi-agent deep reinforcement learning algorithm	Significant reduction in energy consumption and improved task completion rates when compared to existing algorithms in simulations	Scalability issues in highly dynamic vehicular networks
[24]	Minimize network latency in asymmetrical IoV environments through optimized resource allocation	Deep Reinforcement Learning	• Network Delay (44% reduction) • Reward per episode (39% improvement)	Future work needed on end-user mobility and deeper collaboration among network components and the tradeoff between network delay

				and energy consumption have not been focused to compromise among multiple network indicators

IV. DISCUSSION

The conducted literature review provides insights into future research that aims at energy efficiency in the paradigms of both cloud and edge computing along with the approaches that are utilized concerning the reduction of energy consumption. Nevertheless, it also noted that the researchers utilize a combination of techniques in their work towards optimizing energy efficiency for sustainable and efficient systems with reduced operational costs. Moreover, it is noted that the techniques widely spread towards the AI-driven approaches with the advancements in machine learning.

Furthermore, it is also vital to identify the challenges that are encountered when focusing on the energy-efficient aspects in edge computing due to the proliferation of IoT devices and advancements in modern computing. Among the challenges to optimizing energy efficiency in the edge computing paradigm, distributed dynamic workloads among edge nodes with vast range of heterogeneity, distributed, and resource constrained nature is much prominent since accurate modeling would be complicated due to the fluctuating workloads based on user demands. In addition, different and unpredictable workloads have imposed a lot of issues towards the edge computing paradigm. Nevertheless, the task scheduling techniques employed by contemporary research are more towards the independent task-oriented workloads while few studies have focused on complex workloads [13].

Moreover, delayed critical applications that run on devices in the mobile edge computing paradigm also impose challenges to this arena [10] that directly leads to the insufficient quality of experience for the end users and high cost of energy and bandwidth utilization that are unfavourable. Moreover, limited power sources, processing and storage capabilities also impose challenges to energy efficiency optimization strategies for a sustainable edge computing paradigm [49], [50]. Resource management is key to optimizing energy efficiency and has also been a challenging task owing to the highly dynamic nature of IoT traffic. Furthermore, many tasks have dependencies that dictate the order of execution. Managing these dependencies while optimizing resource allocation adds another level of complexity to the task allocation process.

Ensuring that the network meets specific QoS requirements, such as latency and reliability, while performing task allocation is a critical challenge that must be addressed. In addition, striking a balance between energy efficiency and QoS awareness has also been a challenging aspect where the QoS is highly impacted by the majority of mechanisms that are utilized in distributed computing environments [51]. Furthermore, energy efficiency with application performance and user experience is crucial, as overly aggressive energy-saving measures may negatively affect user satisfaction. Addressing these challenges is essential for advancing research and developing effective energy management strategies in MEC environments.

Additionally, the need for extensive data collection for relevant energy-related parameters can introduce overhead and impact performance, while selecting the most pertinent features for modeling remains a challenge. Real-time processing requirements further complicate the development of accurate models, and integrating advanced AI/ML techniques introduces complexities in training and deployment.

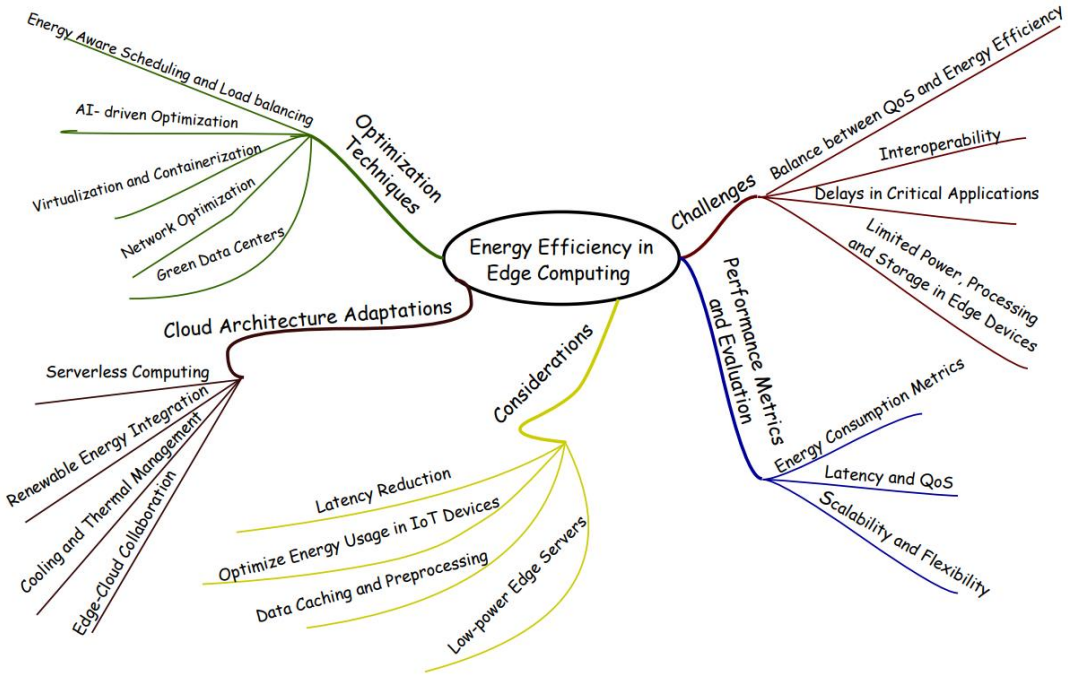


Fig. 1. Mind map with key findings from the conducted review.

With the scalability concerns in both edge and cloud computing, as the number of nodes and tasks increase, maintaining efficient communication and coordination among nodes becomes more difficult. Algorithms must be scalable to handle larger networks without significant performance degradation. Moreover, interoperability also could be a major challenge where a diverse range of IoT devices and platforms can lead to compatibility issues, making it difficult to implement a unified mechanism. Fig. 1 provides a mind map of the key findings from the conducted literature review comprising of energy optimization techniques, cloud architecture adaptations, major considerations and challenges to the energy efficiency aspect of the edge computing paradigm that provides further insights into research in this domain.

Therefore, when the above aspects are concerned, it is apparent that there is a lack of unified metrics and benchmarks for assessing energy efficiency across different edge computing environments, which makes it difficult to compare solutions. In addition, the use of AI/ML models for decision-making in edge computing often introduces significant energy overhead that urges need of optimized lightweight AI/ML algorithms for edge environments without compromising accuracy or efficiency. Heterogeneity of Edge devices also necessitates the scalable, device-agnostic optimization models that can adapt to heterogeneous edge environments. Moreover, real-time applications such as autonomous vehicles, healthcare monitoring systems, etc., have strict latency and reliability requirements, which complicate energy optimization efforts. Therefore, developing solutions that balance energy efficiency with real-time performance guarantees has also been a critical consideration in this research paradigm.

V. Conclusion

The research findings are indicative of the current approaches to energy efficient edge computing systems with reduced energy consumption and costs to provide further insights into future research in this arena. In addition, the different strategies that were identified as the key techniques to energy efficient systems in cloud computing further assists future research while a combination of different strategies has also been noted in contemporary research. Furthermore, AI-driven energy optimization techniques have been widely focused and researched and this approach has been able to provide better mechanisms for optimizing energy efficiency in both edge and cloud computing paradigms.

In conclusion, this comprehensive review on optimizing energy efficiency for edge computing highlights the growing importance of balancing performance and sustainability in modern cloud systems since as edge computing gains prominence in reducing latency and improving data processing efficiency, the need for energy optimization becomes critical. Moreover, various approaches, including workload distribution, resource allocation, and hardware improvements, have demonstrated the potential to significantly reduce energy consumption while balancing the quality of service. As future research, the authors are to refine these strategies and explore innovative methods to further enhance energy efficiency, ensuring sustainable cloud-edge ecosystems that meet the rising demands of modern applications.

References

[1] A. Sunyaev and A. Sunyaev, ‘Cloud computing’, Internet computing: Principles of distributed systems and emerging internet-based technologies, pp. 195–236, 2020.

[2] H. K. Mistry, C. Mavani, A. Goswami, and R. Patel, ‘The Impact Of Cloud Computing And Ai On Industry Dynamics And Competition’, Educational Administration: Theory and Practice, vol. 30, no. 7, pp. 797–804, 2024.

[3] A. K. Y. Yanamala, ‘Emerging Challenges in Cloud Computing Security: A Comprehensive Review’, International Journal of Advanced Engineering Technologies and Innovations, vol. 1, no. 4, pp. 448–479, 2024.

[4] K. Cao, Y. Liu, G. Meng, and Q. Sun, ‘An overview on edge computing research’, IEEE access, vol. 8, pp. 85714–85728, 2020.

[5] L. Kong et al., ‘Edge-computing-driven internet of things: A survey’, ACM Computing Surveys, vol. 55, no. 8, pp. 1–41, 2022.

[6] Q. Luo, S. Hu, C. Li, G. Li, and W. Shi, ‘Resource scheduling in edge computing: A survey’, IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2131–2165, 2021.

[7] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, ‘Edge computing in industrial internet of things: Architecture, advances and challenges’, IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2462–2488, 2020.

[8] Y. Chen, S. Ye, J. Wu, B. Wang, H. Wang, and W. Li, “Fast multi-type resource allocation in local-edge-cloud computing for energy-efficient service provision,” Information sciences, pp. 120502–120502, Mar. 2024, doi: https://doi.org/10.1016/j.ins.2024.120502.

[9] K. Sadatdiynov, L. Cui, L. Zhang, J. Z. Huang, S. Salloum, and M. S. Mahmud, ‘A review of optimization methods for computation offloading in edge computing networks’, Digital Communications and Networks, vol. 9, no. 2, pp. 450–461, 2023.

[10] M. P. J. Mahenge, C. Li, and C. A. Sanga, “Energy-efficient task offloading strategy in mobile edge computing for resource-intensive mobile applications,” Digital Communications and Networks, Apr. 2022, doi: https://doi.org/10.1016/j.dcan.2022.04.001.

[11] M. H. S, S. Kumar T, S. M. F. D. S. Mustapha, P. Gupta, and R. P. Tripathi, “Hybrid Approach for Resource Allocation in Cloud Infrastructure Using Random Forest and Genetic Algorithm,” Scientific Programming, vol. 2021, pp. 1–10, Oct. 2021, doi: https://doi.org/10.1155/2021/4924708.

[12] M. K. Alasmari, S. S. Alwakeel, and Y. A. Alohali, “A Multi-Classifiers Based Algorithm for Energy Efficient Tasks Offloading in Fog Computing,” Sensors, vol. 23, no. 16, pp. 7209–7209, Aug. 2023, doi: https://doi.org/10.3390/s23167209.

[13] A. Jayanetti, S. Halgamuge, and R. Buyya, “Deep reinforcement learning for energy and time optimized scheduling of precedence-constrained tasks in edge-cloud computing environments,” Future Generation Computer Systems, Jun. 2022, doi: https://doi.org/10.1016/j.future.2022.06.012.

[14] D. Alsadie, “Efficient Task Offloading Strategy for Energy-Constrained Edge Computing Environments: A Hybrid Optimization Approach,” IEEE Access, vol. 12, pp. 85089–85102, 2024, doi: https://doi.org/10.1109/access.2024.3415756.

[15] J. A. Ansere et al., ‘Optimal computation resource allocation in energy-efficient edge IoT systems with deep reinforcement learning’, IEEE Transactions on Green Communications and Networking, vol. 7, no. 4, pp. 2130–2142, 2023.

[16] S. Sangeetha, J. Logeshwaran, M. Faheem, R. Kannadasan, S. Sundararaju, and L. Vijayaraja, ‘Smart performance optimization of energy-aware scheduling model for resource sharing in 5G green communication systems’, The Journal of Engineering, vol. 2024, no. 2, p. e12358, 2024.

[17] A. Asghari, H. Azgomi, A. A. Zoraghchian, and A. Barzegarinezhad, ‘Energy-aware server placement in mobile edge computing using trees social relations optimization algorithm’, The Journal of Supercomputing, vol. 80, no. 5, pp. 6382–6410, 2024.

[18] F. Ramezani Shahidani, A. Ghasemi, A. Toroghi Haghighat, and A. Keshavarzi, ‘Task scheduling in edge-fog-cloud architecture: a multi-

objective load balancing approach using reinforcement learning algorithm', Computing, vol. 105, no. 6, pp. 1337–1359, 2023.

[19] J. Wen, J. Yang, T. Wang, Y. Li, and Z. Lv, 'Energy-efficient task allocation for reliable parallel computation of cluster-based wireless sensor network in edge computing', Digital Communications and Networks, vol. 9, no. 2, pp. 473–482, 2023.

[20] M. Raeisi-Varzaneh, O. Dakkak, A. Habbal, and B.-S. Kim, 'Resource scheduling in edge computing: Architecture, taxonomy, open issues and future research directions', IEEE Access, vol. 11, pp. 25329–25350, 2023.

[21] H. Huang, W. Zhan, G. Min, Z. Duan, and K. Peng, 'Mobility-aware computation offloading with load balancing in smart city networks using MEC federation', IEEE Transactions on Mobile Computing, 2024.

[22] Z. Zhou, M. Shojafar, J. Abawajy, H. Yin, and H. Lu, 'ECMS: An Edge Intelligent Energy Efficient Model in Mobile Edge Computing', IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 238–247, 2022.

[23] K. Sathupadi, 'Ai-driven energy optimization in sdn-based cloud computing for balancing cost, energy efficiency, and network performance', International Journal of Applied Machine Learning and Computational Intelligence, vol. 13, no. 7, pp. 11–37, 2023.

[24] T. Cui, R. Yang, C. Fang, and S. Yu, 'Deep reinforcement learning-based resource allocation for content distribution in IoT-edge-cloud computing environments', Symmetry, vol. 15, no. 1, p. 217, 2023.

[25] Y. Mansouri and M. A. Babar, 'A review of edge computing: Features and resource virtualization', Journal of Parallel and Distributed Computing, vol. 150, pp. 155–183, 2021.

[26] C. Jian, L. Bao, and M. Zhang, 'A high-efficiency learning model for virtual machine placement in mobile edge computing', Cluster Computing, vol. 25, no. 5, pp. 3051–3066, 2022.

[27] L. Urblik, E. Kajati, P. Papcun, and I. Zolotová, 'Containerization in Edge Intelligence: A Review', Electronics, vol. 13, no. 7, p. 1335, 2024.

[28] J. Zhang, X. Zhou, T. Ge, X. Wang, and T. Hwang, 'Joint task scheduling and containerizing for efficient edge computing', IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 8, pp. 2086–2100, 2021.

[29] S. Hu, W. Shi, and G. Li, 'CEC: A containerized edge computing framework for dynamic resource provisioning', IEEE Transactions on Mobile Computing, vol. 22, no. 7, pp. 3840–3854, 2022.

[30] F. Zhou and R. Q. Hu, 'Computation Efficiency Maximization in Wireless-Powered Mobile Edge Computing Networks', IEEE Transactions on Wireless Communications, vol. 19, no. 5, pp. 3170–3184, 2020.

[31] X. Zhou, X. Yang, J. Ma, I. Kevin, and K. Wang, 'Energy-efficient smart routing based on link correlation mining for wireless edge computing in IoT', IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14988–14997, 2021.

[32] T. Vaiyapuri, V. S. Parvathy, V. Manikandan, N. Krishnaraj, D. Gupta, and K. Shankar, 'A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing', Wireless Personal Communications, vol. 127, no. 1, pp. 39–62, 2022.

[33] A. Javadpour et al., 'An energy-optimized embedded load balancing using DVFS computing in cloud data centers', Computer Communications, vol. 197, pp. 255–266, 2023.

[34] S. K. Panda, M. Lin, and T. Zhou, 'Energy-efficient computation offloading with DVFS using deep reinforcement learning for time-critical IoT applications in edge computing', IEEE Internet of Things Journal, vol. 10, no. 8, pp. 6611–6621, 2022.

[35] A. Cañete, M. Amor, and L. Fuentes, 'HADES: An NFV solution for energy-efficient placement and resource allocation in heterogeneous infrastructures', Journal of Network and Computer Applications, vol. 221, p. 103764, 2024.

[36] X. Cao, G. Zhu, J. Xu, Z. Wang, and S. Cui, 'Optimized power control design for over-the-air federated edge learning', IEEE Journal on Selected Areas in Communications, vol. 40, no. 1, pp. 342–358, 2021.

[37] X. Cao, G. Zhu, J. Xu, and S. Cui, 'Transmission power control for over-the-air federated averaging at network edge', IEEE Journal on Selected Areas in Communications, vol. 40, no. 5, pp. 1571–1586, 2022.

[38] X. Mo and J. Xu, 'Energy-efficient federated edge learning with joint communication and computation design', Journal of Communications and Information Networks, vol. 6, no. 2, pp. 110–124, 2021.

[39] H. Koumaras et al., '5G-enabled UAVs with command and control software component at the edge for supporting energy efficient opportunistic networks', Energies, vol. 14, no. 5, p. 1480, 2021.

[40] X. Shao, Z. Zhang, P. Song, Y. Feng, and X. Wang, 'A review of energy efficiency evaluation metrics for data centers', Energy and Buildings, vol. 271, p. 112308, 2022.

[41] Q. Zhang et al., 'A survey on data center cooling systems: Technology, power consumption modeling and control strategy optimization', Journal of Systems Architecture, vol. 119, p. 102253, 2021.

[42] M. Manganelli, A. Soldati, L. Martirano, and S. Ramakrishna, 'Strategies for improving the sustainability of data centers via energy mix, energy conservation, and circular energy', Sustainability, vol. 13, no. 11, p. 6114, 2021.

[43] E. Ahvar, A.-C. Orgerie, and A. Lebre, 'Estimating Energy Consumption of Cloud, Fog, and Edge Computing Infrastructures', IEEE Transactions on Sustainable Computing, vol. 7, no. 2, pp. 277–288, 2022.

[44] Q. Wang, L. T. Tan, R. Q. Hu, and Y. Qian, 'Hierarchical Energy-Efficient Mobile-Edge Computing in IoT Networks', IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11626–11639, 2020.

[45] L. Heng, G. Yin, and X. Zhao, 'Energy aware cloud-edge service placement approaches in the Internet of Things communications', International Journal of Communication Systems, vol. 35, no. 1, p. e4899, 2022.

[46] Z. Li et al., 'Energy Efficient Reconfigurable Intelligent Surface Enabled Mobile Edge Computing Networks With NOMA', IEEE Transactions on Cognitive Communications and Networking, vol. 7, no. 2, pp. 427–440, 2021.

[47] L. Ale, N. Zhang, X. Fang, X. Chen, S. Wu, and L. Li, 'Delay-Aware and Energy-Efficient Computation Offloading in Mobile-Edge Computing Using Deep Reinforcement Learning', IEEE Transactions on Cognitive Communications and Networking, vol. 7, no. 3, pp. 881–892, 2021.

[48] M. Fardad, G.-M. Muntean, and I. Tal, 'Decentralized vehicular edge computing framework for energy-efficient task coordination', in 2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring), 2024, pp. 1–7.

[49] K. Kaur, S. Garg, G. S. Aujla, N. Kumar, J. J. P. C. Rodrigues, and M. Guizani, 'Edge Computing in the Industrial Internet of Things Environment: Software-Defined-Networks-Based Edge-Cloud Interplay', IEEE Communications Magazine, vol. 56, no. 2, pp. 44–51, 2018.

[50] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, 'A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications', IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

[51] U. M. Malik, M. A. Javed, S. Zeadally, and S. ul Islam, 'Energy-Efficient Fog Computing for 6G-Enabled Massive IoT: Recent Trends and Future Opportunities', IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14572–14594, 2022.

Malicious Traffic Detection Algorithm for the Internet of Things Based on Temporal Spatial Feature Fusion

Linzhong Zhang
School of Electronic Information Engineering, Tianjin Vocational Institute, Tianjin, 300410, China

***Abstract*—With the rapid development of the Internet of Things, the security issues of its network environment have gradually attracted attention. To enable faster and more accurate identification and detection of malicious traffic attacks in the Internet of Things, an optimized malicious traffic detection algorithm based on fusion of temporal and spatial features is proposed. This method improves the feature extraction performance of traffic data and increases the accuracy of traffic detection. The test results showed that the comprehensive performance of the fusion algorithm was superior to the other four algorithms used for comparison. On the KDD99-CUP dataset, the F1 of the feature fusion algorithm reached 93.16%, while the F1 of algorithms 1-4 were 81.36%, 67.89%, 90.56%, and 92.24%, respectively. On the test set, 182 traffic samples were accurately identified, including 139 correctly identified malicious traffic and 43 correctly identified normal traffic, with recognition accuracy of 98.73% and 97.65%, respectively. Experimental results revealed that the use of fused feature extraction in traffic detection systems could improve detection efficiency and accuracy, providing a safer and more reliable guarantee for the interaction process of the Internet of Things network, and safeguarding the rapid development and application of the Internet of Things.**

***Keywords*—Internet of Things; network security; temporal-spatial characteristics; traffic detection; fusion algorithm**

I. Introduction

With the rapid development of the Internet, the Internet of Things (IoT) has also been widely used in a series of intelligent building systems such as smart cities, smart offices and smart homes [1-2]. However, because some IoT devices are directly exposed to the Internet, they face more security problems than other network interaction methods [3]. IoT based network attacks may affect communication quality, and even cause signal loss, network paralysis, and other phenomena, seriously threatening users' privacy and security [4]. For traditional anomaly traffic detection techniques, due to the concealment and complexity of existing IoT network attacks, and the fact that traffic attacks exhibit different characteristics with different network environments, there are problems with imbalanced traffic datasets and difficult feature extraction [5]. These issues have increased the difficulty of designing malicious traffic identification algorithms. In current traffic detection systems, the main focus is on identifying and analyzing a single type of traffic to achieve abnormal alerts. However, due to the different types and characteristics of attacks, and some attacks being of unknown types, the accuracy of traffic detection systems is not ideal, making it difficult to predict unknown attacks. To solve the above problems, a traffic detection algorithm based on temporal feature fusion is proposed, and malicious traffic analysis and detection in the IoT are completed on this basis.

II. Related Works

In today's era of rapid development of information technology, network traffic analysis has become an important means to ensure network security, optimize network performance, and improve user experience. Furthermore, with the explosion of Internet users and the popularization of various network applications, the complexity and diversity of network traffic are also increasing. Therefore, in-depth analysis of the characteristics and detection methods of malicious traffic is of great importance for network management and security protection. Yang H et al. proposed a fast strategy hill-climbing learning method to optimize the power allocation for malicious traffic detection in intelligent malicious traffic controllers. Therefore, the malicious traffic detection system could quickly achieve the optimal strategy when the malicious traffic model was unknown. The test results showed that the transmission rate of this malicious traffic detection method increased by 12.28% compared to the original, which made the malicious traffic detection system perform better [6]. Salem A et al. proposed an adaptive adaptation scheme that could make the detection of malicious traffic techniques constructive for legitimate users and destructive for eavesdroppers. Based on the average symbol error probability in different scenarios, this method used a finite rate to represent the overall retention rate. Malicious traffic detection technology could achieve an additional gain of 17dB in transmission signal-to-noise ratio and a gain of 10dB in total secrecy rate [7]. Su N et al. used joint design to transmit and receive beamforming and destructive malicious traffic techniques to weaken the eavesdropping signals of eavesdropping radar in wireless networks. The experimental results showed that this technology performed better than dual function radar network technology in terms of secure transmission [8]. Many radars and networks work in a coordinated manner, but Du Z et al. proposed using a non coordinated approach to study the impact of malicious network traffic on radar target detection. The study solved the maximum likelihood estimation in homogeneous clutter to optimize detection performance. Through verification, it was found that the improved target detection system showed significant improvement in performance in network

environments with high levels of malicious traffic [9]. Hosseinali J et al. proposed an improved adaptive algorithm to address the issue of malicious attacks on high-power ranging devices. The algorithm optimized power allocation for each reliable subcarrier, while subcarriers subjected to highly malicious traffic were deactivated. This adaptive technology could reduce the bit error rate to 10-7 under malicious traffic in high-power ranging devices, improving the reliability of network systems [10]. In the scenario of multi-user and multi-transceiver simultaneous network, to eliminate malicious traffic on reconfigurable intelligent surfaces, the Jiang T team proposed an alternating projection algorithm, which took the solution obtained by the algorithm approaching 0 as the initial value for subsequent optimization, and changed the phase of the reconfigurable surface components accordingly. Tests showed that the improved algorithm could detect malicious traffic on reconfigurable surfaces within the experimental range [11].

The malicious traffic detection performance of network systems is largely influenced by algorithms. Some scholars have conducted more in-depth research and experiments on the optimization of deep learning algorithms. Lin J et al. proposed an improved genetic algorithm based on four quadrant photodetectors to improve the accuracy and stability of visible light positioning. This algorithm enabled the detector to locate the measurement point based on the received illuminance value. The average positioning error of the positioning system using optimization algorithms was 4.023cm [12]. Mahmoud B et al. proposed a hybrid model of deep learning algorithm and tabu search to achieve balanced coverage of all targets in sensor networks. The optimized algorithm required the use of multiple sensors for coverage. Several experiments showed that this fusion algorithm outperformed algorithms based on automatic learning [13]. To extend the lifespan of wireless sensor networks, Rajan L et al. proposed a new optimization algorithm based on the grey wolf algorithm using Na deep learning algorithm, which selected the optimal cluster head under constraints such as separation distance and energy consumption. Compared to the classical grey wolf algorithm and particle swarm optimization algorithm, the improved grey wolf algorithm improved overall performance by 28.6% and 31.5%, respectively [14]. Shaikh M et al. proposed using optimized deep learning algorithms to achieve higher accuracy in the calculation of parameters for overhead transmission lines. This optimization algorithm was applied to single-phase and three-phase transmission lines, achieving optimal solutions for the vast majority of benchmark functions. The accuracy and computational efficiency of the optimized deep learning algorithm had been improved [15].

In conclusion, despite the numerous inferences and experiments conducted by scholars on optimizing detection algorithms and enhancing traffic detection performance, the intricate neural network structure inherent to deep learning algorithms results in a slow convergence speed and a notable decline in detection accuracy. To further enhance the performance of malicious traffic detection, an optimized malicious traffic detection algorithm based on the fusion of temporal and spatial features is proposed. This is achieved through the use of a mixed sampling and variational autoencoder data augmentation algorithm, which enables more intelligent and efficient detection results in complex environments.

III. Methods and Materials

A. Flow Detection Algorithm Integrating Temporal and Spatial Features

When faced with malicious traffic attacks, intrusion detection systems can use detection algorithms that continuously learn traffic information characteristics to identify them. When attacked, the detection system can determine the traffic attack behavior [16]. The process of traffic detection mainly consists of network status detection and traffic detection. The former is to detect the operating status of network and host and monitor the fluctuation of network system in real time, while the latter is to extract the characteristics of traffic data and complete the detection and analysis. The characteristics of traffic data can be analyzed from both temporal and spatial dimensions. For the temporal dimension, there is correlation between historical traffic data, while for the spatial dimension, there is local spatial correlation between traffic characteristics [17]. By integrating these two different types of features, traffic detection can simultaneously capture feature information from different dimensions, identify different traffic activities, and make the results of detection algorithms more accurate and reliable. The architecture of the data traffic detection system is depicted in Fig. 1.

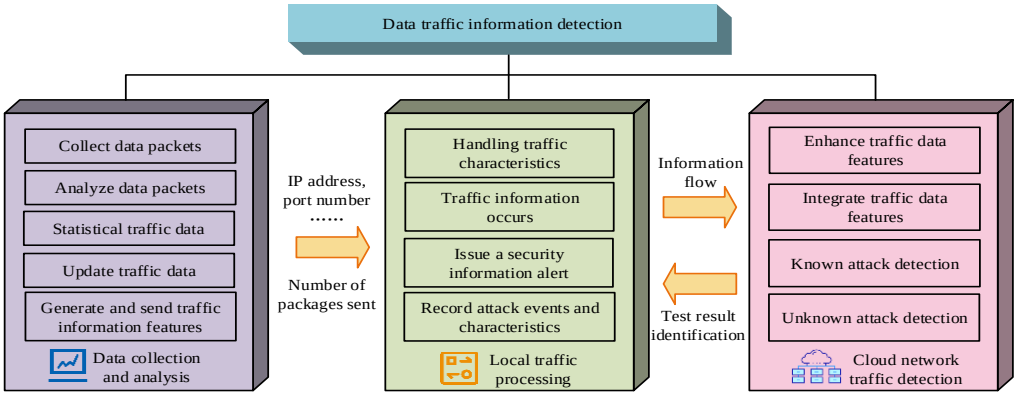


Fig. 1. The architecture of data traffic detection system.

In Fig. 1, the system mainly includes a data collection and analysis module, a local traffic processing module, and a cloud network traffic detection module. A traffic detection method based on temporal and spatial feature fusion has been proposed, and the main detection process is shown in Fig. 2.

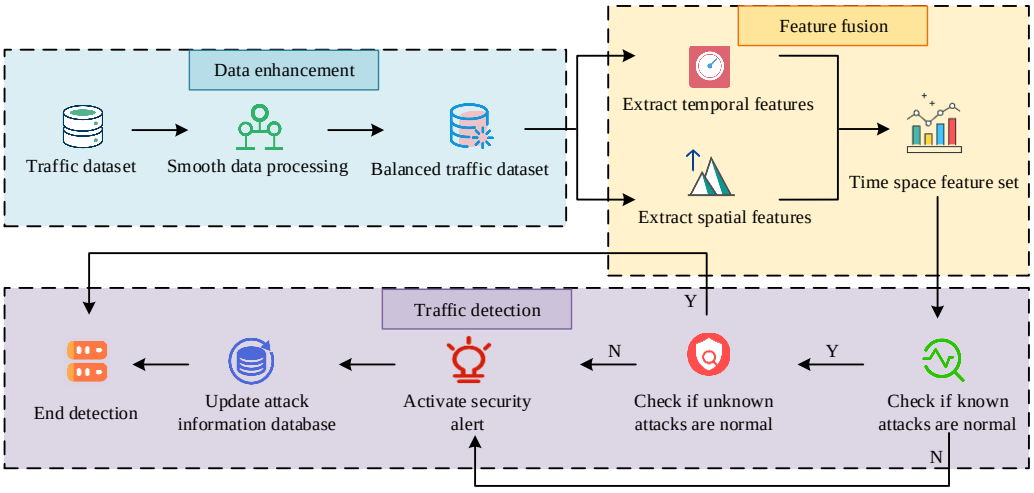


Fig. 2. Main process of detection.

Probability can be mainly divided into parametric estimation and nonparametric estimation, mainly used to estimate the potential probability density function of target information that is invisible [18]. The condition for parameter estimation is that the target information needs to follow a probability distribution and its parameters are unknown, so the corresponding parameters need to be solved through known data. Non parameter estimation requires the target information to have a probability density function, which is solved through observation data. Although it is mainly data-driven and does not require a probability distribution, its computational complexity is relatively high. If the one-dimensional random variable is the probability density function x of $f(x)$ can be represented by Eq. (1).

$$f(x)=\lim_{h\to 0}\frac{F(x+h)-F(x-h)}{2h} \tag{1}$$

In Eq. (1), x represents a one-dimensional random variable, h is the bandwidth width parameter, $F(x)$ is the probability distribution function, and the definition of $F(x)$ can be seen in Eq. (2).

$$F(x)=P(X\le x) \tag{2}$$

Frequency estimation probability can be applied to the dataset. If a one-dimensional random variable has n samples $\{x_1,x_2,x_3,....,x_n\}$, its probability distribution function $\hat{F}(x)$ can also be expressed as Eq. (3).

$$\hat{F}(x)=\frac{k}{n} \tag{3}$$

In Eq. (3), k represents the number of samples smaller than x, and the number of samples is set as m, thus obtaining the estimated equation for the probability density function $\hat{f}(x)$ as shown in Eq. (4).

$$\hat{f}(x)=\frac{m}{2nh} \tag{4}$$

If a uniformly distributed function is defined as $K(x)$, the estimation of the probability density function can also be called a kernel function, which can be represented by Eq. (5).

$$\hat{f}(x)=\frac{1}{nh}\sum_{i=1}^{n}K(\frac{x-x_i}{h}) \tag{5}$$

Multidimensional kernel density estimation can be obtained through univariate kernel density estimation. If a p-dimensional continuous random variable x is set, its multidimensional kernel density estimation equation can be represented by Eq. (6).

$$\hat{f}(x)=\frac{1}{n|H|^{1/2}\,0}\sum_{i=1}^{n}K(H^{-1/2}(x-xi)) \tag{6}$$

Among them, K is a multidimensional kernel function, and H is a symmetric bandwidth matrix. Analysis Eq. (6) shows that the influencing factors of kernel density estimation are mainly determined by the selection of kernel function K and the size of bandwidth width h. When the cloud receives data information, it needs to first enhance the data before completing data feature extraction and fusion. The process flow of the data collection and analysis module can be seen in Fig. 3.

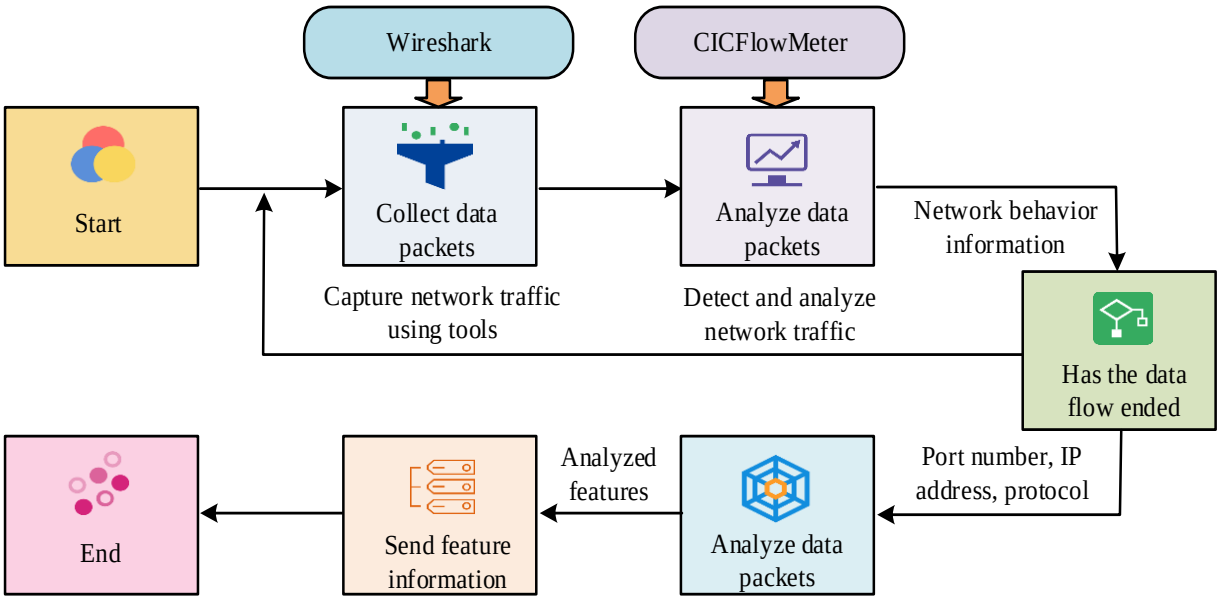


Fig. 3. Data collection and analysis module process.

The extracted and fused feature information will be used for known attack detection. If the detection result is abnormal traffic, further determination of the specific type of abnormal attack is required. If it is detected as normal traffic, further unknown attack detection will be carried out to prevent the IoT from being attacked by unknown traffic. The encoder is mainly composed of an input layer and a fully connected layer. Set the n dimensional feature vector received by the system as x, compress x to obtain a low dimensional latent space z of m dimension, set the neural network parameters of the encoder as f, and the compression function as $h()$, then the encoder can be expressed as Eq. (7).

$$z = h(x, \varphi) \tag{7}$$

The decoder consists of a fully connected layer and an output layer. Nonlinear computation can be used to reconstruct the low dimensional representation of m dimensional latent space as z into n as the eigenvector x. If the $\hat{x}$ neural network parameters of the decoder are set to θ and the reconstruction function is set to $g()$, the decoder can be expressed as Eq. (8).

$$\hat{x} = g(z, \theta) \tag{8}$$

The autoencoder compresses the input by using the encoder to obtain a low dimensional latent space, which preserves the effective features of the input data and enables the decoder to complete the reconstruction process of the original input data. The optimization objective can be represented by Eq. (9).

$$\varphi, \theta = \arg\min_{\varphi,\theta} \sum_{i=1}^{n} L(x_i, \hat{x}_i) \tag{9}$$

In Eq. (9), x_i is the original feature vector input to the autoencoder, and $\hat{x}_i$ is the reconstructed feature vector output by the autoencoder. The function for measuring vector differences is set as $L()$, which can generally be measured using the mean square loss function. The loss function can be expressed as Eq. (10).

$$s = \sum_{i=1}^{n} L(x_i, \hat{x}_i) \tag{10}$$

The compression network is represented by z, and the reconstruction loss of the input layer u and output layer v can be used as a low dimensional representation of the input features, as expressed in Eq. (11).

$$\begin{cases} u = [educlidean\_loss, \cos ine\_loss] \\ v = [z, u] \end{cases} \tag{11}$$

When extracting traffic features, the extraction process can be completed through time and space. Temporal feature extraction mainly targets multiple traffic data, while spatial feature extraction targets individual traffic data, and there are significant differences between these two extraction methods [19]. A feature fusion encoder is proposed by studying the fusion extraction method of temporal and spatial features. It is mainly divided into bidirectional attention temporal encoder and asymmetric multi-scale spatial encoder. The former is mainly responsible for extracting temporal features from spatial features, while the latter is responsible for extracting spatial features from raw traffic data. Through two different extraction methods, different dimensional fusion effects are achieved. The structure of the feature fusion encoder can be seen in Fig. 4.

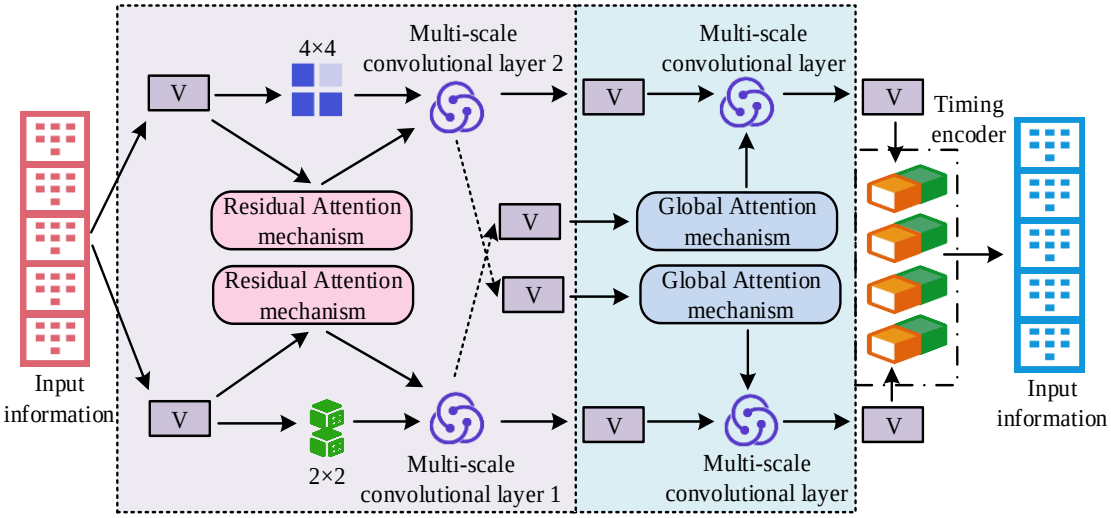


Fig. 4. Structure of fusion encoder.

B. Analysis and Detection of Malicious Traffic in the IoT

For malicious traffic anomaly detection, the balance between the number of normal and abnormal data in the dataset cannot be achieved, so its performance cannot be measured solely by accuracy. Accuracy and recall are two important measurement indicators [20]. If the accuracy is set to Acc, its calculation can be represented by Eq. (12).

$$Acc = \frac{TP + TN}{FN + TN + FP + TP} \tag{12}$$

In Eq. (7), TP represents the number of normal traffic samples detected by the detection model as normal, and TN represents the number of abnormal traffic samples detected by the model as abnormal. FN indicates the total number of samples is represented by the number of normal abnormal traffic samples detected by the detection model, and FP represents the number of normal samples detected as abnormal. The sum of these four types of samples is the total number of samples. If the accuracy of the detection is $\Pr e$, the calculation equation is shown in Eq. (13).

$$\Pr e = \frac{TP}{TP + FP} \tag{13}$$

The recall rate represents the proportion of correct predictions in the normal records of the predictive model. If $\mathrm{Re}c$ is used to represent the recall rate, its expression is shown in Eq. (14).

$$\mathrm{Re}c = \frac{TP}{FN + TP} \tag{14}$$

The relationship between accuracy and recall is quite conflicting. If the accuracy is increased by raising the threshold during detection, the recall rate will decrease. Therefore, when evaluating the performance of detection models, it is necessary to comprehensively evaluate the accuracy and recall rates for a more accurate assessment. If F represents the weighted harmonic of precision and recall, its expression can be seen in Eq. (15).

$$F = \frac{(1+\varepsilon)(\Pr e * \mathrm{Re}c)}{(\alpha^2 * \Pr e) + \mathrm{Re}c} \tag{15}$$

In Eq. (15), in general, the value of α is 1. After determining the evaluation criteria for detection performance, the interaction design between the traffic detection system and external modules is first completed. When the traffic detection system is attacked, the corresponding attack behavior can be detected, and the message can be transmitted to other functional modules through alarm information [21]. The architecture of Dbus is client service, which is a simple and fast communication method that supports point-to-point communication and can send messages to specific processes in a directed manner. Research has chosen Dbus as the mechanism for message notification to facilitate information exchange between the detection system and the external environment. The relationship between the system and external modules can be seen in Fig. 5.

After receiving relevant information, the local processing module completes the processing of information data, alarms and related records. When data information is received from the data acquisition module and the data analysis module, appropriate numerical and normalization processing of the feature data is required. The preprocessed information is sent to the cloud processing module, and after analysis and recognition by the cloud processing module, it is sent back to the local processing module [22]. The local processing module completes the parsing and judgment. If it is judged as normal traffic, it waits for the next traffic information from the data collection and analysis module. If it is judged as malicious attack traffic, a security alarm will be triggered and the traffic event will be sent to the corresponding module for recording. The process flow of the local processing module can be seen in Fig. 6.

The cloud network traffic detection module is mainly responsible for analyzing and judging traffic information. The traffic detection system can be divided into three parts: data collection and analysis, local processing, and cloud network traffic detection. The data collection and analysis module is mainly responsible for parsing traffic packets, attacking and updating traffic messages, and extracting and sending traffic characteristics. The collection and parsing of data packets is the process of parsing the data packets captured by the gateway and generating the specified data format. The statistics and updates of traffic messages involve updating traffic information. The process of generating traffic information features mainly involves transforming the parsed traffic into features such as address, number of packets, duration, port number, etc.

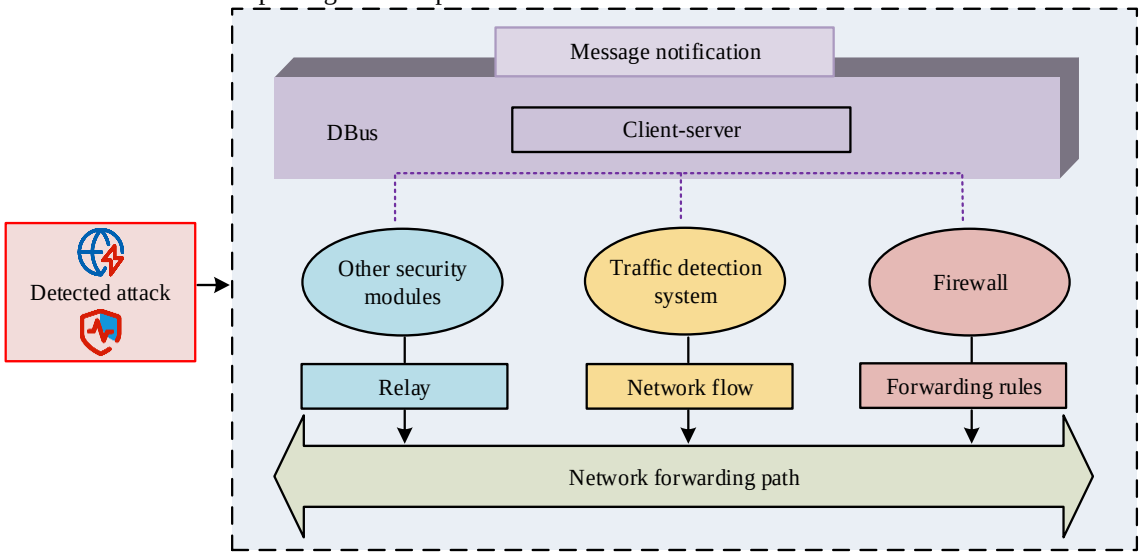


Fig. 5. Relationship between system and external modules.

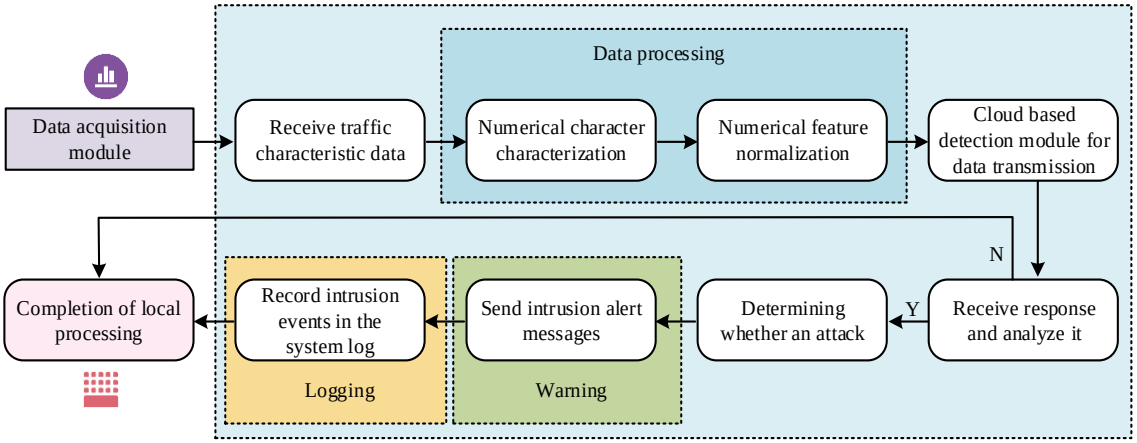


Fig. 6. Flow chart of data local processing module.

IV. Results

A. Performance Testing of Traffic Monitoring Algorithms

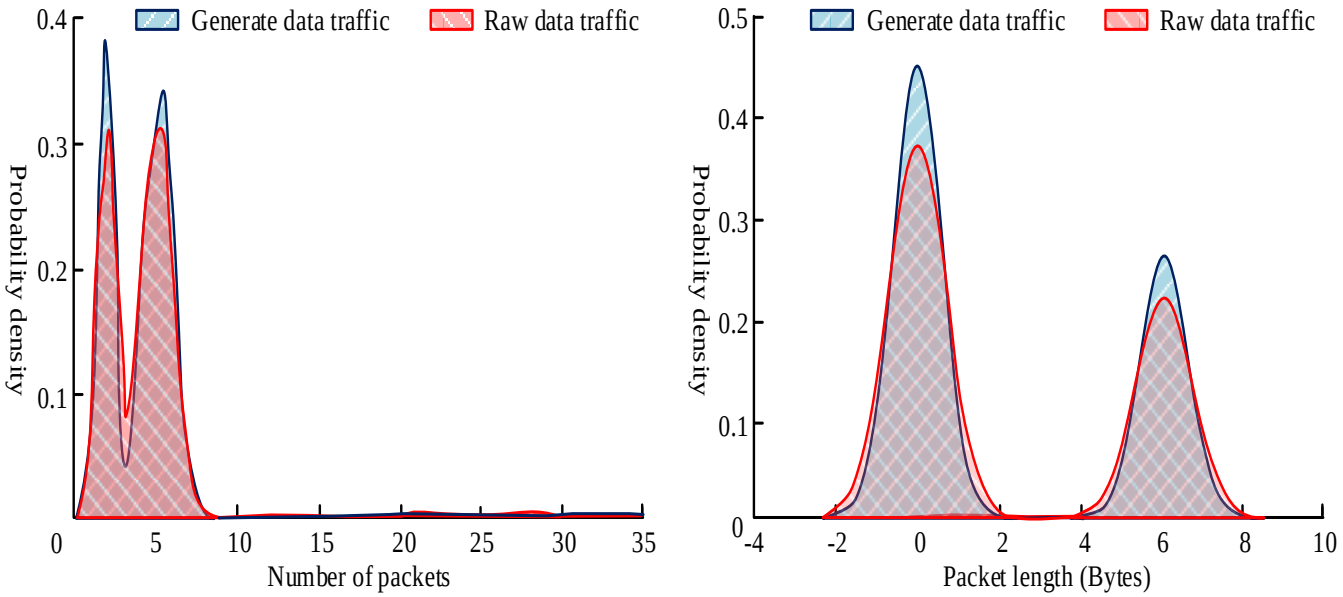
To verify the consistency between the original traffic information and the generated traffic information features based on feature fusion detection, the experiment analyzed the fitting situation before and after balancing from two aspects: actual forwarded data packets and packet length. The feature probability density distribution of the dataset was shown in Fig. 7.

In Fig. 7, the horizontal axis represented features, while the vertical axis represented the corresponding probability density. From Fig. 7(a), when the actual number of forwarded packets was less than 10, the probability density values of both the original data traffic and the preprocessed data traffic fluctuated between 0 and 0.4. When the number of forwarded packets was 2 and 5, the corresponding probability density could reach its maximum value. The probability densities of the original data traffic were 0.31 and 0.32, respectively, and the probability densities of the preprocessed generated data traffic were 0.38 and 0.35, respectively. In Fig. 7(b), when the probability density of the original data flow reached its maximum value of 0.45, the probability density of the generated data flow also reached its maximum value of 0.35. By observing the traffic feature distribution of the original data and the generated data, the feature distribution of the dataset was basically consistent before and after balancing. The data preprocessing method used in the study could ensure

that the data features remained consistent before and after processing. The experiment referred to the single class support vector machine detection algorithm, autoencoder detection algorithm, and isolated forest detection algorithm as detection algorithms 1-3, respectively. The feature fusion detection algorithm proposed in the study was trained on traffic data on both IoTID20 and XIoTID datasets. The IoTID20 dataset was based on smart home environments and mainly collected data from terminal IoT devices corresponding to smart speakers, smartphones, and smart cameras. In simulated attack scenarios, smart speakers and smart cameras were targeted. This dataset contained 83 rich features, with over 70% of the features scoring over 0.5, which could improve the classification ability of detection algorithms and techniques and reduce training time. The XIoTID dataset contained 19 categories, with the majority accounting for 55.24% and the minority accounting for over 0.01%, respectively. From this, the comparison of training effects of different algorithms can be obtained as shown in Fig. 8.

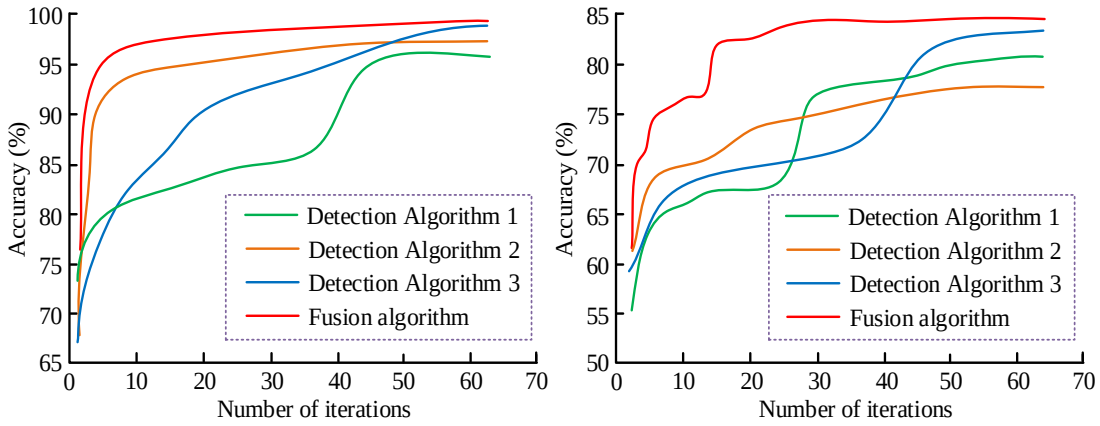
On the IoTID20 dataset in Fig. 8(a), as the number of iterations increases, the accuracy of the four detection algorithms gradually improved and eventually stabilized. The feature fusion detection algorithm proposed in the study showed an increase in accuracy from the initial 77% to 98.3% after the 40th iteration. At this point, the accuracy of the compared detection algorithms 1, 2, and 3 was 95.7%, 94.2%, and 88.2%, respectively. After increasing the number of iterations to 50, the accuracy of the four algorithms remained basically unchanged. On the XIoTID dataset in Fig. 8(b), the accuracy of the four algorithms reached stability after the 45th iteration. At the 60th iteration, the accuracy of the feature fusion algorithm was the highest, at 84.2%. At this time, the accuracy of detection algorithms 1-3 were 79.5%, 76.8%, and 82.6%, respectively. The aforementioned outcomes may be attributed to the proposed spatial and temporal feature fusion methodology, which enabled the comprehensive integration of the original feature map and the deep feature map, and facilitates a thorough examination of the interrelationship between historical data from both temporal and spatial perspectives. This approach enhanced the informativity of the extracted feature data and markedly improved the detection performance. To conduct a more accurate analysis of the detection performance of feature fusion algorithms, the deep autoencoder algorithm was added to the existing comparison algorithms as comparison Algorithm 4 in the experiment. The accuracy, precision, recall, and F1 of each algorithm were recorded and analyzed. The comparison results could be seen in Fig. 9.

From Fig. 9, the comprehensive performance of the fusion algorithm was superior to the other four algorithms. On the KDD99-CUP dataset in Fig. 9(a), the F1 of the feature fusion algorithm could reach 93.16%, while the F1 of algorithms 1-4 were 81.36%, 67.89%, 90.56%, and 92.24%, respectively. On the MTA-KDD dataset in Fig. 9(b), the accuracy of the fusion algorithm was 92.91%, the recall rate was 88.12%, and the F1 was 91.54%, still higher than other algorithms. In Fig. 9(c), Algorithm 2 had the lowest F1 on the N-BaIoT dataset, at 65.02%, while the feature fusion algorithm had the highest F1, at 98.21%. On the MedBIoT dataset in Fig. 9(d), the recall rate of the feature fusion algorithm was 95.08%, and the F1 was 97.33%, which was the highest among the five algorithms. The above results were due to the tendency of the research method to lead to precise resolution of feature roots in low-dimensional feature spaces, thereby optimizing the fitting effect of the data distribution.



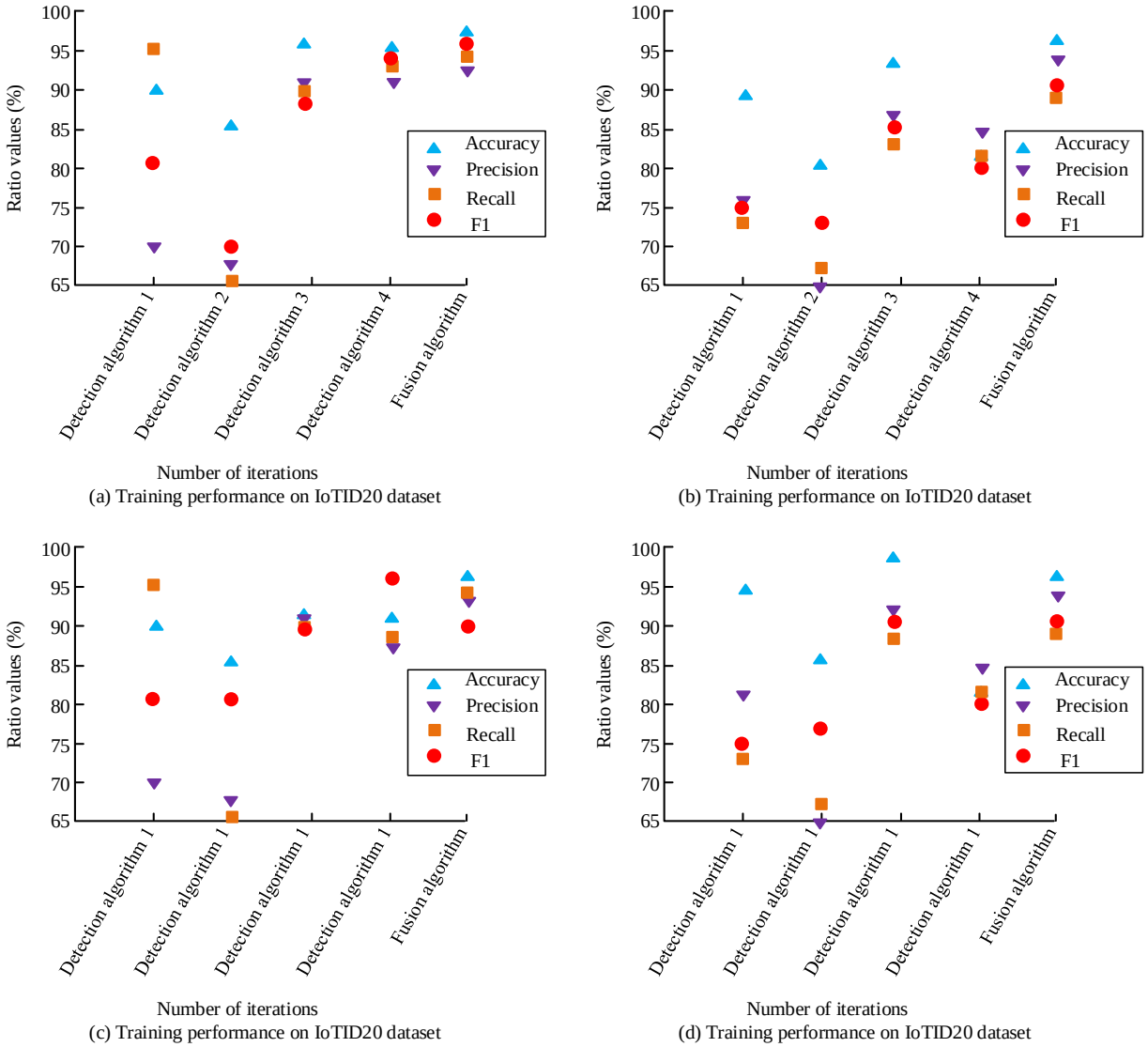
(a) Total forward packets (b) Forwarding packet length

Fig. 7. Distribution of feature probability density in the dataset.



(a) Training performance on IoTID20 dataset (b) Training performance on XIIoTID datasetX

Fig. 8. Comparison of training effects of different algorithms.



(a) Training performance on IoTID20 dataset (b) Training performance on IoTID20 dataset

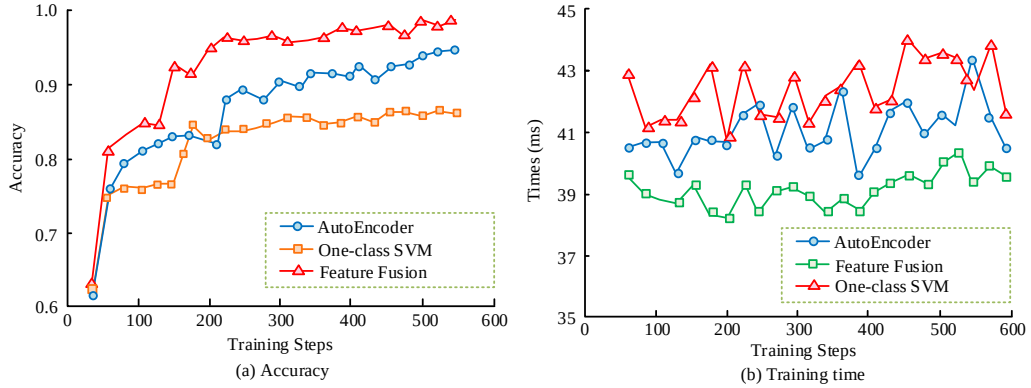
(c) Training performance on IoTID20 dataset (d) Training performance on IoTID20 dataset

Fig. 9. Performance comparison of various algorithms.

B. IoT Malicious Traffic Detection Experiment

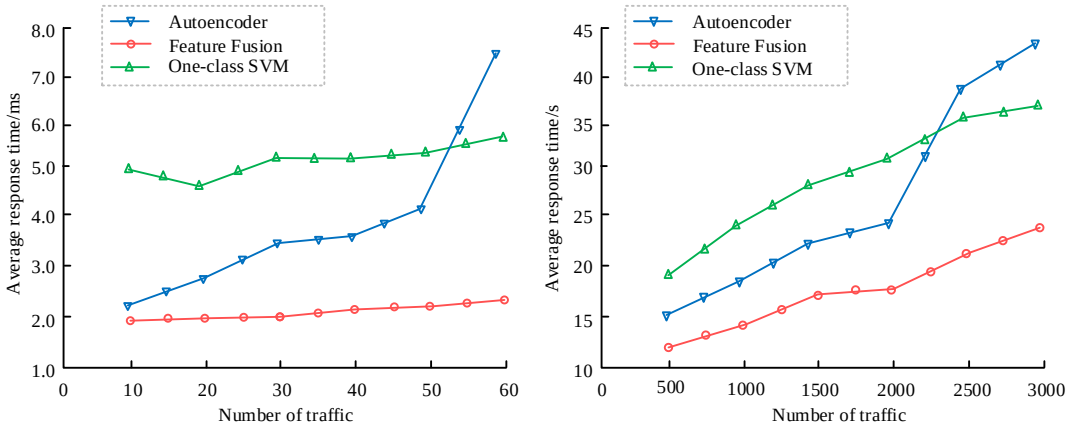
In the experiment on accuracy and model training time, the training steps were set to 600, and the automatic encoding detection model and single classification detection model were selected as controls. The comparison of accuracy and training time of the three models can be seen in Fig. 10.

In Fig. 10(a), when the training steps of the three models were less than 60, the difference in accuracy among the three models was small, and the accuracy of the feature fusion detection model was also below 0.8. As the number of training steps gradually increased, the accuracy of the three models begun to show significant differences. The detection accuracy of the feature fusion detection model proposed in the study was significantly higher than that of the other two models. When the training steps were 500, the accuracy of the feature fusion model reached 0.98, while at this time, the accuracy of the automatic encoding detection model and the single classification detection model were 0.91 and 0.84, respectively. In Fig. 10(b), there was not much difference in training time among the three models. The training time of the feature fusion detection model was slightly shorter than the other two detection models. After calculation, it was known that the average training time of the feature fusion detection model was reduced by 14.3% compared to the automatic encoding detection model and 17.43% compared to the single classification detection model. To verify the detection time of the model in the face of traffic attacks, the control model remained unchanged and the traffic quantity was divided into small-scale and large-scale tests. The comparison of traffic detection time for the three models was shown in Fig. 11.



(a) Accuracy (b) Training time

Fig. 10. Comparison of accuracy and training time.



(a) Small number of traffic (b) Large number of traffic

Fig. 11. Comparison of traffic detection time for various models.

In Fig. 11(a), when the number of attack traffic was small, the average detection time of the feature fusion detection model was relatively stable, and slowly increased with the increase of attack traffic. During the process of increasing the number of attack traffic from 10 to 60, the average detection time fluctuated between 2ms and 2.3ms. The growth rate of autoencoder detection models was relatively large, with the average detection time increasing from the initial 2.1ms to 7.8ms as the number of attack traffic increases. In Fig. 11(b), as the number of attack traffic increased significantly, the average detection time of the three detection models also increased significantly. When the number of attack traffic was 500, the average detection time of the feature fusion detection model was 12ms. When the number of attack traffic increased to 3000, the average detection time also increased to 23ms. At this time, the average detection time of the automatic encoding detection model and the single classification detection model were 43ms and 37ms, respectively. The malicious traffic detection time of the feature fusion detection model was shorter and the detection efficiency was higher than the other

two types of detection models. To further verify the detection performance of the feature fusion detection model, 400 samples were selected for the experiment. 40% of the samples were used as the test model, and 60% of the samples were used as the training model. The analysis and recognition results of the fusion detection model on traffic types were shown in Fig. 12.

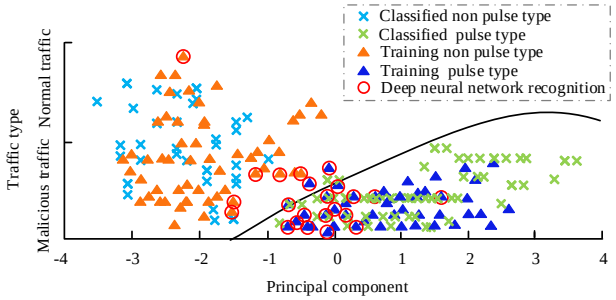


Fig. 12. Analysis and identification results of traffic types by fusion detection model.

In Fig. 12, the probability of correctly identifying the traffic samples used as training models was relatively high. Calculations showed that the accuracy of identifying malicious traffic on the training set was 96.89%. On the test set, 182 traffic samples were accurately identified, including 139 correctly identified malicious traffic and 43 correctly identified normal traffic, with recognition accuracy of 98.73% and 97.65%, respectively. Experimental results showed that both the training set for identifying attack traffic types and the test set for analyzing and judging traffic sample types had excellent performance, with high recognition rates and accuracy for traffic. It also proved that the detection algorithm that integrated temporal and spatial features could efficiently and reliably extract and judge traffic data features, with strong stability in detection and recognition.

To scientifically validate the performance of research methods, the latest malicious traffic detection algorithms were introduced for comparative experiments, namely convolutional neural networks and bidirectional gated space recurrent units (CNN-BiGSRU) based on convolutional neural networks and bidirectional gated space recurrent units, improved k-nearest neighbor based on cost sensitivity (IKN-CS) based on cost sensitivity, stacking and multi feature fusion (SMFF) based on multiple feature fusion, and a hybrid model based on deep learning algorithms and tabu search (DLTS). From this, the performance comparison of different malicious traffic detection algorithms can be obtained, as shown in Table I.

According to Table I, the research method had the best F1 score, accuracy, precision, and recall results, which were 99.2%, 99.5%, 99.6%, and 99.7%, respectively. In addition, the latest mainstream malicious traffic detection algorithms performed well, with all indicators exceeding 95%. The performance of the SMFF method was the worst, which may be due to the fact that the dataset used for testing contained normal and malicious traffic that were not of the same magnitude. However, this method was more suitable for detecting normal and malicious traffic of the same order of magnitude, but in practical application scenarios, normal and abnormal traffic were usually unbalanced. In summary, compared with mainstream methods, the research method still maintained excellent detection performance.

TABLE I. PERFORMANCE COMPARISON OF DIFFERENT MALICIOUS TRAFFIC DETECTION ALGORITHMS

Algorithm	F1 value/%	Accuracy/%	Precision/%	Recall/%
Feature fusion algorithm	99.2	99.5	99.6	99.7
DLTS	98.3	98.3	97.2	98.1
CNN-BiGSRU	97.9	98.1	98.4	97.6
IKN-CS	96.6	97.5	96.7	96.4
SMFF	95.8	96.4	96.3	95.7

V. DISCUSSION

To solve the problem of massive IoT data being vulnerable to attacks, an optimized malicious traffic detection algorithm is studied and designed, which integrates temporal and spatial features and enhances algorithm performance through mixed sampling and variational autoencoder data.

Tests on the IoTID20 dataset revealed that the accuracy of all four detection algorithms increased with the number of iterations and eventually stabilized. After the 40th iteration, the accuracy of the research algorithm increased from the initial 77% to 98.3%. The accuracy results of the XIoTID dataset were as follows, and the research method achieved the highest accuracy of 84.2% at the 60th iteration. Tang D et al. proposed a low-frequency DDOS attack detection algorithm based on multifeature fusion and sperm donation neural network, which could accurately detect DDOS attacks similar to normal traffic. The research results showed that fusing various network features into a feature map to represent the state of the network could effectively help improve the performance of the detection algorithm [23]. The above findings were consistent with this study due to the fact that the feature fusion algorithm integrally considered the correlation of the historical data before and after, which enriched the information content of the extracted feature data.

Compared with the current state-of-the-art malicious traffic detection methods, the results showed that the research method had the best F1 score, accuracy, precision, and recall rate, corresponding to 99.2%, 99.5%, 99.6%, and 99.7%, respectively. In addition, the latest mainstream malicious traffic detection algorithms perform well, with all indicators exceeding 95%. Liu Z et al. proposed a Bayesian meta-learning technique for the detection of encrypted malicious traffic to solve the problem of small sample size. The experimental results showed that when the sample size of malicious traffic was reduced to 100, the detection accuracy of the research model was 96.35% [24]. The study demonstrated that the accuracy of 98.3% can be achieved even with a limited sample size through the incorporation of a data augmentation processing method based on mixed sampling and variational autoencoder. This approach could effectively enhance the accuracy of research methods.

In summary, the research method can effectively improve the security level of IoT access devices, and ensure the security of information data processing and protection.

VI. Conclusion

To improve the detection capability of traffic detection systems for malicious traffic and achieve real-time security checks on IoT devices to achieve system security protection, an optimized malicious traffic detection algorithm was proposed. This research analyzed and identified traffic data by integrating temporal and spatial features, and used hybrid sampling and variational autoencoders to improve algorithm performance. As a result, in both the KDD99-CUP dataset and the XIoTID dataset, the performance of the proposed feature fusion algorithm was the highest, with an F-value of 93.16% in the former dataset and the highest accuracy of 84.2% in the latter dataset. Compared with the latest algorithms, the research method had the best F1, accuracy, precision, and recall results, which were 99.2%, 99.5%, 99.6%, and 99.7%, respectively. It also performed well against the latest mainstream malicious traffic detection algorithms, with all metrics exceeding 95%. Experimental results showed that the detection accuracy and efficiency of the IoT malicious traffic detection model based on feature fusion are high. However, the study only analyzed and identified normal and abnormal traffic, without conducting more in-depth identification and classification of abnormal traffic. Future research will further analyze the identified abnormal traffic to distinguish the types of unknown traffic attacks and achieve more favorable warning effects.

References

[1] Bandewad G, Datta K P, Gawali B W, & Pawar, S. N. Review on Discrimination of Hazardous Gases by Smart Sensing Technology. Artificial Intelligence and Applications. 2023, 1(2): 86-97

[2] Ahmad Muhammad Thantawi, Sri Astuti Indriyati. Conceptual Design Impacts in New Normal Era: The Use of Artificial Intelligence (AI) And Internet of Things (IOT) (Case Studies: Class Room and Restaurant). Acta Informatica Malaysia. 2022; 6(2): 39-42.

[3] Egrioglu E, Grosan C, Bas E. A new genetic algorithm method based on statistical-based replacement for the training of multiplicative neuron model artificial neural networks. Journal of supercomputing, 2023, 79(7): 7286-7304

[4] Senthilkumar M, Murugan BS. Enhancing the Security of An Organization from Shadow Iot Devices Using Blow-Fish Encryption Standard. Acta Informatica Malaysia. 2022; 6(1): 22-24.

[5] Doerr B. The Runtime of the Compact Genetic Algorithm on Jump Functions. Algorithmica, 2021, 83(10): 3059-3107

[6] Yang H, Xiong Z, Zhao J, Niyato D, Wu Q, Poor H, Tornatore M. Intelligent Reflecting Surface Assisted Anti-Jamming Communications: A Fast Reinforcement Learning Approach. IEEE transactions on wireless communications, 2021, 20(3): 1963-1974

[7] Salem A, Masouros C, Wong K. On the Secrecy Performance of Interference Exploitation With PSK: A Non-Gaussian Signaling Analysis. IEEE transactions on wireless communications, 2021, 20(11): 2014-2018

[8] Su N, Liu F, Wei Z, Liu Y, Masouros C. Secure Dual-Functional Radar-Communication Transmission: Exploiting Interference for Resilience Against Target Eavesdropping. IEEE transactions on wireless communications, 2022, 21(9): 7238-7252

[9] Du Z, Zhang F, Zhang Z, Yu W. Radar Detector in Uncoordinated Communication Interference Plus Partially Homogeneous Clutter. IEEE Communications Letters, 2021, 25(6): 1999-2003

[10] Hosseinali J, David M. Multicarrier Spectral Shaping for Non-White Interference Channels: Application to Aeronautical Communications in the L-Band. IEEE Transactions on Vehicular Technology, 2021, 70(10): 10686-10694

[11] Jiang T, Yu W. Interference Nulling Using Reconfigurable Intelligent Surface. IEEE Journal on Selected Areas in Communications, 2022, 40(5): 1392-1406

[12] Lin J, Lin D, Lu X, Chen J, Li C, Lin P, Huang C, Zheng Y. Using four-quadrant photodetector and improved genetic algorithm for visible-light positioning system. Optical Engineering, 2022, 61(4): 44107-44119

[13] Mahmoudi B, Motameni H, Mohamadi H. A new hybrid algorithm integrating genetic algorithm with Tabu search to solve imbalanced k-coverage problem in directional sensor networks. IET communications, 2023, 17(11): 1243-1254

[14] Shaikh M, Hua C, Jatoi M A, Ansari M, Qader A. Application of grey wolf optimisation algorithm in parameter calculation of overhead transmission line system. IET Science, Measurement & Technology, 2021, 15(2): 218-231

[15] Nagarajan L, Thangavelu S. Hybrid grey wolf sunflower optimisation algorithm for energy-efficient cluster head selection in wireless sensor networks for lifetime enhancement. IET communications, 2021, 15(3): 384-396

[16] Chen X, Rechavi O. Plant and animal small RNA communications between cells and organisms. Nature Reviews Molecular Cell Biology, 2021, 23(3): 185-203

[17] Luo J, Chen Z, Castellano D, Bao Bi, Han W, Li J, Kim G, An D, Lu W, Wu C. Lipids regulate peripheral serotonin release via gut CD1d. Immunity, 2023, 56(7): 1533-1547

[18] Nguyen D N, Dam H. Machine learning-aided Genetic algorithm in investigating the structure–property relationship of SmFe12-based structures. Journal of Applied Physics, 2023, 133(6), 63901-639010

[19] Greifenstein M, Dreizler A. MARSFT: Efficient fitting of CARS spectra using a library-based genetic algorithm. Journal of Raman Spectroscopy, 2021, 52(3), 655-663

[20] Yang R, Ma Y, Zhao M, Wei H, Qian L, Zhangyuan C, Aimin W, Szeyun S, Shinji Y, Zhigang Z. Flat visible spectrum by a genetic algorithm optimized photonic crystal fiber in the GHz comb spacing. Optics Letters, 2023, 48(11): 2829-2832

[21] Ji W, Ma K, Zhong L,Ying M, Guolin L. A Genetic Algorithm-Optimized Extreme Learning Machine Model for Process Ethylene Analysis Robustness Enhancement. Spectroscopy, 2021, 23(1): 44-48

[22] Rugo A, Ardagna C, Ioini N. A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis. ACM Computing Surveys (CSUR), 2022, 55(1): 21-55

[23] Tang D, Tang L, Shi W, Zhan S, Yang Q. MF-CNN: a New Approach for LDoS Attack Detection Based on Multi-feature Fusion and CNN. Mobile Networks and Applications, 2020. 26(7):1705-1722.

[24] Liu Z, Lv Z, Zhao L, Li M, Liu X. A malicious traffic detection method based on Bayesian meta-learning for few samples. International Journal of Embedded Systems, 2023, 16(3):235-244.

Replace Your Mouse with Your Hand! HandMouse: A Gesture-Based Virtual Mouse System

Qiujiao Wang[1], Zhijie Xie[2*]
Department of Foundation, Southwest Jiaotong University Hope College, Chengdu, China[1]
Chengdu Transportation + Tourism Big Data Application Technology Research Base, Chengdu, China[1]
School of Computing and Artificial Intelligence, Southwest Jiaotong University, Chengdu, China[2]
Chengdu Office, Shanghai Tecwin Software Technology Co., Ltd, Chengdu, China[2]

Abstract*—The existing gesture-based operating systems can only simply operate a single piece of software or a specific system, and are not compatible with other applications of mainstream operating systems. In this paper, based on the MediaPipe gesture recognition framework, we design HandMouse, a virtual mouse system that operates using hand gestures. It has the following characteristics: 1. The user does not have contact with the computer hardware when using the system; 2. It requires only one hand to operate, and the design of the gesture considers the ergonomics of the hand; 3. It has most of the functions commonly used in a physical mouse; 4. It can locate the operating area with relative precision. We invited 27 participants to use and evaluate the virtual mouse and then conducted an experiment to compare the performance of the virtual mouse with the physical mouse. The results show that this virtual mouse has a good learning effect and is a great alternative to the physical mouse in public places. The demonstrated operation video is available on *https://github.com/wanzhuxie/HandMouse-IJACSA.

***Keywords*—Virtual mouse; ergonomics; gesture; MediaPipe**

I. Introduction

Gesture recognition has been the subject of research for several decades. As early as 1997, paper [1] has provided a comprehensive summary of the accumulated technology of gesture recognition at that time, and it has experienced rapid development over the past 20 years. There are approximately four research directions for gesture recognition. The first direction involves the use of physical sensors to transmit information. For example, papers [2, 3] described sensor gloves with gesture recognition capabilities, while the system proposed in paper [4] processes finger pressure signals, and a virtual keyboard was designed in paper [5]. The second direction involves the use of cameras to extract finger information. Although physical sensors are not in direct contact with the computer, the recognition process requires the assistance of gloves of different colours to help the computer identify gestures, as described in papers [6, 7]. The third direction focuses on processing images without external elements to assist the computer. Advanced algorithms are used to extract hand images from gestures and infer their meaning, as demonstrated in papers [8-10]. The fourth direction involves inferring the coordinates of the key points of the hand and leaving the recognition of gestures to the specific gesture designers. This allows designers to consider more details and design a wider range of gestures. Deep learning techniques are commonly used for this purpose, for example, in 2016, paper [11] presented a gesture recognition system based on recursive 3D convolutional neural networks, achieving an accuracy of 83.8%. In 2017, a paper [12] trained a hand recognition model using 18,000 stereo hand images and the 3D key points in each image in different scenes, demonstrating a good tracking performance. In 2019, Google Artificial Intelligence Laboratory released an open-source gesture recognition framework called MediaPipe Hands [13], which continues to be maintained. MediaPipe Hands was trained using 300 million real-life hand gesture images with the corresponding 3D key point coordinates of the hand, achieving an overall recognition accuracy of 95.7%.

Thanks to the increasing efficiency and accuracy of gesture recognition technology, it has a wide range of applications in areas such as sign language recognition, remote-controlled robots, and human-computer interaction (HCI) [14-16]. Compared with the traditional mouse click or touch screen operation, it is more popular to add gesture operation into human-computer interaction system [17]. Gesture operation has significant appeal to customers due to its novelty, and the potential purchasing power of customers may be stimulated by the exploration or trial of gesture control. Gesture operation enables humans to have no physical contact with the machine, allowing users to be at a greater distance from the device, which enables a better layout planning for venue managers, prevents accidental damage caused by customers touching the device, and prevents the spread of diseases caused by touching. In paper [18], preliminary research on gesture output of Chinese was conducted. In paper [19], a gesture-based image viewer software was designed and applied to touchless operations in surgical room scenarios. The study in [20] proposed a gesture recognition method for controlling in-car devices. Furthermore, gesture recognition has been applied in gaming interactions as discussed in papers [21, 22], and an interesting study conducted in paper [23] explored the use of gestures for simple coding purposes.

Since the gesture commands have been used to realize the simple control of specific software, can they be further developed by using gestures to realise the functions of the physical mouse, such as the commonly used left-clicking, left-double-clicking, right-clicking, etc.? The answer is yes. At present, the gesture-based system can realize all or some of the

*Corresponding author
This work was supported by the Chengdu Philosophy and Social Science Key Research Base: Chengdu Transportation + Tourism Big Data Application Technology Research Base, China (20231003).

functions of the physical mouse and allow the operator to have no direct contact with the machine hardware, for what we can call it a virtual mouse. The virtual mouse has been the subject of extensive research by many researchers over the last decade. Although the result presented in paper [24] focused on the virtual keyboard input, its techniques are still relevant to the virtual mouse and serve as a valuable reference. Paper [25] employed a two-layered Bayesian network technique for gesture recognition and designed a virtual mouse system. Paper [26] designed a gesture-based virtual controller for manipulating 3D objects, taking into account the 3D data of finger movements. In paper [27], used convolutional neural network technology to recognise finger and fist gestures, and then developed a simple virtual mouse control system.

However, current gesture operations are specific to particular systems or software, where each gesture represents a specific command for a particular software. Unlike a physical mouse, these gestures are tailored to specific software and lack universality.

Based on existing gesture recognition technology, combined with the physiological structure of the human hand, this paper designs a set of simple and easy-to-use mouse operation gestures. On this theoretical basis, this paper presents an absolutely contactless, entirely gesture recognition-based virtual mouse system. The virtual mouse is independent of the software that is being operated and has a high degree of versatility. With relatively comprehensive functions, the virtual mouse is like a physical mouse, and most of the functions that can be achieved with a physical mouse can also be achieved with the virtual mouse. The general flow of the system is shown in Fig. 1, where the video frame image is captured by the camera, and the key points of the hand are detected by MediaPipe. The gesture recognition module analyses the coordinates of the key points and identifies the current gesture. When a pre-defined gesture is made, the mouse operation module immediately releases the mouse signals to operate any software.

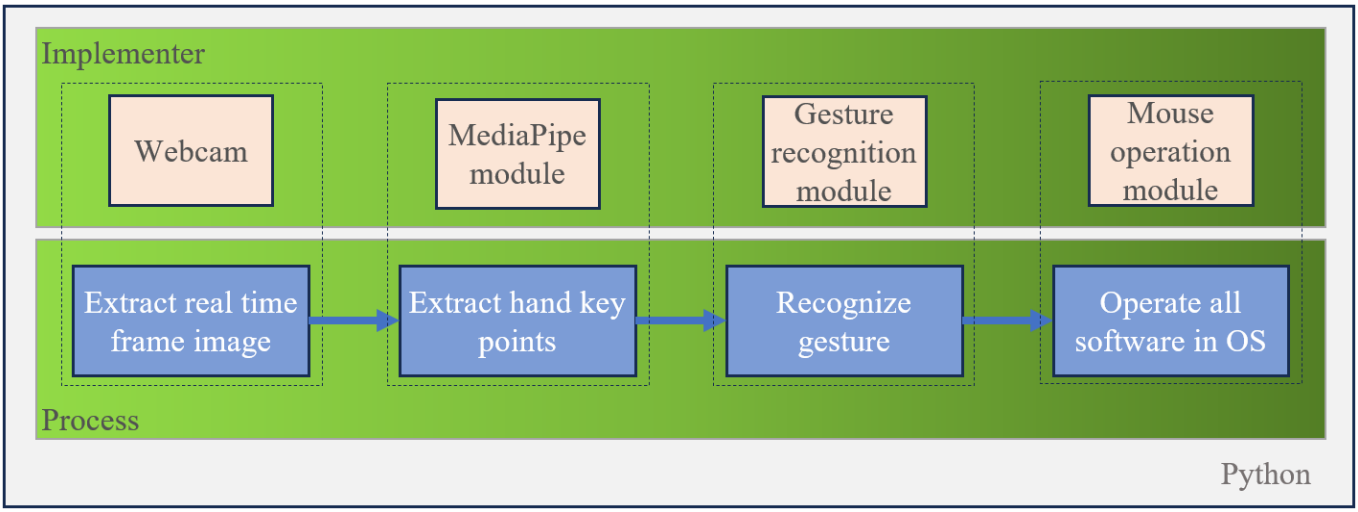


Fig. 1. The system architecture of the virtual mouse system.

II. FOUNDATIONS

A. Key Points of a Hand

There are many ways to recognize various gestures, such as feature matching, extraction of hand key points, and so on. Feature matching can only recognize the pre-defined hand postures, while key points extraction supports all kinds of hand posture, which has stronger speculation ability. As shown in Fig. 2, the 21 key points can basically describe the gesture information of a hand, and the recognition of gesture can be transformed into the analysis of the key points and further into the conversion of abstract image information into specific mathematical information. In this paper, P_n is used to represent the key points at a specific position, where $n \in [0, 20]$, and the sequence number of the starting key point is 0.

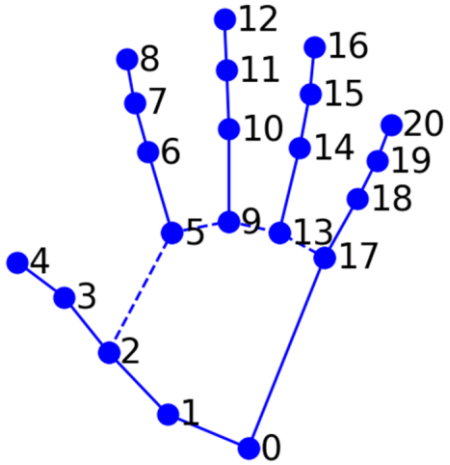


Fig. 2. Key points of a hand.

B. MediaPipe

MediaPipe is a cross-platform machine learning framework [28] that includes a number of sub-frameworks such as gesture recognition, face recognition, whole-body posture recognition, 3D object coordinate inference and so on. It has been widely used in many areas of life and industry. Papers [29-31] apply MediaPipe to home sports equipment, gesture language expression system, and human posture simulator. With the assistance of MediaPipe, papers [32, 33] developed the measurement system for some human rehabilitation movements and the abnormal gesture detection system for patients with the nerve injury. Paper in [34] developed a human emotion detection system using MediaPipe.

MediaPipe Hands is one of the frameworks of MediaPipe, which supports five fingers and gesture tracking, and can infer 21 stereo nodes of one hand from a frame image. Even if the palm is partially displayed or the hands are self-occluded, it can achieve high robustness, high performance, and low time consumption, so it has been applied in a variety of fields. Paper [35] designed a sign language expression system for Japanese; paper [36] captured the motion trajectory of fingers by analyzing the 3D coordinates of the key points of hand, and then designed an air-writing system; paper [37] used MediaPipe to identify the driver's hand information in a driver distraction warning system.

The system described in this paper also uses MediaPipe Hands to extract the coordinate information from the 21 key points of the hand. It reads each frame image captured by the camera and provides three coordinate values of the key points. Since the image can be scaled to meet the needs of image analysis, information transmission, image display and so on, when it is processed, the original coordinate values of the key points are normalised values, i.e. each coordinate value is a proportional value relative to the image size. The normalized datum of the X and Z coordinate value is the width of the image, and the normalized datum of Y coordinate value is the height of the image. Therefore, before using the coordinate value of key points, it is necessary to calculate the pixel coordinates of key points according to the frame image size obtained by the camera.

Although the performance of the MediaPipe Hands was excellent, there is a drop in recognition accuracy when the background colour is similar to the hand colour, or when the overall lighting is poor. The user may also make errors. The system therefore optimises the recognition reliability of MediaPipe. When recognising the current gesture, it is only considered to have changed if the camera captures the same gesture three times in a row. Otherwise, it is considered a single misrecognition by MediaPipe or the user, and the recognition result of the previous frame is returned.

C. Coordinate System

The default coordinate system of the display screen of the system takes the upper left corner as the origin, the horizontal right direction along the screen is the positive direction of the X axis, and the vertical downward direction along the screen is the positive direction of the Y axis. The coordinates (X_{max}, Y_{max}) of the bottom right corner of the screen are related to the screen resolution. When analyzing gestures, the larger the Y coordinate of the hand key point, the lower the position of the point.

III. Basic Design of Gesture Operations

A. Design Principles

First of all, we give three design principles:

1) Single-handed operating. Although two-handed operation can express more information, as in the application scenarios in [38-40], it also increases the demands on the operator. Compared with single-handed operation, it has two disadvantages. Firstly, the operator has to raise both hands at the same time to make gestures during the operation and may feel tired after a short time. Secondly, when two hands are operating together, they may be required to make different gestures, so the error rate of two-handed operation may be higher than that of single-handed operation or the operation of two hands making the same gesture.

2) Simple gestures considering. Due to the physiological structure of the hand, most people can't stretch out their ring finger alone as easily as their index finger. They need to work with other adjacent fingers to make gestures quickly and accurately. Therefore, the system does not use the ring finger alone as an indication signal, which reduces the probability of error gestures.

3) Multiple postures of hand supporting. In the process of specific operation, many scholars have studied the palms parallel to the display screen as a condition for gesture recognition [8, 25, 39, 41]. Meeting this condition can indeed improve the accuracy of detection, but it is not a small challenge to the user's physical strength and patience. In fact, if the palm plane is kept parallel to the screen all the time, the user's arm and wrist will feel tired in a short time and will not be able to perform gesture operations, which will reduce the user's use experience and may also cause the user's resistance. What can be determined is that people would prefer the system to be compatible with multiple postures of the same gesture, so that different postures can be changed during a long period of operation to alleviate the fatigue caused by gesture operation. Therefore, the system supports any angle between the palm plane and the screen plane, and users can make gesture signals according to their customary posture. All postures shown in Fig. 3 indicate that only the index finger is extended. It should be noted that, for ease of expression and understanding, all the gesture images in this paper are generated from the perspective of the operator. The gesture image captured by the camera should be the image observed in the opposite direction. However, this does not affect the design of the algorithm. As mentioned above, the system supports multi-position operation.

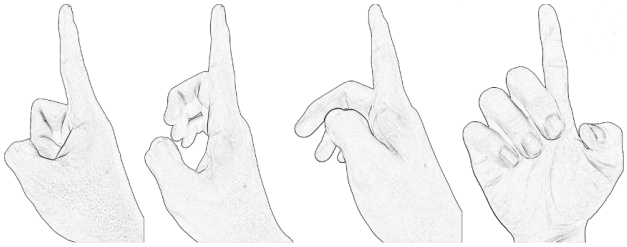


Fig. 3. Multiple gestures express that only the index finger is extended.

B. Gesture Unit Judgment

In this paper, the gesture of a single finger is called a gesture unit. The gesture unit has two states, the extension and closed of the finger. Each gesture signal is a combination of the states of each finger. To improve versatility and fault tolerance, this system does not consider the angle between fingers, but only whether each finger extends. We use five binary numbers to represent gestures for the convenience of display. Each number represents the extension and closed of the corresponding finger, with 1 representing the extension and 0 representing the closed. The numbers from left to right represent the status of the thumb, index finger, middle finger, ring finger, and little thumb. For example, [01000] means that only the index finger is extended.

For the other four fingers except the thumb, the extended condition is that the fingertip's key point is above its corresponding three other key points as shown in Fig. 2, as

$$Y\left(P_i\right) < Y\left(P_j\right) \tag{1}$$

where, $i \in \{8,12,16,20\}$ is the key point indexes of the fingertip and $j \in [i-3, i)$ is one of three other key points indexes.

This determination method is suitable for the scenario where multiple fine-tuned gestures are used to express the same signal, reducing the fatigue caused by the user making the same gesture for a long time.

For the thumb, the relationship between the thumb and the other four fingers is determined first, and then its extension and closed are determined based on the coordinate relationship between the thumb tip key point and the other key points of the thumb. If $X\left(P_2\right) > X\left(P_{17}\right)$, we define the handedness to be the right, and if $X\left(P_3\right) > X\left(P_4\right)$, then the thumb is closed, otherwise it is extended. Similarly, if $X\left(P_2\right) \le X\left(P_{17}\right)$, we define the handedness to be the left, and if $X\left(P_3\right) < X\left(P_4\right)$, then the thumb is closed, otherwise it is extended.

C. Gesture Operation Area

Mouse movement is the most common operation, and in terms of the difficulty of making gestures, it is easier to extend the index finger alone. In addition, using the index finger to guide the mouse pointer is also in line with the public's understanding of the habit. Therefore, this system uses the extension of the index finger as the signal to set the mouse position, and the mouse pointer moves with the movement of the tip of the index finger.

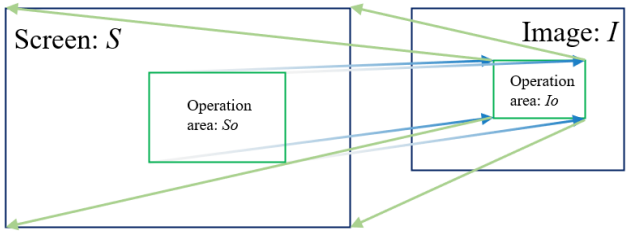


Fig. 4. The correspondence between the screen area and image area.

As shown in Fig. 4, *S* indicates the display screen area, *So* indicates the active area of the index fingertip on the screen *S*, which should be significantly smaller than *S*, otherwise it will cause two problems. Firstly, the components at the bottom of the screen cannot be operated because when the index fingertip is at the bottom of the screen, the hand is outside the screen area, and the recognition rate of a hand is very low, or even impossible. Similarly, when using the right hand, the components on the right side of the screen cannot be manipulated, and when using the left hand, the components on the left side of the screen also cannot be manipulated. Secondly, if the active area of the index fingertip is larger, the active area of the human hand will also be larger, and the range of activity of the arm will increase, which not only tires the arm, but also takes time to position the pointer. In fact, when the physical mouse is positioned, it will move much less than its pointer. Therefore, the size of *So* should be consistent with the motion range of the index fingertip when only the wrist is active. It is therefore necessary to map the fingertip coordinates in *So* to *S* in order to set the pointer coordinates.

In fact, there is another intermediate area between *So* and *S*, which is the corresponding area *Io* in the image of *So* on the screen, as shown in Fig. 4, where *I* is the area of the image captured by the camera. It should be noted that the height-width ratio of the image may not be the same as that of the screen. The coordinates of each key point of the hand are captured from the image, so the operation area in the image should be considered initially. But when the system is working, it is not necessary to display the image area, shown at the top right of Fig. 5, on the screen. The operator is not obliged to calculate the mapping relationship between the image and the screen, but only needs to customize the operation area on the screen. Depending on the size of the image, the system first maps the user-defined operation area So onto the operation area *I*o and then maps *I*o onto the screen, so that the index fingertip can wander around the entire screen and operate on target objects at any position. The above mapping process is also shown in Fig. 4.

It needs to consider multiple factors when setting the area of *S*o. If the area is too large, the swing range of the user's arm needs to increase, which will increase the user's fatigue. If the area is too small, because the area is mapped to the entire screen area, the slight movement of the fingers in this area may produce a large mouse pointer movement effect on the entire screen, which will affect the positioning accuracy. By default, the system sets the size of *S*o to a quarter of the screen size and places it in the centre of the screen. In fact, the size and

position of the operation area depend on the relative position of people and cameras. In order to adapt to cameras with different parameters or different installation positions of cameras with the same parameters, the system supports the operators to adjust the operation area.

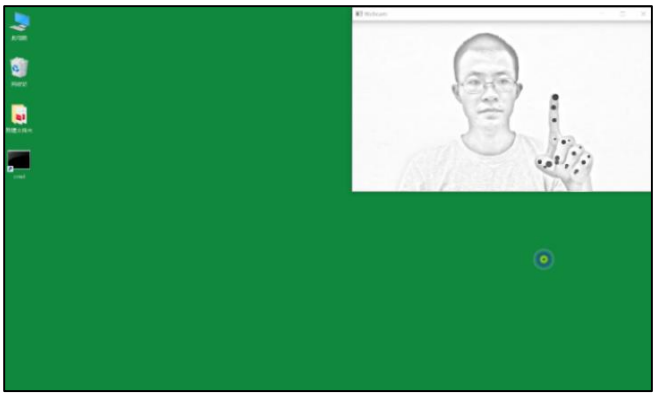


Fig. 5. The real screen area and the image area.

D. Mouse Position Calculation

Before performing mouse operations, the operator needs to use the tip of their index finger to locate the target position on the screen. We use $f(x,y)_s$ representing the coordinates of the index fingertip on the screen, and then we will derive and calculate it.

If R_{io} indicates the size of the operation area in the image, R_i indicates the size of the image, R_{so} indicates the size of the operation area in the screen, and R_s indicates the size of the screen. They have the following corresponding relationship.

$$R_{io} / R_i = R_{so} / R_s \tag{2}$$

The width and height of each of the four areas satisfy the above relationship, i.e., the four dimensions above can represent both width and height.

From the mapping relationship between S_o and I_o we can see that any position in S_o (the image operation area) $f(x,y)_{io}$ and the corresponding position $f(x,y)_{so}$ in I_o (the screen operation area) have the relationship.

$$f(x,y)_{io} = \frac{R_{io}}{R_{so}} f(x,y)_{so} \tag{3}$$

From the mapping relationship between I_o and S, the position of the fingertip in S (the screen) $f(x,y)_s$ has the following relationship with the corresponding position $f(x,y)_i$ in I (the image).

$$f(x,y)_s = \frac{R_s}{R_{io}} \left(f(x,y)_i - f(x,y)_{iom} \right) \tag{4}$$

Where, $f(x,y)_{iom}$ is the upper left corner of I_o (the image operation area), which can be obtained by the following equation.

$$f(x,y)_{iom} = \frac{R_{io}}{R_{so}} f(x,y)_{som} = \frac{R_i}{R_s} f(x,y)_{som} \tag{5}$$

Where, $f(x,y)_{som}$ is the upper left corner of S_o (the screen operation area).

From above equations, we can express the relationship between $f(x,y)_s$ and $f(x,y)_i$ as

$$f(x,y)_s = \frac{R_s^{\,2}}{R_i R_{so}} \left(f(x,y)_i - \frac{R_i}{R_s} f(x,y)_{som} \right) \tag{6}$$

Where, the screen size R_s is fixed; the image size R_i is depends on the camera settings and is also known. The size of the screen operation area R_{so} and its upper left corner $f(x,y)_{iom}$ are user defined or system default given values, which are also known. So $f(x,y)_s$ varies with the variable $f(x,y)_i$, and the latter can be calculated by the logic of the image processing section described above, up to this point we obtain an expression for the coordinates of the index fingertip.

In order to ensure that the value of the index fingertip's coordinate $f(x,y)_s$ does not have a negative value or a value that exceeds the screen area, we place a restriction on the final mouse pointer coordinate value, and the X-coordinate of the mouse pointer satisfies the following equation.

$$P_x = \begin{cases} 0 & , f(x,y)_s|_x \in (-\infty, 0) \\ R_s|_x & , f(x,y)_s|_x \in (R_s|_x, +\infty) \\ f(x,y)_s & , f(x,y)_s|_x \in [0, R_s|_x] \end{cases} \tag{7}$$

Similarly, the Y-coordinate of the mouse pointer satisfies

$$P_y = \begin{cases} 0 & , f(x,y)_s|_y \in (-\infty, 0) \\ R_s|_y & , f(x,y)_s|_y \in (R_s|_y, +\infty) \\ f(x,y)_s & , f(x,y)_s|_y \in [0, R_s|_y] \end{cases} \tag{8}$$

where, $R_s|_x$ is the width in pixels of the screen, $R_s|_y$ is the height in pixels of the screen, $f(x,y)_s|_x$ is the theoretical X-coordinate of the mouse pointer in the screen and $f(x,y)_s|_y$ is the theoretical Y-coordinate of the mouse pointer in the screen.

E. Mouse Sensitivity Design

Due to the hand inevitable tremor in front of the camera, the mouse pointer on the screen often frequently jump caused by the small movement of the hand. Hand tremor is unavoidable, and we can only minimise the effect caused by it [42]. The position can be recorded and compared with the last recorded position, and if the difference is within a certain error range, it is considered to be an invalid signal caused by hand tremor. In fact, this method filters out the effect of hand tremor, but it also ignores the signals that occur when the user actually

intends to move the mouse to another near position. Additionally, when the mouse is moved using gesture signals, the movement of the mouse pointer is not smooth, but rather jumps in discrete steps, with the step size depending on the error value. This may result in a less smooth user experience.

For mouse pointer positioning, this system detects the coordinates of the index fingertip on the screen and calculates a weighted value by combining the fingertip coordinates with the current mouse pointer position as the new pointer position.

The specific algorithm is as follows:

Step 1: Record the last mouse pointer coordinates $P(x_l, y_l)$.

Step 2: Detect the coordinates of the index fingertip in real time and calculate the weighted result of the fingertip coordinates and the last mouse pointer coordinates.

$$P(x_r, y_r) = P(x_l, y_l) + P(a(x_c - x_l), b(y_c - y_l)) \quad (9)$$

where, $P(x_r, y_r)$ is the weighted coordinates, x_c, y_c are the X and Y coordinates of the current index fingertip point respectively, a and b are constants, their range is all (0,1], when $a = b = 1$, it is equivalent to using the current fingertip coordinates as the coordinates of the mouse pointer.

The system correlates the value with the screen resolution, i.e.

$$\frac{a}{b} = \frac{R_s|_x}{R_s|_y} \quad (10)$$

Step 3: The weighted result of the fingertip coordinates and the last mouse pointer coordinates may have values that are outside the screen area, so the weighted result is constrained similarly to the "(8)" and "(9)" to ensure that the mouse pointer coordinate values are not outside the screen area.

IV. Gesture Design

A. Signal Categories and States

The Fig. 6 is the logic flow chart of the system operation, the blue rectangle indicates the system state, we define three states for the system, respectively, the *Ready* state, which is the first state after the system initialisation, the *Pressing* state during the mouse pressing process, and the *Adjusting* state during the operation area adjustment process.

The solid rounded rectangle represents the operation signals. Considering the mouse operations commonly used in the operating system, the operation signals of this system are left click, left double click, right click, scroll wheel up, scroll wheel down, left button press, and left button release, which are seven signals in total. Except for the two operations of scroll wheel, the other operations need to accurately locate the target area before the operation actions, so we call them locating operations, and the two operations of scroll wheel are called non-locating operations. In addition to mouse operations, the system supports customisation of the operation area, including setting its size and position. After initialization, if the system detects that only the index finger is extended [01000], it enters the *Ready* state, in which the mouse pointer follows the tip of the index finger.

The dashed rectangular rectangles indicate the indication signals, which are used to support the state switching and operation signaling.

The design of the gesture signals is the core of this system. For the Locating operations, the first step is to move the mouse pointer to the target object. Once the mouse pointer is placed, it should be held still while the corresponding gesture signal is performed. When making a gesture signal, the index finger should be extended as it plays a role in the composition of the gesture signal. If the index finger needs to be closed during this time, the spatial position of the index finger would change from extended to closed, making it difficult for the system to recognise the actual purpose of the index finger movement. It could be interpreted as a signal for an operation or simply as a movement of the mouse pointer. Therefore, the index finger should remain extended for positioning operations.

Indeed, if someone wants to keep the index finger away from the next action signal, an intermediate state can be introduced before the Locating operation. In this state, the mouse pointer no longer moves with the movement of the index fingertip, but remains stationary on the target object until the next signal action. During this time, the index finger can move freely to perform gestures. However, using this approach would require at least two actions to simulate one operation of the physical mouse, including a state transition action and a mouse operation action, which may introduce inconvenience in the operation process. Therefore, this system adopts the method that the index finger participates in the gesture signal composition for the locating operations.

Furthermore, it should avoid making gestures that may cause significant changes in the position of the index fingertip for the next operation. For example, extending the ring finger may cause an obvious change in the position of the index fingertip. As mentioned earlier in the discussion of mouse sensitivity, any change in the position of the index fingertip will have a larger impact on the screen. Due to this change, the mouse pointer may have moved beyond the intended target area. In fact, the extension and closing of the thumb have minimal impact on the other four fingers. Therefore, the system does not utilize an intermediate state but directly uses the thumb to send the operation signal.

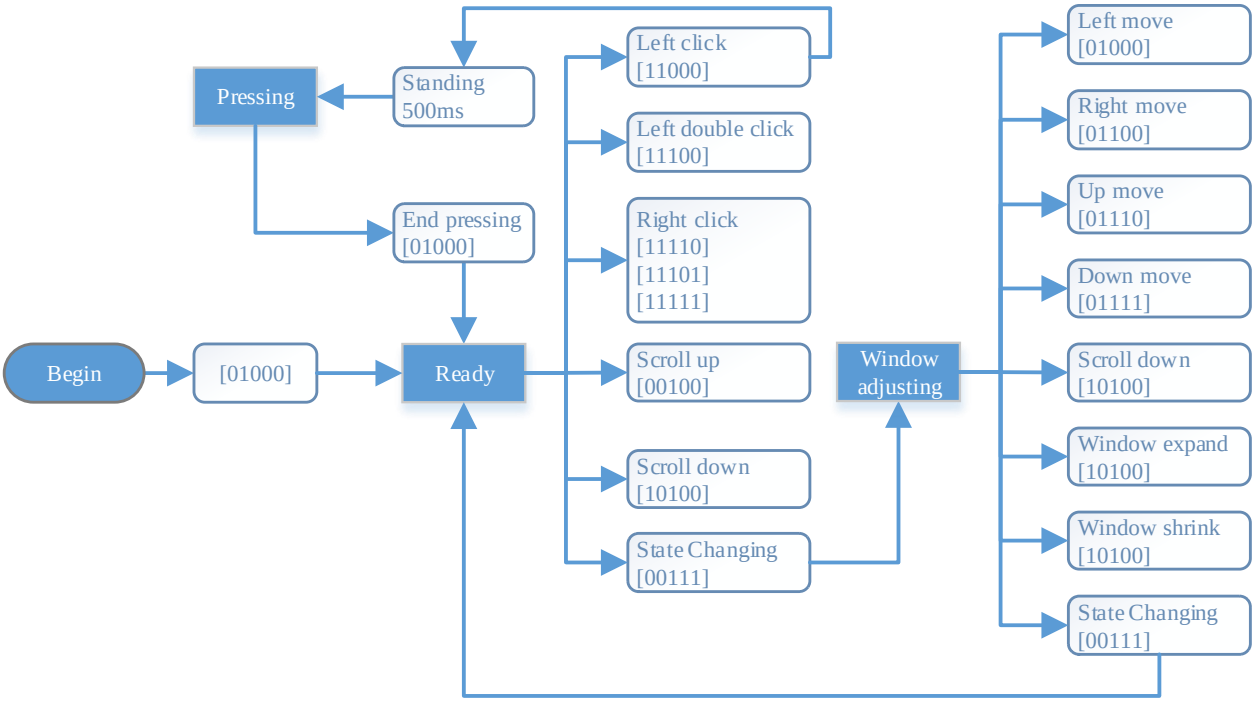


Fig. 6. System flow chart.

B. Operation Signal Design

1) Left clicking, pressing and releasing: Precision control and user comfort are two essential considerations in gesture operations [42, 43]. When designing the signals, the frequency of use of each operation is an important consideration. The more frequently an operation is used, the simpler the corresponding gesture should be. Left-clicking is the most frequently used mouse operation, and we use the index finger as the corresponding gesture for it, similar to the approach used in the references [44, 45]. When users want to left-clicking on an object, they first extend their index finger [01000] and place the mouse pointer over the target area. Keep the index finger stationary, the thumb can be extended. Then the system will detect the [11000] gesture, which represents the execution of a left-clicking. After the click, the thumb should immediately close, maintaining the [01000] gesture to guide the mouse pointer for the next operation. If the thumb remains extended in the target position for more than 0.5 seconds, the system performs a pressing operation on the target position.

The Pressing state is a specific state designed for dragging files. In the Ready state, if the gesture [11000] is held for 0.5 seconds, the system switches from the Ready state to the Pressing state. Similar to the logic of a physical mouse, the pressing action is executed by the system regardless of whether there is a target object under the mouse pointer. In the Pressing state, the mouse pointer drags the file along with the movement of the index finger until the thumb is retracted, at which point the system releases the left button and stops dragging, and the system immediately return to the Ready state.

To provide clearer feedback on the current state of the system, a semi-transparent coloured halo can be displayed around the mouse pointer in the Ready state. Fig. 7 shows the effect of the halo on the target position with four different background colours. This halo not only serves as an indicator but also helps visualize the position of the mouse pointer. When the system transitions to the Pressing state, the halo is hidden to prompt the user for the current drag operation. This is, of course, optional, and unless the scene has a complex background, it is recommended not to use a coloured halo as it may affect the activity of the pointer.

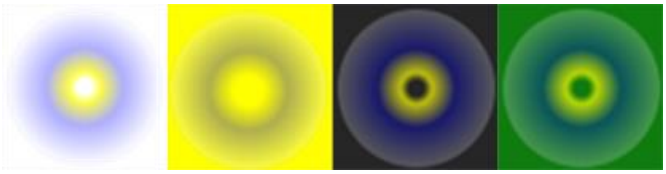


Fig. 7. The halo effect with different background colours.

2) Left-double-clicking: The left-double-clicking operation is also commonly used. From a conventional standpoint, a double-clicking consists of two single-clicks operations, as is the case for the physical mouse. However, when sending a signal, gesture-operated systems generally have a much larger range of motion than the physical mouse. As a result, the time required to perform a double-clicking operation is significantly longer than that of a physical mouse operation. In addition, performing a left-clicking gesture in this system

requires the thumb to be extended and closed once respectively, which can lead to hand fatigue after multiple operations. Therefore, our system uses a combination of the index and middle fingers as the gesture signal for the left double-click. In this case, the user only needs to extend and close the thumb once. When the user wants to make a left double-click on a target area, they can extend both the index finger and middle finger, and the mouse pointer will still follow the movement of the index fingertip. Once the pointer is over the target area, extending the thumb completes the double-click. This approach is similar to the method described in study [45].

3) Right-clicking: Similarly, the gesture corresponding to the right click is the combination of the index, middle and ring fingers. However, due to the physiological structure of the human hand, the ring finger has less dexterity than the other fingers, so the system accepts that the little finger can also act as the ring finger, and the ring finger can of course act on its own. Therefore, there are three gestures corresponding to the right-clicking, respectively [01110], [01101] and [01111].

4) Wheel scrolling and pausing: In most scenarios, scrolling operations with the mouse wheel do not require precise positioning of the mouse pointer. This system uses the gesture [00100] as the signal for scrolling the mouse wheel forward, and uses the gesture [10100] for scrolling the mouse wheel backward. In the *Ready* state, any gesture other than those mentioned above can temporarily pause the current scrolling operation.

C. Operation Area Adjusting

As mentioned above, the size and position of the work area can be adjusted. In order to still be able to operate with single hand, some of the gestures used to adjust the work area will inevitably be the same as those used to operate the mouse pointor, which is why the Adjusting state is raised. The states between Adjusting and others can be switched using the [00111] gesture (OK gesture). In order to minimise the risk of incorrect operations caused by hand movements or tremors, static gestures are used to adjust the operating area instead of dragging. In the Adjusting state, users can easily perform adjusting gestures without worrying about unintended operations. The corresponding gestures for these adjustment operations are listed in Fig. 6.

V. System Test and Discussion

We invited participants to test this virtual mouse system to measure its performance, learning curve and user acceptance. We first determined the unit of measurement of the target area for mouse clicks during the test. The size of the target area operated by the mouse is determined by the desktop application to which the operated object belongs. The smaller the target, the longer it takes to locate it with the mouse. Most UI controls are sized in pixels, so resizing a UI control requires adjusting the pixel values of its width or height accordingly. For mouse controls, however, the physical size of the target area is more important than its pixel size. For example, at resolutions of 1920×1080 and 800×600, an 80×80 target area at the former resolution is smaller than a 60×60 target area at the latter resolution, making it slightly more difficult to focus on using the mouse. Therefore, the target size here refers to the actual physical length, not the number of pixels.

A. User Experience Test

In order to test the learning effect of this virtual mouse system and its acceptance by new users, 27 participants were invited to take part in an experience and learning evaluation of the system. The test was conducted with 2 randomly varying items, the target area to be operated by the mouse and the specific action for each mouse operation. We randomly placed a square target area with sides in the range [30,80] on a 340×195 monitor screen, and randomly appeared an instruction in the square area that required the participant to operate the area. We set up only some of the most commonly used left-clicking, left-double-clicking and right-clicking instructions. The user operated on these target areas according to the instructions, and the next target area to be operated appeared only if the current operation was correct; otherwise the current target area was kept waiting for the user's correct operation. Each test consisted of 20 mouse operations. The operator first performed two tests with the physical mouse to use its average time as a comparison with the virtual mouse, then five tests were performed with the virtual mouse.

Based on the temporal data of the 27 participants' tests, we plotted the learning curve of the system, as shown in Fig. 8, which mainly expresses the mean value of the participants' time for each operation as well as its standard deviation.

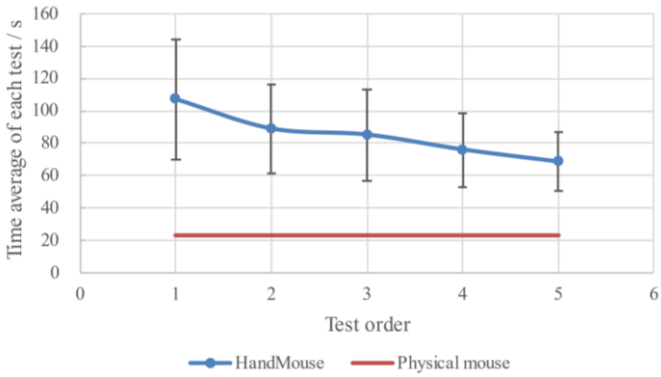


Fig. 8. The learning curve for the system. The blue curve is the learning curve based on the average time taken by the participant to perform the actions using HandMouse, and the red line is the referenced time taken to perform the actions using a physical mouse.

The time curves of the five virtual mouse tests for most participants did not always show a downward trend, but rather significant fluctuations. However, as we can see from Fig. 8, the average value of the test time has an overall decreasing trend, indicating that it still has a relatively positive learning effect. During the testing process, most of the new users would gradually understand and master the use of the system, although not very skillfully. At the same time, however, we can see that the standard deviation of each group's operation is relatively large, indicating that there are relatively large individual differences among the participants. A small number of participants experience a brief period of confusion and disorientation.

B. Subjective User Evaluation

After two physical mouse tests and five virtual mouse tests, each participant was asked to complete a survey to obtain a subjective evaluation of the gesture mouse system from new users. The survey questions were divided into two parts, one based on the NASA-TLX (NASA Task Load Index, https://humansystems.arc.nasa.gov/groups/TLX/) evaluation method, which asked questions about the feel of the operation. The second part compared the virtual mouse with the physical mouse to determine the user's preference between the two and the acceptance of the virtual mouse.

We collected the subjects' feelings from 6 aspects of Mental Demand, Physical Demand, Temporal Demand, Effort, Frustration Level, and Performance, and each of them has a corresponding question. Each item of the NASA-TLX is rated with a score of 20 points, and for each question, we counted the average of the 27 values that subjects rated, and the results are shown in Fig. 9.

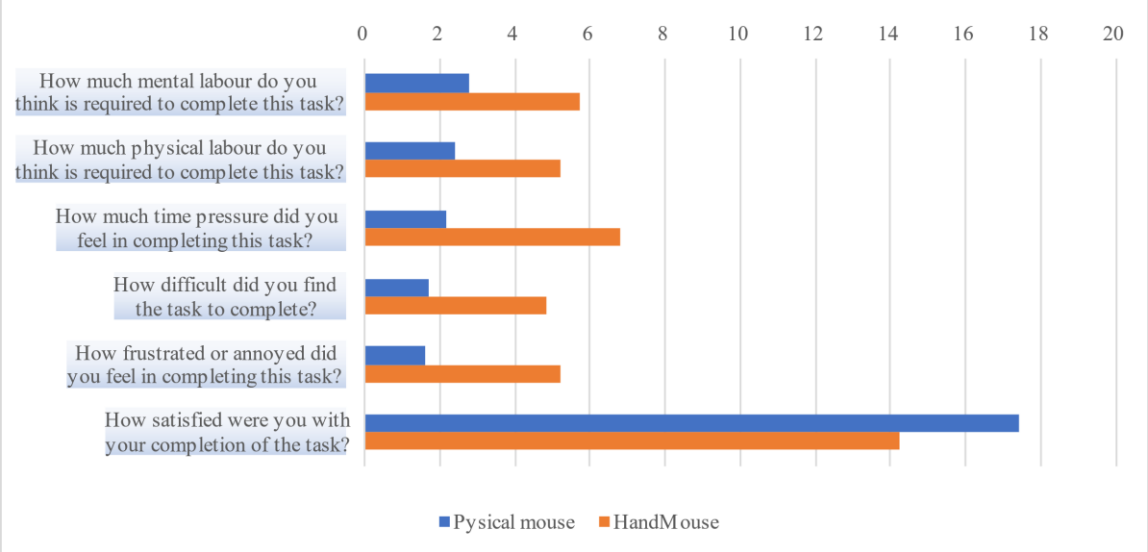


Fig. 9. Evaluation results on NASA-TLX.

The results of the second part of the survey content are shown in Table I, where 22 participants indicated that they would prefer to use this virtual mouse in an HCI system in a public environment, but unfortunately none of them preferred to use it in a work environment. Although this system has tried its best to perform as well as it can, it still has more mental and physical work in using it than a physical mouse. With the need for more precise results in the workplace, this virtual mouse system really isn't a good choice for new users. However, considering its performance, interesting, and technological effects, most of the participants gave it a relatively good rating as a whole.

TABLE I. AVERAGE TIME SPENT ON DIFFERENT OPERATIONS. THE UNIT OF ELAPSED TIME IS MILLISECONDS

Questions	Results
Do you prefer to use a physical mouse or this HandMouse during work or study?	0/27 body selected by HandMouse
Do you prefer to use a physical mouse or this HandMouse in public places such as shopping malls and museums?	22/27 bodies selected by HandMouse
How reasonable do you think the design of the gesture mouse is? (Score [0,20])	15.5 / 20
How satisfied are you with the gesture mouse compared to the physical mouse? (Score [0,20])	15.4 / 20
What is your overall score for this gesture mouse? (Considering rationality of design, technology, interesting, difficulty of operation, etc., Score [0,20])	16.8 / 20

C. Expert Test

To see how the HandMouse is used by experienced users and to explore the limits of its operation, we tested it with smaller target areas. We set the side lengths of the test squares to [6, 8, 12, 16, 20, 25, 30, 40, 50, 60]. Each square was randomly placed on the screen and appeared 20 times in succession. We performed 20 left-clicking operations on each square area and recorded the time taken to perform each operation. We obtained the average test results for different target areas, as shown in Table II and Table III. The open source code repository also contains the test program and the source data.

As can be seen from Table II and Table III, the efficiency of completing a mouse operation is related to the size of the target area and has an overall negative correlation. For the physical mouse, the maximum value of the time spent is about three times the minimum value. The median, mean, and average of Q1-Q3 (values in the middle 50%) are also close to each other, indicating that the physical mouse has great stability when operating on the target area. However, for the gesture mouse, when the target area is less than 12mm, the maximum value is more than 10 times the minimum value because it has one or two obviously large outliers. The overall average is significantly larger than the median and average of Q1-Q3 for the gesture mouse, and the median or average of Q1-Q3 is more representative, but at the same time, the instability of the gesture mouse's functionality should not be ignored.

TABLE II. TIME TAKEN OF PHYSICAL MOUSE OPERATIONS IN DIFFERENT AREAS

Object width / mm	Time taken / ms				
	Max	Min	Average	Median	Average of Q1-Q3
6	1,399	530	1,104	1,092	1,106
8	2,192	639	1,204	1,103	1,111
10	1,423	792	1,020	931	951
12	1,443	712	1,021	1,016	1,017
16	1,483	633	875	823	814
20	1,947	583	868	784	776
25	999	546	717	688	690
30	2,274	450	838	776	777
40	971	527	724	702	706
50	937	454	635	620	617
60	1,208	430	591	516	519

TABLE III. TIME TAKEN OF HANDMOUSE OPERATIONS IN DIFFERENT AREAS

Object width / mm	Time taken / ms				
	Max	Min	Average	Median	Average of Q1-Q3
6	35,464	2,690	7,278	3,991	4,114
8	17,009	1,624	4,884	4,034	4,037
10	18,390	1,876	5,271	3,952	3,889
12	18,526	1,799	4,873	2,957	2,964
16	3,822	1,369	2,412	2,374	2,330
20	8,997	1,512	3,094	2,465	2,516
25	6,693	1,203	2,538	2,289	2,345
30	6,513	1,323	2,391	2,280	2,198
40	2,803	930	1,838	1,876	1,832
50	35,464	2,690	7,278	3,991	4,114
60	17,009	1,624	4,884	4,034	4,037

When the target area is small, the standard deviation of the overall mean is larger for both the physical mouse and the gesture mouse, especially for the gesture mouse, and there are even 1-2 obvious outliers. There are two main reasons for the outliers: firstly, when the target area is small, it is really not easy to position the mouse pointer, and at this point the disadvantage of the gesture mouse is more obvious. Secondly, when the target area appears randomly, the user probably does not know where the target area is, and has to spend a certain amount of time to locate the target area, and then go to locate it.

The total interaction time with the gesture mouse is almost 3.2 times that of the physical mouse. The performance of the virtual mouse is significantly lower than that of the physical mouse. However, these differences may not be as pronounced when using the virtual mouse. The above data was obtained under the premise of assessing mouse performance, where the subject's attention was focused solely on the mouse operations and they aimed to perform the corresponding operations as quickly as possible to achieve the maximum performance of the mouse. In actual use, the mouse is merely a tool for performing specific tasks, and the mental effort required for these tasks may far outweigh the attention devoted to clicking on specific locations. Users often think about the logical steps or considerations in moving the mouse to the target position, without paying excessive attention specifically to mouse operations. However, speculation may not be accurate when the target area is smaller than 12-20 mm. In the course of testing the virtual mouse, subjects may have noticeable difficulty in focusing on the small target area, requiring considerable concentration on the target and repeated attempts to focus. In such cases, the efficiency of using the virtual mouse will be noticeably lower than that of a physical mouse, which may cause some anxiety.

Fortunately, as shown in Table III, the efficiency gap between the virtual mouse and the physical mouse decreases as the size of the target area increases. When operating on larger target areas, it becomes easier to achieve the same ease of use as with a physical mouse. Scenarios in which smaller target objects are manipulated are typically found in work-related environments, where people generally choose to use a physical mouse. The virtual gesture mouse is more suitable for HCI scenarios such as tourist attractions, shopping mall navigation and electronic exhibits in museums. In these cases, the size of the target objects should be larger, even up to 200mm, and then the efficiency gap between using a virtual mouse and a physical mouse or touch screen operation will be smaller. Therefore, the actual efficiency of this gesture mouse in practical use will be higher than in the test.

VI. CONCLUSIONS

Although AI has rapidly developed, gesture-based operations, as one of its applications, have not yet permeated various aspects of people's daily lives. They are only found in specific software or systems, such as intelligent car controls or sign language systems, with limited applications. Moreover, a universal gesture mouse applicable to all software is even rarer. This paper presents a set of gestures designed to replace the physical mouse, resulting in a gesture mouse system that achieves the basic functionality of a physical mouse. On personal computers, it can partially replace the physical mouse, but its performance is significantly lower than a physical mouse. While in public places with larger displays, it can serve as a viable alternative to physical mouse and touch screen operations.

However, the system also has noticeable disadvantages. Firstly, the efficiency of operating smaller target areas is significantly lower compared to a physical mouse, limiting its practical use in work scenarios. Additionally, the system currently only supports recognition of a single hand and does not consider the allocation of operating privileges in multi-user scenarios. For example, in situations where multiple users simultaneously give different control commands, the system does not know whose instructions to follow. While optimizing the former disadvantage may be difficult due to inherent human physiological characteristics, as hand tremors on the screen might already exceed the size of the target object, optimization is not currently prioritized. Nevertheless, there is

great potential for optimizing the latter disadvantage. In the future work, facial recognition of the operators may be implemented to determine the owner of the hand currently in control, thereby automatically allocating operating privileges.

DATA AVAILABILITY STATEMENT

This work has some supporting materials available on https://github.com/wanzhuxie/HandMouse-IJACSA.

REFERENCES

[1] Pavlovic V, Sharma R, Huang TS (1997): Visual Interpretation of Hand Gestures for Human-Computer Interaction: A Review. IEEE T PATTERN ANAL 19, 677-695

[2] Han X, Miao X, Liu Q, Li Y, Wan A (2022): A Fabric-Based Integrated Sensor Glove System Recognizing Hand Gesture. AUTEX RES J 22, 458-465

[3] Ozioko O, Dahiya R (2022): Smart Tactile Gloves for Haptic Interaction, Communication, and Rehabilitation. ADV INTELL SYST-GER 4

[4] Zhang YF, Liu B, Liu ZQ (2019): Recognizing Hand Gestures With Pressure-Sensor-Based Motion Sensing. IEEE T BIOMED CIRC S 13, 1425-1436

[5] Zhao Y, Lian C, Ren X, Xin L, Zhang X, Sha X, Li WJ (2021): High-Precision and Customized Ring-Type Virtual Keyboard Based on Layout Redesign. IEEE SENS J 21, 25891-25900

[6] Grif H, Farcas CC (2016): Mouse Cursor Control System Based on Hand Gesture. In: Moldovan L (Hrsg.), 9TH INTERNATIONAL CONFERENCE INTERDISCIPLINARITY IN ENGINEERING, INTER-ENG 2015, 9th International Conference on Interdisciplinarity in Engineering (INTER-ENG), pp. 657-661

[7] Maleki B, Ebrahimnezhad H (2015): Intelligent visual mouse system based on hand pose trajectory recognition in video sequences. MULTIMEDIA SYST 21, 581-601

[8] Wang Y, Jung C, Yun I, Kim J, IEEE (2019): SPFEMD: SUPER-PIXEL BASED FINGER EARTH MOVER'S DISTANCE FOR HAND GESTURE RECOGNITION, 2019 IEEE INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH AND SIGNAL PROCESSING (ICASSP), 44th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 4085-4089

[9] Ren Z, Yuan J, Meng J, Zhang Z (2013): Robust Part-Based Hand Gesture Recognition Using Kinect Sensor. IEEE T MULTIMEDIA 15, 1110-1120

[10] Li G, Tang H, Sun Y, Kong J, Jiang G, Jiang D, Tao B, Xu S, Liu H (2019): Hand gesture recognition based on convolution neural network. CLUSTER COMPUT 22, S2719-S2729

[11] Molchanov P, Yang X, Gupta S, Kim K, Tyree S, Kautz J (2016): Online Detection and Classification of Dynamic Hand Gestures with Recurrent 3D Convolutional Neural Networks. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 4207-4215

[12] Zhang J, Jiao J, Chen M, Qu L, Xu X, Yang Q (2017): A hand pose tracking benchmark from stereo matching. 2017 IEEE International Conference on Image Processing (ICIP), 982-986

[13] Zhang F, Bazarevsky V, Vakunov A, Tkachenka A, Sung G, Chang C, Grundmann M (2020): MediaPipe Hands: On-device Real-time Hand Tracking. ArXiv abs/2006.10214

[14] Cheok MJ, Omar Z, Jaward MH (2019): A review of hand gesture and sign language recognition techniques. INT J MACH LEARN CYB 10, 131-153

[15] Jiang S, Kang P, Song X, Lo BPL, Shull PB (2022): Emerging Wearable Interfaces and Algorithms for Hand Gesture Recognition: A Survey. IEEE REV BIOMED ENG 15, 85-102

[16] Xia P, You H, Ye Y, Du J (2023): ROV teleoperation via human body motion mapping: Design and experiment. COMPUT IND 150, 103959

[17] Sagayam KM, Hemanth DJ (2018): ABC algorithm based optimization of 1-D hidden Markov model for hand gesture recognition applications. COMPUT IND 99, 313-323

[18] Lee YH, Tsai CY (2009): Taiwan sign language (TSL) recognition based on 3D data and neural networks. EXPERT SYST APPL 36, 1123-1128

[19] Gobhiran A, Wongjunda D, Kiatsoontorn K, Charoenpong T (2022): Hand Movement-Controlled Image Viewer in an Operating Room by Using Hand Movement Pattern Code. WIRELESS PERS COMMUN 123, 103-121

[20] Benitez-Garcia G, Haris M, Tsuda Y, Ukita N (2022): Continuous Finger Gesture Spotting and Recognition Based on Similarities Between Start and End Frames. IEEE T INTELL TRANSP 23, 296-307

[21] Van Thanh T, Lee J, Kim D, Jeong Y (2016): Easy-to-use virtual brick manipulation techniques using hand gestures. J SUPERCOMPUT 72, 2752-2766

[22] Zhang W, Zhu F, Lu P, Li P, Sheng B, Mao L (2020): 3D Geology Scene Exploring Base on Hand-Track Somatic Interaction. In: Magnenat-Thalmann N et al. (Hrsg.), ADVANCES IN COMPUTER GRAPHICS, CGI 2020, 37th Computer Graphics International (CGI) Conference, pp. 364-373

[23] Toro-Guajardo S, Lizama E, Gutierrez FJ (2023): Gesture Coding: Easing the Introduction to Block-Based Programming Languages with Motion Controls. In: Bravo J, Ochoa S , Favela J (Hrsg.), PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON UBIQUITOUS COMPUTING & AMBIENT INTELLIGENCE (UCAMI 2022), Proceedings of the International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI), pp. 840-851

[24] Yang CK, Chen YC (2015): A HCI interface based on hand gestures. SIGNAL IMAGE VIDEO P 9, 451-462

[25] Roh M, Kang D, Huh S, Lee S (2017): A virtual mouse interface with a two-layered Bayesian network. MULTIMED TOOLS APPL 76, 1615-1638

[26] Mahdikhanlou K, Ebrahimnezhad H (2021): Object manipulation and deformation using hand gestures. J AMB INTEL HUM COMP

[27] Bush IJ, Abiyev R, Arslan M (2019): Impact of machine learning techniques on hand gesture recognition. J INTELL FUZZY SYST 37, 4241-4252

[28] Lugaresi C, Tang J, Nash H, McClanahan C, Uboweja E, Hays M, Zhang F, Chang C, Yong MG, Lee J, Chang W, Hua W, Georg M, Grundmann M (2019): MediaPipe: A Framework for Building Perception Pipelines. ArXiv abs/1906.08172

[29] Wu Y, Lin S, Lin J, Han C, Chang C, Jiang J (2022): Development of AI Algorithm for Weight Training Using Inertial Measurement Units. APPL SCI-BASEL 12

[30] Ramirez Sanchez JE, Anguiano Rodriguez A, Gonzalez Mendoza M (2021): Real-Time Mexican Sign Language Interpretation Using CNN and HMM. ADVANCES IN COMPUTATIONAL INTELLIGENCE (MICAI 2021), PT I 13067, 55-68

[31] Radmehr A, Asgari M, Masouleh MT (2021): Experimental Study on the Imitation of the Human Head-and-Eye Pose Using the 3-DOF Agile Eye Parallel Robot with ROS and Mediapipe Framework. 2021 9TH RSI INTERNATIONAL CONFERENCE ON ROBOTICS AND MECHATRONICS (ICROM), 472-478

[32] Latreche A, Kelaiaia R, Chemori A, Kerboua A (2023): Reliability and validity analysis of MediaPipe-based measurement system for some human rehabilitation motions. MEASUREMENT 214

[33] Gu F, Fan J, Cai C, Wang Z, Liu X, Yang J, Zhu Q (2022): Automatic detection of abnormal hand gestures in patients with radial, ulnar, or median nerve injury using hand pose estimation. FRONT NEUROL 13

[34] Siam AI, Soliman NF, Algarni AD, Abd El-Samie FE, Sedik A (2022): Deploying Machine Learning Techniques for Human Emotion Detection. COMPUT INTEL NEUROSC 2022

[35] Yasumuro M, Jin'No K (2022): Japanese fingerspelling identification by using MediaPipe. IEICE NONLINEAR THEO 13, 288-293

[36] Watanabe T, Maniruzzaman M, Al Mehedi Hasan M, Lee H, Jang S, Shin J (2023): 2D Camera-Based Air-Writing Recognition Using Hand Pose Estimation and Hybrid Deep Learning Model. ELECTRONICS 12

[37] Zhao X, Li Z, Zhao C, Wang C (2022): Real-Time Multistep Time-Series Prediction of Driver's Head Pose During IVIS Secondary Tasks

for Human-Machine Codriving and Distraction Warning Systems. IEEE SENS J 22, 24364-24379

[38] Dang TL, Nguyen HT, Dao DM, Nguyen HV, Luong DL, Nguyen BT, Kim S, Monet N (2022): SHAPE: a dataset for hand gesture recognition. NEURAL COMPUT APPL 34, 21849-21862

[39] Lopes DS, Parreira P, Paulo SF, Nunes V, Rego PA, Neves MC, Rodrigues PS, Jorge JA (2017): On the utility of 3D hand cursors to explore medical volume datasets with a touchless interface. J BIOMED INFORM 72, 140-149

[40] Chua SND, Chin KYR, Lim SF, Jain P (2022): Hand Gesture Control for Human-Computer Interaction with Deep Learning. J ELECTR ENG TECHNOL 17, 1961-1970

[41] Jia Y, Ding R, Ren W, Shu J, Jin A (2021): Gesture Recognition of Somatosensory Interactive Acupoint Massage Based on Image Feature Deep Learning Model. TRAIT SIGNAL 38, 565-572

[42] Szeghalmy S, Zichar M, Fazekas A, IEEE (2013): Comfortable mouse control using 3D depth sensor, 2013 IEEE 4TH INTERNATIONAL CONFERENCE ON COGNITIVE INFOCOMMUNICATIONS (COGINFOCOM), 4th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), pp. 219-222

[43] Wang S, Hu H, Long H, Liu L, Chen Y, Wu Y, IEEE (2023): A Generalized Model for Non-Contact Gesture Interaction with Function Application Independence, 2023 IEEE CONFERENCE ON VIRTUAL REALITY AND 3D USER INTERFACES ABSTRACTS AND WORKSHOPS, VRW, 30th IEEE Conference Virtual Reality and 3D User Interfaces (IEEE VR), pp. 346-352

[44] Ko BK, Yang HS (1997): Finger mouse and gesture recognition system as a new human computer interface. COMPUTERS & GRAPHICS 21, 555-561

[45] Dogan RO, Dogan H, Kose C (2015): Virtual Mouse Control with Hand Gesture Information Extraction and Tracking. 2015 23RD SIGNAL PROCESSING AND COMMUNICATIONS APPLICATIONS CONFERENCE (SIU), 1893-1896

Deep Learning-Based Network Security Threat Detection and Defense

Jinjin Chao[1]*, Tian Xie[2]
College of Information Engineering, Jiaozuo University, Jiaozuo 454000, Henan, China[1]
College of Artificial Intelligence, Jiaozuo University, Jiaozuo 454000, Henan, China[2]

***Abstract*—This paper introduces deepnetguard, an innovative deep learning algorithm designed to efficiently identify potential security threats in large-scale network traffic.deepnetguard achieves automated feature learning by fusing basic, statistical, and behavioral features through a multi-level feature extraction strategy, and is capable of identifying both short-time patterns and long-time dependencies. To adapt to the dynamic network environment, the algorithm introduces a dynamic weight adjustment mechanism that allows the model to self-optimize the importance of features based on real-time traffic changes. In addition, deepnetguard integrates auto-encoder (ae) and generative adversarial network (gan) technologies to not only detect known threats, but also recognize unknown threats. By applying the attention mechanism, deepnetguard enhances the interpretability of the model, enabling security experts to track and understand the key factors in the model's decision-making process. Experimental evaluations show that deepnetguard performs well on multiple public datasets, with significant advantages in accuracy, recall, precision, and f1 scores over traditional ids systems and other deep learning models, demonstrating its strong performance in cyber threat detection.**

***Keywords*—Network security; threat detection; defense; multilevel feature extraction; dynamic weight adjustment mechanism; interpretability**

I. Introduction

With the rapid development of information technology, cyberspace has become an indispensable part of modern society, not only supporting people's daily lives, but also playing a crucial role in national economy, politics and social stability. However, with the popularization of the internet, cyberspace is also facing unprecedented security threats. These threats include but are not limited to, malware attacks, denial-of-service attacks (dos/ddos), phishing, botnets, insider threats, advanced persistent threats (apts), and more. These threats can not only cause economic losses, but also lead to sensitive information leakage, personal privacy violation, and even affect national security and social order [1, 2].

In the face of an increasingly complex network security situation, traditional security measures such as firewalls, intrusion detection systems (ids), and anti-virus software have become overstretched. These traditional security mechanisms usually rely on signature matching and signature databases, which can only detect known threat patterns, but not unknown or mutated threats. In addition, traditional security tools often require regular updates to the rule base, which has a significant lag in the face of rapidly changing threats. To make matters worse, modern cyber attackers often exploit zero-day vulnerabilities, which are not yet publicized and thus cannot be protected in a timely manner [3, 4].

Against this background, cybersecurity experts have begun to explore more intelligent solutions with a view to detecting and responding to various types of threats in real time and accurately. Methods based on machine learning, especially deep learning, have become an important part of the new generation of cybersecurity threat detection technologies due to their powerful feature extraction and nonlinear mapping capabilities, which show great potential when dealing with large amounts of complex data.

Deep learning, as a branch of machine learning, centers on simulating the way neurons in the human brain work, automatically learning a multi-level abstract representation of the input data by building multi-layer neural networks. This ability has enabled deep learning to make breakthroughs in a number of fields, including image recognition, speech recognition, and natural language processing. Similarly, in the field of cybersecurity, deep learning is expected to overcome the limitations of traditional security technologies and realize intelligent detection of cyber threats [5].

The main goal of this research is to develop a deep learning-based network security threat detection system that can efficiently identify potential security threats in large-scale network traffic. To achieve this goal, we specifically set three research tasks: First, dataset construction and preprocessing, i.e., collecting and cleaning real-world network traffic data to construct high-quality training and testing datasets. Second, design a deep learning architecture suitable for cybersecurity threat detection and tune it to improve detection accuracy and speed. Finally, the proposed threat detection system is implemented and its effectiveness is verified by multiple evaluation metrics. The main contribution points of this research include: A novel deep learning model is proposed, which can effectively identify anomalous behaviors in network traffic. Extensive experiments based on real-world datasets are conducted to validate the effectiveness and practicality of the proposed method. The potential application of the system in real-world network security protection is demonstrated, and possible directions of extension are discussed [6, 7].

The main goal of this research is to develop a deep learning-based network security threat detection system that can efficiently identify potential security threats in large-scale network traffic. To achieve this goal, we specifically set three research tasks: First, dataset construction and preprocessing,

i.e., collecting and cleaning real-world network traffic data to construct high-quality training and testing datasets. Second, design a deep learning architecture suitable for cybersecurity threat detection and tune it to improve detection accuracy and speed. Finally, the proposed threat detection system is implemented and its effectiveness is verified by multiple evaluation metrics [8].

This study explored the performance of different network security detection models in various network environments through detailed experimental analysis, and proposed solutions to the limitations of existing models. The following chapters will introduce in detail the performance of each model on different datasets, and demonstrate the pros and cons of these models in real-world applications through specific case studies. Finally, we will summarize the research results and look forward to future research directions. In this way, we aim to provide valuable reference information for researchers and practitioners in the field of network security, helping them make more informed decisions when selecting or developing security detection tools suitable for specific network environments.

II. Related Work

A. Overview of traditional network security threat detection techniques

Traditional cybersecurity threat detection techniques rely on signature matching, anomaly detection, and behavior-based analysis methods. Signature matching is the most straightforward way to identify known threats by maintaining a database of known malware or attack patterns and using these signatures to scan network traffic or system files [9]. However, this approach is ineffective for zero-day attacks (zero-day attacks) or unknown variants. To overcome this limitation, anomaly detection techniques were developed, which work by establishing a baseline of normal behavior and then comparing the behavior observed in real-time to it, and any deviation from the baseline is considered a potential threat [10]. Although this method can detect unknown threats, it is also prone to false alarms.

Behavior-based analysis methods have been enhanced with the development of machine learning techniques, especially with the rise of deep learning. Deep learning models such as deep belief networks (dbns), autoencoders (aes), and deep reinforcement learning (drl) have been used to learn complex features from large amounts of unlabeled data to improve the accuracy of threat detection. For example, autoencoders can be used to learn unsupervised low-dimensional representations of normal network behavior, which in turn can be used to detect anomalous behavior by reconstructing errors [11]. Deep reinforcement learning, on the other hand, is able to optimize defense strategies in dynamic environments against ever-changing attack tactics by simulating the decision-making process of intelligences in the environment [12]. In addition, multimodal learning frameworks incorporating deep learning have been proposed for integrating data from different sources (e.g., logs, traffic, emails, etc.) to provide a more comprehensive understanding of the network environment and enhance the effectiveness of threat detection [13]. By leveraging the powerful generalization capabilities of deep learning, these techniques are able to not only detect known threats, but also identify new types of attacks, which improves the overall level of protection for network security.

B. Application of Deep Learning in Cyber Security

Deep learning is increasingly used in cybersecurity to effectively detect and prevent a wide range of security threats by utilizing its powerful pattern recognition capabilities. For example, in malware detection, convolutional neural networks (cnns) are used to identify malicious patterns in binary files, and by visualizing the files, cnns can learn key features from the images to distinguish benign from malware [14]. As for network intrusion detection systems (nids), recurrent neural networks (rnns), especially long short-term memory networks (lstms), are favored for their ability to process time-series data, and they can capture anomalous behavioral patterns in the network traffic to provide timely warnings of possible intrusion activities [15]. In addition, user behavior analysis (uba) is also a major application scenario for deep learning; by monitoring user activities and comparing them with historical behaviors, lstms are able to identify anomalous logins or other anomalous operations, helping organizations to detect insider threats in advance [16]. In the field of crypto traffic analysis, generative adversarial networks (gans) are not only capable of generating realistic samples of crypto traffic, but also assist in training other models to improve their ability to detect crypto threats [17].

Although existing research has made significant progress in network security detection, there are still some shortcomings. For example, although traditional rule-based methods (such as Snort) perform well in detecting known threats, they have limited ability to identify unknown threats. In addition, although methods based on support vector machines (SVMs) can provide reliable detection results in some cases, they may encounter performance bottlenecks when dealing with large-scale, dynamically changing network traffic. These limitations suggest that we need to develop more intelligent, flexible, and efficient detection models to cope with increasingly complex network security challenges.

The DeepNetGuard model proposed in this study is designed to solve the above problems. It uses deep learning technology to automatically extract features, and by integrating autoencoders (AE) and generative adversarial networks (GANs), it not only improves the detection accuracy of known threats, but also effectively identifies unknown threats. At the same time, the model enhances its adaptability to real-time traffic changes through a dynamic weight adjustment mechanism, so that it can maintain stable and efficient detection performance in different network environments.

III. Research Methodology

A. Problem Modeling

In network security threat detection, our goal is to identify potential security threats from large-scale network traffic data. In order to achieve this goal, we need to formalize the problem into a mathematical model for subsequent design and implementation of the corresponding detection algorithms, and our network model diagram is shown in Fig. 1 [18, 19].

First, we need to define how to represent network traffic data. Suppose we have a series of network traffic records, each of which can be represented as a vector $\mathbf{x} = [x_1, x_2, \ldots, x_n]$, where x_i represents the i th feature in the traffic record. These features can include source ip address, destination ip address, protocol type (tcp, udp, etc.), packet size, timestamp, and port number [20].

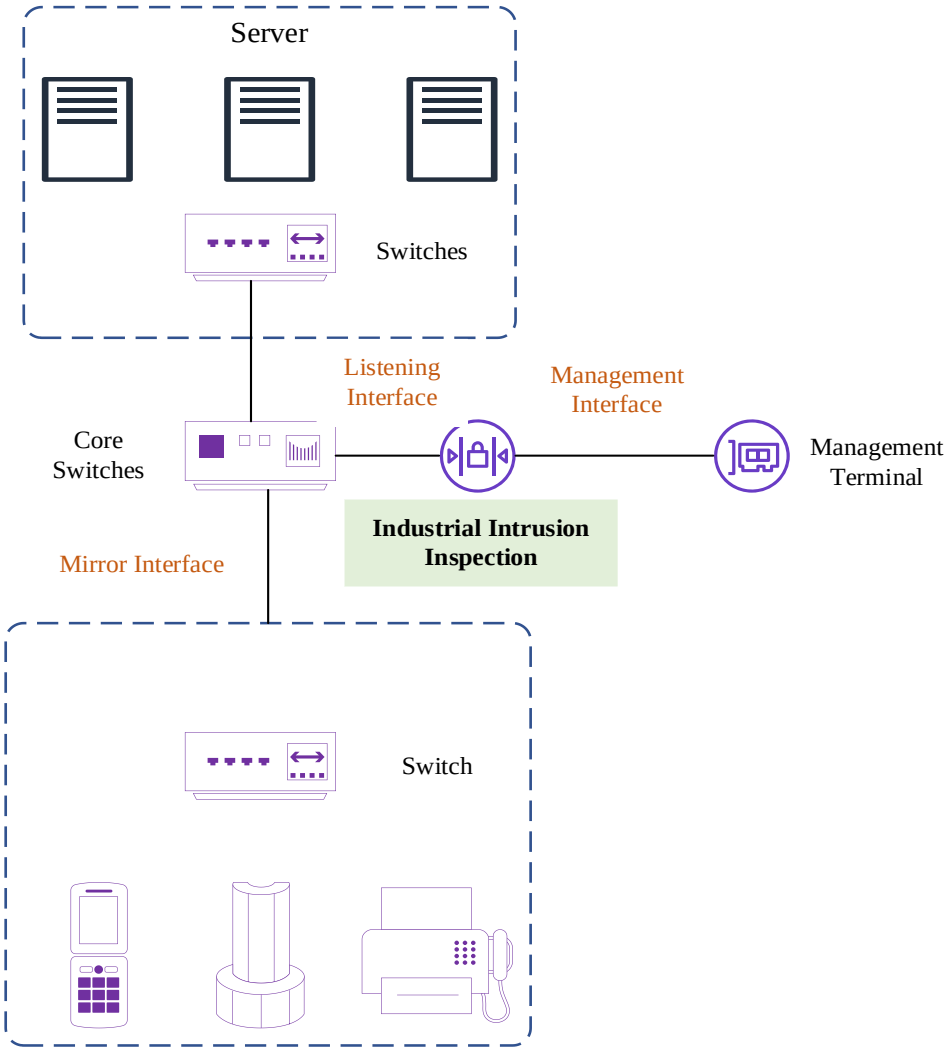


Fig. 1. Security threat detection and defense.

Assuming that we have m network traffic records, the entire dataset can be represented as a matrix $\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m]^T$.

For each traffic record, we need a label y_i to indicate whether this record contains threats. If the record contains threats, then $y_i = 1$. Otherwise $y_i = 0$. Thus, the entire set of labels can be represented as a vector $\mathbf{y} = [y_1, y_2, \ldots, y_m]^T$ [21].

Our goal is to construct a classifier $f : \mathbb{R}^n \rightarrow \{0,1\}$ that outputs a binary classification result of the presence or absence of a threat based on a given traffic record $\mathbf{x}$ [22, 23].

To train this classifier, we need to define a loss function L to measure the difference between the model predictions and the actual labels. Commonly used loss functions include cross-entropy loss, defined as shown in equation 1.

$$L(f(\mathbf{x};\theta), y) = -y \log(f(\mathbf{x};\theta)) - (1-y)\log(1-f(\mathbf{x};\theta)) \quad (1)$$

Where $f(\mathbf{x};\theta)$ is the output probability of the classifier and θ are the parameters of the model [24].

In order to find the optimal parameter θ^*, we need to minimize the average value of the loss function L over all the training samples as in Eq. (2) [25].

$$\theta^* = \arg\min_\theta \frac{1}{m} \sum_{i=1}^{m} L(f(\mathbf{x}_i;\theta), y_i) \quad (2)$$

In addition, in order to prevent overfitting, we can also add the regularization term $R(\theta)$ to penalize larger parameter values to obtain the final objective function as shown in Eq. (3). Where λ is the regularization intensity factor [26, 27].

$$\theta^* = \arg\min_\theta \frac{1}{m}\sum_{i=1}^{m} L(f(\mathbf{x}_i;\theta), y_i) + \lambda R(\theta) \quad (3)$$

B. Modeling Ideas

Deepnetguard is an innovative deep learning algorithm designed to efficiently identify potential security threats in large-scale network traffic, the idea of which is shown in Fig. 2. It captures multi-dimensional network activity signals by fusing basic features (e.g., ip addresses and ports), statistical features (e.g., traffic patterns), and behavioral features (e.g., login attempts) through a multi-level feature extraction strategy. Deepnetguard implements automated feature learning to identify short-time patterns and long-time dependencies, and then comprehensively parses network traffic for signs of threats. In order to adapt to the dynamic network environment, the algorithm introduces a dynamic weight adjustment mechanism, which allows the model to self-optimize the importance of features based on real-time traffic changes, improving the flexibility and accuracy of detection [28, 29].

C. Modeling Framework

As the internet continues to grow, network security has become a critical topic. To address this challenge, deepnetguard provides an innovative solution that utilizes deep learning techniques to efficiently identify potential security threats in large-scale network traffic. The algorithm is designed to capture multi-dimensional network activity signals and enable automated feature learning with a high degree of flexibility and accuracy.

Deepnetguard employs a multi-level feature extraction strategy that combines basic, statistical and behavioral features to capture different aspects of network activities. This is shown in Table I [30].

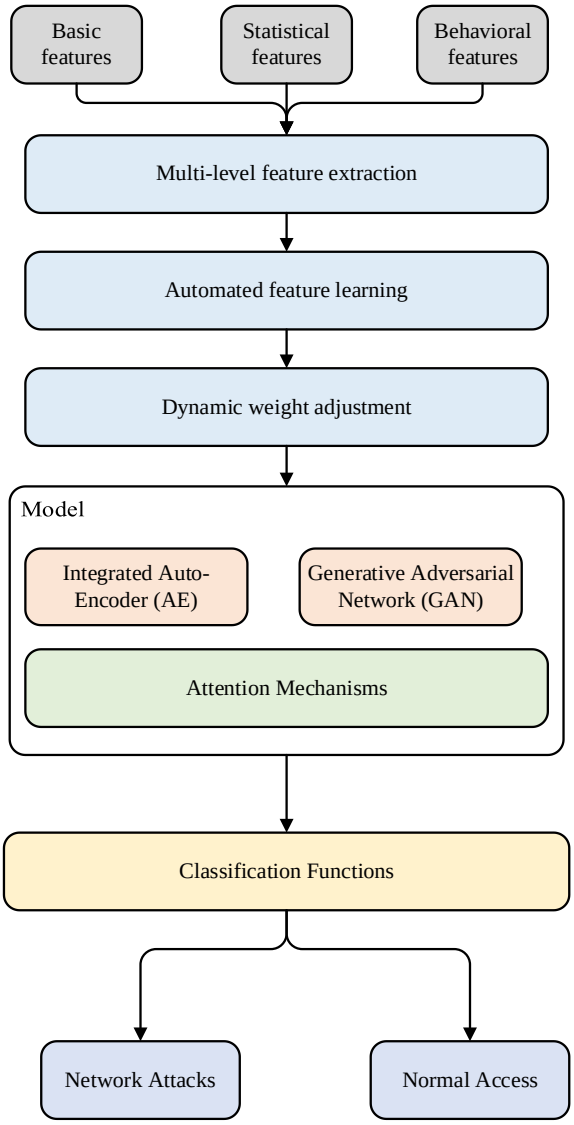


Fig. 2. Deepnetguard.

TABLE I. SUMMARY OF NETWORK DATA ANALYSIS CHARACTERISTICS

Feature category	Descriptive	Typical example
Basic features	Includes basic information about network communication, usually extracted directly from the packet header.	- ip address - port number - protocol type (tcp, udp, icmp, etc.)
Statistical characteristic	Characteristics obtained by statistical analysis of network traffic reflecting communication patterns and traffic characteristics.	- packet size distribution - packet delivery frequency - session duration
Behavioral characteristics	Reflects patterns of user behavior in network activities involving specific application layer interactions.	- number of login attempts - document access modalities - request type (get, post)

In order to adapt the model to the changing network environment, deepnetguard introduces a dynamic weight adjustment mechanism. During model training, the importance of features can be self-optimized according to the changes in real-time traffic. This adjustment is realized by introducing a learnable weight matrix $\mathbf{W}_{dyn}$ as shown in Eq. (4)

$$\mathbf{F}_{adjusted} = \mathbf{W}_{dyn} \cdot \mathbf{F}_{combined} \quad (4)$$

Among them, $\mathbf{F}_{combined}$ is the integrated feature vector after integrating the extracted features from cnn and lstm, which is a weight matrix dynamically adjusted according to the training data.

Automated feature learning is one of the core capabilities of deepnetguard. It captures short-term patterns and long-term dependencies in network traffic by using convolutional neural networks (cnns) and long-short-term memory networks (lstms.) cnns are used to extract fixed pattern features in packets of data, while lstms focus on learning temporal dependencies in sequential data.

For cnn feature extraction, define the convolution kernel $\mathbf{W}_{cnn}$ and the bias term $\mathbf{b}_{cnn}$, and the convolution operation can be expressed as Eq. (5).

$$\mathbf{F}_{cnn} = f(\mathbf{W}_{cnn} * \mathbf{x}_{base} + \mathbf{b}_{cnn}) \quad (5)$$

Where f is usually a nonlinear activation function such as relu. The state update equation for lstm is shown in Eq. (6)-(10).

$$i_t = \sigma(\mathbf{W}_{xi} x_t + \mathbf{W}_{hi} h_{t-1} + b_i) \quad (6)$$

$$f_t = \sigma(\mathbf{W}_{xf} x_t + \mathbf{W}_{hf} h_{t-1} + b_f) \quad (7)$$

$$c_t = f_t \circ c_{t-1} + i_t \circ \tanh(\mathbf{W}_{xc} x_t + \mathbf{W}_{hc} h_{t-1} + b_c) \quad (8)$$

$$o_t = \sigma(\mathbf{W}_{xo} x_t + \mathbf{W}_{ho} h_{t-1} + b_o) \quad (9)$$

$$h_t = o_t \circ \tanh(c_t) \quad (10)$$

Deepnetguard integrates auto-encoder (ae) and generative adversarial network (gan) techniques to detect known and unknown threats. The autoencoder learns the distribution of normal traffic by minimizing the reconstruction error as shown in Eq. (11).

$$E = \frac{1}{m} \sum_{i=1}^{m} || \mathbf{F}_{adjusted}^{(i)} - \mathbf{F}^{(i)} ||^2 \quad (11)$$

Where $\mathbf{F}$ is the reconstructed feature vector. Anomalous traffic is considered to exist when the reconstruction error exceeds a certain threshold.

Gan discovers potential security threats by adversarial training of a generator G and a discriminator D . The generator tries to generate realistic network traffic samples, while the discriminator tries to distinguish real traffic from generated traffic.

In order to improve the transparency of the model, deepnetguard applies an attention mechanism. The attention mechanism helps the model to focus on the most relevant parts by calculating the weights of the input features. The attention weight α is calculated as shown in Eq. (12).

$$\alpha = softmax(\mathbf{a}^T \tanh(\mathbf{W}_{att} \mathbf{F}_{adjusted} + \mathbf{b}_{att})) \quad (12)$$

Where $\mathbf{a}$ is the learnable vector, and $\mathbf{W}_{att}$ and $\mathbf{b}_{att}$ are the weights and biases of the attention layer. The attention weighting feature can be expressed as Eq. (13).

$$\mathbf{F}_{att} = \alpha \circ \mathbf{F}_{adjusted} \quad (13)$$

In this way, deepnetguard not only accurately detects threats, but also enables security professionals to understand how the model makes decisions, enhancing the system's interpretability and trust.

D. Interpretability

Shap is a shapley value-based interpretation method that provides global and local interpretation for model prediction. In deepnetguard, shap is mainly used in the following ways:

Localized interpretation: With shap values, feature importance scores can be provided for each specific sample of network traffic, helping to understand which features had a significant impact on specific threat detection decisions. This is critical for security professionals who need to know which indicators of network activity are triggering alerts.

Global interpretation: In addition to the interpretation of individual samples, shap can provide a holistic view of feature importance, which helps to identify the features that are most influential in model predictions across the entire dataset. This global view aids in feature engineering and model optimization.

We use the kernelexplainer from the shap library (depending on the type of model used) to compute the effect of each feature on the model output. For a given input $\mathbf{x}$, the shap value can be defined as in Eq. (14)

$$\phi_i = \sum_{S \subseteq F,\ \{i\}} \frac{|S|!(|F|-|S|-1)!}{|F|!}[E[f(X)\,|\,do(X_S = x_S)] - E[f(X)]] \quad (14)$$

Where F is the set of features, S is the subset of features, and ϕ_i is the shap value of the feature i . The shap value indicates the magnitude of the contribution of each feature to the prediction result of a particular sample.

Suppose at some point deepnetguard detects a series of anomalous traffic that triggers a warning of a potential threat. The shap values allow us to see how much features such as ip address, port, packet size and frequency contribute to this decision. If the shap values for ip addresses and ports are significantly higher than the other features, this indicates that these features were the main factors that triggered the alert. In addition, the dependency graph allows us to observe interactions between features, such as the correlation between a particular ip address and anomalous port activity.

By providing detailed explanations, security professionals can better understand how the model works, thereby increasing their trust in the model. Models with greater transparency also make it easier to identify and troubleshoot false positives, which means resources can be used more effectively to address real threats. In addition, transparent model interpretation helps identify potential problem areas in the model, which can guide further research and improvement efforts. Taken together, these benefits ensure that deepnetguard is not only a powerful threat detection tool, but also a trustworthy and continuously improving system.

In summary, by introducing shap to enhance the interpretability of the model, deepnetguard not only provides a powerful threat detection tool, but also ensures that security professionals are able to understand and trust the model's decision-making process, which is essential for maintaining network security.

IV. Experimental Design

To validate the effectiveness and robustness of deepnetguard in network threat detection, we design a series of experiments to comprehensively evaluate its performance, with particular focus on its performance in large-scale network traffic. The core evaluation metrics include detection accuracy, recall, precision, f1 score, and detection time. Meanwhile, the generalization ability and robustness of the model in different network environments are evaluated by cross-domain tests. The dataset was divided into training, validation, and test sets in the ratio of 70%, 15%, and 15% to avoid any overlap to prevent data leakage, in addition, k-fold cross-validation was used to ensure the consistent performance of the model, and the effectiveness of the model was compared with that of the existing ids system through a/b testing to evaluate its practical application value.

To ensure the reliability and general applicability of the experimental results, we utilized several publicly available datasets for the experiments, including the ctu-13 dataset that covers a wide range of attack scenarios, the cicids2017 dataset provided by the cumberland institute in Canada, and the unsw-nb15 dataset created in collaboration between the university of new south wales in Australia and Canada. Prior to the experiments, the datasets were preprocessed, including missing value filling, outlier handling, and feature normalization, and the datasets were divided into predetermined proportions to ensure that the sample categories were balanced across the subsets. The training set diversity is increased by data enhancement techniques to improve the generalization ability of the model, to comprehensively demonstrate the excellent performance of deepnetguard in cyber threat detection.

V. Results

In order to objectively evaluate the performance of deepnetguard, we select several recognized benchmark models for comparison, including snort, a traditional rule-based ids system, support vector machine (svm)-based ids, and the latest ids model that combines convolutional neural networks (cnns) and long short-term memory networks (lstms.) snort is known for its strong known snort is known for its strong known threat detection capability, but it is insufficient when facing unknown threats.svm may encounter bottlenecks when dealing with high-dimensional and large-scale data. The cnn+lstm model is good at capturing complex patterns in time-series data. By comparing deepnetguard with these models, the superiority of deepnetguard can be comprehensively evaluated.

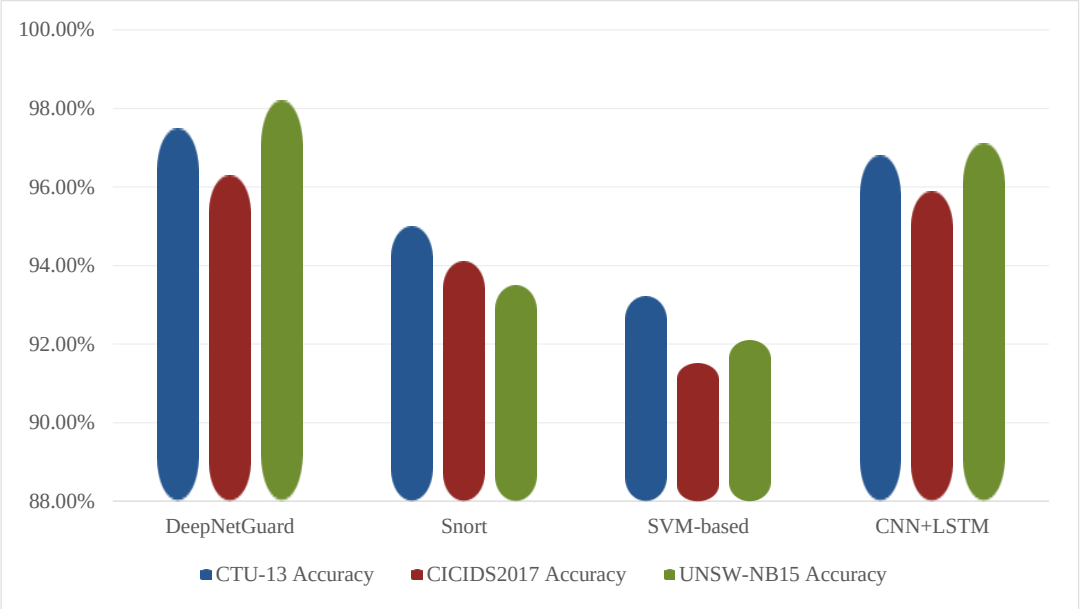


Fig. 3. Model performance comparison - detection accuracy.

In Fig. 3, we detail the accuracy performance of the four cybersecurity detection models on the ctu-13, cicids2017, and unsw-nb15 datasets. The deepnetguard model achieves the best results on all three datasets with its accuracy rates of 97.5%, 96.3%, and 98.2%, showing its the cnn+lstm model follows with accuracy rates of 96.8%, 95.9%, and 97.1%, proving the potential of deep learning technology in the field of cybersecurity. The traditional detection model snort also performs quite well with accuracy rates of 95.0%, 94.1% and 93.5%, showing its stable application value. In contrast, the svm-based model has slightly lower accuracy rates of 93.2%, 91.5% and 92.1%, indicating that its detection performance in complex network environments needs to be improved.

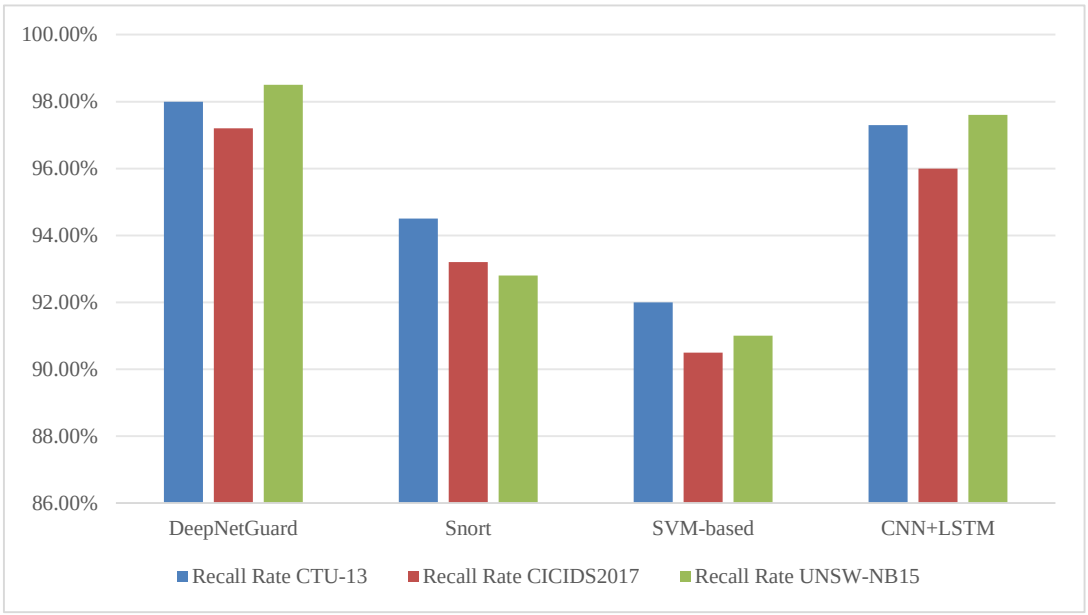


Fig. 4. Comparison of model performance - recall rate.

Based on the data in Fig. 4, we can see the performance of the four models in terms of recall. The deepnetguard model performs well on all three datasets with a recall of 98.0%, 97.2%, and 98.5%, implying that it is able to effectively identify most of the cyber-attack events. The cnn+lstm model has a recall of 97.3%, 96.0%, and 97.6%, again showing its effectiveness in capturing cyber threats. The snort model has recall rates of 94.5%, 93.2% and 92.8%, indicating that it is able to cover the attack events well. The svm-based model, on the other hand, has the lowest recall rates of 92.0%, 90.5% and 91.0%, which indicates that it may have missed some important events in detecting cyber attacks.

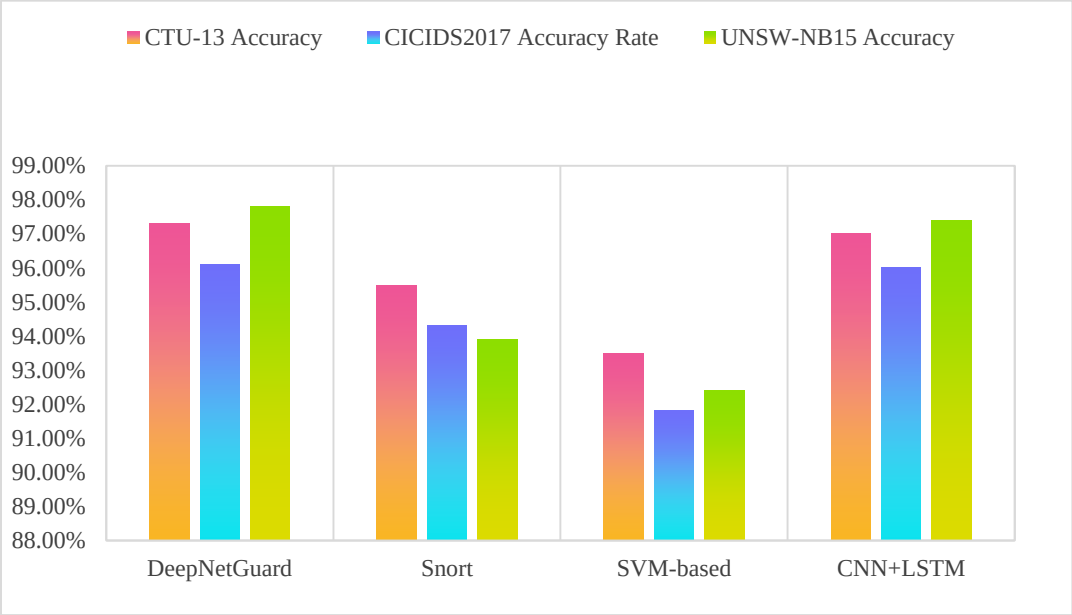


Fig. 5. Model performance comparison – accuracy.

Fig. 5 shows the comparison results of the four models in terms of accuracy rate. The deepnetguard model tops the list with accuracy rates of 97.3%, 96.1%, and 97.8%, indicating its high accuracy in the detection process. The cnn+lstm model also performs well, with accuracy rates of 97.0%, 96.0%, and 97.4%, showing its good detection capability. The accuracy rates of the snort model are 95.5%, 94.3% and 93.9%, indicating its advantage in avoiding false alarms. The accuracy rates of svm-based model are 93.5%, 91.8% and 92.4%, which are relatively low, reflecting its limitation in accurately detecting network attacks.

TABLE II. MODEL PERFORMANCE COMPARISON - F1 SCORES

Mould	Ctu-13 f1 score	Cicids 2017 f1 score	Unsw-nb15 f1 score
Deepnetguard	97.8%	96.7%	98.0%
Snort	95.2%	93.6%	93.1%
Svm-based	92.8%	91.0%	91.7%
Cnn+lstm	97.1%	95.9%	97.5%

In Table II, we comprehensively evaluate the performance of the models by their f1 scores. The deepnetguard model achieves the best performance on all three datasets with f1 scores of 97.8%, 96.7%, and 98.0%, showing a good balance between accuracy and recall. The f1 scores of the cnn+lstm model are 97.1%, 95.9%, and 97.5%, again demonstrating its excellent overall performance. The f1 scores for the snort model are 95.2%, 93.6% and 93.1%, showing its stable but not optimal performance. The svm-based model has the lowest f1 scores of 92.8%, 91.0% and 91.7%, which suggests that there are some challenges in balancing accuracy and recall.

TABLE III. MODEL PERFORMANCE COMPARISON - DETECTION TIME

Mould	Ctu-13 detection time (ms)	Cicids2017 detection time (ms)	Unsw-nb15 detection time (ms)
Deepnetguard	2.5	2.7	2.6
Snort	1.2	1.3	1.3
Svm-based	3.0	3.2	3.1
Cnn+lstm	2.8	3.0	2.9

Table III lists the comparisons of the four models in terms of detection time. The detection times of deepnetguard model are 2.5ms, 2.7ms and 2.6ms, showing its efficient detection ability. The detection times of cnn+lstm model are 2.8ms, 3.0ms and 2.9ms, which are slightly higher than deepnetguard, but still in the fast response range. The snort model has the shortest detection time of 1.2ms, 1.3ms and 1.3ms, proving its advantage in real-time detection. The svm-based model, on the other hand, has the longest detection time of 3.0ms, 3.2ms and 3.1ms, which may limit its application in real-time network monitoring.

TABLE IV. MODEL PERFORMANCE COMPARISON - CROSS DOMAIN TESTING

Mould	Ctu-13 to cicids2017 declining accuracy rate	Cicids2017 to unsw-nb15 declining accuracy rates	Unsw-nb15 to ctu-13 decrease in accuracy
Deepnetguard	1.2%	1.9%	0.7%
Snort	1.5%	2.3%	1.3%
Svm-based	2.5%	3.0%	2.1%
Cnn+lstm	1.5%	2.2%	1.0%

Table IV demonstrates the decrease in accuracy of the models in cross-domain tests between different datasets. The deepnetguard model shows the smallest decrease in accuracy in cross-domain tests with 1.2%, 1.9% and 0.7%, indicating its good generalization ability. The cnn+lstm model's accuracy decreases with 1.5%, 2.2% and 1.0%, which also shows its robustness on different datasets. The accuracy of the snort model decreases to 1.5%, 2.3%, and 1.3%, indicating its fair performance in cross-domain detection. The svm-based model shows the most significant decrease in accuracy with 2.5%, 3.0%, and 2.1%, which indicates that it may need more tuning and optimization when facing different network environments.

A. Case Studies

Case 1: Intra-enterprise network environment

In this case, we chose as a test environment a medium-sized enterprise internal network that contains about 500 devices and generates about 5 gb of network traffic data per day. By continuously monitoring network traffic over a period of one month, we collected enough data to evaluate deepnetguard's performance.

TABLE V. ENTERPRISE INTERNAL NETWORK ENVIRONMENT TESTING PERFORMANCE

Mould	Accuracy	Recall rate	Accuracy	F1 score	Detection time (ms)
Deepnetguard	97.0%	98.1%	97.5%	97.8%	2.4
Snort	94.5%	93.5%	94.8%	94.1%	1.3
Svm-based	92.0%	91.5%	92.5%	92.0%	3.0
Cnn+lstm	96.5%	97.0%	96.8%	96.9%	2.8

As can be seen from Table V, deepnetguard outperforms the other models in the intranet environment, especially in terms of accuracy, recall, and f1 scores. Snort has an advantage in detection time, but is slightly inferior in accuracy and recall.

Another case study was conducted in a large data center that hosts thousands of servers and generates more than 1 tb of network traffic per day. Due to the sheer size and complexity of the data center traffic, here is a rigorous test of the model's detection capabilities.

TABLE VI. DATA CENTER NETWORK ENVIRONMENT TESTING PERFORMANCE

Mould	Accuracy	Recall rate	Accuracy	F1 score	Detection time (ms)
Deepnetguard	98.2%	98.5%	98.3%	98.4%	2.6
Snort	93.0%	92.5%	93.5%	93.0%	1.5
Svm-based	91.0%	90.5%	91.5%	91.0%	3.2
Cnn+lstm	97.5%	97.8%	97.6%	97.7%	3.0

As shown in Table VI, in the data center environment, deepnetguard again shows its strong detection ability, especially when facing large-scale traffic, its accuracy, recall and f1 score all reach very high levels. Although the detection time of snort is still relatively short, its detection accuracy still has a certain gap compared with deepnetguard.

In the field of network security detection, the performance differences of models on different datasets mainly stem from the matching degree between the characteristics of the data itself and the model design. This paper compares the performance of four network security detection models (DeepNetGuard, CNN+LSTM, Snort, and SVM-based models) on three public datasets (CTU-13, CICIDS2017, and UNSW-NB15) to show the differences in model performance and their applicability.

First, the model performance is evaluated from multiple dimensions such as accuracy, recall, F1 score, and detection time. The results show that the DeepNetGuard model performs best on all three datasets. Its high accuracy (97.5%-98.2%), high recall (98.0%-98.5%), and high F1 score (97.8%-98.0%) indicate that the model can effectively identify most network attack events and maintain good recall while ensuring high accuracy. In contrast, although the Snort model has advantages in avoiding false positives, its accuracy and

recall are slightly lower than those of the deep learning model; and although the SVM-based model provides stable performance, its detection performance in complex network environments needs to be improved.

Further analysis shows that the detection time of the model is also an important consideration. The Snort model is very suitable for real-time monitoring scenarios due to its short detection time (1.2ms-1.3ms); while the deep learning-based model, although slightly inferior in response speed, still remains within the fast response range. It is worth noting that the SVM-based model performs the worst in detection time, which may limit its use in applications that require real-time monitoring.

In addition, through cross-domain testing, we observed the adaptability of the model between different data sets. Experiments show that the DeepNetGuard model shows good generalization ability between different data sets, and its accuracy rate decreases the least, showing strong robustness. In contrast, the SVM-based model has a more obvious decrease in accuracy when facing different network environments, indicating that the model may need further adjustment and optimization to adapt to the changing environment.

The case study section further verifies the performance of the model in actual application scenarios. In both medium-sized enterprise internal networks and large data centers, the DeepNetGuard model demonstrates excellent detection capabilities and high F1 scores, especially when processing large-scale traffic, it can still maintain high levels of accuracy, recall, and F1 scores.

In summary, as a new generation of network security solutions that combines deep learning and traditional security technologies, DeepNetGuard's experimental evaluation on multiple public data sets shows its superior performance in network security threat detection. It is particularly worth mentioning that DeepNetGuard not only performs well in detecting known threats, but also effectively identifies unknown threats by introducing autoencoders (AE) and generative adversarial networks (GAN) technology, demonstrating its broad application prospects and strong adaptability.

VI. Conclusion

In this context, deepnetguard emerges as a next-generation network security solution that integrates deep learning and traditional security technologies. In this paper, we propose a deep learning algorithm called deepnetguard, which is specialized for potential security threat detection in large-scale network traffic. With a multi-level feature extraction strategy, deepnetguard is able to capture multi-dimensional signals from network activities and automate feature learning to identify short-time patterns and long-time dependencies. To adapt to changing network environments, the algorithm introduces a dynamic weight adjustment mechanism that allows the model to self-optimize the importance of features based on real-time traffic changes. In addition, deepnetguard integrates auto-encoder (ae) and generative adversarial network (gan) techniques, which not only improves the detection of known threats, but also effectively recognizes unknown threats. By introducing an attention mechanism, deepnetguard also enhances the interpretability of the model, enabling security experts to better understand the key factors in the model's decision-making process to validate the effectiveness of the detection results. Deepnetguard has demonstrated its superior performance in cyber threat detection through experimental evaluations on multiple publicly available datasets. Compared with traditional rule-based ids systems (e.g., snort) and other deep learning models, deepnetguard demonstrates significant advantages in terms of accuracy, recall, precision, and f1 score. In particular, deepnetguard's detection capability is fully validated in both internal and data center network environments, demonstrating its broad applicability and robustness in different application scenarios. In addition, through cross-domain testing, we found that deepnetguard has good generalization ability and can maintain stable detection performance in different network environments.

In future work, we will continue to optimize the DeepNetGuard model and explore more feature extraction methods and technology combinations to further improve the detection efficiency and accuracy of the model. At the same time, we plan to expand the scale of experiments and collect more types of data sets for testing to ensure the reliability and stability of the model in various complex network environments. In addition, we will also conduct in-depth research on the interpretability of the model so that security experts can better understand the decision-making process of the model and enhance the transparency and trust of the system. The ultimate goal is to build a comprehensive, intelligent and trustworthy network security protection system.

References

[1] N. Abdi, A. Albaseer, and M. Abdallah, "The Role of Deep Learning in Advancing Proactive Cybersecurity Measures for Smart Grid Networks: a Survey," IEEE Internet of Things Journal, vol. 11, no. 9, pp. 16398–421, 2024.

[2] X. M. Liu, L. H. Xie, Y. P. Wang, J. Zou, J. B. Xiong, Z. B. Ying, and A. V. Vasilakos, "Privacy and Security Issues in Deep Learning: a Survey," IEEE Access, vol. 9, pp. 4566–4593, 2021.

[3] K. A. Alissa, F. S. Alrayes, K. Tarmissi, A. Yafoz, R. Alsini, O. Alghushairy, et al., "Planet Optimization with Deep Convolutional Neural Network for Lightweight Intrusion Detection in Resource-Constrained IoT Networks," Applied Sciences-Basel, vol. 12, no. 17, p. 15, 2022.

[4] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, "Enhancing IoT Network Security Through Deep Learning-Powered Intrusion Detection System," Internet of Things, vol. 24, p. 36, 2023.

[5] F. S. Alrayes, M. Zakariah, M. Driss, and W. Boulila, "Deep Neural Decision Forest (DNDF): a Novel Approach for Enhancing Intrusion Detection Systems in Network Traffic Analysis," Sensors, vol. 23, no. 20, p. 41, 2023.

[6] E. L. Lydia, C. Santhaiah, M. Altafahmed, K. V. Kumar, G. P. Joshi, and W. Cho, "An Equilibrium Optimizer with Deep Recurrent Neural Networks Enabled Intrusion Detection in Secure Cyber-Physical Systems," Aims Mathematics, vol. 9, no. 5, pp. 11718–34, 2024.

[7] K. Roshan, A. Zafar, and S. B. Ul Haque, "Untargeted white-box adversarial attack with heuristic defense methods in real-time deep learning-based network intrusion detection system," Computer Communications, vol. 218, pp. 97–113, 2024.

[8] S. Y. Wu, B. Wang, Z. L. Wang, S. H. Fan, J. H. Yang, and J. Li, "Joint prediction on security event and time interval through deep learning," Computers & Security, vol. 117, p. 12, 2022.

[9] Q. Y. Lin, R. Ming, K. L. Zhang, and H. B. Luo, "Privacy-enhanced intrusion detection and defense for cyber-physical systems: a deep reinforcement learning approach," Security and Communication Networks, vol. 2022, p. 9, 2022.

[10] M. K. Roshan and A. Zafar, "Boosting robustness of network intrusion detection systems: a novel two-phase defense strategy against untargeted white-box optimization adversarial attack," Expert Systems with Applications, vol. 249, p. 20, 2024.

[11] R. Sultana, J. Grover, and M. Tripathi, "Intelligent defense strategies: comprehensive attack detection in VANET with deep reinforcement learning," Pervasive and Mobile Computing, vol. 103, p. 18, 2024.

[12] R. H. Hwang, M. C. Peng, C. W. Huang, P. C. Lin, and V. L. Nguyen, "An unsupervised deep learning model for early network traffic anomaly detection," IEEE Access, vol. 8, pp. 30387–30399, 2020.

[13] M. Sewak, S. K. Sahay, and H. Rathore, "Deep reinforcement learning in the advanced cybersecurity threat detection and protection," Information Systems Frontiers, vol. 25, no. 2, pp. 589–611, 2023.

[14] S. Kim, S. Yoon, J. H. Cho, D. S. Kim, T. J. Moore, F. Free-Nelson, and H. Lim, "DIVERGENCE: Deep reinforcement learning-based adaptive traffic inspection and moving target defense countermeasure framework," IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 4834–4846, 2022.

[15] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. H. Han, M. M. Iqbal, and K. J. Han, "Enhanced network anomaly detection based on deep neural networks," IEEE Access, vol. 6, pp. 48231–48246, 2018.

[16] D. Q. Li and Q. M. Li, "Adversarial deep ensemble: Evasion attacks and defenses for malware detection," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3886–3900, 2020.

[17] R. T. Feng, S. Chen, X. F. Xie, G. Z. Meng, S. W. Lin, and Y. Liu, "A performance-sensitive malware detection system using deep learning on mobile devices," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1563–1578, 2021.

[18] K. Koo, D. Moon, J. H. Huh, S. H. Jung, and H. Lee, "Attack graph generation with machine learning for network security," Electronics, vol. 11, no. 9, p. 25, 2022.

[19] Z. H. Lv, D. L. Chen, B. Cao, H. B. Song, and H. B. Lv, "Secure deep learning in defense in deep-learning-as-a-service computing systems in digital twins," IEEE Transactions on Computers, vol. 73, no. 3, pp. 656–668, 2024.

[20] S. T. Mehedi, A. Anwar, Z. Rahman, K. Ahmed, and R. Islam, "Dependable intrusion detection system for IoT: A deep transfer learning based approach," IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 1006–1017, 2023.

[21] H. M. Rouzbahani, H. Karimipour, and L. Lei, "Multi-layer defense algorithm against deep reinforcement learning-based intruders in smart grids," International Journal of Electrical Power & Energy Systems, vol. 146, p. 10, 2023.

[22] S. Mohan, A. Annadurai, and K. Gunaseelan, "An efficient spoofing attack detection using deep learning-based physical layer security technique," Defence Science Journal, vol. 74, no. 4, pp. 526–534, 2024.

[23] P. Tian, Z. Y. Chen, W. Yu, and W. X. Liao, "Towards asynchronous federated learning based threat detection: a DC-Adam approach," Computers & Security, vol. 108, p. 16, 2021.

[24] S. Salmi and L. Oughdir, "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network," Journal of Big Data, vol. 10, no. 1, p. 25, 2023.

[25] Y. Liu, C. Tantithamthavorn, L. Li, and Y. P. Liu, "Deep learning for Android malware defenses: a systematic literature review," ACM Computing Surveys, vol. 55, no. 8, p. 36, 2023.

[26] B. H. Tang, J. F. Wang, Z. K. Yu, B. H. Chen, W. H. Ge, J. Yu, and T. T. Lu, "Advanced persistent threat intelligent profiling technique: a survey," Computers & Electrical Engineering, vol. 103, p. 21, 2022.

[27] K. M. Abuali, L. Nissirat, and A. Al-Samawi, "Advancing network security with AI: SVM-based deep learning for intrusion detection," Sensors, vol. 23, no. 21, p. 19, 2023.

[28] O. Kuznetsov, D. Zakharov, E. Frontoni, and R. Maranesi, "AttackNet: Enhancing biometric security via tailored convolutional neural network architectures for liveness detection," Computers & Security, vol. 141, p. 12, 2024.

[29] D. S. Rao and A. J. Emerson, "Cyberattack defense mechanism using deep learning techniques in software-defined networks," International Journal of Information Security, vol. 23, no. 2, pp. 1279–1291, 2024.

[30] F. Q. Zuo, D. M. Zhang, L. Li, Q. He, and J. X. Deng, "GSOOA-1DDRSN: Network traffic anomaly detection based on deep residual shrinkage networks," Heliyon, vol. 10, no. 11, p. 23, 2024.

Development of Fuzzy Logic CRITIC Coupling Coordination Degree Evaluation Algorithm

Practice of Cultural and Tourism Integration Development in the Yangtze River Economic Belt, China

Fangfang Hu
School of Humanities and Tourism, Zhejiang Institute of Economics and Trade, Hanzhou 310018, Zhejiang, China

***Abstract*—The integrated development of culture and tourism in the Yangtze River Economic Belt refers to a strategic initiative to push economic development and regional coordinated development with culture and tourism as the core. The purpose of this paper is to evaluate the coupling coordination degree of the integrated development of culture and tourism in the Yangtze River Economic Belt, by analysing the integrated development of culture, tourism and economy, and constructing an evaluation index system based on culture and tourism, in which 5 normative indicators and 19 basic indicators are constructed under the cultural perspective, and 4 normative indicators and 10 basic indicators are constructed under the tourism perspective, and its role and impact on regional economic development is explored based on the construction of the index system. Based on the construction of the indicator system, the role and influence of the indicators in regional economic development are explored. The CRITIC algorithm is used to calculate the importance of stratified indicators and stratified evaluation results, and finally, the coupling coordination degree of the research object is calculated through the coupling coordination degree model, which shows that the 13 provinces (municipalities directly under the central government) along the Yangtze River Economic Belt have a slightly different degree of coordination, but the least of them have reached the primary level of coordination, but it also proves that this paper proves the feasibility and necessity of the research method, and it can provide a good solution for the integrated development of culture and tourism in the Yangtze River Economic Belt. However, it also proves the feasibility and necessity of the research method of this paper, which can provide theoretical and practical guidance for the integrated development of culture and tourism in the Yangtze River Economic Belt, and provide new ideas and methods for the development of local tourism along the way.**

***Keywords*—Cultural and tourism integration; Yangtze River Economic Belt; coupling coordination degree; CRITIC algorithm**

I. INTRODUCTION

In China, the integrated development of culture and tourism has become a topic of great concern and has made some progress in academic research and practice. As a country with a long history and rich cultural heritage, China is endowed with unique cultural and tourism resources. Therefore, the integrated development of culture and tourism has become an important way to promote the development of tourism, cultural heritage and cultural industry, and domestic research on the integrated development of culture and tourism has gradually gained attention and importance [1-3]. Scholars have explored the theoretical basis, practice mode, policy support and other aspects of the integrated development of culture and tourism through field research, literature analysis and case studies, not only focusing on the impact of tourism on cultural heritage and the role of cultural resources in promoting tourism, but also putting forward a series of valuable ideas and suggestions [4-6]. Secondly, government departments and related institutions have also begun to pay attention to the integrated development of culture and tourism, and have issued a series of policies and measures to support the integration of culture and tourism, which aim to promote the sharing, complementation and integration of cultural and tourism resources, to promote the development of cultural and tourism industries, and to enhance the quality of tourism experience and cultural heritage. At the same time, some regions and scenic spots in China have begun to explore the development mode of integrating culture and tourism by organising cultural festivals, traditional performances, cultural experience activities, etc., integrating cultural elements into tourism products and services, which enriches the tourism experience, attracts more tourists, and promotes the development of the local economy [7-8].

It is believed abroad that such integrated development of culture and tourism can not only promote economic growth but also enrich people's spiritual lives and enhance international mutual understanding and friendship. In foreign countries, many scholars and research institutions have conducted in-depth research on the integrated development of culture and tourism and put forward many theoretical and practical results, which have made important contributions to the development of this field. Therefore, in foreign countries, many universities and research institutions have established interdisciplinary research teams to conduct in-depth research on the integrated development of culture and tourism, which has promoted the academic development of this field [9-10]. Foreign scholars have put forward many theoretical frameworks and models for the integrated development of culture and tourism, such as the theory of cultural tourism industry chain, the theory of cultural creative industry, the theory of cultural heritage protection, etc. [11-12]. These theoretical explorations have provided theoretical support and guidance for the integrated development of culture and tourism, and theoretical guidance for the relevant practices, and so along with this, many foreign research institutes have carried out in-depth studies on the practical cases of the integrated development of culture and tourism, and summarised the successful cases. In-depth study, summed up the

successful case experience and failed lessons, these practice case studies for the integration of culture and tourism development in other regions to provide reference and warning. Relevant research tasks cultural and creative industries as an important support for the integrated development of culture and tourism, so they have conducted in-depth research on the development path, innovation mode and policy support of cultural and creative industries, which provides important ideas for the integrated development of culture and tourism [13-15].

However, how to promote the deep integration and sustainable development of culture and tourism, and determine the degree of integration of culture and tourism at this stage, especially the degree of coordinated development of regional culture and tourism has become a new research hotspot, this paper considers that the Yangtze River Economic Belt, as one of the most important regions of China's economy, and the integration of culture and tourism development is of great significance to its economic development, so it adopts the CRITIC algorithm [16] to carry out a study on the degree of significance of the basic indicators in the indicator system of culture and tourism integration. Based on the coupling coordination degree [17] to determine the degree of cultural and tourism integration. In order to provide in-depth exploration and expansion of the concept of cultural and tourism integration, and to promote the continuous improvement and innovation of the theory of cultural and tourism integration.

II. Evaluation Model Construction

A. Overview of the Study Area and Sources of Data

1) Study area: In this paper, the study area is selected as provinces and municipalities along the route, mainly considering that the Yangtze River Economic Belt is located in the economically developed areas of China, with rich resources and good industrial foundation, which is one of the important pillars of China's economy, and the study of the coupling and coordination degree of the development of culture and tourism fusion in this region can make full use of the economic advantages of the Yangtze River Economic Belt, and promote the development of the culture and tourism industry [18]. Secondly, the Yangtze River Economic Belt spans across the developed provinces and cities in eastern China, and is connected to the upstream, midstream and downstream areas of the Yangtze River Basin, with an advantageous geographic location, which in turn provides rich regional cultural and tourism resources for the integrated development of culture and tourism, as well as broad market space for the integrated development of the culture and tourism industry [19-20]. At the same time, the Yangtze River Economic Belt has rich natural and human resources, but also faces the challenge of ecological environmental protection and governance, the study of the coupling and coordination degree of the integrated development of culture and tourism can help to promote the green development of the Yangtze River Economic Belt, and achieve the coordinated development of the economy and ecology. In addition, the government has put forward the development strategy of the Yangtze River Economic Belt in recent years, which provides policy support and financial guarantee for the development of the region, so the study of the degree of coupling and coordination of the integrated development of culture and tourism can be in line with the government's strategy, and better realise the integrated development of the regional economy and the culture and tourism industry [21]. The Yangtze River Economic Belt is a densely populated region in China, and its economic and social development level has an important impact on the whole country. By studying the coupling and coordination degree of the integrated development of culture and tourism, we can promote the economic and social development of the Yangtze River Economic Belt, and drive the development of the whole country's culture and tourism industry [22].

Studying the coupling and coordination degree of the integrated development of culture and tourism in the Yangtze River Economic Belt is of great practical significance and strategic significance, which helps to promote the regional economic development, cultural inheritance and the prosperity of the tourism industry, and fully demonstrates that the Yangtze River Economic Belt is suitable to be an ideal choice for studying the integrated development of culture and tourism.

2) Research data sources: Considering that this paper studies the development status of culture and tourism integration in the Yangtze River Economic Belt over the years, which is spatial in nature, the data for the indicators come from China Statistical Yearbook, China Environmental Statistical Yearbook, China Tertiary Industry Statistical Yearbook, China Tourism Statistical Yearbook, China Culture and Related Industries Statistical Yearbook, China Cultural Relics and Culture Statistical Yearbook, China Regional Economy Statistical Yearbook China Informatisation Statistical Yearbook", as well as the official website of the Ministry of Culture and Tourism, the database of the National Research Network, the Dawei Patent Search Engine, the official website of the State Civil Aviation Administration, the statistical yearbooks of provinces and districts along the Yangtze River Economic Belt and the annual statistical bulletin of national economic and social development, the mean value of the research data of the indexes is used to characterise the degree of development of the study area over the years, and at the same time it is dimensionless. The model is utilised to the extent that it can be utilised.

B. Constructing a System of Research Characterisation Factors

Through relevant research, it can be seen that the coupling coordination degree evaluation of cultural and tourism integration development needs to consider the richness and characteristics of tourism resources such as natural landscape, human landscape, historical and cultural heritage, and the degree of development and utilisation of tourism resources, because tourism resources are an important factor in attracting tourists, and also the main support for the development of cultural and tourism integration. Secondly, the development level of the regional economy and industrial structure has a direct impact on the coupling coordination degree of the integrated development

of culture and tourism, mainly in the economic prosperity, industrial diversification will provide more support and demand for the integration of culture and tourism; in addition, the government's support for the integrated development of culture and tourism policies and regulations have a profound impact on the evaluation of the degree of coordination, the soundness of the policy or not, the support, guidance, etc., will have a direct impact on the coordination degree of the integrated development of culture and tourism. However, relevant scholars believe that national policy considerations can be weakened in the study of the Yangtze River Economic Belt, because the importance of the cities along the line for its development can be seen. Of course, the social and cultural background of the region, customs and traditions, cultural heritage, etc. will have an impact on the degree of coordination of the integrated development of culture and tourism, cultural heritage and innovation, social inclusion and sharing are for cultural recognition, tourism integration of the details of the factors. The slogan of "green water and green mountains are golden mountains" is familiar, so it can be considered that the overall quality of the regional environment, ecological protection and governance, resource utilisation and sustainable development is the basis for the integrated development of culture and tourism.

Based on the above, the influencing factor indicator system can be constructed initially, but for the evaluation model, the following principles need to be considered when constructing the influencing factor indicator system for evaluating the coupling coordination degree of culture and tourism integration and development:

1) The principle of multi-dimensionality: Consider the influence of multiple factors. The integrated development of culture and tourism involves culture, tourism, economy, society and other fields, so the evaluation indicator system should be multi-dimensional, including cultural value, tourism resources and other aspects of the indicators, in order to comprehensively evaluate the degree of coordination of the integrated development of culture and tourism.

2) Principle of operability: The indicators should be operable and measurable. Evaluation indicators should be measurable and observable for assessment and monitoring in practical application. At the same time, the design of the indicators should take into account the feasibility of practical operation and be easy to be used by the government, enterprises and research institutions.

3) Principle of uniformity: The indicator system should have a certain degree of uniformity, and the evaluation indicators should have a certain degree of coordination and consistency in the whole, in order to ensure the objectivity and comparability of the evaluation results, therefore, this paper has carried out a dimensionless processing for the collected data of the research objects in section 2.1.2 to complete the consistency of the measurements.

4) Principle of sustainability: Consider the sustainability factors of development. The integrated development of culture and tourism needs to consider long-term sustainability, and the evaluation index system should take into account sustainability factors such as environmental protection, resource utilisation, social benefits, etc., in order to promote the sustainability of the integrated development of culture and tourism.

5) Participatory principle: Promote the participation of relevant stakeholders. The construction of the evaluation indicator system should take into account the opinions and needs of all stakeholders, and encourage them to participate in the selection of indicators and the evaluation process, in order to enhance the fairness and rationality of the evaluation.

The role of these principles is to ensure that the evaluation index system for integrated cultural and tourism development is scientific, practical and fair, so that it can comprehensively and objectively evaluate the degree of coordination of integrated cultural and tourism development and provide a scientific basis for decision-making and planning. At the same time, these principles also help to promote the participation and consensus of all stakeholders and promote the sustainability and coordination of integrated cultural and tourism development.

Based on this, this paper finally constructs the indicator system as shown in Table I.

As seen through Table I, based on the current research results, construction principles and visit records, this paper constructs a total of 29 basic indicators, of which a total of 19 indicators are constructed in the field of culture, and a total of 10 indicators are constructed under the tourism perspective, which can be seen that the indicators under the cultural perspective are higher than those under the tourism perspective, and analysed that the main reason is that how culture is embedded in the development of tourism is more concerned at the present time, i.e., how to promote the tourism Evolution into a harmonious win-win situation of culture and tourism is the current issue, which is not only a challenge to the inclusiveness of the tourism industry, but also a great challenge to the penetration and friendly integration of the cultural industry. And this also proves that it is more appropriate to adopt the degree of coupling coordination to analyse the degree of win-win between the two.

C. Degree of Impact and Evaluation based on the CRITIC Approach

The CRITIC algorithm is a risk assessment methodology for evaluating and managing risk in projects and decisions. CRITIC is an acronym for "Criticality, Recoverability, Inherent Risk, Time Criticality, Impact, and Controllability", and it includes the following six risk factors:

- Criticality: The degree of importance of the event and its impact on the project objectives.
- Recoverability: The ability of a project or organisation to return to a normal state after a risk event.
- Inherent Risk: The likelihood of a risk event occurring and the magnitude of its impact, regardless of the controls already in place.
- Time Criticality: The degree to which a risk event affects the timetable and schedule of a project or organisation.
- Impact: The degree of impact on the project or organisation following the occurrence of a risk event, including financial, environmental and social impacts.

- Controllability: The degree of control and ability of a project or organisation to control risk events.

TABLE I. EVALUATION INDEX SYSTEM OF COUPLING COORDINATION DEGREE OF CULTURAL AND TOURISM INTEGRATION DEVELOPMENT IN THE YANGTZE RIVER ECONOMIC BELT [22, 23]

Target level	Normative layer	Indicator layer	Interpretation of indicators
Cultures	Cultural Services Facilities	Number of public libraries	For assessing the distribution and coverage of cultural and educational resources.
		Number of performing arts venues	The number of performing arts venues in a city or region, which is used to assess the abundance of performing arts activities and opportunities for cultural exchange.
		Number of museums	Number of museums in the city or region, used to assess the preservation and presentation of historical and cultural heritage.
		Number of mass cultural institutions	Number of mass cultural institutions in the city or region for assessing the transmission and development of cultural traditions and intangible cultural heritage.
	Cultural services staff	Public Library Practitioners	The number of staff in public libraries, which is used to assess the quality and efficiency of library services.
		Museum practitioners	The number of staff in museums is used to assess the level of heritage conservation and display management in museums.
		Practitioners of mass cultural institutions	The number of staff in mass cultural institutions is used to assess the transmission of cultural traditions and the implementation of intangible cultural activities.
		Performing arts organisations	The number of staff of performing arts organisations, which is used to assess the scale and professionalism of performing arts activities.
	Cultural Services Benefits	Museum income	The museum's income is used to assess the museum's own operations and economic performance.
		Income from mass cultural institutions	The income of mass cultural institutions is used to assess the economic efficiency and sustainability of cultural activities.
		Revenue from performances at performing arts venues	The performance income of performing arts venues is used to assess the market performance and audience feedback of performing arts activities.
	Cultural service recipients	Public library circulation	Circulation of books in the public library collection is used to assess the library's reading service and the utilisation of book resources.
		Audience at arts performance venues	Audience size of performing arts venues, which is used to assess the audience size and social impact of performing arts activities.
		Museum Visit	Visits to museums, which are used to assess the social engagement and cultural impact of museums.
	Inputs to cultural services	Training in mass cultural institutions	Information on training activities provided by mass cultural institutions is used to assess the transmission of cultural traditions and the teaching of intangible cultural skills.
		Total expenditure on public libraries	The total expenditures of public libraries are used to assess the operating costs and funding of libraries.
		Total expenditure on mass cultural institutions	The total expenditure of the mass cultural institutions is used to assess the efficiency of financial expenditure and management of cultural activities.
		Total museum expenditure	The total expenditure of the museum is used to assess the museum's financial commitment and heritage conservation work.
		Expenditure on performing arts venues	Expenditure on performing arts venues, which is used to assess the operating costs and management efficiency of performing arts activities.
Journey	Tourism Service Facilities	Travel agents	Number and services of travel agencies in the city or region, used to assess the level of coverage and quality of tourism services.
		Starred hotel	The number and services of star-rated hotels in the city or region are used to assess the quality and reception capacity of tourism accommodation services.
		Scenic area	The number of attractions and visits within a city or region, which are used to assess the attractiveness of the attraction and the visitor experience.
	Tourist service staff	Travel agents	The number of staff in travel agencies, which is used to assess the level of professionalism and service attitude of travel services.
		Star-rated hotel workers	The number of staff in star-rated hotels is used to assess the scale of the service and the level of management of the hotels.
		Scenic Area Practitioners	The number of staff in the scenic area is used to assess the level of scenic area management and visitor services.
	Revenue from tourism services	Operating income from star-rated hotels	The operating income of star-rated hotels is used to assess the economic efficiency and market competitiveness of hotel operations.
		Gross tourism income from scenic spots	The total tourism revenue of the scenic spot is used to assess the economic efficiency and tourism attractiveness of the scenic spot.
	Tourism service recipients	Number of domestic and foreign tourists received by travel agencies	The number of domestic and foreign tourist arrivals received by travel agencies is used to assess the capacity and market demand for tourism services.
		Scenic Area Reception	The number of tourists received by the scenic spot is used to assess the flow of tourists and tourism impact of the scenic spot.

This paper considers adopting the CRITIC algorithm, mainly because it can comprehensively consider the importance and interconnectedness of multiple criteria or factors, so as to comprehensively assess the degree of tourism integration and development, which can help to avoid one-sided and localised evaluations, and improve the comprehensiveness and comprehensiveness of the assessment. Moreover, the CRITIC algorithm is based on mathematical models and quantitative analysis, which can provide objective evaluation results and reduce the influence of subjectivity and personal bias. At the same time, for diverse samples, this paper also proposes in section II.B that it is necessary to consider a clear evaluation process and calculation method, so that the evaluation process is operable and replicable, and the evaluator using the CRITIC algorithm can carry out standardised processing according to the standards and data, so as to carry out effective evaluation and comparison. In addition, the CRITIC algorithm can flexibly adjust and weigh different criteria or factors according to the actual situation, which helps to provide a flexible and comprehensive assessment of different aspects of integrated tourism development.

Taken together, the CRITIC algorithm, as a multi-criteria decision analysis method, has the advantages and strengths of comprehensiveness, objectivity, operability, flexibility and visualisation in assessing the degree of coupled coordination of tourism integration and development. The calculation steps are shown below.

1) Standardisation: Let the number of objects to be evaluated be *m*, the number of evaluation indicators be *n*, and the matrix of data elements be denoted as $X = (x_{ij})_{m\times n}$.

$$x_{ij}^{`} = \frac{x_{ij} - min \quad x_j}{max \quad x_j - min \quad x_j} \tag{1}$$

In Eq. (1), where: x'_{ij} - Data matrix elements after normalisation;

x_{ij} -Initial element of the data matrix.

2) Indicator variability

$$\sigma_j = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(x_i - \mu\right)^2} \tag{2}$$

In Eq. (2), where: σ_j - standard deviation;

x_i -*i* data for the *jth* indicator;

N - The number of x_i ;

μ - Arithmetic mean of x_i .

3) Calculation of quantitative indicators of the conflicting nature of the indicators.

$$R_{ij} = \sum_{i=1}^{n}(1 - r_{ij}) \tag{3}$$

In Eq. (3), where: R_{ij} - correlation coefficient;

r_{ij} -Evaluate the correlation coefficient between indicators *i* and *j*.

4) Calculation of the combined informativeness of the indicators.

$$C_j = \sigma_j \sum_{i=1}^{n}(1 - R_{ij}) \tag{4}$$

In Eq. (4), where: C_j - the amount of information for the jth indicator;

σ_j -standard deviation;

R_{ij} -correlation coefficients.

N -Number of quantities for the ith indicator.

5) Calculation of indicator weights

$$\omega = \frac{C_j}{\sum_{j=1}^{N} C_j} \tag{5}$$

In Eq. (5), where: ω - Objective weight of the jth indicator;

C_j -The amount of information in the jth indicator;

N -Number of quantities of the jth indicator.

6) Calculation of scores

$$S_i = \sum_{j=1}^{n}\left(\omega_j x'_{ij}\right) \tag{6}$$

In Eq. (6), Where: S_i - Score.

D. Degree of Coupling Coordination

The Coupled Coordination Degree Evaluation Model (CCDEM) is a model used to assess the degree of coordination and coupling between parts of a system. It is usually used to analyse the degree of interaction and coordination between different parts of a complex system in order to identify potential problems and opportunities for improvement. In the coupled coordination degree evaluation model, three aspects are usually considered: degree of coupling, degree of coordination, and degree of coupled coordination [17, 27].

Coupling degree refers to the degree of interdependence between the parts of the system, high coupling degree means high complexity of the system; Coordination degree refers to the degree of synergy between the parts of the system, high coordination degree can promote the overall performance and efficiency of the system; Coupling Coordination Degree Index: evaluate the coupling degree and coordination degree between the parts of the system through the quantitative index, so as to provide the overall performance of the system to assess and improve the direction.

Coupling C:

$$C = \left(\frac{\prod_{i=1}^{n} U_i}{\left(\frac{1}{n} \sum_{i=1}^{n} U_i \right)^n} \right)^{\frac{1}{n}} \quad (7)$$

In Eq. (7):U_i -Cultural System and Tourism System Score;

n-Number of systems.

Coordination T:

$$T = \sum_{i=1}^{n} \omega_i U_i \quad (8)$$

In Eq. (8):U_i -Cultural System and Tourism System Score;

n-Number of systems;

ω_i -System weighting, this paper considers two systems equally important each with 0.5.

Coupling coordination degree D, Eq. (9):

$$D = \sqrt{CT} \quad (9)$$

In this paper, the grading of the coupling coordination degree is listed in the following Table II.

TABLE II. CRITERIA FOR CLASSIFYING THE DEGREE OF COUPLING COORDINATION

Interval of D-values for coupling coordination	Level of coordination	Degree of coupling coordination
[0.0~0.1)	1	extreme disorder
[0.1~0.2)	2	severe disorder
[0.2~0.3)	3	moderate disorder
[0.3~0.4)	4	mild disorder
[0.4~0.5)	5	on the verge of becoming dysfunctional
[0.5~0.6)	6	sue for coordination
[0.6~0.7)	7	primary coordination
[0.7~0.8)	8	intermediate level coordination
[0.8~0.9)	9	good coordination
[0.9 to 1.0]	10	quality coordination

III. EMPIRICAL ANALYSES

A. Impact Level Analysis Based on the CRITIC Approach

This paper collects data from a total of 11 provinces (municipalities directly under the central government) in the study area to be analysed, and the degree of importance of the indicators is calculated by the equation (1-5) as shown in Table III and the evaluation scores are calculated according to the Formula (6) as shown in Table IV.

TABLE III. RESULTS OF THE CALCULATION OF THE IMPORTANCE OF IMPACT FACTORS

Indicator layer	Weights	Combined weights	Normative layer	Weights	Combined weights
Number of public libraries	0.0289	0.2028	Cultural Services Facilities	0.1427	0.2188
Number of performing arts venues	0.0374	0.2622			
Number of museums	0.0364	0.2552			
Number of mass cultural institutions	0.0399	0.2797			
Public Library Practitioners	0.0344	0.2515	Cultural services staff	0.1369	0.2099
Museum practitioners	0.0319	0.2333			
Practitioners of mass cultural institutions	0.0352	0.2571			
Performing arts organisations	0.0353	0.2581			
Museum income	0.0386	0.4045	Cultural Services Benefits	0.0954	0.1463
Income from mass cultural institutions	0.0285	0.2981			
Revenue from performances at performing arts venues	0.0284	0.2974			
Public library circulation	0.0301	0.2948	Cultural service recipients	0.1022	0.1567
Audience at arts performance venues	0.0394	0.3852			
Museum Visit	0.0327	0.3200			
Training in mass cultural institutions	0.0310	0.1772	Inputs to cultural services	0.1749	0.2682
Total expenditure on public libraries	0.0354	0.2025			
Total expenditure on mass cultural institutions	0.0366	0.2093			
Total museum expenditure	0.0378	0.2160			
Expenditure on performing arts venues	0.0341	0.1950			

Travel agents	0.0393	0.3427	Tourism Service Facilities	0.1145	0.3293
Starred hotel	0.0358	0.3122			
Scenic area	0.0395	0.3451			
Travel agents	0.0317	0.3268	Tourist service staff	0.0970	0.2788
Star-rated hotel workers	0.0360	0.3710			
Scenic Area Practitioners	0.0293	0.3022			
Hotel operating income	0.0304	0.4757	Revenue from tourism services	0.0639	0.1836
Gross tourism income from scenic spots	0.0335	0.5243			
Number of domestic and foreign tourists received by travel agencies	0.0364	0.5020	Tourism service recipients	0.0725	0.2083
Scenic Area Reception	0.0361	0.4980			

TABLE IV. CALCULATION OF EVALUATION SCORES AT THE NORMATIVE LEVEL

Normative layer	Cultural services	Cultural services staff	Cultural Services Benefits	Cultural service recipients	Inputs to cultural services	Tourism Service Facilities	Tourist service staff	Revenue from tourism services	Tourism service recipients
1.Shanghai	83.2869	84.5821	87.4249	96.6634	84.1007	89.6605	78.5996	86.4663	87.9603
2. Jiangsu	84.5421	85.3188	84.3863	76.6446	86.7828	91.9699	78.1524	80.8154	90.5059
3.Zhejiang	79.9165	86.7350	85.1465	91.9531	87.0892	85.9976	87.5799	91.9124	81.9722
4. Anhui	87.1009	81.1571	86.1479	80.9492	82.2495	89.7680	84.2653	85.4757	94.4901
5. Jiangxi	86.4581	84.7022	74.1042	91.6417	83.2003	81.6308	85.7542	83.1065	86.9485
6. Hubei	86.3460	95.8199	81.7004	88.7103	82.9198	80.8930	83.9925	82.1361	95.0000
7. Hunan	84.0908	87.7905	85.8790	77.3955	90.7249	74.7696	82.2110	84.1456	77.0278
8.Chongqing	85.6325	89.0495	75.6793	82.8763	84.0890	95.0610	87.9582	85.5148	82.5456
9. Sichuan	81.6045	90.6656	74.4052	90.5026	83.5206	78.8681	86.2626	75.9030	95.9921
10.Yunnan	83.3183	84.4954	88.5933	93.2479	82.3395	77.6426	82.5502	80.7183	93.0238
11. Guizhou	86.4300	90.8907	87.4380	82.8316	84.1804	93.8852	86.0219	83.7669	83.5059

TABLE V. CALCULATION OF EVALUATION SCORES AT THE TARGET LEVEL

Target level	Cultures	Journey
1. Shanghai	86.4791	85.6362
2. Jiangsu Province	84.0455	85.7647
3. Zhejiang Province	85.9233	86.6861
4. Anhui Province	83.4487	88.4296
5. Jiangxi Province	84.2203	84.1592
6. Hubei Province	87.1058	84.9243
7. Hunan Province	85.8589	79.0361
8. Chongqing	84.0469	88.7207
9. Sichuan Province	84.3610	83.9527
10. Yunnan Province	85.6311	82.7800
11. Guizhou Province	86.3462	87.6728

B. Analysis of the Results of the CRITIC Method

From Table VI, it can be seen that in the guideline layer results, the better development belongs to Shanghai Municipality and Guizhou Province, closely followed by Zhejiang Province and Hubei Province.

Observation of the economic zone research curve graph can be seen, the cultural perspective, to the best development of Hubei Province, based on the tourism perspective can be seen, Anhui Province, Sichuan Province, the development trend is better, to the worst development of Hunan Province, but the overall score is greater than 75, proving that the development of although compared with the high and low points, but there is no development of the bad provinces (municipalities).

C. Coupled Coordination Degree Model

The model evaluation of the study area is carried out according to Eq. (7-9), and the degree of coupling, coordination, and coupling co-ordination are now listed in the Table VI shown.

TABLE VI. EVALUATION RESULTS OF COUPLING COORDINATION DEGREE

Target level	Cultures	Journey	Coupling C-value	Harmonisation index T-value	D-value of coupling coordination	Level of coordination	Degree of coupling coordination
1. Shanghai	86.4791	85.6362	0.9940	0.7640	0.8710	9	good coordination
2. Jiangsu	84.0455	85.7647	0.7720	0.5890	0.6880	7	Primary coordination
3. Zhejiang	85.9233	86.6861	0.9990	0.7560	0.8690	9	good coordination
4. Anhui	83.4487	88.4296	0.7240	0.5690	0.6420	7	Primary coordination
5. Jiangxi	84.2203	84.1592	0.9790	0.4380	0.6550	7	Primary coordination
6. Hubei	87.1058	84.9243	0.9710	0.7980	0.8800	9	good coordination
7. Hunan	85.8589	79.0361	0.8530	0.5530	0.6910	7	Primary coordination
8. Chongqing	84.0469	88.7207	0.8520	0.6500	0.7440	8	Intermediate level coordination
9. Sichuan	84.3610	83.9527	0.9900	0.4430	0.7440	7	Primary coordination
10. Yunnan	85.6311	82.7800	0.9660	0.5250	0.7120	8	Intermediate level coordination
11. Guizhou	86.3462	87.6728	0.9990	0.8520	0.9230	10	Quality coordination

Based on Table VI, the coupling coordination degree of the Yangtze River Economic Belt as a whole does not appear coordination degree imbalance phenomenon, but Jiangsu Province, Anhui Province, Jiangxi Province, Hunan Province, Sichuan Province only for the primary coordination, which indicates that the degree of integration of culture and tourism still needs to be further strengthened; at the same time, only the degree of integration of culture and tourism in Guizhou Province to achieve a high quality degree of coordination, which indicates that at this stage, the local culture, tourism, the degree of collaboration is relatively high, and the development of the development presents a good trend.

According to Table VI, although different provinces (municipalities directly under the central government) of the degree of coupling, degree of coordination, coupling degree of coordination there is a certain degree of variability, all show a high value of coupling degree, which indicates that the integration of culture, tourism is an extremely complex system, perhaps there are certain differences, but also just show the degree of difficulty of the differences between the places, but the degree of coordination exists there is a low phenomenon, indicating that the system's synergistic operation efficiency Low, especially in Jiangxi Province, but the coupling degree in Jiangxi Province is very high, which indicates that the more complex the system is, the less easy it is to coordinate the operation, so Jiangxi Province must put forward reasonable and feasible measures to strengthen the integration of culture and tourism.

IV. CONCLUSION

As an important support region for China's economic development, the coupling and coordination degree of the integrated development of culture and tourism in the Yangtze River Economic Belt plays a crucial role in its development. By evaluating the coupling coordination degree of culture and tourism integrated development in the Yangtze River Economic Belt, it can be seen that the coupling coordination degree of culture and tourism integrated development in the Yangtze River Economic Belt presents a good trend as a whole, and the coordination and cooperation and resource sharing among regions make the culture and tourism industry develop better and provide strong support for the comprehensive development of the economic belt. However, there are some problems and challenges in the evaluation of the coordination degree of culture and tourism integrated development in the Yangtze River Economic Belt. Some areas in the integrated development of culture and tourism still have deficiencies in the synergistic development between culture and tourism industries, the combination of cultural resources and tourism products is not high, and the depth and breadth of the integration of culture and tourism need to be strengthened. This requires strengthening the integration and sharing of resources for the integrated development of culture and tourism, increasing investment, optimising resource allocation, promoting the integration and sharing of culture and tourism resources, and improving the quality and level of integration of culture and tourism. At the same time, the coordination and cooperation among regions of the Yangtze River Economic Belt should be strengthened, the regional coordination of the integrated development of culture and tourism should be promoted, and the sharing and complementation of resources among regions should be facilitated, so as to achieve the synergistic development of the integrated development of culture and tourism.

In summary, the evaluation of the coupling coordination degree of the integrated development of culture and tourism in the Yangtze River Economic Belt is of great significance, and in the future, it is necessary to continuously strengthen the coordination and cooperation to promote the synergistic development of the integrated development of culture and tourism, to inject new vitality into the economic and social development of the Yangtze River Economic Belt, and to achieve the goal of high-quality development

ACKNOWLEDGMENT

This work is supported by The Fundamental Research Funds for the Provincial Universities, Zhejiang Institute of Economics and Trade (Grant No.:2YQ01).

REFERENCES

[1] Wu, M. Y., Tong, Y., Li, Q., Wall, G., & Wu, X. (2023). Interaction rituals and social relationships in a rural tourism destination. Journal of Travel Research, 62(7), 1480-1496.

[2] Liang, F., Pan, Y., Gu, M., Liu, Y., & Lei, L. (2022). Research on the paths and strategies of the integrated development of culture and tourism industry in urban historical blocks. Frontiers in Public Health, 10, 1016801. Health, 10, 1016801.

[3] Zhang, F., Sarker, M. N. I., & Lv, Y. (2022). Coupling coordination of the regional economy, tourism industry, and the ecological environment: Evidence from western China. Sustainability, 14(3) , 1654. Sustainability, 14(3) , 1654.

[4] Li, X., Liang, X., Yu, T., Ruan, S., & Fan, R. (2022). Research on the integration of cultural tourism industry driven by digital economy in the context of COVID-19-based on the data of 31 Chinese provinces. Chinese provinces. Frontiers in Public Health, 10, 780476.

[5] Butler, Gareth, Gerti Szili, and Huanling Huang. "Cultural heritage tourism development in Panyu District, Guangzhou: community perspectives on pride and preservation, and concerns for the future." Journal of Heritage Tourism 17.1 (2022): 56-73.

[6] Yu, J., Safarov, B., Yi, L., Buzrukova, M., & Janzakov, B. (2023). The Adaptive Evolution of Cultural Ecosystems along the Silk Road and Cultural Tourism Heritage: A Case Study of 22 Cultural Sites on the Chinese Section of the Silk Road World Heritage. Sustainability, 15(3), 2465.

[7] Shen, Jing, and Rung-Jiun Chou. "Rural revitalization of Xiamei: The development experiences of integrating tea tourism with ancient village preservation." Journal of Rural Studies 90 (2022): 42-55. Rural revitalization of Xiamei: The development experiences of integrating tea tourism with ancient village preservation." Journal of Rural Studies 90 (2022): 42-52.

[8] He, H., Tuo, S., Lei, K., & Gao, A. (2024). Assessing quality tourism development in China: an analysis based on the degree of mismatch and its influencing factors. Environment, Development and Environment, Development and Sustainability, 26(4), 9525-9552.

[9] Kastenholz, Elisabeth, and Werner Gronau. "Enhancing competences for co-creating appealing and meaningful cultural heritage experiences in tourism ." Journal of Hospitality & Tourism Research 46.8 (2022): 1519-1544.

[10] Zunaidi, A., Nofirman, N., Juliana, J., & Wurarah, R. N. (2022). The Impact Of The Development Of Cultural Tourism On The Cultural, Economic, And Social Aspects Of Local Communities. dinar: Jurnal Ekonomi dan Keuangan Islam, 9(2), 88-105.

[11] Mai, N. T. T., Tuan, H. T., Tien, N. H., Van Tho, D., Trang, N. T. T., & Mai, N. P. (2023). Cultural tourism resources: State policy and solutions for SMEs in tourism industry. International Journal of Entrepreneurship and Small Business.

[12] Macleod, D. (2023). Cultural realignment, islands and the influence of tourism: a new conceptual approach. in Islandscapes and Tourism: An Anthology (pp. 9-22). GB: CABI. Macleod, D. (2023).

[13] de Oliveira, R. A., Baracho, R. M. A., & Cantoni, L. (2024). The perception of UNESCO World Heritage Sites' managers about concepts and elements of cultural sustainability in tourism. Journal of Cultural Journal of Cultural Heritage Management and Sustainable Development, 14(3), 297-311.

[14] Tolkach, Denis, and Stephen Pratt. "Globalisation and cultural change in Pacific Island countries: the role of tourism." Island Tourism Sustainability and Resiliency. Routledge, 2022. 10-35.

[15] Sharpley, Richard. "Tourism and development theory: Which way now?." Tourism Planning & Development 19.1 (2022): 1-12.

[16] WANG Liang,YIN Zhigang,CONG Peijiang,et al. Safety evaluation of small and medium-sized earth and rock dams based on combined empowerment-cloud model[J]. Journal of Hydraulic and Architectural Engineering,2022,20(04):91-97+119.

[17] Xing, Lu, Minggao Xue, and Mingsheng Hu. "Dynamic simulation and assessment of the coupling coordination degree of the economy-resource -environment system: case of Wuhan City in China." Journal of Environmental Management 230 (2019): 474-487.

[18] Feng Fei. Research on resource evaluation, utilisation efficiency and influencing factors of cultural and tourism integration industry in the Yangtze River Economic Belt[D]. East China Normal University,2020.DOI:10.27149/d.cnki.ghdsu.2020.000067.

[19] Ran, P., Hu, S., Frazier, A. E., Qu, S., Yu, D., & Tong, L. (2022). Exploring changes in landscape ecological risk in the Yangtze River Economic Belt from a spatiotemporal perspective. Ecological Indicators, 137, 108744.

[20] Xue Mingda. Exploration of Xi Jinping's Important Discourse on the Yangtze River Economic Belt[J]. Journal of Luoyang Institute of Technology (Social Science Edition),2024,39(03):39-42.[23]

[21] WANG Zhaofeng,LIANG Zhiqiang. Spatio-temporal evolution and influencing factors of the integration development level of culture and tourism industry in the Yangtze River Economic Belt[J]. Journal of Shaanxi Normal University (Natural Science Edition),2023,51(06):97-110.DOI:10.15983/j.cnki.jsnu.2023133.

[22] Tang, C., Liu, Y., Wan, Z., & Liang, W. (2023). Evaluation system and influencing paths for the integration of culture and tourism in traditional villages. Journal of Geographical Sciences, 33(12), 2489-2510. Journal of Geographical Sciences, 33(12), 2489-2510.

[23] Wu Rulian. Research on the coupled coordination measurement, evolution and spatial effect of high-quality development of tourism and rural revitalisation [D]. Jiangxi University of Finance and Economics,2022.DOI:10.27175/d.cnki.gjxcu.2022.000469.

Performance Comparison of Pretrained Deep Learning Models for Landfill Waste Classification

Hussein Younis[1], Mahmoud Obaid[2]
Department of Computer System Engineering, Arab American University, Jenin, Palestine[1, 2]

***Abstract*—The escalating challenge of waste management, particularly in developed nations, necessitates innovative approaches to enhance recycling and sorting efficiency. This study investigates the application of Convolutional Neural Networks (CNNs) for landfill waste classification, addressing the limitations of traditional sorting methods. We conducted a performance comparison of five prevalent CNN models—VGG-16, InceptionResNetV2, DenseNet121, Inception V3, and MobileNetV2—using the newly introduced "RealWaste" dataset, comprising 4,752 labeled images. Our findings reveal that EfficientNet achieved the highest average testing accuracy of 96.31%, significantly outperforming other models. The analysis also highlighted common challenges in accurately distinguishing between metal and plastic waste categories across all models. This research underscores the potential of deep learning techniques in automating waste classification processes, thereby contributing to more effective waste management strategies and promoting environmental sustainability.**

Keywords*—Waste management; deep learning; waste classification; real-waste dataset; performance comparison

I. Introduction

The increase in waste generation, particularly in developed countries, poses a significant challenge to effective waste management and recycling efforts. By 2050, it is projected that developed nations will experience a 19% increase in per capita daily waste production, emphasizing the critical need for more efficient waste management strategies [1]. Traditional waste sorting methods, such as manual sorting and visual inspection, have limitations in terms of subjectivity, scalability, and labor requirements [1]. To address these challenges, the integration of deep learning techniques, particularly Convolutional Neural Networks (CNNs), into waste sorting processes can enhance automation and improve waste classification based on its features [2], [3].

CNNs are a class of deep learning models that excel in processing visual data, making them well-suited for tasks like waste classification [3]. These networks automatically extract relevant information from input data through their layers, with convolutional layers specifically extracting spatial features from images, making CNNs highly efficient for image-related tasks [4]. By leveraging advanced technologies like deep learning, waste sorting processes can be optimized, recycling rates can be increased, and a more sustainable waste management system can be achieved [5].

Automated waste classification systems, powered by deep learning models like CNNs, have become essential for addressing the global waste problem and promoting sustainable development [6]. These systems offer a more objective and scalable approach to waste sorting compared to traditional methods, contributing to more efficient recycling processes and waste management overall [7]. The incorporation of deep learning methods in waste classification not only streamlines the sorting process but also plays a crucial role in achieving environmental sustainability by reducing waste and promoting recycling efforts [8].

In conclusion, the adoption of deep learning techniques, particularly CNNs, in waste classification is pivotal for enhancing automation, improving waste sorting accuracy, and ultimately aiming to create a waste management system that is more effective and sustainable in light of the rising amount of garbage produced worldwide.

This paper presents a performance comparison of five common CNN pre-trained models applied on a dataset called "RealWaste" and provides a critical analysis of the results to see the impact of the quality of the dataset and more detailed classes of the waste. Hence, the main contributions of this paper are as follows:

- Provide a performance comparison of five common CNN models in landfill waste classification.
- Evaluate the performance of the selected models when the type of material over different items is important to be detected.
- Employ transfer learning and fine-tune the learning process using the scheduling of the learning rate.
- Achieve superior classification accuracy compared to previous work.

The remainder of this paper is structured as follows: Section II discusses the related works. The RealWaste dataset and the proposed models for evaluation are detailed in Section III and Section IV. Section V discusses the results and outcomes, and Section VI concludes the paper.

II. Literature Review

Table I presents the top accuracies achieved by different datasets in waste classification tasks. It includes datasets such as RealWaste and DiversionNet, Waste dataset, Custom dataset, Sekar's waste classification, OrgalidWaste, Waste Classification data, and the proposed work using RealWaste. The accuracy values range from 49.69% to 99.43%, highlighting the varying performance levels of the datasets in accurately classifying waste materials.

TABLE I. COMPARATIVE ANALYSIS OF DATASETS AND TOP ACCURACIES IN WASTE CLASSIFICATION

Ref.	Dataset	Top Accuracy
[9]	RealWaste and DiversionNet	49.69% using DiversionNet and 89.19% using RealWaste
[10]	Waste dataset	70%
[11]	Custom dataset	99.43%
[12]	Sekar's waste classification	80.88%
[13]	OrgalidWaste	88.42%
[14]	Waste Classification data	96.7%
Our proposed work	RealWaste	96.31%

In study [9], the authors propose a new dataset called RealWaste and evaluate the performance of five deep learning models (VGG-16, InceptionResNetV2, DenseNet121, Inception V3, and MobileNetV2) for waste classification using the "RealWaste" dataset and the existing "DiversionNet" dataset. The classification accuracy for the "DiversionNet" dataset was limited to 49.69% for the "RealWaste" dataset, the models were able to achieve much higher classification accuracy where Inception V3, reached 89.19% classification accuracy on the full spectrum of labels required for accurate waste modeling.

In research [10], the authors use a custom CNN model architecture with four and five convolution layers to classify four categories of solid waste including plastic, glass, organic, and paper materials. They use a "Waste dataset" that contains 100 RGB images for each category. The five-layer DCNN architecture achieved a 70% accuracy rate in distinguishing the different waste types, while the four-layer architecture had a 61.67% accuracy rate. Plastic waste was the most challenging to classify accurately, with 37% and 56.7% accuracy rates in the four-layer and five-layer architectures, respectively. The key limitations were around classification accuracy, particularly for plastic waste, as well as the need for further optimization and exploration of a broader range of waste types and real-world application considerations.

In study [11], the authors use a custom CNN model with two, six, and eight convolutional layers with a custom dataset of 878 carrot images captured in-house, which they preprocessed and augmented to train and evaluate their proposed CNN models. The authors found that the eight convolutional layers model with the mixed pooling layer achieved the best performance, reaching 99.43% accuracy in classifying regular and irregular carrot shapes on 24x24 pixel images. The study was conducted using a dataset of 878 carrot images, which may be considered a relatively small dataset for training deep learning models. Also, the study was conducted in a controlled laboratory setting using images captured under specific lighting conditions. The authors acknowledge that while the proposed CNN-based approach showed promising results in the laboratory setting, further research and real-world validation would be needed to fully assess the practical applicability and limitations of the system.

In study [12], the authors developed a bespoke 5-layer CNN architecture and trained it on two different image resolutions (80x45 and 225x264 pixels) of the augmented "Sekar's waste classification" dataset consisting of 25,077 images of organic (13,966) and recyclable (11,111) waste objects. The research aims to explore the possibility of training an efficient lightweight model with high accuracy and less computational demand compared to standard CNN architectures. The smaller model (80.88%) outperformed the larger model (76.19%), but the larger model seems more generalizable based on the observed behavior of loss and accuracy during training, validation, and testing. The key limitations include the data paucity and limited categories.

In study [13], the authors use various CNN models for waste classification, including AlexNet, GoogLeNet, EfficientNet-B0, and ResNet-50 with a transfer learning approach. Also, they use a custom four-layer CNN. They used a dataset called "OrgalidWaste" which comprises approximately 5,600 images categorized into four waste classes: organic, glass, metal, and plastic. The performance evaluation of the models in the study was based on accuracy and cross-entropy loss observed during training, validation, and testing. The VGG16 model achieved the highest accuracy of 88.42%, outperforming other CNN architectures like VGG19, Inception-V3, and ResNet50. The study highlighted the need to further enhance classification accuracy for practical deployment despite the promising results obtained.

In study [14], the authors use convolutional neural networks (CNNs) and faster region-based convolutional neural networks (R-CNNs) to classify e-waste. The proposed system aims to facilitate communication between individuals requesting WEEE pickup and waste collection companies, enabling efficient collection planning based on the identified type and size of the e-waste items. They used a dataset called "Waste Classification data" containing 24,705 images of refrigerators, washing machines, and monitors/TVs. The geometric transformations were used as data augmentation with 13 transformations such as rotation, color transformation, zoom, and blur. The proposed CNN model achieved an average accuracy of 90-96.7% and the faster R-CNN network provided slightly lower accuracy, around 90% on average, but had the advantage of being able to detect and determine the size of the objects in the images. The key limitations were around the limited e-waste categories.

III. DATASET

The study leveraged the newly developed landfill waste dataset, "RealWaste," which comprises 4,752 raw and fully labeled RGB images. This dataset was meticulously collected during the biannual residential waste audit at the Wollongong Waste and Resource Recovery Centre's landfill [9]. The collection process involved capturing images of various waste items as they were sorted, ensuring a representative sample of the types of materials commonly found in residential waste.

Fig. 1 shows samples of RealWaste images with their label.

(a) (b) (c) (d)

Fig. 1. Sample images from the dataset for: (a) Cardboard; (b) Food Organics; (c) Glass; (d) Metal.

The RealWaste dataset includes samples across nine distinct labels representing different landfill waste categories including Cardboard, Food Organics, Glass, Metal, Miscellaneous Trash, Paper, Plastic, Textile Trash and Vegetation.

An analysis of the dataset reveals that it exhibits some degree of imbalance in the distribution of images across the labels. Table II presents the count and percentage of images for each label, highlighting the variations.

TABLE II. LABELS AND IMAGE COUNT IN DATASET

Label	Images Count	Percentage Of Each Label in The Dataset
Cardboard	461	9.69%
Food Organics	411	8.65%
Glass	420	8.83%
Metal	790	16.62%
Miscellaneous Trash	495	10.41%
Paper	500	10.51%
Plastic	921	19.38%
Textile Trash	318	6.69%
Vegetation	436	9.17%

This imbalance may pose challenges for model training, particularly in ensuring that the model generalizes well across all categories. The predominance of plastic images, for instance, could lead to bias in classification outcomes if not adequately addressed.

IV. METHODOLOGY

This section addresses a significant gap in waste classification literature, focusing on dataset limitations and inadequate labeling in waste auditing studies. To enhance the accuracy and practicality of waste classification models, data is preprocessed and augmented for use by the pre-trained CNN models EfficientNet, GoogLeNet, ResNet-152, ShuffleNet, and VGG-19. The objectives include evaluating the use of clean material datasets for training models in real waste classification, comparing dataset approaches by training on real waste samples, and identifying the best model for waste classification in real-world scenarios.

As shown in Fig. 2, the proposed methodology consists of the following main steps:

- Data Splitting: The dataset was split into training, validation, and testing subsets using a standard split ratio, where 50% of the data was used for training, 20% for validation, and 30% for testing. This ensures that the model is trained on a diverse set of data, validated on a separate subset, and finally tested on unseen data [15].
- Hyperparameter tuning: Hyperparameters–such as batch size, learning rate, number of epochs, momentum, and learning rate decay–are set. These hyperparameters play a crucial role in the training process and should be carefully chosen through experimentation and validation [16].
- Training and Validation: Each model is trained and validated using a stochastic gradient descent optimizer. Additionally, the use of automatic mixed precision (auto-cast) is considered to accelerate training without sacrificing model accuracy. Furthermore, a learning rate scheduler is employed to adjust the learning rate during training [17].
- Model Evaluation: Each model uses metrics such as accuracy, precision, recall, F1 score, receiver operating characteristic curve, and confusion matrix analysis. These metrics provide a comprehensive understanding of the model's performance, such as correctly classifying instances, handling imbalanced classes, and discriminating between classes [18].

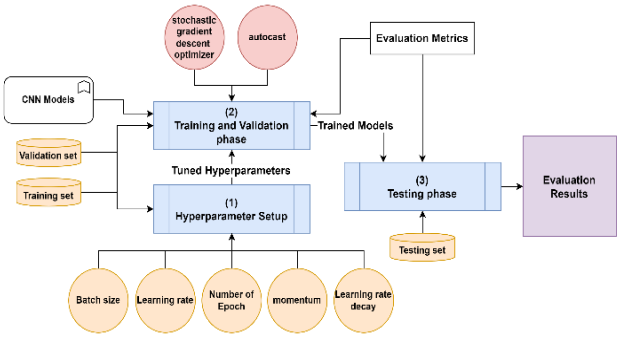


Fig. 2. The proposed methodology.

A. Data Preprocessing and Augmentation

CNNs typically require input images to be of a fixed size to avoid issues with model training and performance. Variations in image dimensions can be addressed by resizing images before inputting them into the CNN. This can be done using techniques like Bicubic interpolation, which involves averaging 16 neighboring pixels to determine pixel values in the resized image [19], [20]. Data augmentation techniques, which improve models' ability to generalize and perform well on diverse datasets and solve unbalanced dataset issues such as:

- Color Jitter which introduces random variations in the hue and saturation levels of images to augment the dataset. The hue indicates the range of random hue adjustments applied to the image, while saturation represents the range of random saturation adjustments.

- Randomly rotates images within the specified range of degrees.

The incorporation of augmented images with diverse textures and appearances enhanced the diversity and richness of the dataset. As a result, this contributed to an improved generalization of models and enhanced their performance across all classes. Each image in the dataset was used to generate two new images: The first was generated by adding Color Jitter with a hue value of 0.05 and a saturation of 0.05 to the original image. The second was generated by applying random rotations to images in the dataset with a range from 0 to 180 degrees.

B. The Selected Models

The CNN models including EfficientNet, GoogLeNet, ResNet-152, ShuffleNet, and VGG-19 were selected for this experimental study to analyze the performance in classifying landfill waste due to their proven capabilities in image classification tasks. EfficientNet is renowned for its efficiency in balancing model size and accuracy. GoogLeNet introduces the inception module for feature extraction. ResNet-152 utilizes residual connections to tackle the vanishing gradient problem. ShuffleNet emphasizes computational efficiency through channel shuffling. VGG-19 is acknowledged for its deep architecture with small convolutional filters [21], [22], [23]. The strengths of these models in image classification position them as ideal candidates for accurately classifying landfill waste:

- EfficientNetV2, introduced in 2021 by Tan and Le, improves training speed and parameter efficiency compared to the original EfficientNet. It addresses slow training with larger image resolutions by combining MBConv and Fused-MBConv blocks through neural architecture search and model scaling. This optimization enhances training efficiency [24].
- GoogLeNet: GoogLeNet developed by Google in 2015, is a deep convolutional neural network for image classification. It uses multiple convolutional layers with different filter sizes and pooling operations to extract features at various scales. The architecture consists of 19 layers, featuring inception modules for feature extraction, auxiliary classifiers to address the vanishing gradient issue and overfitting, and ensuring computational efficiency. It also includes max-pooling layers, an average pooling layer, a dropout layer, and a linear layer for the final output [25].
- ResNet-152: ResNet-152 was introduced in 2015 by Microsoft. It is part of the ResNet (short for Residual Network) family of models, known for their deep structure and the use of residual connections. ResNet-152 specifically has 152 layers, making it a very deep network, and it has been widely used for various computer vision tasks, such as image classification and object detection [26].
- ShuffleNet V2: Introduced in 2018 as an evolution of the original ShuffleNet, focuses on enhancing computational efficiency and model performance. By integrating channel shuffling and pointwise group convolutions, it improves performance while preserving computational efficiency. These elements enhance its effectiveness in feature extraction and representation learning. With 164 layers, ShuffleNet V2 incorporates operations like depthwise separable convolutions, concatenation, and channel shuffling to facilitate efficient information exchange and feature extraction within the network [27], [28].
- VGG19: VGG19, a deep convolutional neural network that comprises 19 layers, was developed in 2014. It is known for its simplicity and effectiveness in image recognition tasks. The network architecture consists of a series of convolutional layers that are followed by max pooling layers and culminates in three fully connected layers [29].

C. Hyperparameters and Optimization Technique

Hyperparameters are parameters that govern the learning process and dictate the values of the model parameters acquired by a learning algorithm. The use of the prefix "hyper" indicates the significance of the parameters in determining both the learning process and resulting model parameters [30]. Specifically, hyperparameters are settings or configurations that are not learned from the data but are set before training the model, and in the proposed methodology, the following hyperparameters were used: learning rate, loss function, number of epochs, and batch size.

Optimizers are essential for adjusting model weights and learning rates to minimize errors or maximize efficiency. For instance, stochastic gradient descent is a popular optimization algorithm in deep learning, a variation of gradient descent. It minimizes loss functions by training models. Unlike traditional gradient descent, stochastic gradient descent computes gradients using data subsets, known as "mini-batches," making it faster and more scalable for large datasets. This approach accelerates convergence, especially beneficial for handling extensive datasets [31], [32]; therefore, it was used in the proposed methodology. The objective function $f(x)$, which is the average loss function, is given by the following equation:

$$f(x) = \frac{1}{n}\sum_{i=1}^{n} f_i(x) \quad (1)$$

where n is the number of input data taken from the training dataset. The gradient of the objective function is computed for each iteration of the training phase by the following equation:

$$\nabla f(x) = \frac{1}{n}\sum_{i=1}^{n} \nabla f_i(x) \quad (2)$$

The stochastic gradient descent algorithm reduces the computational cost at each iteration by randomly shuffling the training data to ensure that the mini-batches used for computing the gradients are representative of the entire dataset and compute the gradient $\nabla f_i(x)$ to update x by the following equation [33]:

$$x \leftarrow x - \eta \nabla f_i(x) \quad (3)$$

where η is the learning rate.

D. Evaluation Metrics

Various evaluation metrics were utilized to appraise the performance of the selected models, including the confusion matrix, accuracy, F1 score, precision, recall, and receiver operating characteristic (ROC) curve [34]. The confusion matrix evaluates the classification performance of the CNN model by juxtaposing actual and predicted values. In this matrix, rows correspond to actual values while columns represent predicted values. The results obtained from this evaluation encompass four potential outcomes: True Positive (TP) - denoting correct prediction of the positive class, False Positive (FP) - indicating incorrect prediction of the positive class, True Negative (TN) - signifying accurate prediction of the negative class, and False Negative (FN) - representing erroneous prediction of the negative class [35].

Accuracy refers to the extent to which the model effectively categorizes all instances within a dataset. It is computed by dividing the total number of correct predictions by the overall number of predictions made [36]. The following equation calculates accuracy:

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (4)$$

The F1 score is a numerical measure of the balance between precision and recall [37]. It is calculated by taking the harmonic mean of precision and recall using the following equation:

$$F1\ score = 2 * \frac{(precision * recall)}{(precision + recall)} \quad (5)$$

Where precision is the ratio of true positives to the sum of true positives and false positives, measuring the accuracy of positive predictions. Recall, on the other hand, is the proportion of true positives to the sum of true positives and false negatives, indicating the ability to identify actual positives accurately.

The ROC curve evaluates a CNN model's ability to distinguish labels by examining the true positive rate (TPR) and false positive rate (FPR) at different thresholds. It assesses the model's accuracy in classification by graphing TPR against FPR at various threshold levels [38]. The TPR and FPR are calculated using the following equations:

$$TPR = \frac{TP}{(TP + FN)} \quad (6)$$

$$FPR = \frac{FP}{(FP + FN)} \quad (7)$$

V. Results and Discussions

A. Experimental Setup

The original dataset was cleaned, preprocessed, and enhanced as outlined in Section III to prepare it for training CNN models. The image quantity was increased to 19,008 labeled images, with each label representing around 3% of the dataset, totaling 9 unique labels. One-hot encoding was utilized for label encoding. Various hyperparameters such as learning rate, loss function, epochs, batch size, optimizer, momentum, learning rate decay, and weight initialization were set for training the CNN models as shown in Table III. The selected models' weights were initialized by loading pre-trained weights from ImageNet, enhancing their performance and efficiency while reducing the need for extensive training on the dataset.

TABLE III. Hyperparameters and their Values Tuning

Hyperparameters	Value
Learning rate	0.001
Loss function	Cross-entropy loss
Number of epochs	50
Batch sizes	64
Optimizer	Stochastic gradient descent
Momentum	0.9
Learning rate decay	0.0005
Weight initialization	Transfer learning

All experiments were carried out locally on a computer with the following specifications:

- Processor: AMD Ryzen 9 5900HX, 3301 MHz, 8 Core(s), 16 Logical Processor(s).
- Physical Memory (RAM): 32.0 GB.
- Graphics Card: NVIDIA GeForce RTX 3080 Laptop GPU.

B. Models Training Performance

All models were trained using the same dataset and with hyperparameter values as listed in Table III to analyze the learning behavior of each model. Table IV presents the average training and validation accuracy, as well as the average training and validation loss for various models including EfficientNet, GoogLeNet, ResNet-152, ShuffleNet, and VGG-19. ResNet-152 has the highest average training among the models listed, with a value of 99.07%.

TABLE IV. Hyperparameters and their Values Tuning

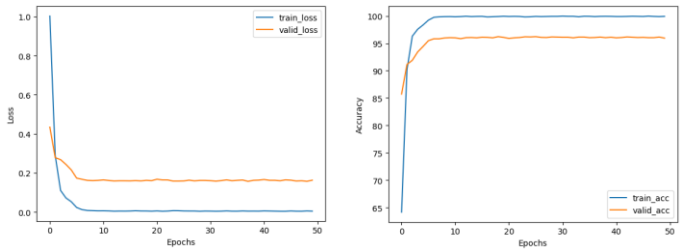
#	Model	Average Training Accuracy	Average Validation Accuracy	Average Training Loss	Average Validation Loss
1	EfficientNet	98.82%	95.57%	0.036	0.174
2	GoogLeNet	98.93%	92.93%	0.035	0.234
3	ResNet-152	99.07%	94.63%	0.029	0.198
4	ShuffleNet	92.83%	86.42%	0.270	0.430
5	VGG-19	97.94%	91.22%	0.063	0.343

ShuffleNet has the lowest average training accuracy at 92.83% but still demonstrates strong performance. EfficientNet and GoogLeNet demonstrate competitive performance in terms of accuracy and loss, while VGG-19 shows slightly lower accuracy, but relatively lower loss compared to ResNet-152.

Overall, the analysis shows that ResNet-152 performs exceptionally well in terms of both accuracy and loss, while ShuffleNet appears to face challenges in generalizing to validate data. This comparative analysis can provide valuable

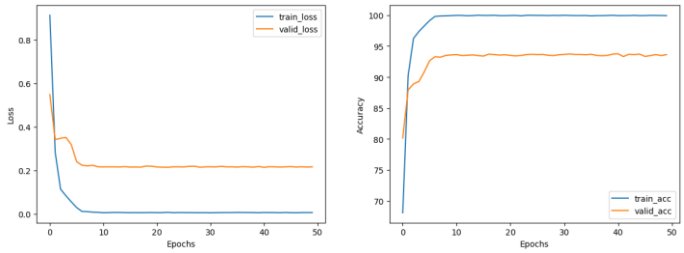
insights for selecting the most suitable model based on specific performance criteria.

Fig. 3 to Fig. 7 visualize the loss values and average accuracy percentage for all models per epoch.



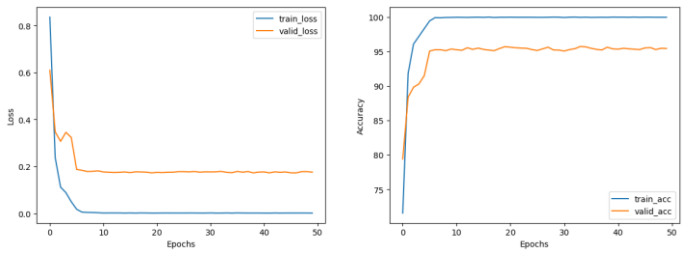
(a) (b)

Fig. 3. EfficientNet training performance: (a) Losses values per epoch (b) Average accuracy percentage values per epoch.



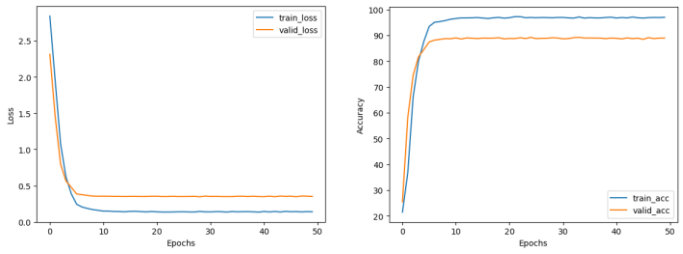
(a) (b)

Fig. 4. GoogLeNet training performance: (a) Losses values per epoch (b) Average accuracy percentage values per epoch.



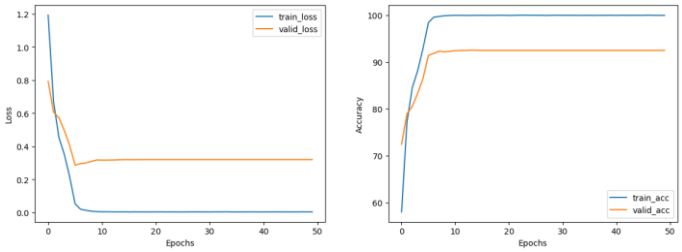
(a) (b)

Fig. 5. ResNet-152 training performance: (a) Losses values per epoch (b) Average accuracy percentage values per epoch.



(a) (b)

Fig. 6. ShuffleNet training performance: (a) Losses values per epoch (b) Average accuracy percentage values per epoch.



(a) (b)

Fig. 7. VGG-19 training performance: (a) Losses values per epoch (b) Average accuracy percentage values per epoch.

C. Models Testing Performance

Table V provides a comprehensive overview of the performance metrics including accuracy, precision, recall, and F1 score for different models. Among these models, EfficientNet stands out with the highest Average Testing Accuracy of 96.31%, highlighting its effectiveness in classification tasks. This exceptional performance can be attributed to Efficient Net's sophisticated architecture that incorporates compound scaling and efficient model scaling methods, allowing it to achieve superior accuracy.

TABLE V. HYPERPARAMETERS AND THEIR VALUES TUNING

#	Model	Average Testing Accuracy	Average Precision	Average Recall	Average F1 Score
1	EfficientNet	96.31%	0.9342	0.9631	0.9643
2	GoogLeNet	94.25%	0.8965	0.9425	0.9432
3	ResNet-152	95.49%	0.9183	0.9549	0.9555
4	ShuffleNet	89.11%	0.8113	0.8911	0.8924
5	VGG-19	92.91%	0.8727	0.9291	0.9296

ResNet-152 and GoogLeNet also demonstrate strong performance with accuracy rates of 95.49% and 94.25% respectively. ResNet-152, known for its deep architecture with residual connections, excels in capturing intricate features within the data, leading to high precision, recall, and F1 scores. On the other hand, Google Net's inception modules and efficient use of parameters contribute to its competitive performance across all metrics.

ShuffleNet and VGG-19, while slightly lower in accuracy compared to the top performers, still exhibit respectable results. Shuffle Net's emphasis on computational efficiency through channel shuffle operations enables it to achieve a balance between accuracy and resource utilization. VGG-19, with its deeper architecture comprising multiple convolutional layers, maintains a strong performance across precision, recall, and F1 score metrics.

D. Models Performance Analysis

To gain a deeper understanding of the models' classification performance, a detailed analysis was conducted using the AUC, as shown in Fig. 8.

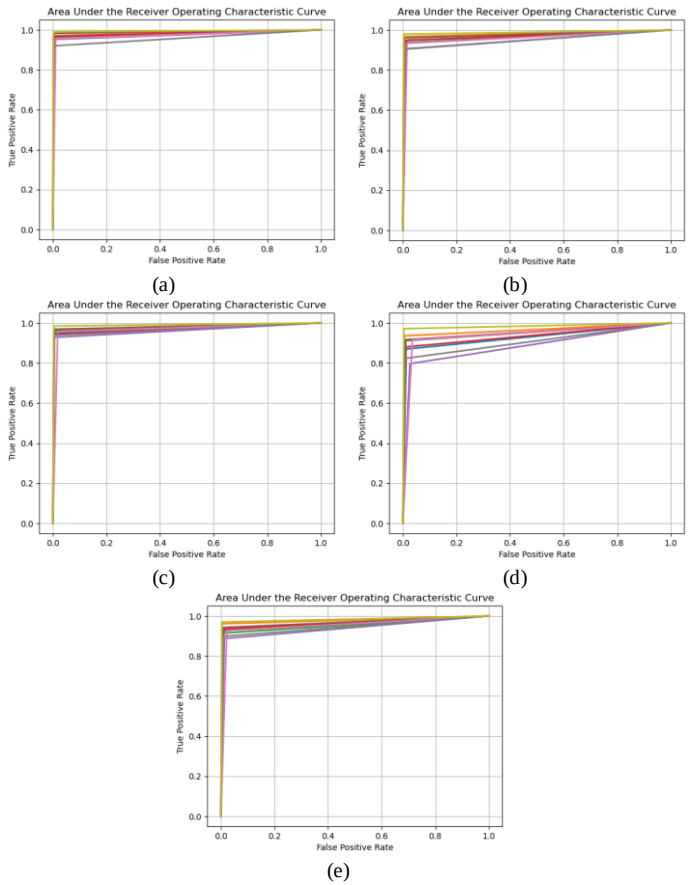


Fig. 8. AUC values for different Labels across various models including (a) EfficientNet (b) GoogLeNet (c) ResNet-152 (d) ShuffleNet and (e) VGG-19.

EfficientNet demonstrates strong performance across most classes with consistently high AUC values, particularly excelling in classes such as Food Organics and Vegetation where it achieved AUC scores of 0.99. This suggests that EfficientNet is effective in distinguishing these classes from others with high accuracy. GoogLeNet also performs well overall, with notable AUC scores for classes such as Glass and Vegetation. However, it shows slightly lower performance compared to EfficientNet in some classes like Metal and Miscellaneous Trash. ResNet-152 showcases consistent performance across various classes, with competitive AUC values for most categories. It performs particularly well in distinguishing classes like Cardboard and Paper. ShuffleNet exhibits varying performance across different classes, with lower AUC scores for categories such as Miscellaneous Trash and Textile Trash compared to other models. VGG-19, similar to GoogLeNet, demonstrates strong performance in classes like Glass and Vegetation but shows lower AUC values for categories like Miscellaneous Trash and Textile Trash.

In summary, EfficientNet stands out as a top performer in this analysis, followed closely by ResNet-152 and GoogLeNet. These models show effectiveness in classifying diverse classes accurately, with variations in performance observed across different models and classes.

Also, the confusion matrix was utilized to analyze the model's classification performance in correctly classifying different waste categories and reveal the presence of false negatives and false positives. Fig. 9 to Fig. 13 visualize the confusion matrix for the five models.

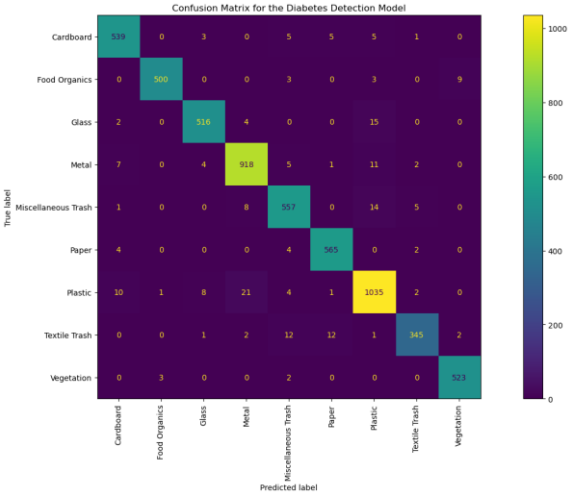


Fig. 9. Confusion Matrix for EfficientNet model in classifying landfill waste.

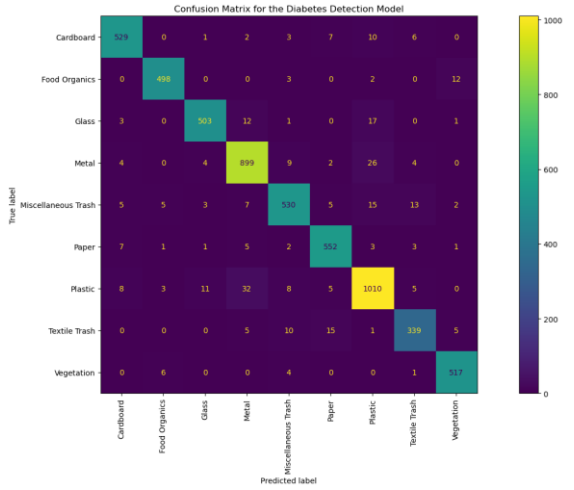


Fig. 10. Confusion Matrix for GoogLeNet model in classifying landfill waste.

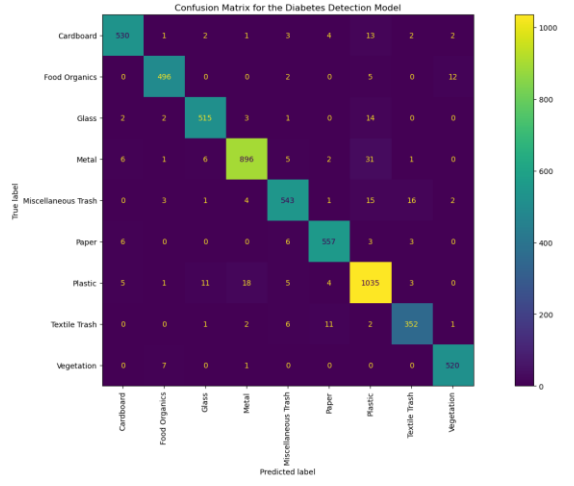


Fig. 11. Confusion Matrix for ResNet-152 model in classifying landfill waste.

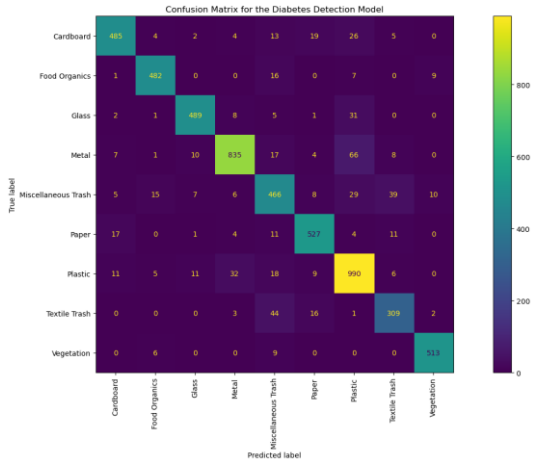


Fig. 12. Confusion Matrix for ShuffleNet model in classifying landfill waste.

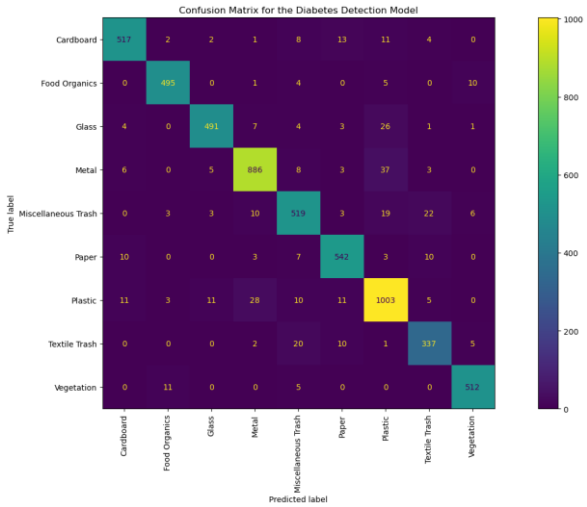


Fig. 13. Confusion Matrix for VGG-19 model in classifying landfill waste.

The confusion matrix for all models shows that the model's performance reveals notable confusion among various waste labels, particularly between metal and plastic categories. For EfficientNet, the model achieved a high accuracy rate of 92.41% in correctly identifying metal objects but misclassified four items as plastic. The accuracy of the plastic label was slightly lower at 84.78%, with six items mistakenly classified as metal and one item as cardboard. For GoogLeNet, the model's performance metrics show a similar trend with notable confusion between metal and plastic categories. Similarly, the ResNet-152 model exhibited challenges in distinguishing between metal and plastic categories, leading to misclassification. VGG-19 model's performance also indicated confusion between metal and plastic labels, impacting the accuracy of classification. In summary, all models struggled with distinguishing between metal and plastic waste categories, highlighting a common challenge across the different models in accurately classifying these materials. The difficulty in distinguishing between metal and plastic waste categories in the models could be attributed to several factors:

- Multi-Structured Shapes and Textures: Both metal and plastic items have varied shapes and textures, which further complicates the classification problem for the models.
- Data Variability: The reason why models fail to differentiate between waste materials made of metal and those that are made of plastic may partly be attributed to the lack of diversity in examples used during training concerning these two classes.

To address the challenges faced by models in accurately classifying metal and plastic waste, several strategies can be implemented:

- **Diverse Data Sources**: Where the current dataset is established, further research could explore the utilization of other sources of images taken in different surroundings and conditions of light. This would help create a more comprehensive dataset that captures a wider range of metal and plastic items.
- **Improved Image Augmentation**: While augmentation has been done, checking out advanced augmentation techniques, such as changes in brightness, contrast, and adding artificial noise, might yield a better generalization performance across different conditions.

E. Comparison with State-of-the-Art

To ensure an unbiased comparison, we have chosen to evaluate our work by benchmarking it against other studies that have utilized the same dataset. This approach allows for a fair assessment of the effectiveness and performance of our methodology within the context of the specific dataset, promoting a more accurate evaluation of our contributions in the field.

In study [9], they achieved an accuracy of 49.69% using DiversionNet and 89.19% using RealWaste. The accuracy of using RealWaste was notably higher compared to DiversionNet, indicating the effectiveness of RealWaste in the classification process. However, our work demonstrated a higher accuracy of 96.31% using the RealWaste dataset. It showed a significant improvement in accuracy compared to Work 1's results with RealWaste.

In summary, our proposed work exhibited superior performance in waste classification using the RealWaste dataset compared to study [9], showcasing advancements in accuracy and potentially innovative approaches in the classification process.

VI. Conclusion

Incorporating deep learning techniques, especially Convolutional Neural Networks (CNNs), into waste classification processes is crucial for enhancing automation, improving waste sorting accuracy, and striving towards a more sustainable and efficient waste management system amidst the escalating global waste production. The performance evaluation of five common CNN pre-trained models on the RealWaste dataset not only demonstrated advancements in accuracy but also highlighted potential innovative approaches in waste classification methodologies. This study contributes to the continuous enhancement of waste management strategies and the promotion of environmental sustainability through the

utilization of cutting-edge technologies like deep learning. Notably, EfficientNet emerged as the top performer with the highest Average Testing Accuracy of 96.31%, underscoring its effectiveness in classification tasks. Additionally, the performance of five well-known CNN pre-trained models was compared in this research using the RealWaste dataset as a test. The evaluation aimed to understand the impact of the dataset quality and the inclusion of more detailed waste classes, shedding light on the importance of data quality in achieving accurate waste classification outcomes. By addressing these aspects, the research contributes to advancing waste management practices and fostering environmental sustainability through advanced deep-learning methodologies. Looking ahead, future work will focus on expanding the dataset to include more diverse samples and exploring advanced data augmentation techniques to address class imbalances. These efforts aim to further enhance model robustness and improve waste classification systems, ultimately contributing to more effective waste management practices and fostering environmental sustainability.

REFERENCES

[1] A. Sevinç and F. Ozyurt, "Classification of recyclable waste using deep learning architectures," FIRAT UNIVERSITY JOURNAL OF EXPERIMENTAL AND COMPUTATIONAL ENGINEERING, vol. 1, no. 3, 2022, doi: 10.5505/fujece.2022.83997.

[2] A. U. Gondal et al., "Real time multipurpose smart waste classification model for efficient recycling in smart cities using multilayer convolutional neural network and perceptron," Sensors, vol. 21, no. 14, 2021, doi: 10.3390/s21144916.

[3] V. Gadre, S. Sashte, and A. Sarnaik, "WASTE CLASSIFICATION USING RESNET-152," INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, vol. 07, no. 01, 2023, doi: 10.55041/ijsrem17421.

[4] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," Commun ACM, vol. 60, no. 6, 2017, doi: 10.1145/3065386.

[5] D. O. Melinte, A. M. Travediu, and D. N. Dumitriu, "Deep convolutional neural networks object detector for real-time waste identification," Applied Sciences (Switzerland), vol. 10, no. 20, 2020, doi: 10.3390/app10207301.

[6] Q. Zhang et al., "Recyclable waste image recognition based on deep learning," Resources, Conservation and Recycling, vol. 171. 2021. doi: 10.1016/j.resconrec.2021.105636.

[7] Sivaranjani S, Priyanka Sherllyn S, Deepaharshini G R, and Eunice J, "Green Symphony: A Brief Review of Waste Segregation Techniques," International Research Journal on Advanced Engineering Hub (IRJAEH), vol. 2, no. 03, 2024, doi: 10.47392/irjaeh.2024.0056.

[8] K. O. Mohammed Aarif, C. Mohamed Yousuff, B. A. Mohammed Hashim, C. Mohamed Hashim, and P. Sivakumar, "Smart bin: Waste segregation system using deep learning-Internet of Things for sustainable smart cities," Concurr Comput, vol. 34, no. 28, 2022, doi: 10.1002/cpe.7378.

[9] S. Single, S. Iranmanesh, and R. Raad, "RealWaste: A Novel Real-Life Data Set for Landfill Waste Classification Using Deep Learning," Information (Switzerland), vol. 14, no. 12, 2023, doi: 10.3390/info14120633.

[10] A. Altikat, A. Gulbe, and S. Altikat, "Intelligent solid waste classification using deep convolutional neural networks," International Journal of Environmental Science and Technology, vol. 19, no. 3, 2022, doi: 10.1007/s13762-021-03179-4.

[11] A. Jahanbakhshi, M. Momeny, M. Mahmoudi, and P. Radeva, "Waste management using an automatic sorting system for carrot fruit based on image processing technique and improved deep neural networks," Energy Reports, vol. 7, 2021, doi: 10.1016/j.egyr.2021.08.028.

[12] R. Faria, F. Ahmed, A. Das, and A. Dey, "Classification of Organic and Solid Waste Using Deep Convolutional Neural Networks," in IEEE Region 10 Humanitarian Technology Conference, R10-HTC, 2021. doi: 10.1109/R10-HTC53172.2021.9641560.

[13] N. Nnamoko, J. Barrowclough, and J. Procter, "Solid Waste Image Classification Using Deep Convolutional Neural Network," Infrastructures (Basel), vol. 7, no. 4, 2022, doi: 10.3390/infrastructures7040047.

[14] P. Nowakowski and T. Pamuła, "Application of deep learning object classifier to improve e-waste collection planning," Waste Management, vol. 109, 2020, doi: 10.1016/j.wasman.2020.04.041.

[15] K. M. Kahloot and P. Ekler, "Algorithmic Splitting: A Method for Dataset Preparation," IEEE Access, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3110745.

[16] P. Probst, A. L. Boulesteix, and B. Bischl, "Tunability: Importance of hyperparameters of machine learning algorithms," Journal of Machine Learning Research, vol. 20, 2019.

[17] K. Wang, Y. Dou, T. Sun, P. Qiao, and D. Wen, "An automatic learning rate decay strategy for stochastic gradient descent optimization methods in neural networks," International Journal of Intelligent Systems, vol. 37, no. 10, 2022, doi: 10.1002/int.22883.

[18] A. Tharwat, "Classification assessment methods," Applied Computing and Informatics, vol. 17, no. 1, 2018, doi: 10.1016/j.aci.2018.08.003.

[19] P. Sengupta, A. Mehta, and P. S. Rana, "Enhancing Performance of Deep Learning Models with a Novel Data Augmentation Approach," in 2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023, 2023. doi: 10.1109/ICCCNT56998.2023.10308298.

[20] W. Liang, Y. Liang, and J. Jia, "MiAMix: Enhancing Image Classification through a Multi-Stage Augmented Mixed Sample Data Augmentation Method," Processes, vol. 11, no. 12, 2023, doi: 10.3390/pr11123284.

[21] M. H. Huynh, P. T. Pham-Hoai, A. K. Tran, and T. D. Nguyen, "Automated Waste Sorting Using Convolutional Neural Network," in Proceedings - 2020 7th NAFOSTED Conference on Information and Computer Science, NICS 2020, 2020. doi: 10.1109/NICS51282.2020.9335897.

[22] J. Bobulski and M. Kubanek, "Deep Learning for Plastic Waste Classification System," Applied Computational Intelligence and Soft Computing, vol. 2021, 2021, doi: 10.1155/2021/6626948.

[23] G. Lu, Y. Bin Wang, H. X. Xu, H. Y. Yang, and J. Zou, "Deep multimodal learning for municipal solid waste sorting," Sci China Technol Sci, vol. 65, no. 2, 2022, doi: 10.1007/s11431-021-1927-9.

[24] M. Tan and Q. V. Le, "EfficientNetV2: Smaller Models and Faster Training," in Proceedings of Machine Learning Research, 2021.

[25] P. Aswathy, Siddhartha, and D. Mishra, "Deep GoogLeNet Features for Visual Object Tracking," in 2018 13th International Conference on Industrial and Information Systems, ICIIS 2018 - Proceedings, 2018. doi: 10.1109/ICIINFS.2018.8721317.

[26] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2016. doi: 10.1109/CVPR.2016.90.

[27] R. Doss, J. Ramakrishnan, S. Kavitha, S. Ramkumar, G. Charlyn Pushpa Latha, and K. Ramaswamy, "Classification of Silicon (Si) Wafer Material Defects in Semiconductor Choosers using a Deep Learning ShuffleNet-v2-CNN Model," Advances in Materials Science and Engineering, vol. 2022, 2022, doi: 10.1155/2022/1829792.

[28] N. Ma, X. Zhang, H. T. Zheng, and J. Sun, "Shufflenet V2: Practical guidelines for efficient cnn architecture design," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018. doi: 10.1007/978-3-030-01264-9_8.

[29] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in 3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings, 2015.

[30] Y. Bengio, "Practical recommendations for gradient-based training of deep architectures," Lecture Notes in Computer Science (including

subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 7700 LECTURE NO, 2012, doi: 10.1007/978-3-642-35289-8_26.

[31] H. Zhang, K. Hao, L. Gao, B. Wei, and X. Tang, "Optimizing Deep Neural Networks Through Neuroevolution With Stochastic Gradient Descent," IEEE Trans Cogn Dev Syst, vol. 15, no. 1, 2023, doi: 10.1109/TCDS.2022.3146327.

[32] Q. Qian, R. Jin, J. Yi, L. Zhang, and S. Zhu, "Efficient distance metric learning by adaptive sampling and mini-batch stochastic gradient descent (SGD)," Mach Learn, vol. 99, no. 3, 2015, doi: 10.1007/s10994-014-5456-x.

[33] Y. Zhou, M. Zhang, J. Zhu, R. Zheng, and Q. Wu, "A Randomized Block-Coordinate Adam online learning optimization algorithm," Neural Comput Appl, vol. 32, no. 16, 2020, doi: 10.1007/s00521-020-04718-9.

[34] M. Soomro, M. A. Farooq, and R. H. Raza, "Performance evaluation of advanced deep learning architectures for offline handwritten character recognition," in Proceedings - 2017 International Conference on Frontiers of Information Technology, FIT 2017, 2017. doi: 10.1109/FIT.2017.00071.

[35] D. Silwal, "Confusion Matrix, Accuracy, Precision, Recall & F1 Score: Interpretation of Performance Measures," Linkedin.

[36] H. Palus and D. Bereska, "COLOUR REPRODUCTION ACCURACY OF VISION SYSTEMS," in Computer Vision and Graphics, 2006. doi: 10.1007/1-4020-4179-9_40.

[37] R. Joshi, "Accuracy, Precision, Recall & F1 Score: Interpretation of Performance Measures - Exsilio Blog," 2016.

[38] C. Marzban, "The ROC curve and the area under it as performance measures," Weather Forecast, vol. 19, no. 6, 2004, doi: 10.1175/825.1.

Yolov5-Based Attention Mechanism for Gesture Recognition in Complex Environment

Deepak Kumar Khare[1], Amit Bhagat[2], R. Vishnu Priya[3], Prashant Kumar Nag[4], Sunil Malviya[5]
Department of Mathematics, Bioinformatics and Computer Applications, Maulana Azad National Institute of Technology, Bhopal, Madhya Pradesh, India[1, 2, 4, 5]
Department of Computer Applications, National Institute of Technology, Tiruchirappalli, Tamil Nadu, India[3]

***Abstract*—Object detection is a fundamental task in gesture recognition, involving identifying and localising human hand or body gestures within images or videos amidst varying environmental conditions. To address the inadequate recognition rate of gesture detection algorithms in intricate surroundings caused by issues such as inconsistent illumination, background colors resembling skin tones, and diminutive gesture scales, a gesture recognition approach termed HD-YOLOv5s is presented. An adaptive Gamma image enhancement preprocessing technique grounded in Retinex theory is employed to mitigate the effects of lighting variations on gesture recognition efficacy. A feature extraction network incorporating an adaptive convolutional attention mechanism (SKNet) is developed to augment the network's feature extraction efficacy and mitigate background interference in intricate situations. A novel bidirectional feature pyramid architecture is implemented in the feature fusion network to fully leverage low-level features, thereby minimizing the loss of shallow semantic information and enhancing the detection accuracy of small-scale gestures. A cross-level connection strategy is employed to enhance the model's detection efficiency. To assess the efficacy of the suggested technique, experiments were performed on a custom dataset featuring diverse lighting intensity fluctuations and the publicly available NUS-II dataset with intricate backdrops. The recognition rates attained were 99.5% and 98.9%, respectively, with a detection time per frame of about 0.01 to 0.02 seconds.**

Keywords*—Gesture recognition; Yolov5; object detection; attention mechanism; bidirectional feature pyramid

I. INTRODUCTION

With the continuous development of human-computer interaction (HCI) technology, people's lives are becoming increasingly intelligent [1-2]. Traditional HCI methods rely on contact-based devices such as a mouse, keyboard, and joystick. However, with the advancement of technologies like voice recognition and gesture recognition, contactless interaction has become one of the main research directions. Gesture recognition, as a form of body language, is simple, direct, and convenient. It enables HCI in various fields such as in-vehicle cabin control, aerospace, smart homes, and intelligent education, making it a research hotspot in HCI technology. For example, using gesture recognition in smart homes allows for remote control with simple gestures, greatly enhancing convenience in people's lives. However, in practical applications, gesture recognition algorithms still face many challenges in complex environments due to factors like lighting, background, distance, and skin tone. Gestures can be categorized as either static or dynamic, where dynamic gestures can be viewed as a sequence of interrelated static gestures. Therefore, static gesture recognition serves as a fundamental basis for studying dynamic gestures and their applications. This paper focuses on static gesture recognition. Gesture recognition [3] technology has undergone multiple phases of development to date. Conventional gesture recognition is often investigated via sensor-based techniques or computer vision methodologies. Gesture recognition reliant on sensors generally necessitates hardware devices to gather and interpret gesture data, like wearable data gloves, Leap Motion, and Kinect. While these approaches are rapid and precise and exhibit less sensitivity to fluctuations in intricate external surroundings, they depend on hardware devices, which may be cumbersome and costly to utilize. Gesture identification based on computer vision predominantly uses depth cameras, color spaces (RGB [4], HSV [5], YCbCr [6]), or skin color detection to delineate the gesture area. Following segmentation, recognition approaches such as template matching [7] and support vector machines (SVM) [8-9] are employed. These approaches depend on manually crafted feature extraction, rendering them vulnerable to external influences and leading to diminished robustness and suboptimal identification rates.

In recent years, the advent of deep learning has prompted numerous academics to implement deep learning techniques for gesture detection in intricate contexts, with the objective of enhancing recognition accuracy. For instance, the Yu et al. [10] utilized a skin color model to identify gesture regions and applied convolutional neural networks (CNN) for feature extraction and detection. This approach is susceptible to fluctuations in lighting and skin color in complicated situations, diminishing its generalizability and robustness. The Diba et al. [11] directly utilized CNN to identify motions from raw photos; however, when the image features analogous skin and background hues, the CNN is unable to extract pertinent information, resulting in elevated false detection rates. The swift advancement of deep learning-based object detection algorithms has led many academics to recognize that utilizing these techniques for gesture recognition in intricate contexts can enhance performance. For example, the Gao et al. [12] employed the Faster R-CNN algorithm for gesture identification, utilizing Gaussian filters for image pre-processing. The Fan et al. [13] used neural networks with the SSD (single shot multibox detector) to extract essential points in motions. Despite enhancements in gesture recognition [14] in tough conditions such lighting and skin tone fluctuations, the substantial model sizes and prolonged detection times hinder real-time identification in intricate environments. To tackle this

issue, Huang et al. [3] enhanced the YOLO (You Only Look Once) algorithm and introduced the DSN algorithm for gesture detection, employing CNN for recognition. This system improved recognition rates under uneven lighting and skin-tone background interference while enhancing detection speed, attaining real-time target detection. Nonetheless, it exhibited subpar performance in identifying little actions inside intricate settings.

In terms of recognition accuracy, speed, and real-time performance, the YOLOv5 algorithm, which was recently introduced, surpasses other algorithms in the YOLO series. Although the YOLOv5 model has demonstrated satisfactory performance on extensive public datasets, it is still necessary to make specific enhancements in order to optimize the model's performance for specific target objects based on the characteristics of the selected datasets. For instance, the detection capability of small objects such as traffic lights was enhanced by Premaratne et al. [15] and colleagues through the modification of the backbone convolution network and the construction of a feature fusion network. The following challenges are presented when the YOLOv5 model is explicitly applied to gesture recognition in complex environments, despite the significance of high gesture recognition rates:

- The algorithm's generalization and robustness are subpar when recognizing gestures in uneven lighting.
- When skin tones blend with background colors, high false detection rates occur.
- The algorithm experiences high miss rates and low recognition accuracy when recognizing gestures at a distance or on a small scale.

To address the current challenges in gesture recognition, such as missed detection, false detection, and low recognition rates caused by uneven lighting, skin-tone backgrounds, small-scale gestures, and complex environments, this paper proposes an improved YOLOv5-based gesture recognition method, HD-YOLOv5s. The main contribution of this paper is as follows:

- First, an adaptive Gamma image enhancement method is used to pre-process the dataset, mitigating the effects of lighting variations in complex environments on gesture recognition.
- To tackle background interference in complex environments, the attention mechanism module SK from the dynamic selection network is incorporated into the final feature extraction layer of the feature extraction network.
- This allows for adaptive adjustment of the convolution kernel size for different scales of images, which helps in extracting effective features and improving feature extraction capabilities.
- Finally, the PANet structure in the feature fusion network is replaced with an adjusted bidirectional feature pyramid structure (BiFPN), which improves the recognition rate of small-scale gestures in complex environments.

II. YOLOv5s Network Structure

YOLOv5 is a neural network architecture employed for object detection. As network depth and weights increase, YOLOv5 is categorized into four variants: YOLOv5s, YOLOv5m, YOLOv5l, and YOLOv5x. The YOLOv5s model is the smallest and exhibits the highest inference speed among these options. The YOLOv5 architecture comprises three components: the feature extraction network (Backbone), the feature fusion network (Neck), and the detection network (Prediction).

A. Feature Extraction Network (Backbone)

The Backbone comprises the CSPDarknet, Focus, and SPP (Spatial Pyramid Pooling) modules, which primarily operate to extract high (deep), intermediate, and low (shallow) level features from images. The backbone network of YOLOv5 is CSPDarknet53. In contrast to the Darknet53 network, the $C3_X$ module partitions the feature mappings of the base layer into two segments and subsequently integrates them via partial local cross-layer fusion. This not only mitigates the problem of excessive computation due to duplicated gradient information during network optimization, but also guarantees precision while diminishing computational burden. The Focus module enhances feature extraction efficiency by segmenting and recombining input feature maps within the backbone network, hence reducing the number of network layers. This significantly decreases computational burden and enhances detection velocity while preserving precision. The SPP module is incorporated following the CSPDarknet53 architecture to extract prominent characteristics from photos. The SPP architecture enhances the receptive field of the prediction box, addresses the alignment discrepancy between the target box and the feature map, and guarantees both effective feature extraction and the operational speed of the network.

B. Feature Fusion Network (Neck)

The fundamental components of the Neck are feature pyramid networks (FPN) [16] and path aggregation networks (PAN) [17], which primarily enhance the model's capacity to recognize objects across various scales. Deep feature maps possess enhanced semantic features but diminished localization information, whereas shallow feature maps have superior localization information but reduced semantic features. FPN segments the feature maps into various scales and integrates them. It transmits profound semantic information to the superficial layers, augmenting semantic representation across various scales.

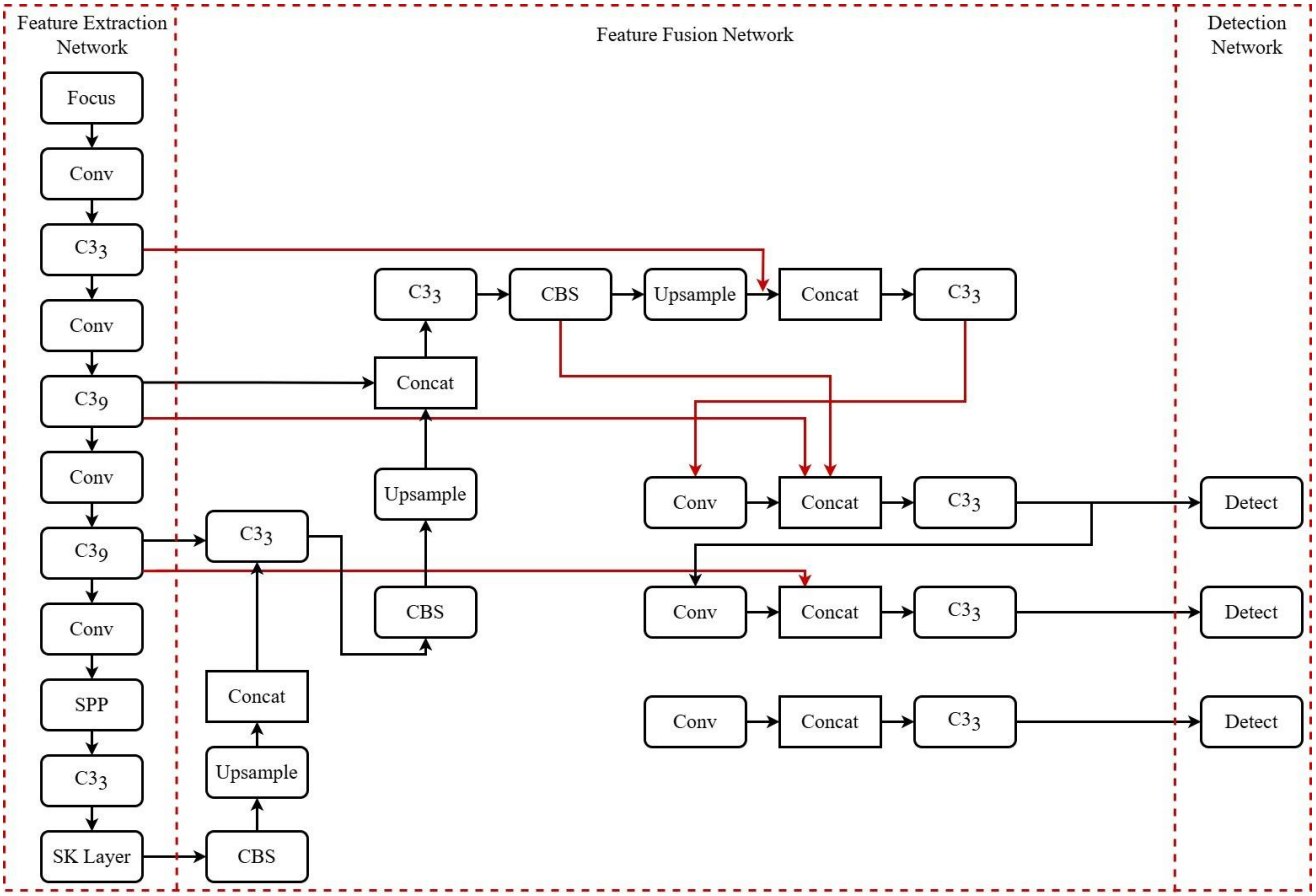


Fig. 1. HD-YOLOv5s network structure.

Conversely, PAN conveys superficial localization data to the deeper layers, enhancing localization proficiency across various scales. The PANet feature pyramid architecture incorporates a bottom-up pathway structure in addition to the Feature Pyramid Network (FPN) [18-19]. FPN improves object detection by integrating characteristics from both deep and shallow layers, particularly enhancing the identification of small objects. Object identification involves pixel-level categorization, and shallow features, which often capture edges and forms, are essential for this process. The bottom-up path architecture effectively employs shallow layer characteristics for segmentation. Incorporating this upgrade into FPN, PANet enables deep feature maps to leverage the extensive localization information from shallow layers, hence enhancing the detection of huge objects.

C. Detection Network (Prediction)

Traditional neural networks only input the deepest layer of network features into the detection layer, leading to the loss of small object features as they are passed from lower layers to higher layers. This results in difficulty in recognizing small objects and a low detection rate. YOLOv5 adopts a multi-scale detection method, dividing the feature maps into three scales through 32x, 16x, and 8x down sampling. By utilizing different receptive fields, larger feature maps detect small objects and smaller feature maps detect large objects, overcoming the limitations of top-layer features.

III. HD-YOLOv5 Network Structure

The gesture recognition technique introduced in this research, HD-YOLOv5s, represents an enhancement of the YOLOv5s model. Fig. 1 illustrates the architecture of the HD-YOLOv5s model, whereas Fig. 2 depicts the configuration of each module within the HD-YOLOv5s model. In Fig. 1, the newly incorporated features relative to the original YOLOv5s model are distinguished by various colors.

A. Feature Extraction Network with SKNet

In complex background environments, gesture targets may be small in size or have backgrounds similar in color to skin, which makes it challenging to recognize targets of varying scales. This requires higher feature extraction capabilities from the network model. Attention mechanisms can enhance the network's ability to express model features by strengthening important features and weakening general features. Therefore, this paper adopts an attention mechanism to enhance the network's feature extraction capability.

The selective kernel neural network (SKNet) employs an adaptive selection method.

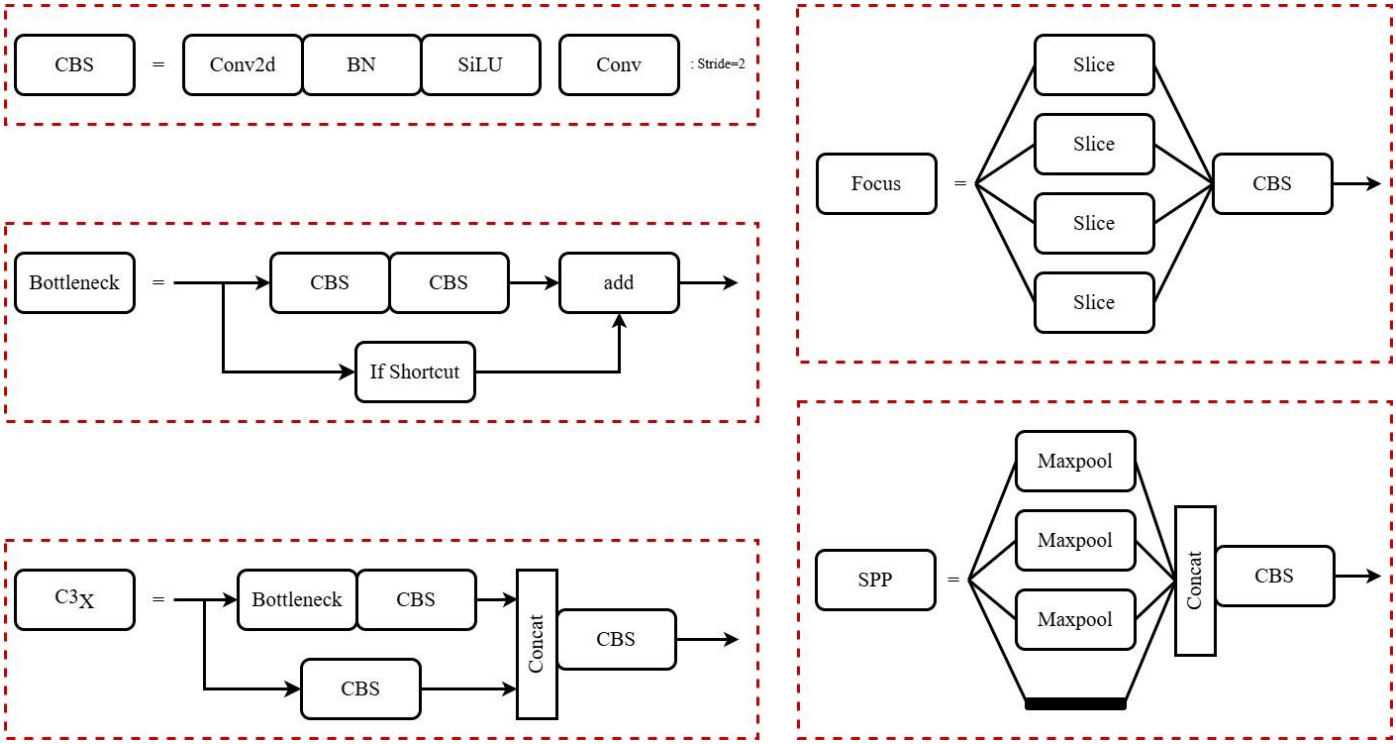


Fig. 2. HD-YOLOv5 module structure.

The advantage resides in its consideration of several convolutional kernels, enabling neurons to select the suitable kernel size according to input information of varying scales, so efficiently modifying the receptive field size. This allows the network to concentrate on significant features. Conversely, conventional convolutional networks often employ a singular convolutional kernel per layer, and throughout feature extraction, the kernel size remains constant at each layer, resulting in a static receptive field. The dimensions of the receptive field directly affect the scale of the features, and the features derived from conventional convolutional networks are generally more homogeneous, which imposes specific constraints. Structures such as Inception incorporate numerous convolutional kernels to accommodate multi-scale pictures; however, the weights of these kernels remain constant, and post-training, the parameters are immutable. This leads to the indiscriminate utilization of all multi-scale information. Undoubtedly, employing a dynamic selection method such as SKNet offers greater advantages.

SKNet, an enhancement of the SENet network, incorporates multi-branch convolutional networks, dilated convolutions, and group convolutions. It examines the interactions among channels while also addressing the function of convolutional kernels. SKNet enables the network to prioritize channels beneficial for recognition during feature extraction and autonomously identifies the ideal convolutional operator, hence enhancing recognition performance. SKNet operates through three phases: splitting, fusing, and selecting, as illustrated in Fig. 3.

The specific steps are as follows:

1) Split: Given an input feature $X \in R^{G\times Z\times C}$, two convolution operations are performed with convolutional kernels of sizes 3×3 and 5×5, resulting in two outputs: $\tilde{F}: X \to \tilde{V} \in R^{G\times Z\times C}$ and $\hat{F}: X \to \hat{V} \in R^{G\times Z\times C}$. To further improve efficiency, dilated convolution with a dilation rate of 2 is used in place of the 5×5 convolution.

2) Fuse: To adaptively adjust the receptive field size, the two branch results are first fused by element-wise summation, expressed as follows:

$$V = \tilde{V} + \hat{V} \tag{1}$$

Secondly, use the global pooling operation on the integrated information to obtain the global information, as shown in the following formula:

$$T_c = F_{\mathrm{hQ}}(V_c) = \frac{1}{G\times Z}\sum_{i=1}^{G}\sum_{j=1}^{Z} V_c(i,j) \tag{2}$$

In the formula, F_{hQ} represents the global average pooling operation function, T_c represents the output of the c channel, and $V_c(i,j)$ represents the coordinates of the c channel. G Is the height of the feature map, and Z is the width of the feature map, where i and j are the coordinate values for the height and width of the feature map, respectively.

Finally, $T_c$is reduced in dimension by the fully connected layer to obtain U, as follows:

$$U = F_{\mathrm{fc}}(T) = \delta\big(\beta(Z_T)\big) \tag{3}$$

$$d = \max\left(\frac{c}{r}, L\right) \tag{4}$$

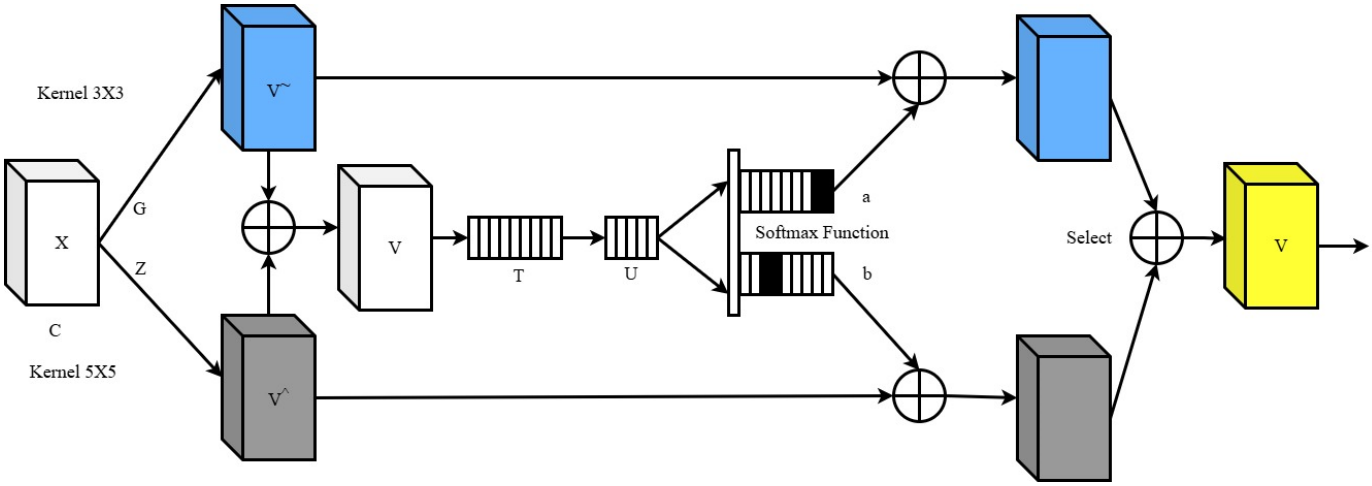


Fig. 3. SKNet network structure.

In the equation, F_{fc} denotes the fully connected operation function, δ signifies the non-linear activation function, β represents the batch normalization (BN) layer, and d indicates the fully connected layer regulated by the reduction ratio. L represents the minimum value of d, where $Z \in \mathrm{R}^{d\times c}$, $U \in \mathrm{R}^{d\times 1}$.

3) Selection: First, the channel attention is generated, and then adaptive selection of information at different scales is made, as expressed below:

$$\begin{cases} a_c = \frac{e^{A_c U}}{e_c A_c + e^{B_c U}} \\ b_c = \frac{e_c U}{e_\varepsilon U} + e^{B_c U} \end{cases} \quad (5)$$

In the formula, $A, B \in \mathrm{R}^{c\times d}, a_c, b_c$ represent the attention vectors corresponding to $\tilde{V}$ and $\hat{V}$ respectively, where A_c represents the c row and a_c represents the c element of a.

Finally, the features output by the two branches are weighted and fused to obtain V_c, as follows:

$$W_c = a_c \tilde{V}_c + b_c \hat{V}_c; a_c + b_c = 1 \quad (6)$$

In, $W = [W_1, W_2, \cdots, W_c], W_c \in \mathrm{R}^{G\times Z}$.

SKNet is a lightweight embedded module composed of multiple SK (Selective Kernel) convolutional units. In this paper, the SK convolution layer is added to the C3 module at the end of the HD-YOLOv5s backbone network, enabling the network to focus more on extracting effective features. The process is as follows: the initial feature map size is set to 640×640×3, and the channel scaling factor is set to 0.5. After one Focus operation and four CBS operations, the output feature map size of the final C3 module is 20×20×512, which is used as the input for the SK module.

First, the feature map is passed through two convolution kernels, 3×3 and 5×5, using grouped convolution, outputting two feature maps of different scales, each with 512 channels, denoted as $\tilde{V}$ and $\hat{V}$. Then, the results of the two branches are added element-wise. After global average pooling, the output is a 1×1×512 feature map. Next, after two fully connected layers for dimensionality reduction and expansion, a feature map of size 1×1×d is obtained. This is then dynamically and adaptively adjusted using the softmax activation function, automatically selecting the optimal convolution operators a and b, which control the receptive field feature maps of the two branches. Finally, the two branches are weighted and fused as $W = \tilde{V} \times a + \hat{V} \times b = 20 \times 20 \times 512$ to produce the output of this network layer, allowing the network to focus more on the gesture information that is useful for recognition.

Abhishesh Pal et al. [20] and Prabu Selvam et al. [21] was integrated SKNet into YOLOv3 and SSD networks, enhancing the feature extraction capability and improving the mean average precision (mAP) of the networks to varying degrees. Therefore, SKNet is added to the HD-YOLOv5s algorithm proposed in this paper to improve the network's detection performance.

B. Feature Fusion Network

This work focuses on hand gesture recognition, encompassing small and varied-sized objects. The YOLOv5s network model employs the PANet (Path Aggregation Network) architecture to tackle the challenge of multi-scale input. Nonetheless, because to the disparate resolutions of the gesture region features, PANet frequently amalgamates features indiscriminately while integrating various input features. This may nevertheless result in false positives and overlooked detections, particularly with little objects. This research proposes utilizing a modified weighted bidirectional feature pyramid network (BiFPN) to supplant PANet for feature fusion, hence augmenting the model's detection efficiency and expanding the network's capability to identify hand gesture targets across varying scales.

The Google Brain team introduced BiFPN in the EfficientDet object detection algorithm [22], characterized by efficient bidirectional cross-scale connections and weighted feature fusion. The BiFPN feature fusion technique assigns weights to features derived from the bidirectional feature pyramid and aggregates them pixel-wise, while the original YOLOv5s algorithm concatenates features along the channel dimension. This study integrates the bidirectional feature pyramid network (BiFPN) into the feature fusion network of the YOLOv5s model, employing channel-wise concatenation for

feature fusion and implementing cross-level cascade to augment the network's feature fusion efficacy. Fig. 4 illustrates the feature fusion network of the original YOLOv5s method. In the diagram, $Ci(i = 2 \sim 5)$represents the multi-scale features extracted by the feedforward network. F represents the $C3_3$ operator, Qi represents the output features, where 2× refers to two-fold up sampling achieved via bilinear interpolation, and 0.5× refers to down sampling. The features of different scales $\{C2, C3, C4, C5\}$, extracted by the backbone network, are input into the feature fusion network. With the original image resolution set to 640×640, after bidirectional cross-scale connections and weighted feature fusion, three different scale features $\{Q3, Q4, Q5\}$ are obtained as the detection layers of YOLOv5s, with resolutions of $20 \times 20, 40 \times 40, 80 \times 80$, respectively.

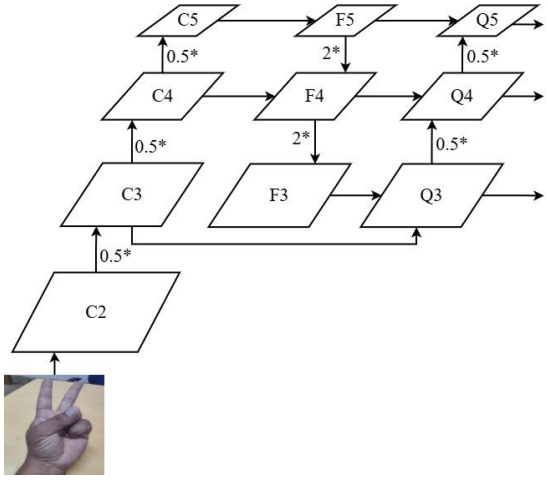


Fig. 4. Feature fusion network of the original YOLOv5s algorithm.

The specific improvements are as follows:

- **To enhance the accuracy of small object detection**, this paper proposes a feature fusion method that fully utilizes low-level features. It makes full use of the Q2 feature by incorporating high-resolution Q2 information into the feature fusion process. By establishing a connection between the small object detection feature Q3 and the previous level feature C2, it alleviates the loss of the F3 feature caused indirectly by network down sampling, thus further improving the network's supervision ability over small objects.
- **To improve the model's efficiency**, while performing bidirectional feature fusion from top to bottom and bottom to top, a cross-scale lateral connection is added between the input and output nodes at the same scale. This cross-level connection allows surface-level details, edge information, and contour information to be integrated into the deeper layers of the network, enabling precise edge regression of the target without increasing computational costs. This reduces the feature loss caused by having too many layers. The improved feature fusion network structure is shown in Fig. 5.

In Fig. 5, the dashed lines represent cross-level connections. Cross-level connections refer to adding a skip connection between the input and output nodes at the same scale. Since they are at the same level, this allows for more feature fusion without significantly increasing computational cost. As shown in Fig. 5, to reduce computation and shorten inference time, cross-level weighted fusion was not applied to the low-level Q2 feature. Instead, cross-level weighted fusion was used only when obtaining the Q3 and Q4 features for final detection. The low-level Q2 feature was fully utilized by introducing high-resolution feature information into the feature fusion process, improving the model's performance in small object detection and enhancing the backbone network's learning ability for target detection across different scale gesture regions.

The weighted feature fusion uses a fast normalization fusion formula, as shown in Eq. (7). The normalization process is achieved by dividing each weight by the sum of all weights, with the normalized weights constrained between [0, 1], which improves GPU processing speed and reduces additional time costs.

$$O = \sum_i \frac{z_i}{\varepsilon + \sum_j z_j} \cdot I_i \quad (7)$$

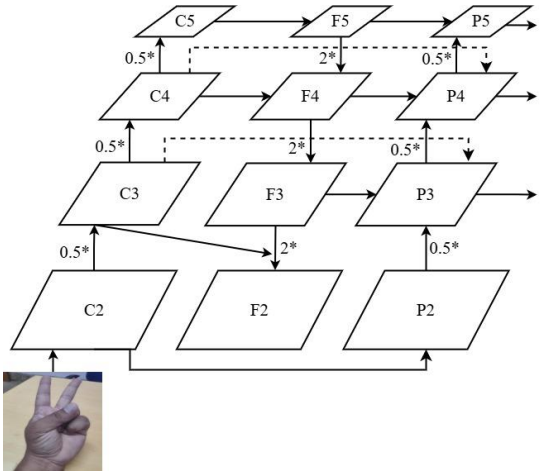


Fig. 5. Improved feature fusion network.

C. Image Enhancement Preprocessing

During the collection of gesture datasets, issues such as uneven lighting or background colors similar to skin tones often occur. These issues can degrade image quality, affecting the model's ability to recognize gestures and leading to missed or incorrect detections. To address these problems, this paper introduces an adaptive contrast adjustment image enhancement method based on the original network, specifically an adaptive Gamma enhancement algorithm improved from the Retinex (Retina and Cortex) theory [22-23]. This algorithm is effective in addressing uneven lighting, providing better contrast, naturalness, and efficiency. Common image enhancement algorithms, such as histogram equalization and Retinex, tend to cause over-enhancement, color distortion, and halo effects during the enhancement process [24].

The Retinex-based adaptive Gamma enhancement algorithm adapts to the brightness level of different regions of an image, reducing the brightness in overexposed areas and increasing it in underexposed areas. This helps minimize over-enhancement issues during image processing, resulting in better contrast. Moreover, this algorithm retains more detailed

information after adaptive correction, reducing color distortion and halo effects. Additionally, when processing images with uneven lighting, the algorithm can adjust the Gamma parameter adaptively based on the distribution characteristics of the lighting component, saving the time required for manually setting the Gamma value. The main steps of this image enhancement algorithm are as follows:

- Use the Retinex theory to separate the brightness component and reflection component of the image.

$$R^c(x,y) = \frac{I^u(x,y)}{L(x,y)}, c \in \{r,h,b\} \quad (8)$$

where, $R^c(x,y)$ represents the separated reflection component, $I^u(x,y)$ represents the brightness of each RGB channel, and $L(x,y)$represents the brightness component of the image.

- Apply the adaptive Gamma correction algorithm to the brightness component.

$$L_{\text{en}}(x,y) = L(x,y)^{\gamma(x,y)} \quad (9)$$

$$\gamma(l) = 1 - \sum_{v=0}^{l} \frac{Q_\omega(v)}{T_q} \quad (10)$$

$$T_q = \sum_{i=0}^{l} Q_\omega(l) \quad (11)$$

where, $L_{\text{en}}(x,y)$ is the corrected brightness component, $\gamma(x,y)$is the coefficient matrix, $\sum_{v=0}^{L} Q_\omega(v)$is the cumulative distribution function of the brightness component, and $Q_\omega(l)$ is the distribution function of the brightness values.

$$Q_\omega(l) = \frac{Q(l) - q_{\min}}{p_{\max} - q_{\min}} \quad (12)$$

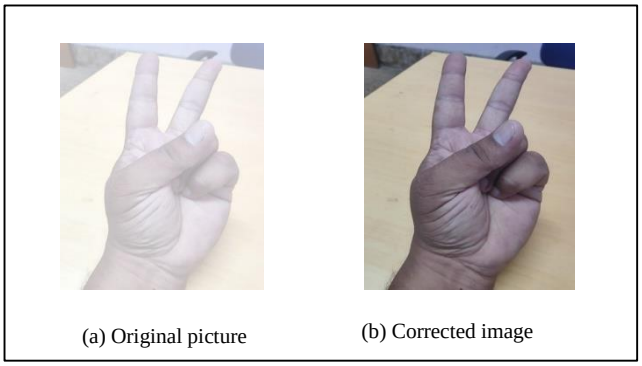
$$Q(l) = \frac{n_l}{n_q} \quad (13)$$

where, $Q(l)$ is the probability density function of the brightness component, n_l represents the number of pixels with a corresponding brightness, and n_q represents the total number of pixels in the brightness component.

- By merging $L_{\text{en}}(x,y)$ and $R^c(x,y)$the final enhanced image $I^c_{\text{en}}(x,y)$ is obtained, restoring the original image's color and details.

$$I^c_{\text{en}}(x,y) = R^c(x,y) \cdot L_{\text{en}}(x,y), c \in \{r,\text{h},b\} \quad (14)$$

The experimental comparison of the corrected images is shown in Fig. 6.



(a) Original picture (b) Corrected image

Fig. 6. Comparison of images before and after Gamma correction

Experimental results show that correcting images with uneven lighting not only significantly improves the clarity of the pre-processed images but also increases the diversity of lighting conditions in the dataset. By performing lighting enhancement pre-processing on the dataset, the quality of gesture images is improved, which in turn increases the accuracy and recall rate of gesture recognition. The flowchart of the HD-YOLOv5s gesture recognition method with the added image enhancement algorithm is shown in Fig. 7.

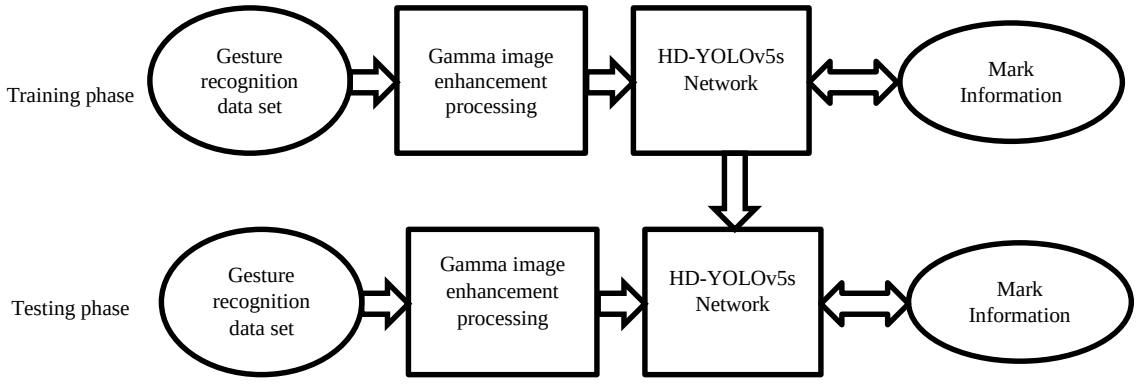


Fig. 7. Flowchart of the HD-YOLOv5s gesture recognition method.

IV. Experimental Detail and Results Analysis

A. Gesture Dataset Preparation

This paper uses the NUS-II dataset [25], which contains 2,750 samples divided into 10 categories. The dataset was collected from 40 participants of different hand shapes and ethnicities in various complex indoor and outdoor environments. The gesture images in this dataset vary in size, dimension, and skin tone, with complex backgrounds, meeting the research criteria of this paper. Some examples from the dataset are shown in Fig. 8.

Fig. 8. NUS-II dataset examples.

A custom gesture dataset was collected using an infrared camera, capturing the gestures of five participants under different lighting conditions and at various distances. Each participant performed seven different gestures, including numerical gestures 0-5 and the "OK" gesture. To augment the dataset, data augmentation techniques such as flipping, scaling, and shifting were applied to the images. The expanded dataset contains 300 samples per class, resulting in a total of 2,100 images.

Fig. 9. Custom dataset examples.

The gesture datasets used in this paper are formatted according to the VOC dataset format. For the custom dataset, images in JPEG format were manually annotated using the label image tool. The 2,100 samples were then split into a training set and a test set at a 9:1 ratio. Some examples from the custom dataset are shown in Fig. 9.

B. Evaluation Metrics

To better assess the model's detection performance before and after the comparative experiments, the evaluation metrics commonly used in mainstream object detection algorithms were adopted. The specific detection metrics used in this paper are as follows:

1) Precision (P): The proportion of correctly predicted targets out of all predicted targets.

$$\text{Precision} = \frac{TP}{TP+FP} \tag{15}$$

Recall (R): The proportion of targets predicted correctly by the model among all true targets.

$$\text{Recall} = \frac{TP}{TP+FN} \tag{16}$$

In the formula:

- TP (True Positives) refers to the number of correctly recognized gesture images.
- FP (False Positives) refers to the number of incorrectly identified gesture images.
- FN (False Negatives) refers to the number of missed gesture images.

2) Average Precision (AP): The precision value for a single category in the dataset, with a range from 0 to 1. Since using the 11-point interpolation sampling method can lead to a loss of precision, this paper adopts the AP calculation method introduced after VOC 2010, defined as follows:

$$AP = \int_0^1 P_{\text{smooth}}(r)\mathrm{d}r \tag{17}$$

$$P_{\text{smooth}}(r) = \max_{r'r' \geqslant r} P(r') \tag{18}$$

In the equation, average precision (AP) is the mean of the precision values over the Precision-Recall (P-R) curve. The P-R curve is a graphical representation of recall values on the horizontal axis and precision values on the vertical axis, creating a curve on the coordinate plane. The P-R curve is initially smoothed by utilizing all real recall values as thresholds. For each threshold when the recall r′ surpasses a specified value, the maximum accuracy value is designated as $P_{\text{smooth}}(r)$. The ultimate AP value is determined by integrating the area beneath the smoothed curve.

3) Mean Average Precision (mAP): The mean of the Average Precision (AP) values over all categories in the dataset, sometimes referred to as the recognition rate. The formula for computation is presented in Eq. (19), where k represents the total number of target categories detected.

$$mAP = \frac{1}{k}\sum_{i=1}^{k} AP_i \tag{19}$$

C. Experimental Setup

All comparative experiments in this study were performed on a Windows 10 operating system with an NVIDIA GTX970 GPU. The experimental setup comprised the deep learning framework PyTorch 1.10.0, CUDA version 10.2, and cuDNN version 8.2.4. The learning rate was established at 0.01 to facilitate rapid convergence in localized areas, while the batch size was determined to be 16 to enhance training efficiency.

D. Result Analysis

1) Comparative experiments: To address the low recognition rate of small-scale gestures in complex environments, this paper improved the feature fusion network of the YOLOv5s model. The accuracy and parameter counts of mainstream feature fusion networks, including FPN, PANet,

and BiFPN, were compared to select the best-performing multi-scale fusion network.

As shown in Table I, FPN only performs unidirectional feature fusion from top to bottom, resulting in low detection accuracy. PANet, which adds a bottom-up path to FPN, integrates strong localization information from lower-level features and shows significant improvement in detection accuracy. BiFPN further enhances PANet by adding bidirectional cross-scale connections. Although the parameter count of BiFPN increases by 13.2% compared to PANet, the computational cost (FLOPs) remains nearly unchanged, and the mAP value increases by 1.4 percentage points. Therefore, adding cross-scale connections enables the network to fuse more features without significantly increasing computational costs, making its detection accuracy superior to other networks.

TABLE I. COMPARISON OF FEATURE FUSION NETWORK PERFORMANCE

Feature Fusion Network	mAP/%	M/106	FLOPs/10^9
FPN	94.5	6.52	15.2
PANet	95.9	7.03	15.9
BiFPN	97.3	8.1	16.3

To better demonstrate the advantages of the improved model in this paper, a comparison was made with several classic object detection algorithms, including the two-stage model Faster R-CNN, and the one-stage models SSD, YOLOv3, and YOLOv5s. All models were trained and validated using the NUS-II dataset, as shown in Table II**.**

TABLE II. COMPARISON BETWEEN MAINSTREAM TARGET DETECTION ALGORITHMS AND THE PROPOSED METHOD

Model	mAP/ %	M/10 6	Model size/106	Inference time/ms
Faster R-CNN	94.5	60.1	159	44
SSD	92.3	24.2	92.1	20.73
YOLOv3	93.9	61.9	235	16.06
YOLOv5s	95.9	7.03	15.9	9.07
HD-YOLOv5s	99.5	13.6	17.8	10.51

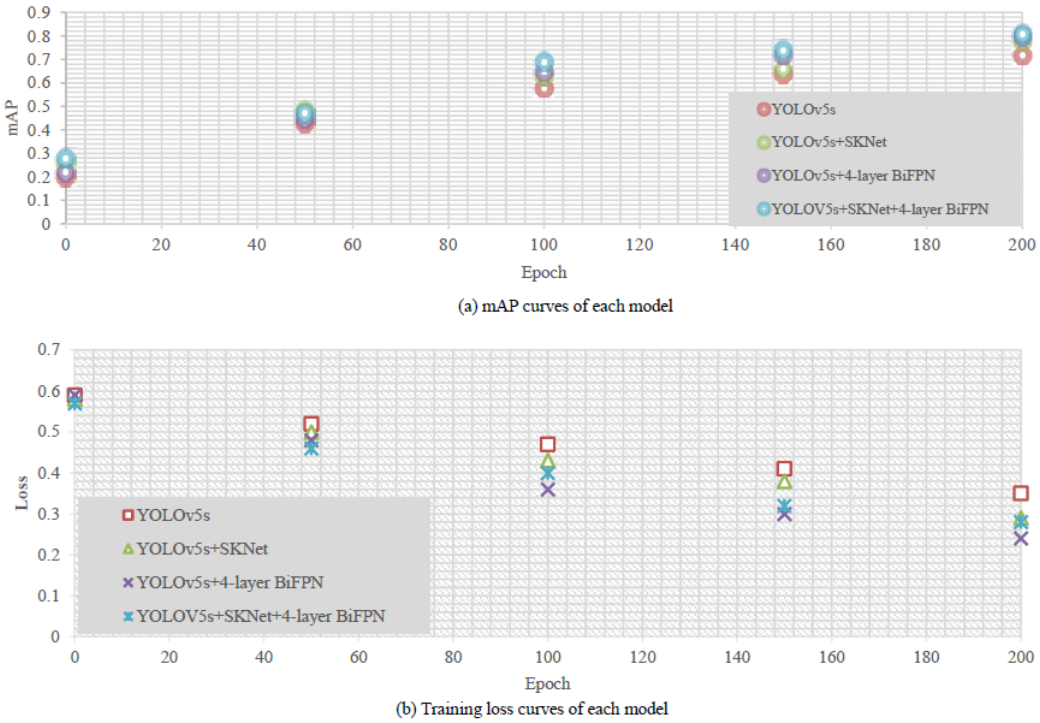
From Table II, it can be seen that the sizes of the Faster R-CNN, SSD, and YOLOv3 models are 6 to 10 times larger than that of the HD-YOLOv5s model, and the number of parameters is 3 to 10 times that of HD-YOLOv5s. Therefore, HD-YOLOv5s can be considered a lightweight network compared to these models. The size of the HD-YOLOv5s model is not significantly different from that of YOLOv5s, although HD-YOLOv5s adds a feature layer to the original YOLOv5s feature fusion network, resulting in increased computational complexity and a 1.44 ms. slower inference time than YOLOv5s. Nonetheless, the detection accuracy has increased by 3.6 percentage points relative to YOLOv5s. HD-YOLOv5s surpasses Faster R-CNN, SSD, and YOLOv3 in detection accuracy and inference speed, achieving detection speeds for a single frame image between 0.01 and 0.02 seconds, thereby fulfilling the real-time criteria for gesture recognition. To comprehensively confirm the efficacy of the gesture recognition approach presented in this research, it was compared with alternative gesture recognition methods utilizing the public NUS-II dataset, with the experimental findings displayed in Table III.

TABLE III. COMPARISON BETWEEN MAINSTREAM GESTURE RECOGNITION ALGORITHMS AND THE PROPOSED METHOD

References	Recognition method	mAP/%
Wang et al. [26]	Bayesian attention + multi-class SVM	93.7
Yi Li et al. [27]	Skin color detection + CNN	95.6
Yi Tan et al.[28]	Deep convolutional neural network	96.2
Fatma M. et al.[29]	Dual channel convolutional neural network (DC-CNN) + Softmax classifier	98
Proposed Model	HD-YOLOv5s	99.5

During the segmentation and detection phase, gestures were classified directly, resulting in a recognition rate of 96.2%. Fatma M. et al. [29] introduced a gesture identification technique utilizing a dual-channel convolutional neural network (DC-CNN), wherein the gesture picture and edge image were input independently into two distinct channels. Following the pooling processes, the characteristics were integrated in the fully connected layer to derive more profound categorization insights, yielding a recognition rate of 98.0%. From these results, the subsequent conclusions may be inferred:

- Yi Li et al. [27] employed gesture segmentation and skin color detection techniques, which are susceptible to contextual influences, resulting in diminished recognition rates in intricate settings. This paper presents a method that enhances feature extraction by incorporating image enhancement pre-processing and integrating the SKNet attention module into the feature extraction network, thereby augmenting the model's generalization and robustness in complex environments, which results in improved gesture recognition rates.
- Yi Tan et al. [28] identified gestures by direct classification or by augmenting network layers. This framework can mitigate the effects of inconsistent illumination and intricate backdrops, enhancing the model's adaptability to complicated surroundings. Nonetheless, its performance in recognizing small-scale movements is merely mediocre. This research presents an approach that, through the development of an innovative feature fusion network, augments the model's capacity to identify small-scale gestures from considerable distances, hence enhancing gesture recognition rates.



(a) mAP curves of each model

(b) Training loss curves of each model

Fig. 10. Training curves of each model.

2) Ablation experiment: To verify the effectiveness of each improvement module in the YOLOv5s network model, an ablation experiment will be conducted based on the YOLOv5s model, comparing the performance of different improved models. As shown in Table IV, '—' indicates not used, and '√' indicates used.

Table IV indicates that the mAP value of the enhanced network model HD-YOLOv5s attained 99.5%. In Improved Model 1, the SKNet attention mechanism was incorporated into the original backbone extraction network. The parameter count (M) remained rather stable, while the mAP enhanced by 1.5 percentage points in comparison to the previous model. SKNet, as a lightweight embedded module, produces more rational weight coefficients by autonomously picking the ideal operator, hence augmenting the network's feature extraction capability while maintaining a steady parameter count.

Improved Model 2 incorporated a novel bidirectional feature pyramid network (BiFPN) into the original feature fusion network. In comparison to the BiFPN in Table I, which has three levels of fusion feature layers, the BiFPN enhanced with low-level features exhibits superior fusion capability. By fully leveraging the low-level P2 characteristics, the model's efficacy in small item recognition was enhanced. In contrast to Improved Model 3, which has four detection layers, Improved Model 2 omits low-level features in the bidirectional feature fusion, leading to a 0.3 percentage point reduction in mAP, while decreasing the computational load by 0.5% and the parameter count by 4.9%. Consequently, to alleviate computational burden and decrease inference duration, bidirectional feature fusion was not utilized for the low-level P2 features in this study.

TABLE IV. PERFORMANCE COMPARISON OF EACH IMPROVED MODEL

Model	Feature layer	Detection layer	Gamma	SKNet	BiFPN	mAP/%	M/10^6	FLOPs/10^9
YOLOv5s	3	3	—	—	—	95.9	7.03	15.9
Improved model 1	3	3	—	√	—	97.4	7.24	16.2
Improved model 2	4	3	—	—	√	98	13.5	17.8
Improved model 3	4	4	—	√	√	98.3	14.2	17.9
Improved model 4	4	3	—	√	√	99.3	13.6	17.9
HD-YOLOv5s	4	3	√	√	√	99.5	13.6	17.9

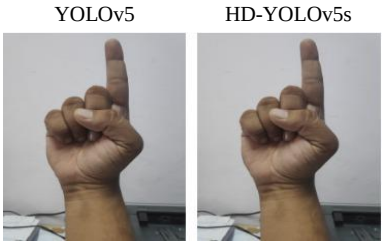
TABLE V. DETECTION PERFORMANCE OF DIFFERENT GESTURE CATEGORIES ON THE NUS-II TEST SET

Model	YOLOv5s	HD-YOLOv5s
Gesture a	0.958	0.985
Gesture b	0.963	0.990
Gesture c	0.941	0.980
Gesture d	0.973	0.992
Gesture e	0.958	0.988
Gesture f	0.960	0.989
Gesture g	0.974	0.990

Gesture h	0.952	0.973
Gesture i	0.970	0.988
Gesture j	0.962	0.985

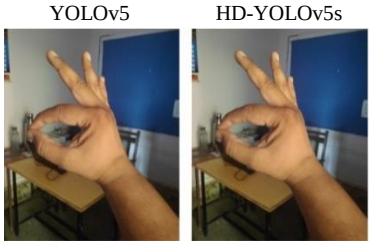
TABLE VI. DETECTION PERFORMANCE OF DIFFERENT GESTURE CATEGORIES ON THE CUSTOM TEST SET

Model	YOLOv5s	HD-YOLOv5s
Gesture 0	0.954	0.993
Gesture 1	0.969	0.982
Gesture 2	0.947	0.991
Gesture 3	0.966	0.995
Gesture 4	0.963	0.978
Gesture 5	0.965	0.990
Gesture OK	0.970	0.980



(a) Strong light with recognition rate 96-100% for one finger

(b) Weak light with recognition rate 95-99% for two fingers



(c) Uneven lighting with recognition rate 95-99% for three fingers

Fig. 11. Recognition effect under different lighting conditions.

Enhanced Model 4 integrated the attention mechanism and the refined feature fusion module into the network. In comparison to Improved Model 2, the computational burden and parameter count exhibited no growth, while the mean Average Precision (mAP) rose by 1.3 percentage points. The mAP improved by 3.4 percentage points relative to the previous model. The enhanced HD-YOLOv5 model utilized Gamma image enhancement preprocessing on the dataset during the input phase, attaining a mAP value of 99.5%, representing a 3.6 percentage point increase compared to the original YOLOv5s network.

Fig. 10 illustrates the training result curves for the different models prior to and following enhancement on the custom training set. The iterations were established at 200, the learning rate at 0.01, and the momentum factor at 0.937. In Fig. 10(a), the horizontal axis denotes the training epochs, whereas the vertical axis indicates the mAP value at an IOU of 0.5. The performance of the enhanced models surpasses that of the pre-enhancement ones. In Fig. 10(b), the enhanced HD-YOLOv5s model exhibited a more rapid convergence and a reduced loss value relative to the YOLOv5 model, signifying superior convergence capabilities of the improved model.

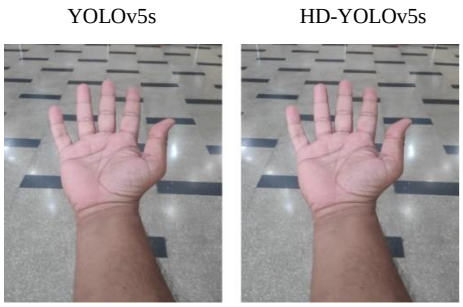
V. RESULTS AND DISCUSSION

This study utilizes the publicly available NUS-II dataset [30] for training, with validation findings presented in Table V. The NUS-II dataset, while encompassing a variety of intricate backgrounds, contains a limited number of gesture photos across different lighting situations. To enhance the verification of the universality and robustness of the new technique, validation experiments were undertaken on a bespoke dataset encompassing diverse illumination situations. The validation outcomes are presented in Table VI. The HD-YOLOv5s model demonstrated a notable enhancement in recognition accuracy on the custom dataset. This illustrates that the enhanced algorithm exhibits strong performance across diverse complicated backgrounds and increases resilience to interference.

To verify the feasibility of the improved HD-YOLOv5s model, several gesture images from the test set were selected for testing. Fig. 11 compares the gesture recognition results between the YOLOv5s and HD-YOLOv5s models under different lighting conditions. Fig. 11(a) and 11(b) show the recognition results in strong and weak lighting environments, while Fig. 11(c) shows the recognition results under uneven lighting. In these comparisons, the left images are from the YOLOv5s model, and the right images are from the HD-YOLOv5s model. The results show that the improved HD-YOLOv5s model achieves varying degrees of improvement in gesture recognition accuracy under different lighting conditions. In Fig. 11(c), the left image misclassifies the "OK" gesture and part of the windowsill as gestures "5" and "0," whereas the right image correctly identifies them with higher accuracy.

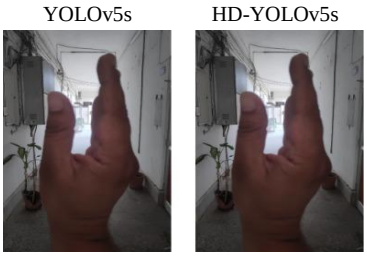
Fig. 12 compares the recognition results of the models before and after improvement in situations where the background color is similar to skin tone. Fig. 12(a) and 12(b) display the recognition of gestures in simple and complex backgrounds, respectively. In Fig. 12(a), the performance difference between the original and improved models is minimal in a simple background. However, in Fig. 12(b), the improved model achieves significantly higher accuracy in a complex background, showing a substantial improvement in recognizing gestures with backgrounds close to skin color.

(a) Simple background with 96-98% recognition rate

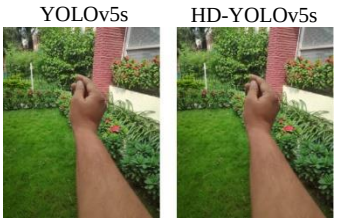


(b) Complex background with 93-99 recognition

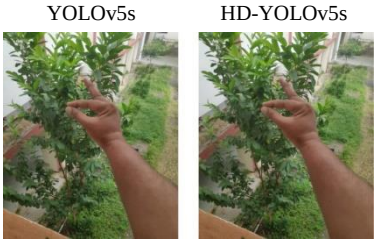
Fig. 12. Recognition effect when the background is close to skin color.



(a) Uneven lighting with 88-90% recognition rate



(b) Simple background with 95-98% recognition rate



(c) Complex background with 93-99% recognition rate

Fig. 13. Recognition effect of small-scale gestures in complex environments.

Fig. 13 shows the recognition performance of the models before and after improvement for small-scale gestures in complex environments. Fig. 13(a), 13(b), and 13(c) represent the detection of small gestures at a distance in different complex scenarios. Especially in Fig. 13(a), under uneven lighting and a complex background, the improved model shows a clear improvement in recognizing small gestures.

In summary, the improved HD-YOLOv5s model outperforms the original YOLOv5s model in recognition performance. The YOLOv5s model performs poorly in complex environments with uneven lighting or skin-tone-like backgrounds, leading to misdetections and weak performance in recognizing small gestures at a distance. In contrast, the HD-YOLOv5s model can accurately recognize gestures in complex environments with a higher recognition rate and resolves the original model's issue of low accuracy in detecting small gestures. The performance improvement of the improved model is not due to any single method but results from overall enhancements in feature extraction and feature fusion capabilities.

VI. Conclusion

This study presents a gesture recognition methodology, HD-YOLOv5s, which attains great precision even in intricate settings, hence enhancing human-computer interface technology. The adaptive Gamma image enhancement technique grounded in Retinex theory was employed to preprocess the dataset. The SKNet adaptive convolutional attention mechanism model was subsequently integrated into the feature extraction network to augment its feature extraction capabilities. The modified BiFPN structure was incorporated into the feature fusion network, enhancing the network's capacity to identify tiny objects. The experimental findings indicate that HD-YOLOv5s attained a mAP value of 99.5%. In comparison to the Faster R-CNN, SSD, and YOLOv3 models, the suggested technique identifies a single image in about 0.01 to 0.02 seconds. The model is compact and efficient, satisfying the real-time demands of gesture recognition in intricate situations. Accuracy increased by 3.6 percentage points vs to the previous YOLOv5s model. Furthermore, in comparison to other prevalent gesture recognition algorithms, our model demonstrates superior generalization and robustness. Validation trials performed on a proprietary dataset and the NUS-II public dataset with intricate backgrounds attained identification rates of 99.5% and 98.9%, respectively. This research presents an enhanced network model that demonstrates superior recognition ability and resilience against challenges such as inconsistent lighting, backdrops resembling skin tones, and diminutive gesture sizes. It fulfills the real-time demands of gesture recognition in intricate situations. Effective static gesture identification is a crucial basis for the examination of dynamic gestures and their applications. The results indicate that this technique exhibits strong robustness and real-time efficacy in intricate situations. This technology is intended for future application in dynamic gesture tracking amongst complicated background variations to resolve challenges associated with low identification rates, hence improving its utility in human-computer interaction domains.

REFERENCES

[1] Zuopeng Zhao, Tianci Zheng, Kai Hao, Junjie Xu, Shuya Cui, Xiaofeng Liu, Guangming Zhao, Jie Zhou, Chen He,YOLO-PAI: Real-time handheld call behavior detection algorithm and embedded application,Signal Processing: Image Communication,Volume 120,2024,117053,ISSN 0923-5965.

[2] Seungwoon Lee, Sijung Kim, Byeong-hee Roh,Mixed Reality Virtual Device (MRVD) for seamless MR-IoT-Digital Twin convergence,Internet of Things,Volume 26,2024,101155,ISSN 2542-6605.

[3] J. Huang and H. Kang, "Automatic Defect Detection in Sewer Pipe Closed- Circuit Television Images via Improved You Only Look Once Version 5 Object Detection Network," in *IEEE Access*, vol. 12, pp. 92797-92825, 2024.

[4] Wei-Chun Kao, Yi-Ling Fan, Fang-Rong Hsu, Chien-Yu Shen, Lun-De Liao,Next-Generation swimming pool drowning prevention strategy integrating AI and IoT technologies,Heliyon,Volume 10, Issue 18,2024, e35484,ISSN 2405-8440.

[5] Zonghui Li, Yongsheng Dong, Longchao Shen, Yafeng Liu, Yuanhua Pei, Haotian Yang, Lintao Zheng, Jinwen Ma,Development and challenges of object detection: A survey,Neurocomputing,Volume 598,2024,128102,ISSN 0925-2312.

[6] Zhao Qianyi, Liang Zhiqiang,Research on multimodal based learning evaluation method in smart classroom,Learning and Motivation,Volume 84,2023,101943,ISSN 0023-9690.

[7] Wupeng Deng, Quan Liu, Feifan Zhao, Duc Truong Pham, Jiwei Hu, Yongjing Wang, Zude Zhou,Learning by doing: A dual-loop implementation architecture of deep active learning and human-machine collaboration for smart robot vision,Robotics and Computer-Integrated Manufacturing,Volume 86,2024,102673, ISSN 0736-5845.

[8] Yu Zhou, Ronggang Cao, Ping Li,A target spatial location method for fuze detonation point based on deep learning and sensor fusion,Expert Systems with Applications,Volume 238, Part F,2024,122176,ISSN 0957-4174.

[9] Tao Wang,Intelligent long jump evaluation system integrating blazepose human pose assessment algorithm in higher education sports teaching,Systems and Soft Computing,Volume 6,2024,200130,ISSN 2772-9419.

[10] Guoyan Yu, Ruilin Cai, Jinping Su, Mingxin Hou, Ruoling Deng,U-YOLOv7: A network for underwater organism detection,Ecological Informatics,Volume 75,2023,102108,ISSN 1574-9541.

[11] Bidita Sarkar Diba, Jayonto Dutta Plabon, M.D. Mahmudur Rahman, Durjoy Mistry, Aloke Kumar Saha, M.F. Mridha,Explainable federated learning for privacy-preserving bangla sign language detection,Engineering Applications of Artificial Intelligence,Volume 134,2024,108657,ISSN 0952-1976.

[12] Zicheng Gao, Xufeng Yuan, Jie Lei, Hao Guo, Francesco Marinello, Lorenzo Guerrini, Alberto Carraro,A vision-based dietary survey and assessment system for college students in China,Food Chemistry,2024,141739,ISSN 0308-8146.

[13] Yuhe Fan, Lixun Zhang, Canxing Zheng, Yunqin Zu, Xingyuan Wang, Jinghui Zhu,Real-time and accurate meal detection for meal-assisting robots,Journal of Food Engineering,Volume 371,2024,111996,ISSN 0260-8774.

[14] Ahmed Bin Kabir Rabbi, Idris Jeelani,AI integration in construction safety: Current state, challenges, and future opportunities in text, vision, and audio based applications,Automation in Construction,Volume 164,2024,105443,ISSN 0926-5805.

[15] Prashan Premaratne, Inas Jawad Kadhim, Rhys Blacklidge, Mark Lee,Comprehensive review on vehicle Detection, classification and counting on highways,Neurocomputing,Volume 556, 2023,126627,ISSN 0925-2312.

[16] Narit Hnoohom, Pitchaya Chotivatunyu, Nagorn Maitrichit, Chayawat Nilsumrit, Pawinee Iamtrakul,The video-based safety methodology for pedestrian crosswalk safety measured: The case of Thammasat University, Thailand,Transportation Research Interdisciplinary Perspectives,Volume 24,2024, 101036,ISSN 2590-1982.

[17] Nishant Ketan Gajjar, Khansa Rekik, Ali Kanso, Rainer Müller,Human intention and workspace recognition for collaborative assembly,IFAC-PapersOnLine,Volume 55, Issue 10,2022,Pages 365-370,ISSN 2405-8963.

[18] Zhuo Wang, Xiangyu Zhang, Liang Li, Yiliang Zhou, Zexin Lu, Yuwei Dai, Chaoqian Liu, Zekun Su, Xiaoliang Bai, Mark Billinghurst,Evaluating visual encoding quality of a mixed reality user interface for human–machine co-assembly in complex operational terrain,Advanced Engineering Informatics,Volume 58,2023,102171,ISSN 1474-0346.

[19] Junqi Wang, Lanfei Jiang, Hanhui Yu, Zhuangbo Feng, Raúl Castaño-Rosa, Shi-jie Cao,Computer vision to advance the sensing and control of built environment towards occupant-centric sustainable development: A critical review,Renewable and Sustainable Energy Reviews,Volume 192,2024,114165,ISSN 1364-0321.

[20] Abhishesh Pal, Antonio Candea Leite, Pål Johan From,A novel end-to-end vision-based architecture for agricultural human–robot collaboration in fruit picking operations,Robotics and Autonomous Systems,Volume 172,2024,104567,ISSN 0921-8890.

[21] Prabu Selvam, Joseph Abraham Sundar K,Chapter 23 - A deep learning framework for surgery action detection,Editor(s): Harish Garg, Jyotir Moy Chatterjee,Deep Learning in Personalized Healthcare and Decision Support,Academic Press,2023,Pages 315-328,ISBN 9780443194139.

[22] Yaping Xu, Yanyan Li, Yunshan Chen, Haogang Bao, Yaqian Zheng,Spontaneous visual database for detecting learning-centered emotions during online learning,Image and Vision Computing,Volume 136, 2023,104739,ISSN 0262-8856.

[23] Mohita Jaiswal, Abhishek Sharma, Sandeep Saini,Hardware acceleration of Tiny YOLO deep neural networks for sign language recognition: A comprehensive performance analysis,Integration,Volume 100,2025,102287,ISSN 0167-9260.

[24] Zhilin Lyu, Chongyang Wang, Xiujun Sun, Ying Zhou, Xingyu Ni, Peiyuan Yu,Real-time ship detection system for wave glider based on YOLOv5s-lite-CBAM model,Applied Ocean Research,Volume 144,2024,103833,ISSN 0141-1187.

[25] Yi Li, Haojie Zhou, Jing Feng, Xing Li, Xiaobin Xu, Pingzhi Hou, Xiaomin Hu,An improved smoking behavior detection algorithm via incorporating an interference information filtering network,Engineering Applications of Artificial Intelligence,Volume 136, Part B,2024,109050,ISSN 0952-1976.

[26] Yi Tan, Wenyu Xu, Penglu Chen, Shuyan Zhang,Building defect inspection and data management using computer vision, augmented reality, and BIM technology,Automation in Construction,Volume 160,2024,105318, ISSN 0926-5805.

[27] Fatma M. Talaat, Walid El-Shafai, Naglaa F. Soliman, Abeer D. Algarni, Fathi E. Abd El-Samie, Ali I. Siam,Real-time Arabic avatar for deaf-mute communication enabled by deep learning sign language translation,Computers and Electrical Engineering,Volume 119, Part A,2024,109475,ISSN 0045-7906.

[28] Surbhi Kapoor, Akashdeep Sharma, Amandeep Verma,Diving deep into human action recognition in aerial videos: A survey,Journal of Visual Communication and Image Representation,Volume 104,2024,104298,ISSN 1047-3203.

[29] Yong Pan, Chengjun Chen, Zhengxu Zhao, Tianliang Hu, Jianhua Zhang,Robot teaching system based on hand-robot contact state detection and motion intention recognition,Robotics and Computer-Integrated Manufacturing,Volume 81,2023,102492,ISSN 0736-5845.

[30] Gege Zhang, Luping Wang, Liang Wang, Zengping Chen,Hand-raising gesture detection in classroom with spatial context augmentation and dilated convolution,Computers & Graphics,Volume 110,2023,Pages 151-161,ISSN 0097-8493.

Multi-Label Aspect-Sentiment Classification on Indonesian Cosmetic Product Reviews with IndoBERT Model

Ng Chin Mei[1], Sabrina Tiun[2], Gita Sastria[3]
Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia, Malaysia[1, 2]
Jurusan Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Riau, Indonesia[3]

***Abstract*—For an existing cosmetic company to expand, it is crucial to understand customers' opinions regarding cosmetic products through product reviews. Aspect-based sentiment classification (ABSC), which consists of text representation and classification stages, is typically employed to automatically extract the interested insights from review. Existing studies of ABSC primarily used single-label classification, which fails to capture relationships between multiple aspects in a review. Additionally, the use of contextual embeddings like IndoBERT for representing Indonesian-language cosmetic product reviews has been underexplored. This study addresses these issues by developing a multi-label classification model that leverages IndoBERT, including IndoBERT[b], IndoBERT[k], and IndoBERTweet, to better represent context and capture relationships across multiple aspects in a review. The model is trained and evaluated using a dataset of Indonesian-language cosmetic product reviews from Female Daily. The multi-label models can be constructed using IndoBERT directly as end-to-end model or employing IndoBERT solely as word embedding model. The latter model, also known as conventional multi-label model, needs to be coupled with problem transformation approach and classifier for classification. Single label classification model with Word2Vec serves as baseline to assess the improvement of multi-label model's performance on Female Daily cosmetic product reviews dataset. The empirical results revealed that the multi-label approach was more effective in identifying sentiments for pre-defined aspects in reviews. Among the models, end-to-end IndoBERT[b] achieved the highest accuracy (86.98%), while conventional multi-label models combining IndoBERT[b], Label Powerset (LP), and Support Vector Machine (SVM) performed best with 69.64%. This study is significant as it provides a more generalized understanding of the BERT embedding within the context of multi-labels classification and explores the effect of contextual embedding in the cosmetic domain.**

Keywords*—Aspect-based sentiment analysis; IndoBERT; multi-label classification; IndoBERTweet; problem transformation

I. Introduction

Recently, it can be observed that the worldwide cosmetic industry has generally experienced tremendous growth [1]. Specifically, in Indonesia, the cosmetic industry market size is anticipated to grow from USD 1.17 billion from 2020 to roughly double the amount, which is USD 2.38 billion within eight years period [2].

In order for cosmetic companies to capitalize on these future prospects, it is imperative to understand the customer's needs and opinion, and one of the methods to achieve this is through customer's product reviews, as these heavily influence purchasing decisions [3] [4]. Sentiment analysis is a suitable technique to extract the insights from reviews due to the nature of review itself, which is opinionated with a sentiment polarity, either positive, negative, or neutral. In sentiment analysis, classification of sentiment can be performed at three levels of extraction in terms of granularity, namely document level, sentence level and aspect level. Analyzing reviews at aspect level using aspect-based sentiment analysis (ABSA) is crucial since it identifies sentiments tied to specific product aspects, offering deeper insights than document or sentence-level analysis.

Aspect-based sentiment classification (ABSC) is one of the tasks in ABSA that involves solely sentiment classification. Typically, ABSC is implemented as a pipeline consisting of two stages, namely text representation and classification. The first stage involves the transformation of the text data into its numerical representation. Traditional text representation methods such as Term Frequency - Inverse Document Frequency (TF-IDF) and static word embedding model (e.g., Word2Vec) are relatively inaccurate in representing text as they fail to capture contextual meanings between words [5]. The emergence of contextual word embedding model addresses this limitation. One state-of-the-art contextual model is BERT (Bidirectional Encoder Representations from Transformers). The effectiveness of BERT is demonstrated by the findings of several studies [6] [7] [8] [38].

Subsequently, text representation enables the next stage which is classification. Classification is where sentiment for each aspect of an individual review text can be determined. A notable limitation in the classification stage of ABSC in prior research is the reliance on a single-label classification approach [28] [29] [30] [31] [32]. This method determines the sentiment for each aspect independently, failing to capture correlations between sentiments across different aspects of a review [9]. In real-world scenarios, multiple aspects in a customer review may have related sentiments, and ignoring these dependencies can reduce the performance of the classification model. Although [9] proposed a multi-label approach to account for these correlations, their work did not directly compare it with single-label models, and their dataset was from a different domain. Furthermore, there is a gap in exploring multi-label classification for Indonesian-language datasets, which have

been under-explored compared to more dominant languages like English.

This study focuses on investigating ABSC of cosmetic products reviews written in the Indonesian language. Several issues have been observed in this context. Firstly, there is a scarcity of prior ABSC research in Indonesian cosmetic products reviews. Secondly, none of the prior works have explored the effect of contextual embedding models such as BERT on this domain. Thirdly, existing studies primarily employed single label classification, but this classification approach presents limitations by disregarding possible relationship between multiple aspects within single review [9]. Thus, this study aimed to address these issues by developing a reliable multi-label ABSC model, at the same time, exploring the performance of contextual word embedding in representing words from cosmetic domain. As the focus is on the Indonesian language, IndoBERT, which is a BERT designed for Indonesian language, was employed as the contextual embedding model in this study.

In this study, this multi-label ABSC model was built with two alternative methods, one using IndoBERT as an end-to-end model, and the other built with a combination of text representation method, multi-label problem transformation approach, and machine learning classifier. The former method performs multi-label classification by directly processing the text and generating sentiment predictions within a single model, while the latter method analyses the word vectors transformed by IndoBERT, then combines the multi-label approach with a classifier to categorize the aspect-sentiment labels for each cosmetic product review. The second method was referred to conventional multi-label model. This study is organized as follows: Section II presents the background information and related works. Section III demonstrates the methodology. Section IV presents the results. Discussion is given in Section V. Finally, the paper is concluded in Section V.

II. Literature Review

A. IndoBERT

1) Variants of IndoBERT: There are three variants of IndoBERT, which are IndoBERT[k], IndoBERT[b], and IndoBERTweet. The key differences among IndoBERT variants lie in the training datasets used. IndoBERT[k], introduced by [10] was trained on the INDOLEM dataset, which consists solely of formal text, limiting its effectiveness with colloquial Indonesian. To address this, [11] introduced IndoBERT[b], trained on the mixed formal and informal dataset INDONLU. Additionally, IndoBERTweet was developed specifically for informal social media language [12].

2) Word embedding model: Previous comparative studies consistently highlight the superiority of IndoBERT variants when applied to Indonesian product review datasets across various domains. For example, [13] demonstrated that IndoBERT[b] outperformed Word2Vec when paired with a Convolutional Neural Network (CNN) classifier in categorizing restaurant customer reviews across four dimensions: Price, Food, Place, and Service. This finding is corroborated by study [14], who showed that IndoBERT[k] performed better than both Word2Vec and FastText in representing the reviews related to COVID vaccines. Moreover, the IndoBERT[b] showed more effectiveness than Word2Vec with all seven classifiers such as SVM, Naïve Bayes (NB), and Random Forest (RF) when dealing with hotel reviews in study [15], further supporting the superiority of IndoBERT as word embedding models in transforming the text.

3) End-to-end model: IndoBERT also plays a good role as end-to-end model in ABSC as shown in study [16]. In the study of [17], sentiment classification on online reviews was conducted using IndoBERT as end-to-end model, with the aim to investigate the satisfaction of customer towards ride-hailing company Gojek from seven aspects. A relatively high accuracy of 96% was achieved, suggesting the superiority of IndoBERT. Similar promising results were obtained in the study of [18]. Other studies such as [19] and [20] showed the effectiveness of IndoBERT implementations as an end-to-end model when comparing its performance to other deep learning language models and traditional machine learning method.

B. Multi-Label Classification

Existing research categorizes multi-label approaches into three categories: Problem transformations, algorithm adaptations, and pre-trained language model. Problem transformation methods, such as Binary Relevance (BR), Classifier Chain (CC), and Label Powerset (LP), convert multi-label problems into binary or multi-class problems for classification. BR treats each label as a separate binary problem, while CC predicts labels sequentially, and LP transforms labels into a multi-class problem. RAkEL D, an ensemble of LP, addresses LP's limitations by training on label subsets. Algorithm adaptation modifies existing algorithms, like ML-kNN and ML-DT, to handle multi-label tasks directly.

In most previous works on multi-label classification, emphasis was placed mainly on text categorization [21] [22] [23] [24]. The literature review reveals that there was only a limited of studies on ABSC that specifically address multi-labels classification. Related existing studies primarily assessed the multi-label aspect-sentiment model efficiency through multi-label metrics: Accuracy and Hamming Loss.

The study in [25] explored drug effectiveness using problem transformation methods (BR, CC, LP) combined with various classifiers, finding that SVM performed best, followed by DT and NB. Among the transformation methods, LP outperformed CC and BR. Despite this study evaluating all three popular problem transformation methods, there was a lacking exploration of the algorithms that specifically adapted for multi-label problems.

The research in [9] compared three categories of multi-labels approaches using customer reviews from restaurants, wine, and movies, demonstrating pre-trained language models such as BERT outperformed other categories, followed by problem transformation and algorithm adaptation. For problem transformation, the author obtained the same results as [25]: LP consistently outperformed CC and BR.

The study in [26] further confirmed the findings of [9], demonstrating BERT's superiority in sentiment classification

and showing that LP outperformed BR and CC within problem transformation approaches.

In the Indonesian context, BERT variants, IndoBERT has shown excellent performance in multi-label tasks, outperforming other models, as evidenced by studies like [27] and [15].

C. Aspect-based Sentiment Classification (ABSC) on Indonesian Cosmetic Product Reviews

Previous ABSC studies of cosmetic product reviews in Indonesian language, primarily using datasets from Female Daily, focused on determining the overall sentiment of user reviews. These studies explored various aspects, with most focusing on four predefined aspects: packaging, quality, scent, and price [28] [29] [30] [31].

Traditional text representation approaches like TF-IDF and NB yielded moderate performance, with studies like [28] achieving an average F1-score of 62.81% across these four aspects. Their results indicated room for improvement, potentially due to the limitations of TF-IDF and NB, which rely on word frequency for representation and independence assumptions for classification.

Subsequent research improved performance by employing Word2Vec static word embeddings and different classifiers, such as SVM, on similar datasets with the same aspects. [29] achieved a 68.25% F1-score using Word2Vec for text representation while maintaining NB as the classifier. The improvement is likely due to Word2Vec enhanced the contextual richness of sentiment representations compared to TF-IDF. The study in [30] demonstrated further improvements by using SVM with TF-IDF as the text representation method.

Other studies, like those by [32], explored additional aspects but found limitations in performance using approaches like Bag of Words (BOW), achieving only a 53.04% F1-score. The study in [31] employed a hybrid method of TF-IDF and semantic similarity, achieving a high accuracy of 90.33%, likely due to fewer predicted aspects.

Notably, none of these studies applied contextual embeddings or addressed multi-label classification in the cosmetic domain, highlighting areas for future improvement in ABSA methods.

III. Methodology

A. Research Methods Overview

Generally, there are two strategies that can be used to build a multi-label model using IndoBERT, as shown in Fig. 1. In the first strategy, IndoBERT was used as an end-to-end model to directly perform multi-label classification. In second strategy, IndoBERT was used solely as a word embedding model to transform text into dense word vectors, which were then passed to machine learning classifiers. The model from second strategy, known as the conventional multi-label model, involved using word embeddings for text representation, multi-label problem transformation methods, and classifiers.

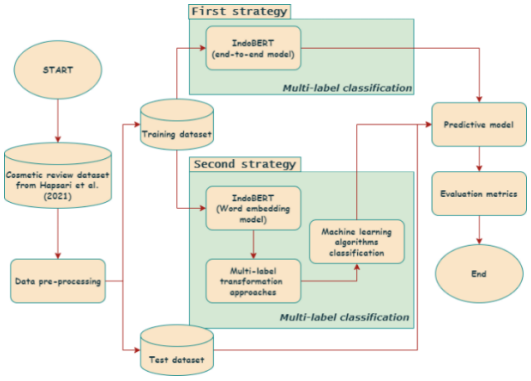


Fig. 1. General workflow for building multi-label models using IndoBERT.

In this study, three interconnected experiments were conducted: -

1) Experiment I: This experiment was focused on evaluating the performance of multi-label classification in ABSC context, with single-label model from [29] serving as the baseline. To rule out any external factors which might affect the results, the experiment established the baseline by replicating the literature experiment [29].

2) Experiment II: Experiment II concentrated on assessing the different variants of IndoBERT as word embeddings, alongside the promising multi-label approaches identified from experiment I. This experiment exploited Word2Vec as the baseline word embedding. The IndoBERT variants used were IndoBERT[b], IndoBERT[k], and IndoBERTweet.

3) Experiment III: Building upon the findings of Experiment I and II, this experiment further explored the performance of IndoBERT in multi-label classification by incorporating the multi-label capabilities into model, using IndoBERT directly as end-to-end model, serving as both text representation and classifier. Conventional multi-label models with classifiers such as Gaussian NB, SVM, Linear SGD, and RF were also employed for comparison.

B. Dataset

The study investigated a secondary dataset that was exclusively sourced from journal article published by [29]. The dataset consists of a total of 3960 customer reviews on cosmetic products collected from Female Daily website and written in Indonesian language. Each review was pre-annotated with sentiments across four different aspects, with the sentiment distribution summarized in Table I.

TABLE I. Sentiment Distribution Across Four Aspects in Cosmetic Product Reviews

Aspect	Sentiment Count		
	Positive	***Negative***	***Neutral***
Product	659	688	2612
Packaging	447	189	3323
Price	1056	716	2187
Scent	669	218	3072

C. Exploratory Data Analysis (EDA)

Before data modeling, a Chi-square test was conducted during the EDA stage to assess dependencies between the targeted aspects. This test provided insights into the relationships between aspect-sentiments, helping determine if single-label or multi-label classification would be more suitable. In this study, the null hypothesis claimed that there is no significant association between the targeted aspects in the investigated dataset. A p-value threshold of 0.05 was used; any value below this indicated significant associations between aspects, suggesting the need for a multi-label classification approach in the dataset.

D. Preprocessing

For multi-label classification, the aspect columns were transformed into aspect-sentiment labels for further analysis. Each aspect was further divided into three labels, following the patterns of 'aspect_pos,' 'aspect_neg,' and 'aspect_other', with the number 0 or 1 indicating the presence of each aspect-sentiment label.

E. Word Embedding (Text Representation) using IndoBERT

Before being processed by IndoBERT, the review text must first pass through the IndoBERT tokenizer to obtain special input format. In this stage, the input sentence was concurrently tokenized and added with special tokens of [CLS] and [SEP] tokens at the beginning and the end of tokenized sequence respectively. For the input length, the maximum sentence length was limited to 128 tokens in this study. After that, these modified sequences were fed into token, segment, and position embeddings sequentially to generate the initial input embedding, which in turn fed into encoder layers within IndoBERT for further processing.

In IndoBERT, the initial embedding of each token was passed through multiple sub-layers consisting of multi-head self-attention and Feed-forward Network to incorporate the contextual information. The final output contextualized embedding was extracted through a mean pooling strategy. The overview of the word embedding process for IndoBERT is illustrated in Fig. 2.

F. Multi-Label Classification

1) Conventional multi-label classification: To build conventional multi-label models, the output contextualized embeddings and target labels were transformed using problem transformation methods. Binary Relevance (BR), Classifier Chain (CC), and Label Powerset (LP) were used to convert the data into binary or multi-class problems. Classifiers such as Gaussian Naïve Bayes (NB), Support Vector Machine (SVM), Random Forest (RF), and Linear Stochastic Gradient Descent (SGD) were then applied for classification.

2) IndoBERT (As end-to-end model): To perform multi-label classification directly using IndoBERT, an additional classifier layer was added at the uppermost level of the model. Final output embedding from mean pooling layer was fed into the classifier layer directly for multi-label classification as shown in Fig. 3. In this strudy, the hyperparameters values of classifier layer mirrored the literature findings of [33], which set to "learning rate = 2e-5, batch size = 8, and epoch =5", optimizing with Adam optimizer. Because IndoBERT was designed to perform multi-label classification, sigmoid function was used rather than SoftMax in classification layer. The formula of sigmoid function is shown in (1). The output probability from sigmoid activation function for each aspect-label is a real number within the range of 0 to 1. Given that the study applied the default threshold value of 0.5, any predicted probability of the label greater than 0.5 was referred to present and less than 0.5 was considered as absent.

$$\sigma(x)= 1/(1+e^{(-x)}) \quad (1)$$

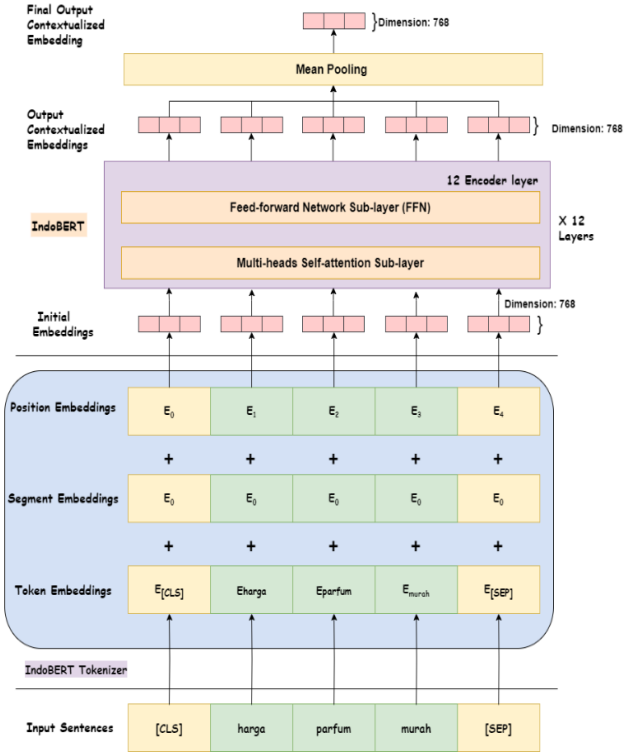


Fig. 2. Overview of word embedding process for input sentence by IndoBERT.

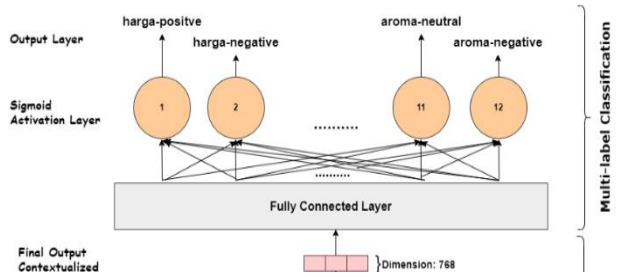


Fig. 3. Multi-label classification process within IndoBERT.

G. Evaluation Metrics

In this study, several evaluation metrics were employed to evaluate the sentiment classification model performance.

1) Accuracy per label: This metric assesses the number of correctly predicted labels over the total number of instances,

computing using (2), where TP and TN refer to True Positive and True Negative, respectively. Given that it evaluates the model's correctness on individual labels (column) independently, accuracy is commonly used in single label classification. In this study, this metric was utilized for comparing the performance of multi-label with single-label models in Experiment I.

$$\text{Accuracy per label} = (TP + TN) / Total \quad (2)$$

2) Accuracy: This accuracy metric calculates the probability of the correctly classified labels by considering the overlap between the true data, Y_i and predictive data, Z_i for each instance, as computed by the (3). In this study, this metric was used as one of the main references in assessing the multi-label sentiment classification model performance in Experiment II and III.

$$Accuracy = 1/N * \Sigma | Yi \cap Zi | / | Yi \cup Zi | \quad (3)$$

3) Hamming loss: Hamming Loss is the prominent evaluation metric of multi-label classification that measures the proportion of wrongly classified labels over all instances. In contrast with typical metrics, the lower the value hamming loss represents the higher performance of model. The formula for computing hamming loss is shown in (4). It was used to evaluate the multi-label model performance in this study.

$$\text{Hamming Loss} = 1/N * \Sigma | Yi \, \Delta \, Zi | \quad (4)$$

4) Micro-F1 score: Micro F1-score is a harmonic mean of precision and recall calculated based on classes, shown in (5), where P and R represent precision and recall respectively. Precision measures the proportion of the chosen items that are correct over the actual instances that are predicted as chosen while recall is a metric uses to gauge the percentage of correct items that are selected. The formula of precision and recall is shown in (6) and (7).

$$F1-score = 2PR/(P+R) \quad (5)$$

$$Precision = 1/N * \Sigma | Yi \cap Zi | / | Zi | \quad (6)$$

$$Recall = 1/N * \Sigma | Yi \cap Zi | / | Yi | \quad (7)$$

IV. Results

A. (EDA) Results

Table II presents the Chi-square test results between aspects, showing that most p-values were below 0.05, indicating variable dependency. From the results, it can be observed that nearly all the resulting p-values were less than threshold value 0.05.

TABLE II. Chi-Square Test Results Between Different Aspects of Cosmetic Product

Variable 1	Variable 2	p value	Null hypothesis
harga	pengeamsan	0.0147	Rejected
	produk	6.5113e-24	Rejected
	aroma	3.4954e-12	Rejected
pengemasan	produk	4.3069e-13	Rejected
	aroma	0.0689	Accepted
produk	aroma	1.2633e-25	Rejected

B. Experimental Results I

In this experiment, the baseline single label classification model was replicated based on the methodology from [29]. The method primarily employed Word2Vec to vectorize the text reviews and utilized Gaussian NB to classify the sentiment for each aspect independently. Given that there were four aspects, the model iterated four times to complete the prediction for all aspects. Table III presents the empirical outcomes of baseline from our experiment and [29].

TABLE III. Comparison of Accuracy Per Label of Baseline Single Label Model and Our Experiment

Source	Average Accuracy per Label (%)	Accuracy per Label (%)			
		Price	***Packaging***	***Product***	***Aroma***
[29]	68.17	70.96	68.79	56.36	76.57
Our experiment	62.47	60.33	74.39	48.18	66.99

From Table III, it shows that there was approximately 6% reduction in average accuracy when comparing the replicated model with [29]. The differences can be attributed to factors such as differences in the parameters setting of Gaussian NB as [29] did not include any details about their parameters while this study proceeded with default settings. To mitigate the influences from external factors, an accuracy of 62.47% is used as a reference value for comparing the performance of multi-label models.

Fig. 4 shows that multi-label models perform differently in determining sentiment for Indonesian cosmetic product reviews. Models using BR and CC problem transformation methods had performance comparable to the baseline. The BR model achieved the same accuracy of 62.47% as the baseline, likely due to their similar classification approach. However, the other two multi-models with LP and RAkEL D, exhibited notable enhancement in accuracy over the baseline single label model, achieving 70.18% and 70.16%, respectively.

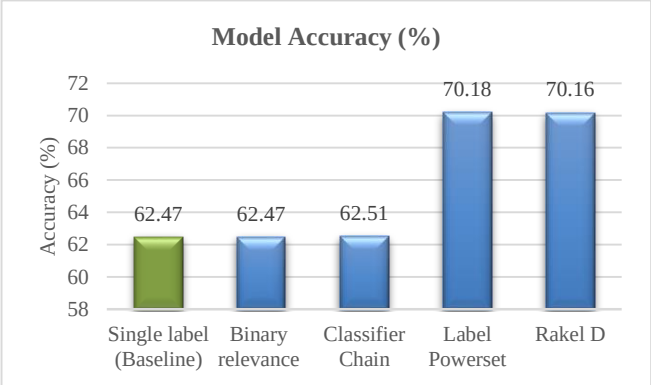


Fig. 4. Average of accuracy per label for single label and multi-label models.

C. Experimental Results II

In Experiment II, the study evaluates the performance of IndoBERT as word embeddings in representing the words from cosmetic domain, using Word2Vec as the baseline. Building upon the findings of Experiment I, LP and RAkEL D, each was used to transform the multi-label problem in the model while Gaussian NB classifier was utilized to classify the aspect-sentiment labels to each review, along with Word2Vec. The IndoBERT word embedding model was employed in parallel, aiming to determine its effectiveness compared to Word2Vec. The results are summarized in Table IV.

TABLE IV. PERFORMANCE OF MULTI-LABEL MODELS USING DIFFERENT EMBEDDING MODELS IN EACH MULTI-LABEL APPROACH

Transformation Approach	IndoBERT version	Accuracy (%)	Hamming Loss (%)	Micro F1-score (%)
Label Powerset	Word2Vec	54.75	22.27	66.66
	IndoBERT[b]	60.39	19.15	71.28
	IndoBERT[k]	47.70	26.18	60.73
	IndoBEETweet	61.10	18.72	71.91
RAkEL D	Word2Vec	53.60	24.96	66.12
	IndoBERT[b]	57.79	20.81	69.97
	IndoBERT[k]	41.86	31.87	56.21
	IndoBERTweet	57.55	21.09	69.76

Overall, both IndoBERT[b] and IndoBERTweet consistently outperformed the baseline Word2Vec embedding model, regardless of the problem transformation approaches used in classification model. For models with LP approach, there was an approximate 5% to 6% improvement in accuracy and micro F1-score when comparing the multi-label models with Word2Vec to IndoBERT[b] and IndoBERTweet. On the other hand, the models employing RAkEL D exhibited only a 2% to 3% enhancement in accuracy and micro F1-score. For hamming loss in the models employing both LP and Rakel D, an approximately range of 3% to 4% reduction was observed when comparing the baseline with each of the IndoBERT[b] and IndoBERTweet, indicating a decrease in misclassification occurrences in models employing both methods.

D. Experimental Results III

This experiment evaluated IndoBERT's performance in direct multi-label classification. Building on results from Experiments I and II, conventional multi-label models using IndoBERT[b] and IndoBERTweet were developed with various classifiers. The results are shown in Tables V and VI, while Table VII presents IndoBERT's empirical performance.

TABLE V. PERFORMANCE OF CONVENTIONAL MULTI-LABEL MODEL USING INDOBERT[B] AS TEXT REPRESENTATION METHOD

Model	Accuracy (%)	Hamming Loss (%)	Micro F1-score (%)
Label Powerset + NB	60.45	19.12	71.33
Label Powerset + SVM	69.64	14.20	78.69
Label Powerset + RF	63.3	17.45	73.82
Label Powerset + SGD	65.48	16.36	75.47
RakEL D + NB	56.81	21.43	68.90
RakEL D + SVM	68.31	14.26	78.59
RakEL D + RF	62.93	16.60	74.18
RakEL D + SGD	65.31	15.99	75.94

TABLE VI. PERFORMANCE OF CONVENTIONAL MULTI-LABEL MODEL USING INDOBERTWEET AS TEXT REPRESENTATION METHOD

Model	Accuracy (%)	Hamming Loss (%)	Micro F1-score (%)
Label Powerset + NB	61.15	18.70	71.95
Label Powerset + SVM	68.14	14.92	77.61
Label Powerset + RF	62.54	17.82	73.26
Label Powerset + SGD	63.38	17.54	73.69
RakEL D + NB	56.71	21.49	69.13
RakEL D + SVM	66.88	14.86	77.57
RakEL D + RF	61.94	17.42	73.26
RakEL D + SGD	64.71	16.35	75.75

TABLE VII. PERFORMANCE OF MULTI-LABEL MODELS WITH INDOBERT AS END-TO-END MODEL

Model	Accuracy (%)	Hamming Loss (%)	Micro F1-score (%)
IndoBERT[b]	86.98	5.45	91.70
IndoBERTweet	86.21	5.85	91.12

The results show that the end-to-end model significantly outperformed the conventional multi-label models. It can be observed that there was a significant enhancement in end-to-end model performance when using IndoBERT[b] and IndoBERTweet, with accuracy increasing by approximately 18% to 30% and the micro F1-score by 13% to 22%, compared to both the highest and lowest performing conventional models based on the same IndoBERT embedding. In terms of hamming loss, using IndoBERT[b] and IndoBERTweet directly for multi-label classification reduced significantly (8% to 16%) in classifying wrongly the aspect-sentiment label for cosmetic product review.

V. DISCUSSION

The results of p-values from EDA showed that most of the null hypotheses were rejected, suggesting that the variables are dependent on each other. These dependencies indicate the presence of an aspect's sentiment might affect the prediction of sentiment of another aspect. Given this dependency, it implies a need to explore the Indonesian cosmetic product review dataset with multi-label model.

There are three categories of multi-label classification methods: Problem transformation, algorithm adaptations, and pre-trained language model. For the problem transformation, the BR model transforms the multi-label task into 12 single-label problems, performing independent classification for each label, much like the baseline. Unlike BR, multi-label model with CC

problem transformation method considered label correlation into account. However, it still demonstrated comparable accuracy with 62.51% to baseline. One of the possible reasons might be the influences by the arbitrary arrangement of labels, which could lead to the poor performance in CC model [34] [35]. In contrast with BR and CC, the other two multi-models with LP and RAkEL D, exhibited notable enhancement in accuracy over the baseline single label model, achieving 70.18% and 70.16%, respectively. There was approximately 8% improvement of accuracy in multi-label models with LP and Rakel D methods over baseline. This suggests LP and RAkEL D are more suitable for multi-aspect sentiment classification. The improvement is probably due to both multi-label models considering label dependencies, with LP capturing co-occurrence relationships by converting the problem into combinations of labels, and RAkEL D enhancing performance by training Gaussian NB on distinct label subsets, improving label correlation handling.

In terms of text representation, as expected, IndoBERT outperformed Word2Vec as a word embedding model due to its architectural design. Word2Vec, using the CBOW architecture with a fixed window produces static embeddings, which lack contextual information. In contrast, IndoBERT generates contextualized embeddings by learning from masked tokens, capturing semantic relationships and nuances. This contextual richness allows IndoBERT to provide more refined input vectors, enabling the Gaussian NB classifier to more accurately classify aspect-sentiment labels. IndoBERT[k] performed worse than the baseline Word2Vec, indicating that contextualized embeddings don't always outperform static embeddings, as seen in study [36]. The varying performance among IndoBERT variants may stem from differences in pre-training datasets. IndoBERT[k], trained primarily on formal text, struggles with the informal language in product reviews. In contrast, IndoBERT[b] and IndoBERTweet, pre-trained on informal data like social media, are better equipped to handle the mixed linguistic style found in the reviews.

Given that multi-label classification can be performed directly using pre-trained language models as end-to-end model, this paper proposes using IndoBERT and IndoBERTweet for classification, as these two pre-trained language models have demonstrated high accuracy in terms of text representation. The results show that the proposed end-to-end model significantly outperformed the conventional multi-label models. These findings align with outcomes from [9] and [15], suggesting that IndoBERT generalizes multi-label classification tasks better than conventional models. This is likely due to the architectural differences between IndoBERT and traditional classifiers. IndoBERT, using neural networks, is more complex, flexible, and better equipped to handle intricate patterns in the dataset compared to simpler linear, tree-based, or probabilistic classifiers like SGD, SVM, RF, and Gaussian NB [37].

For conventional multi-label models, it can be observed that a similar trend of classifier performance was exhibited across multi-label transformation approach and word embedding. Notably, SVM consistently demonstrated superiority in correctly multi-classifying labels, followed by linear SGD, RF and Gaussian NB. These results aligned with classification results for two out of three datasets in the study of [9], which found that SVM outperformed linear SGD, followed by RF, regardless of whether LP or Rakel D was used.

VI. Conclusion

This study developed a reliable multi-label ABSC model while exploring the performance of contextual word embedding in representing words from the Indonesian cosmetic domain. Three experimental experiments evaluated different multi-label classification approaches. The results showed that IndoBERT[b] and IndoBERTweet provided more refined text representation, improving performance approximately by 2% to 6% compared to Word2Vec. The findings also demonstrated that multi-label models using IndoBERT as an end-to-end model outperformed conventional methods. IndoBERT[b] achieved the best accuracy of 86.98%, showing a 17.34% to 30.27% improvement over the baseline, confirming its superiority for multi-label classification in this domain. Although this study demonstrated notable improvements, certain limitations remain. The study investigated only one type of contextual embedding model, IndoBERT. To further enhance the multi-label model, future work could explore other contextual embeddings, such as DistilBERT and RoBERTa. Additionally, the hyperparameter settings for the end-to-end IndoBERT model were restricted to "learning rate = 2e-5, batch size = 8, and epoch = 5." Future research could experiment with different hyperparameter combinations, as there is no one-size-fits-all setting for optimizing the model.

Acknowledgment

The authors would like to acknowledge the Ministry of Higher Education (MoHE) for supporting this research through the Fundamental Research Grant Scheme (FRGS), under grant number FRGS/1/2020/ICT02/UKM/02/1.

References

[1] [A. Berg and S. Hudson, “The beauty market in 2023: A special state of Fashion report,” May 2023. Accessed: May 14, 2024. [Online]. Available: https://www.mckinsey.com/industries/retail/our-insights/the-beauty-market-in-2023-a-special-state-of-fashion-report#/

[2] Satista, “Cosmetics - Indonesia.” Accessed: May 23, 2024. [Online]. Available: https://www.statista.com/outlook/cmo/beauty-personal-care/cosmetics/indonesia

[3] K. Saleh, “The importance of online customer reviews,” Invesp. Accessed: Apr. 24, 2024. [Online]. Available: https://www.invespcro.com/blog/the-importance-of-online-customer-reviews-infographic/

[4] Boxwell, “Why customer reviews are important for business,” Boxwell. Accessed: Apr. 24, 2024. [Online]. Available: https://boxwell.co/why-customer-reviews-are-important-for-business/#:~:text=86%25%20of%20people%20will%20hesitate,increase%20in%20a%20business’s%20revenue.&text=Customer%20reviews%2C%20whether%20it’s%20a,inspire%20confidence%20in%20your%20brand.

[5] D. S. Asudani, N. K. Nagwani, and P. Singh, “Impact of word embedding models on text analytics in deep learning environment: a review,” Artif Intell Rev, vol. 56, no. 9, pp. 10345–10425, Sep. 2023, doi: 10.1007/s10462-023-10419-1.

[6] K. Ethayarajh, “How contextual are contextualized word representations? Comparing the geometry of BERT, ELMo, and GPT-2 embeddings,” in Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), Stroudsburg, PA, USA: Association for Computational Linguistics, 2019, pp. 55–65. doi: 10.18653/v1/D19-1006.

[7] N. Lakshmidevi, S. Keshari Swain, and M. Vamsikrishna, "A hybrid enhancing aspect-based sentiment analysis with BERT for aspect extraction and diverse ml classifiers," in 2023 International Conference on Network, Multimedia and Information Technology, NMITCON 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/NMITCON58196.2023.10275957.

[8] Y. Peng, S. Yan, and Z. Lu, "Transfer learning in biomedical natural language processing: An evaluation of BERT and ELMo on ten benchmarking datasets," in Proceedings of the 18th BioNLP Workshop and Shared Task, Stroudsburg, PA, USA: Association for Computational Linguistics, 2019, pp. 58–65. doi: 10.18653/v1/W19-5006.

[9] J. Tao and X. Fang, "Toward multi-label sentiment analysis: a transfer learning based approach," J Big Data, vol. 7, no. 1, Dec. 2020, doi: 10.1186/s40537-019-0278-0.

[10] F. Koto, A. Rahimi, J. H. Lau, and T. Baldwin, "IndoLEM and IndoBERT: A benchmark dataset and pre-trained language model for Indonesian NLP," Online, 2020. [Online]. Available: https://huggingface.co/

[11] B. Wilie et al., "IndoNLU: Benchmark and resources for evaluating Indonesian natural language understanding," 2020. [Online]. Available: https://github.com/annisanurulazhar/absa-playground

[12] F. Koto, J. H. Lau, and T. Baldwin, "IndoBERTweet: A pretrained language model for Indonesian Twitter with effective domain-specific vocabulary initialization," in Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing, 2021, pp. 10660–10668. [Online]. Available: https://huggingface.co/huseinzol05/

[13] P. R. Amalia and E. Winarko, "Aspect-based sentiment analysis on Indonesian restaurant review using a combination of convolutional neural network and contextualized word embedding," IJCCS (Indonesian Journal of Computing and Cybernetics Systems), vol. 15, no. 3, pp. 285–294, Jul. 2021, doi: 10.22146/ijccs.67306.

[14] C. B. P. Putra, D. Purwitasari, and A. B. Raharjo, "Stance Detection on Tweets with Multi-task Aspect-based Sentiment: A Case Study of COVID-19 Vaccination," International Journal of Intelligent Engineering and Systems, vol. 15, no. 5, pp. 515–526, Oct. 2022, doi: 10.22266/ijies2022.1031.45.

[15] N. K. Nissa and E. Yulianti, "Multi-label text classification of Indonesian customer reviews using bidirectional encoder representations from transformers language model," International Journal of Electrical and Computer Engineering, vol. 13, no. 5, pp. 5641–5652, Oct. 2023, doi: 10.11591/ijece.v13i5.pp5641-5652.

[16] A. Jazuli, Widowati, and R. Kusumaningrum, "Aspect-based sentiment analysis on student reviews using the Indo-Bert base model," E3S Web of Conferences, vol. 448, p. 02004, Nov. 2023, doi: 10.1051/e3sconf/202344802004.

[17] N. Mahfudiyah and A. Alamsyah, "Understanding user perception of ride-hailing services sentiment analysis and topic modelling using IndoBERT and BERTopic," in 2023 International Conference on Digital Business and Technology Management, ICONDBTM 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICONDBTM59210.2023.10327320.

[18] H. Imaduddin, F. Yusfida A'la, and Y. S. Nugroho, "Sentiment analysis in Indonesian healthcare applications using IndoBERT approach," 2023. [Online]. Available: www.ijacsa.thesai.org

[19] E. I. Setiawan, L. Kristianto, A. T. Hermawan, J. Santoso, K. Fujisawa, and M. H. Purnomo, "Social media emotion analysis in Indonesian using fine-tuning BERT model," in 3rd 2021 East Indonesia Conference on Computer and Information Technology, EIConCIT 2021, Institute of Electrical and Electronics Engineers Inc., Apr. 2021, pp. 334–337. doi: 10.1109/EIConCIT50028.2021.9431885.

[20] L. F. Simanjuntak, R. Mahendra, and E. Yulianti, "we know you are living in Bali: Location prediction of Twitter users using BERT language model," Big Data and Cognitive Computing, vol. 6, no. 3, Sep. 2022, doi: 10.3390/bdcc6030077.

[21] N. Endut, W. M. A. F. W. Hamzah, I. Ismail, M. Kamir Yusof, Y. Abu Baker, and H. Yusoff, "A systematic literature review on multi-label classification based on machine learning algorithms," TEM Journal, vol. 11, no. 2, pp. 658–666, May 2022, doi: 10.18421/TEM112-20.

[22] H. Setiawan, C. Fatichah, and A. Saikhu, "Multilabel classification of student feedback data using BERT and machine learning methods," in 2023 14th International Conference on Information and Communication Technology and System, ICTS 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 147–152. doi: 10.1109/ICTS58770.2023.10330849.

[23] R. K. Shah, S. Kumar, and Shashank, "Multilabel news category classification using machine learning," in Proceedings of the 8th International Conference on Communication and Electronics Systems, ICCES 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1245–1250. doi: 10.1109/ICCES57224.2023.10192826.

[24] N. K. Singh and S. Chand, "Machine learning-based multilabel toxic comment classification," in 3rd IEEE 2022 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 435–439. doi: 10.1109/ICCCIS56430.2022.10037626.

[25] J. Ashok Kumar, S. Abirami, and T. E. Trueman, "Multilabel aspect-based sentiment classification for abilify drug user review," in Proceedings of the 11th International Conference on Advanced Computing, ICoAC 2019, Institute of Electrical and Electronics Engineers Inc., Dec. 2019, pp. 376–380. doi: 10.1109/ICoAC48765.2019.246871.

[26] Z. Jin, X. Lai, and J. Cao, "Multi-label sentiment analysis base on BERT with modified TF-IDF," in 2020 IEEE International Symposium on Product Compliance Engineering-Asia (ISPCE-CN), IEEE, Nov. 2020, pp. 1–6. doi: 10.1109/ISPCE-CN51288.2020.9321861.

[27] R. Rivaldo, A. Amalia, and D. Gunawan, "Multilabeling Indonesian toxic comments classification using the Bidirectional Encoder Representations of Transformers model," in 2021 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA), IEEE, Nov. 2021, pp. 22–26. doi: 10.1109/DATABIA53375.2021.9650126.

[28] C. H. Yutika, A. Adiwijaya, and S. Al Faraby, "Analisis sentimen berbasis aspek pada review Female Daily menggunakan TF-IDF dan Naïve Bayes [Aspect-based sentiment analysis on Female Daily reviews using TF-IDF and Naïve Bayes]," Jurnal Media Informatika Budidarma, vol. 5, no. 2, p. 422, Apr. 2021, doi: 10.30865/mib.v5i2.2845.

[29] C. C. P. Hapsari, W. Astuti, and M. D. Purbolaksono, "Naive Bayes Classifier and Word2Vec for sentiment analysis on Bahasa Indonesia cosmetic product reviews," in 2021 International Conference on Data Science and Its Applications, ICoDSA 2021, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 22–27. doi: 10.1109/ICoDSA53588.2021.9617544.

[30] N. P. Arthamevia, Adiwijaya, and M. D. Purbolaksono, "Aspect-based sentiment analysis in beauty product reviews using TF-IDF and SVM algorithm," in 2021 9th International Conference on Information and Communication Technology, ICoICT 2021, Institute of Electrical and Electronics Engineers Inc., Aug. 2021, pp. 197–201. doi: 10.1109/ICoICT52021.2021.9527489.

[31] I. Salsabila and Y. Sibaroni, "Multi aspect sentiment of beauty product reviews using SVM and semantic similarity," Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 5, no. 3, pp. 520–526, Jun. 2021, doi: 10.29207/resti.v5i3.3078.

[32] S. Liviani Mahfiz and A. Romadhony, "Aspect-based opinion mining on beauty product reviews," 2020, [Online]. Available: https://github.com/syitilv/Opinion-Mining

[33] M. R. Mahardika, I. P. J. Wijaya, A. R. Prayoga, H. Lucky, and I. A. Iswanto, "Exploring the performance of BERT models for multi-label hate speech detection on Indonesian Twitter," in 2023 4th International Conference on Artificial Intelligence and Data Sciences: Discovering Technological Advancement in Artificial Intelligence and Data Science, AiDAS 2023 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 256–261. doi: 10.1109/AiDAS60501.2023.10284596.

[34] A. Kleczewski, "Multilabel classification using a classifier chain," Scikit learn. Accessed: May 08, 2024. [Online]. Available: https://scikit-learn.org/stable/auto_examples/multioutput/plot_classifier_chain_yeast.html#multilabel-classification-using-a-classifier-chain

[35] Serafín. Moral-García, J. G. Castellano, C. J. Mantas, and J. Abellán, "A new label ordering method in Classifier Chains based on imprecise

probabilities," Neurocomputing, vol. 487, pp. 34–45, May 2022, doi: 10.1016/j.neucom.2022.02.048.

[36] P. C.-I. Pang, "Performance evaluation of text embeddings with online consumer reviews in retail sectors," in 2022 IEEE/ACIS 22nd International Conference on Computer and Information Science (ICIS), IEEE, Jun. 2022, pp. 170–175. doi: 10.1109/ICIS54925.2022.9882478.

[37] F. Mota, "Gradient Boosted Machines vs. Transformers (the BERT Model) with KNIME," Medium. Accessed: May 11, 2024. [Online].

[38] S. Alshattnawi, A. Shatnawi, A. M. R. AlSobeh, and A. A. Magableh, "Beyond word-based model embeddings: Contextualized representations for enhanced social media spam detection," Applied Sciences, vol. 14, no. 6, p. 2254, Mar. 2024, doi: 10.3390/app14062254.

CCNet: CNN CapsNet-Based Hybrid Deep Learning Model for Diagnosing Plant Diseases Using Thermal Images

Hassan Al_Sukhni[1], Qusay Bsoul[2], Rami Hasan AL-Ta'ani[3], Fadi yassin Salem Al jawazneh[4], Basma S. Alqadi[5], Misbah Mehmood[6], Asif Nawaz[7], Tariq Ali[8] , Diaa Salama AbdElminaam*[9]
Cybersecurity Department-Faculty of Science and Information Technology, Jadara University, Irbid, Jordan[1]
Cybersecurity Department-College of Computer Sciences and Informatics, Amman Arab University, Amman, 11953, Jordan[2]
Department of Software Engineering, Zarqa University, Zarqa, Jordan[3]
Faculty of Information Technology, Applied Science Private University, Amman 11931, Jordan[4]
Computer Science Department-College of Computer and Information Sciences,
Al Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia[5]
University Institute of Information Technology, PMAS Arid Agriculture University, Rawalpindi, 46000, Pakistan[6, 7, 8]
MEU Research Unit, Middle East University, Amman 11831, Jordan[9]
Jadara Research Center, Jadara University, Irbid, 21110[9]

***Abstract*—Plant disease diagnosis at an early stage enables farmers, gardeners and agricultural experts to manage and control the spread of illnesses in a timely and suitable manner. The traditional methods of plant disease diagnosis are expensive and might need significant manpower and advanced level machinery. In addition to that, conventional methods, such as visual inspections are prone to subjectivity, time constraints and error susceptibility. In comparison to that, computer based methods such as machine learning is accurately predicting plant diseases underscore the need for a transformative approach. However, by focusing solely on visualized contents and thermal images, these methods overlook the potential insights hidden within customer-posted images that may leads to low accuracy. This study is an attempt to addresses these gaps by proposing an alternative methodology which relies on a hybrid deep learning framework called CCNET. The core CCNET is the utilization of the superiorities of Convolutional Neural capsule network models to get better architecture for plant diseases diagnosis. The proposed CCNET effectively amalgamates the strengths of convolutional layers for spatial feature extraction and the sequential modelling capabilities of CNN and CapsNet for capturing temporal dependencies within image data. The performance of the CCNET has been evaluated through rigorous experimentation. The outcomes underscore the remarkable prowess of the proposed model with the accuracy of 94%. When it compared to the conventional methods, the CCNET surpasses all of them in terms of precision, recall, F-Score, and accuracy.**

***Keywords*—CapsNet; classification; CNN; feature extraction; plant disease; thermal images**

I. Introduction

The agricultural industry holds immense significance for numerous nations globally, serving as a crucial source of sustenance, materials and energy to support the expanding population. Apart from its economic value, agriculture plays a pivotal role in addressing pressing global issues such as climate change, ensuring food security, and promoting sustainable development. As per the Food and Agriculture Organization of the United Nations (FAO), agriculture engages over one billion individuals worldwide and contributes approximately 3% to the overall global gross domestic product (GDP) [1].

However, this sector encounters noteworthy obstacles, including the imperative to augment food production to fulfill the rising needs of the world's growing inhabitants. While concurrently mitigating the environmental impact associated with agricultural practices. Additionally, the prevalence of plant diseases poses a substantial menace to agricultural productivity, leading to crop losses that range from 10% to 40% on a global scale [2]. Plant diseases can cause extensive damage to crop, resulting in significant economic losses for farmers worldwide. Fig. 1 shows the typical leave disease that effect the production of plant. As per the Food and Agriculture Organization (FAO) of the United Nations, plant diseases account for the annual loss of approximately 20–40% of global crop production [3]. An efficient and effective plant disease management system is therefore essential for ensuring the sustainability and productivity of the agriculture sector.

Fig. 1. Leaf disease example adopted from study [5].

*Corresponding Author

The conventional farm management practices rely on human experts to monitor plants in the field for signs of disease, which can be time-consuming, labor-intensive and prone to errors. However, visual symptoms of plant diseases usually appear several days after infection, indicating that the illness has already disseminated and the quality of yield has declined, leading to significant losses in productivity [4]. Most of the disease control process usually adopted appropriate control measures, such as the utilization of resilient crop strains, farming techniques and chemical treatments. But due to the increasing number of diseases and expensive chemical, this job become quiet hectic and time consuming.

Alternative to the conventional methods, Smart farm management practices, which rely on vision technology and machine learning, have revolutionized plant disease management by allowing for early detection and prevention of crop losses. According to a study [6], smart farm management practices have led to increased agricultural productivity and improved food security in many countries. These technologies are particularly useful in remote areas where access to expert knowledge and resources is limited. By implementing these practices, farmers can detect plant diseases before visual symptoms appear, ultimately increasing crop yields and contributing to the overall economic growth of the country.

The development and adoption of new technologies, including the use of computer science and artificial intelligence, can be better attempt that helps in the timely identification and control of plant diseases. Vision technology, which is widely used in modern smart farm management practices, has the potential to address some of these challenges by processing and analysing images of infected plants to identify disease patterns [7]. However, this approach is limited in that it does not accomplish early detection, presuming that plants are still in the incubation phase prior to the disease's manifestation [8]. This highlights the need for alternative approaches that can detect diseases at an early stage, before visible symptoms appear, to prevent significant crop losses and increase productivity.

However, the variations of diseases at different of plants and temperature discrepancies in the infected plants that are imperceptible to the human eye may require more sophisticated mechanism [9]. The application of thermal imaging as depicted in Fig. 2, in plant disease management has emerged as a promising approach for early detection and control of diseases. By recording the temperature of plants, thermal imaging enables the identification of temperature changes that can indicate the presence of disease. These temperature changes are a result of internal chemical alterations that occur in plants following disease inoculation. Analysing these temperature variations allows for the early detection of diseases before visible symptoms manifest.

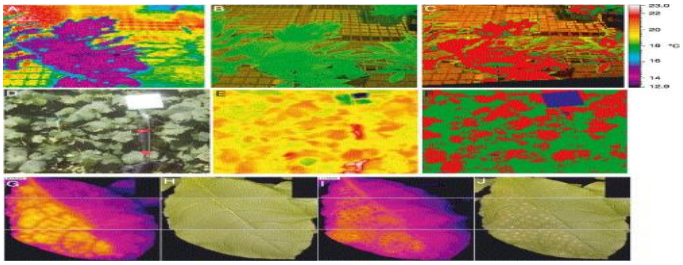


Fig. 2. The Geo-informatics-based view of plant thermal images.

It is concluded that thermal imaging and machine learning technologies have the potential to revolutionize plant disease management and increase crop productivity by predicting and preventing the spread of plant diseases. This research addresses the above discussed gaps by proposing an alternative methodology that is based on hybrid deep learning model called CCNET. The core CCNET is the utilization of the superiorities of Convolutional Neural Network-Gated Recurrent, Bidirectional Long Short-Term Memory and Conditional Random Field models to get better architecture for plant diseases diagnosis from thermal images. The proposed CCNET effectively amalgamates the strengths of convolutional layers for spatial feature extraction and the sequential modelling capabilities of CNN and CapsNet for capturing temporal dependencies within image data.

A. *Research Contribution*

The key contribution of the proposed research are as follows:

1) The proposed CCNET is an attempt to efficiently diagnosing plant disease by using thermal images that perform detection at early stage before visible symptoms appear that is not tackled in the previous literature to prevent significant crop losses.

2) The utilization of advance level deep learning methods such as CNN and CapsNet provide better identification as compared to machine learning algorithms that are based on static similarity measures.

3) Experimental evaluation on thermal imaging and comparative analysis with benchmark methods has proved that the performance of proposed CCNET surpasses the existing works by obtaining an accuracy of 94 %.

The rest of the paper is organized as follows: An overview of the relevant research is presented in Section II. The proposed CCNET is briefly described in Section III. The experimental evaluation and discussion has been discussed in Section IV. The conclusion and future work are given in Section V.

II. Related Work

The utilization of digital images for the categorization of plant diseases presents a significant hurdle. However,

advancements in machine learning techniques, particularly deep learning, have facilitated the identification, detection, and diagnosis of plant diseases. In the article [10], a combined model is proposed that merges two pre-trained convolutional neural networks (CNNs), specifically VGG16 and VGG19, to classify images of healthy and diseased leaves for the purpose of diagnosing plant diseases. CNNs are employed due to their capacity to overcome the technical intricacies associated with the classification of plant diseases. Nonetheless, CNNs pose a challenge in terms of hyper parameters, necessitating manual identification of specific architectures to attain optimal performance. To tackle this challenge, the paper utilizes the orthogonal learning particle swarm optimization (OLPSO) algorithm to optimize the hyper parameters by determining the optimal values instead of relying on traditional trial and error methods.

In another work, specifically focuses on charcoal rot, a fungal disease that affects soybean crops globally and is transmitted through soil [11]. In their study, the authors propose a unique 3D deep convolutional neural network (DCNN) that directly incorporates hyper spectral data and provides meaningful physiological explanations through model interrogation. Their proposed model achieves an impressive classification accuracy of 95.73% and an infected class F1 score of 0.87 when analysing hyper spectral images of both inoculated and mock-inoculated stem samples. By employing an explainable deep learning model, the study not only achieves high accuracy but also provides valuable physiological insights into the model's predictions, thereby increasing confidence in the reliability of these predictions.

The work of study [12] provide a comprehensive overview of the existing literature on neural network techniques that are employed for processing image data in the detection of crop diseases. They claim that predictions are particularly relevant for precision agriculture and research applications that utilize automated phenotyping platforms. The goal of this survey is to enhance the performance and accuracy of deep learning in detecting plant diseases, with the potential to significantly impact sustainable agriculture. Hyper spectral imaging has emerged as a potent tool for plant disease identification, but its effectiveness heavily relies on the choice of deep learning models. Convolutional neural networks (CNNs) have been identified as the most promising models for diagnosing and predicting crop infections.

TABLE I. COMPARATIVE ANALYSIS OF THE EXISTING RESEARCH METHODS

Reference	Methodology	Data Set	Accuracy	Limitations
[15]	Support Vector Machines (SVM)	Thermal images	90%	The study was only conducted on wheat crops under moisture stress conditions, which limits the generalizability of the findings to other crops and growing conditions.
[16]	Support vector machine (SVM), Gaussian kernel and Random Forest	High-resolution thermal image	82%	Only evaluates model accuracy for detecting decline, not effectiveness of management interventions, and is geographically specific.
[17]	Feature weighted random forest (FWRF)	27 olive orchards	92%	Study's insights on olive orchards affected by Xf and Vd outbreaks in 2011-2017 Italy and Spain may not apply to other regions or timeframes.
[18]	Multiple Linear Regression (MLR)	IoT-sensed crop Dataset	91%	Restricted to blister blight in tea plants, doesn't address other diseases, and relies on IoT sensor accuracy for environmental data.
[19]	Dual-stream hierarchical bilinear pooling model	Field-obtained dataset	84.71%	The study only demonstrates accuracy in identifying plants and diseases on a specific field dataset, with uncertain generalizability to other crops or datasets.
[20]	14-DCNN	147,500 images of 58 different healthy and diseased plant lea.	91.79%	Does not discuss the real-world application and the limitations that the proposed model may face when deployed in the actual environment.

Gadekallu et al. [13] emphasizes the importance of ensuring a consistent supply of healthy food for the growing global population, as well as the economic significance of agriculture in developing countries. To overcome these challenges, their study focuses on harnessing the power of machine learning models to classify tomato diseases, with the aim of proactively addressing agricultural crises. Their research utilized a publicly available dataset from plant-village to train and evaluate their model. They employed a hybrid approach that combines dimensionality reduction method. The extracted features were then fed into a deep neural network for the classification of tomato diseases. To demonstrate the effectiveness of their proposed model, they compared their work with traditional machine learning techniques, showcasing its superior performance in terms of accuracy and loss rate metrics.

The utilization of automated approaches, such as machine learning and deep learning, for the prediction of plant species and diseases has been explored in the work of study [14]. In addition to this they also proposed a novel multi-task learning strategy, which leverages shared representations between these related tasks to enhance overall performance. Their proposed approach utilizes a multi-input network that incorporates raw images and transferred deep features extracted from a pre-trained deep model to predict both the plant's type and disease. An end-to-end multi-task model is developed, enabling the simultaneous execution of multiple learning tasks by integrating Convolutional Neural Network (CNN) features and transferred features. This approach has the potential to address the challenges associated with plant species and disease prediction by providing accurate predictions, reducing the time and cost required for manual prediction, and guiding decision-making processes in the context of sustainable agriculture.

From the above discussion, it has been concluded that, instead of traditional diagnosis methods that are hectic, expensive, and time-consuming, machine learning models perform better disease diagnosis. However, the detection of diseases at an early stage is still challenging. By foreseeing and halting the development of plant illnesses, thermal imaging, and machine learning technologies hold the promise of revolutionizing plant disease management and boosting

agricultural output. This research tries to fills the gaps of previously mentioned literature by giving an improved architecture by utilizing the advantages of Convolutional Neural Network-Gated Recurrent, Bidirectional Long Short-Term Memory, and Conditional Random Field models.

III. MATERIALS AND METHODS

This section discusses the proposed CCNET's core methodology, which is composed of data collection, pre-processing, feature extraction, and final classification. Fig. 3 depicts the diagrammatic flow of the proposed CCNET.

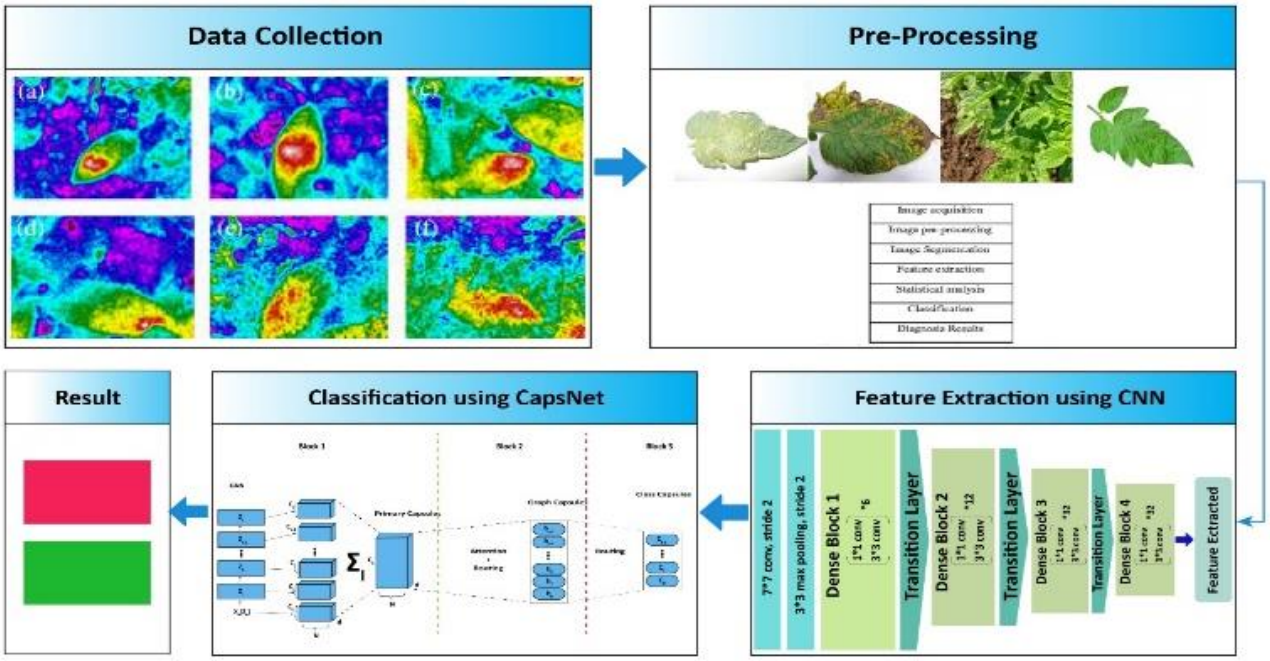


Fig. 3. The CCNET architecture for plant disease detection.

A. Data Collection and Description

In this research, thermal image-based datasets that are publicly available on the Kaggle repository have been used. The first dataset, DS-I, encompasses roughly 87,000 RGB images of plant leaves, categorized into 38 distinct health-related classes. Offline augmentation techniques were employed during its construction to ensure both authenticity and diversity. A separate collection comprising 33 test images was also established solely for predictive purposes. Another dataset that is DS-II, has 1132 images that focus on corn and maize leaf disease, derived from reputable sources like Plant Village and Plant Doc, meticulously tailored to address issues related to corn or maize leaf diseases.

The last dataset is DS-III, which contains 1401 images of rice leaf diseases. This dataset holds particular significance for regions characterized by low to lower-middle-income economies, where rice is crucial to food security. This dataset serves as a comprehensive compilation of crop leaf images, offering researchers in the agricultural science domain an opportunity to utilize it for further examination and exploration. The availability of such a dataset can facilitate the development of robust and precise models, aiding in the detection and classification of crop diseases and empowering farmers to identify such diseases at an early stage, thereby mitigating potential crop yield losses.

B. Pre-processing

After the formation of the dataset, the very next phase is the pre-processing. Algorithm 1 outlines the proposed pre-processing procedure. Initially, images are resized to a consistent dimension of 256x256 pixels. Pixel values are normalized via min-max normalization, representing pixel (x, y). Each image is randomly rotated within a defined angle range, and random horizontal or vertical flips are applied. A random zoom transformation is also employed. Additionally, images are converted to grayscale. Data is then organized into batches and shuffled using a randomized seed for training randomness assurance.

Algorithm 1: The Data Pre-Processing

```
def preprocess_image(image):
    resized = resize(image, (256, 256))
    normalized = (resized - np.min(resized)) / (np.max(resized) - np.min(resized))
    rotated = rotate(normalized, random.uniform(-30, 30))
    flipped = np.fliplr(rotated) if random.choice([True, False]) else np.flipud(rotated)
    zoomed = zoom(flipped, random.uniform(0.8, 1.2))
    grayscale = rgb2gray(zoomed)
    return grayscale
random.seed(42)
preprocessed_data = [preprocess_image(image) for image in original_data]
random.shuffle(preprocessed_data)
batches = [preprocessed_data[i:i+batch_size] for i in range(0, len(preprocessed_data), batch_size)]
```

By applying these pre-processing steps, the dataset is prepared in a format that can be effectively utilized for training deep learning models. Resizing the images ensures that the models can handle images of different sizes, while normalization and data augmentation techniques help enhance the dataset's diversity and reduce overfitting [21]. Finally, batching and shuffling the data enable efficient model training.

C. Feature Extraction

There exist too many deep learning models that are used for image based feature extraction. However, convolutional neural networks (CNNs) are the most demanding due to their exceptional ability to capture hierarchical patterns and spatial dependencies in images [22-26]. In the proposed CCNET, the CNN model starts with the convolution operation, where the dot product is calculated between input image patches and adaptable filter weights, uncovering specific attributes within localized areas as shown in Fig. 4. Subsequently, the Pooling operation comes into play, particularly Max pooling. This technique is renowned for its efficiency, selectively highlighting the highest value within a predefined window, distilling the essential information while retaining the core of the data. The process culminates with flattening, a transformative step that restructures pooled feature maps into a streamlined one-dimensional vector. This sequence effectively transforms raw images into compact yet enriched features, crucial for subsequent analytical processes.

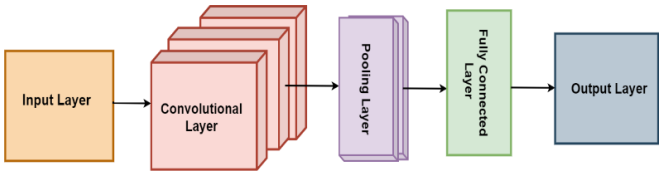


Fig. 4. The feature extraction workflow using CNN.

D. Classification

In comparison to the traditional CNN, Capsule Networks (CapsNet), is an alternative architecture for image classification. CapsNet was introduced by Geoffrey Hinton and his colleagues in 2017 [27-34] and was designed to address some of the limitations of CNNs, especially when it comes to handling spatial hierarchies, pose variations, and viewpoint changes. The CapsNet is a layered network in which the first layer of a Capsule Network typically consists of primary capsules. Each primary capsule is responsible for detecting a particular visual feature along with it numeric values in an image. Instead of using convolutional layers like CNNs, Capsule Networks use a combination of convolutional layers and capsules. These capsules output a vector representing a specific feature's presence along with its pose information. Whereas the pose estimation layer handles variations in the pose (position, orientation, etc.) of the detected features. Each capsule outputs a vector representing the probability of the feature's presence and pose parameters (such as position and orientation). The architecture is shown in Fig. 5.

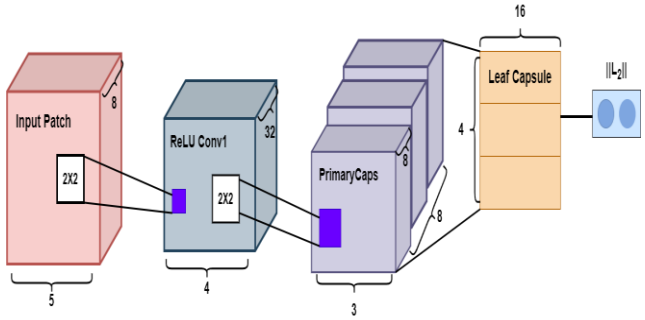


Fig. 5. The typical CapNet architecture for thermal image classification.

One of the key innovations of CapsNet is the routing algorithm. This algorithm aims to find the agreement between capsules in one layer and capsules in the subsequent layer. It ensures that capsules with similar features and poses "agree" with their predictions. This process helps to establish a more coherent and dynamic representation of hierarchical features. In addition to this, dynamic routing involves iterative updates of the coupling coefficients between capsules in different layers. This process encourages capsules that agree to have higher coupling coefficients, while capsules that disagree have lower coefficients. It allows the network to learn better feature hierarchies and spatial relationships. The final layer of capsules is used for classification. Each capsule in this layer represents a specific class, and the length of the capsule's output vector indicates the probability of the image belonging to that class.

IV. Experimental Results

This section thoroughly examines the experimental analysis and evaluates the proposed methodology. The proposed CCNET has been evaluated on three different datasets already discussed in the data collection section. It has also been compared with three baseline techniques and five machine learning models to test its accuracy and efficiency through a series of rigorous experiments.

A. Baseline Method

The following baseline reference models have been considered for comparison and evaluation of efficiency.

1) Banerjee et al. [24]: This study employed thermal imaging technology to capture images of wheat crop canopies and aimed to estimate the leaf area index (LAI) under varying moisture stress conditions. Their method was based on Maximum Likelihood Estimation, Box Classifier, and Support Vector Machines.

2) Poblete et al. [25]: They employed a Feature Weighted Random Forest (FWRF) classification model on olive orchards affected by specific outbreaks (Xf and Vd) in a limited timeframe and region might restrict the generalizability of its findings to other areas and time periods.

3) Zhiyan Liu [26]: This study focused on IoT-sensed crop fields, specifically addressing blister blight in tea plants with the utilization of multiple linear regression (MLR).

B. Results

Fig. 6 shows a comprehensive overview of the experimental results of CCNET on three distinct datasets—DS-I, DS-II and DS-III. On DS-I, the CCNET achieved 0.92 accuracy, 0.91 precision and 0.90 recall indicating that the model is enough capable to correctly predict plant disease. Whereas for DS-II, the accuracy remains high at 0.93, signifying the model's consistent ability to make accurate predictions across different datasets. In the last, the accuracy on DS-III is 0.94, indicating that the model remains robust in different plant health contexts. Whereas, the precision score is 0.92, suggesting that the model effectively predicts plant diseases without excessive false positives. Based on this measure, the predicted ROC curve is also demonstrated in Fig. 7 to clearly mention the superiority of CCNET.

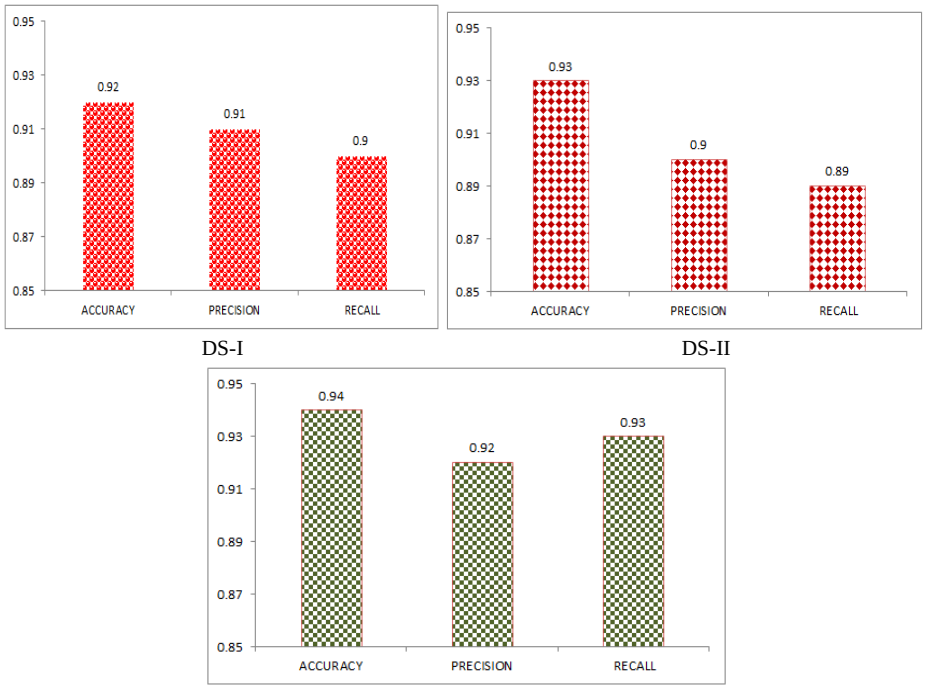


Fig. 6. Experimental results of CCNET in terms of precision, recall and accuracy.

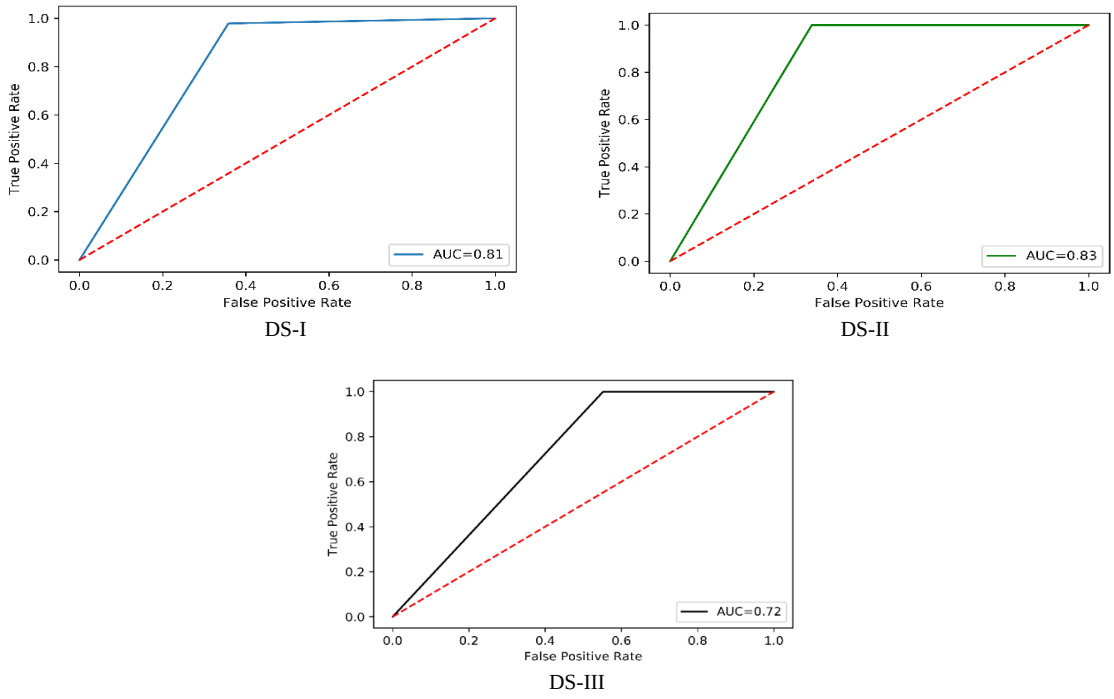


Fig. 7. ROC curves on DS 1, DS II and DS III.

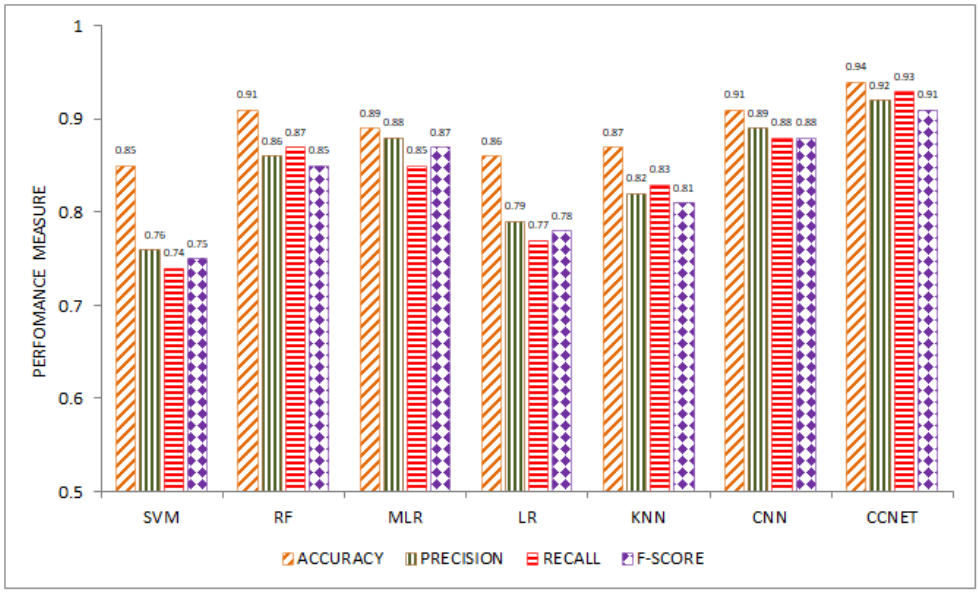


Fig. 8. Comparison of CCNET with machine learning models.

Fig. 8 presents a comprehensive comparative analysis between the proposed CCNET techniques and with standard machine learning model. The graphical values show that CCNET achieves a remarkable performance with 0.92 precision, 0.93 recall, 0.91 F1-Score and 0.94 Accuracy. This results shows that the CCNET gets a significant fraction of correctly identified positive instances in relation to the total actual positive instances.

In the last experiment, a thorough comparison of the CCNET with baseline methods was conducted by using DS-I, DS-II and DS-III to assess the accuracy. The graphical demonstration at Fig. 9 shows the superiority of the CCNET by beating the baseline with the variation of 6%, 7% and 9% respectively.

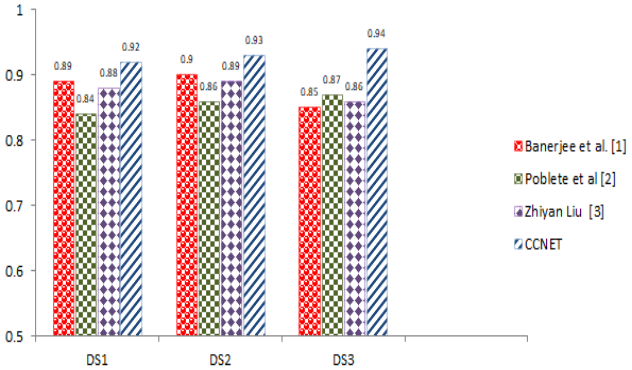


Fig. 9. Experimental analysis of CCNET with baseline models.

V. Conclusion

Plant disease diagnosis at early stages enables farmers to manage and control the spread of diseases in a timely and appropriate manner. Traditional methods for diagnosing plant diseases are costly and may necessitate a large number of personnel and sophisticated equipment. In addition, conventional methods, including visual inspections, are subject to subjectivity, time constraints, and error susceptibility. Whereas, the machine learning models based solution are limited to thermal images and leads to poor accuracy. In this research, a new model CCNET based on deep learning model has been proposed. The key steps of CCNET are data collection of thermal images, feature extraction and CapsNet based final classification. The evaluation of CCNET has been performed on three different datasets. The experimental results and comparative analysis provides a compelling evidence of the significant potential CCNET. The results demonstrate that the CCNET gets high accuracy with the value of 0.94, 0.93 and 0.92 on three different datasets and beat the base line methods with the variation of 6%, 7% and 9%. Looking forward, future research should concentrate on integrating multiple imaging modalities, such as hyperspectral or multispectral data, to further heighten disease detection accuracy. Expanding the training dataset to encompass a broader range of diseases and addressing class imbalances will bolster the model's generalization and robustness. Additionally, incorporating contextual information, developing interpretability techniques, and optimizing the model for real-time implementation are pivotal areas for advancement.

Acknowledgment

This research funded by the Deanship of Research in Zarqa University/Jordan

References

[1] Food and Agriculture Organization of the United Nations, "The future of food and agriculture - Trends and challenges," FAO, 2020. [Online]. Available: http://www.fao.org/3/ca9692en/CA9692EN.pdf.

[2] S. Savary, L. Willocquet, S. J. Pethybridge, P. Esker, N. McRoberts, and A. Nelson, "The global burden of pathogens and pests on major food crops," *Nature Ecology & Evolution*, vol. 3, no. 3, pp. 430-439, 2019, doi: 10.1038/s41559-018-0793-y.

[3] M. M. Rahman, M. Z. Islam, M. S. Islam, M. M. Rahman, M. T. Islam, and M. M. Molla, "Precision agriculture and smart farm: A review on

agriculture 4.0," *Precision Agriculture*, vol. 21, no. 4, pp. 803-830, 2020, doi: 10.1007/s11119-019-09724-5.

[4] M. Fuxreiter, I. Simon, and S. Bondos, "Dynamic protein-DNA recognition: beyond what can be seen," *Trends in Biochemical Sciences*, vol. 36, no. 8, pp. 415-423, 2011, doi: 10.1016/j.tibs.2011.04.006.

[5] A. A. Adedeji et al., "Non-Destructive Technologies for Detecting Insect Infestation in Fruits and Vegetables under Postharvest Conditions: A Critical Review," *Foods*, vol. 9, no. 7, p. 927, 2020, doi: 10.3390/foods9070927.

[6] S. Gull et al., "A review on thermal imaging for disease detection in plants," *Computers and Electronics in Agriculture*, vol. 165, p. 104943, 2019, doi: 10.1016/j.compag.2019.104943.

[7] A. M. Siddiqui, S. M. Nizamani, and T. R. Soomro, "Application of thermal imaging for plant diseases: A review," *International Journal of Agricultural and Biological Engineering*, vol. 12, no. 3, pp. 1-16, 2019, doi: 10.25165/j.ijabe.20191203.4817.

[8] H. G. Jones, "Application of thermal imaging and infrared sensing in plant physiology and ecophysiology," *Advances in Botanical Research*, vol. 41, pp. 107-163, 2004, doi: 10.1016/S0065-2296(04)41003-9.

[9] R. Ishimwe, K. Abutaleb, and F. Ahmed, "Applications of Thermal Imaging in Agriculture—A Review," *Advances in Remote Sensing*, vol. 3, pp. 128-140, 2014, doi: 10.4236/ars.2014.33011.

[10] A. D. Richardson et al., "Climate change, phenology, and phenological control of vegetation feedbacks to the climate system," *Agricultural and Forest Meteorology*, vol. 169, pp. 156-173, 2013, doi: 10.1016/j.agrformet.2012.09.012.

[11] R. Calderón, J. A. Navas-Cortés, C. Lucena, P. J. Zarco-Tejada, and J. Tardaguila, "High-resolution airborne thermal imagery for early detection of sharka disease (plum pox virus; PPV) in peach orchards," *Remote Sensing*, vol. 7, no. 11, pp. 14979-15003, 2015, doi: 10.3390/rs71114979.

[12] C. I. Fernández, B. Leblon, J. Wang, A. Haddadi, and K. Wang, "Detecting Infected Cucumber Plants with Close-Range Multispectral Imagery," *Sensors*, vol. 21, no. 15, p. 5181, 2021, doi: 10.3390/s21155181.

[13] J. Ugarte Fajardo et al., "Early detection of black Sigatoka in banana leaves using hyperspectral images," *Applications in Plant Sciences*, vol. 8, no. 8, p. e11383, 2020, doi: 10.1002/aps3.11383.

[14] S. Banerjee, S. Roy, and J. K. Kalita, "Plant Disease Recognition from Leaf Images: A Comprehensive Review," *Computers and Electronics in Agriculture*, vol. 169, p. 105153, 2020, doi: 10.1016/j.compag.2019.105153.

[15] F. A. Elazegui, "Rice Diseases," in *Diseases of Fruits and Vegetables: Diagnosis and Management*, Springer US, 2003, pp. 439-479.

[16] S. P. Mohanty, D. P. Hughes, and M. Salathé, "Using Deep Learning for Image-Based Plant Disease Detection," *Frontiers in Plant Science*, vol. 7, p. 1419, 2016, doi: 10.3389/fpls.2016.01419.

[17] A. Picon, A. Morales, M. Á. Hoya, and F. M. Cazorla, "Automatic detection and severity estimation of olive diseases using deep convolutional neural networks," *Sensors*, vol. 18, no. 5, p. 1675, 2019, doi: 10.3390/s18051675.

[18] A. L. S. P. Annabel, T. Annapoorani, and P. Deepalakshmi, "Machine Learning for Plant Leaf Disease Detection and Classification – A Review," in *2019 International Conference on...*, IEEE, 2019.

[19] A. Darwish, D. Ezzat, and A. E. Hassanien, "An optimized model based on convolutional neural networks and orthogonal learning particle swarm optimization algorithm for plant diseases diagnosis," Elsevier, 2020.

[20] K. Nagasubramanian, S. Jones, A. K. Singh, S. Sarkar, and A. Singh, "Plant disease identification using explainable 3D deep learning on hyperspectral images," *Plant Methods*, vol. 15, no. 1, p. 1, 2019, doi: 10.1186/s13007-019-0394-1.

[21] M. Nagaraju and P. Chawla, "Systematic review of deep learning techniques in plant disease detection," *International Journal of System Assurance Engineering and Management*, vol. 11, no. 3, pp. 547-560, 2020, doi: 10.1007/s13198-020-01013-9.

[22] T. R. Gadekallu et al., "A novel PCA–whale optimization-based deep neural network model for classification of tomato plant diseases using GPU," *International Journal of System Assurance Engineering and Management*, vol. 11, no. 3, pp. 547-560, 2020, doi: 10.1007/s13198-020-01013-9.

[23] A. S. Keceli, A. Kaya, C. Catal, and B. Tekinerdogan, "Deep learning-based multi-task prediction system for plant disease and species detection," *Department of Computer Engineering*, Hacettepe University, Ankara, Turkey, 2022.

[24] K. Banerjee, P. Krishnan, and N. Mridha, "Application of thermal imaging of wheat crop canopy to estimate leaf area index under different moisture stress conditions," *Biosystems Engineering*, vol. 166, pp. 96-106, 2018.

[25] A. Hornero et al., "Modelling hyperspectral- and thermal-based plant traits for the early detection of Phytophthora infestations," *Agricultural and Forest Meteorology*, 2021, doi: 10.1016/j.agrformet.2021.108570.

[26] T. Poblete et al., "Discriminating Xylella fastidiosa from Verticillium dahliae infections in olive trees using thermal- and hyperspectral-based plant traits," *ISPRS Journal of Photogrammetry and Remote Sensing*, 2021.

[27] B. N. Madhukar, S. H. Bharathi, M. P. Ashwin, and A. J. Imaging, "Classification of breast cancer using ensemble filter feature selection with triplet attention based efficient net classifier," Int. Arab J. Inf. Technol., vol. 21, no. 1, pp. 17-31, 2024.

[28] D. Wang, J. Wang, Z. Ren, and W. Li, "DHBP: A dual-stream hierarchical bilinear pooling model for plant disease multi-task classification," *Agricultural and Forest Meteorology*, vol. 319, p. 108570, 2022, doi: 10.1016/j.agrformet.2021.108570.

[29] X. Ye et al., "Deep learning-based plant disease recognition using 14-layer deep convolutional neural network with data augmentation techniques," *Computers and Electronics in Agriculture*, vol. 183, p. 106003, 2021, doi: 10.1016/j.compag.2020.106003.

[30] I. Bhakta, S. Phadikar, K. Majumder, H. Mukherjee, and A. Sau, "A novel plant disease prediction model based on thermal images using modified deep convolutional neural network," *Precision Agriculture*, vol. 24, no. 1, pp. 23-39, 2023, doi: 10.1007/s11119-022-09902-4.

[31] G. Delnevo, R. Girau, C. Ceccarini, and C. Prandi, "A deep learning and social IoT approach for plants disease prediction toward a sustainable agriculture," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7243-7250, 2021, doi: 10.1109/JIOT.2021.3065447.

[32] G. Geetharamani and A. Pandian, "Identification of plant leaf diseases using a nine-layer deep convolutional neural network," *Computers & Electrical Engineering*, vol. 76, pp. 323-338, 2019, doi: 10.1016/j.compeleceng.2019.04.011.

[33] T. R. Gadekallu et al., "A novel PCA–whale optimization-based deep neural network model for classification of tomato plant diseases using GPU," *Journal of Real-Time Image Processing*, vol. 18, pp. 1383-1396, 2021, doi: 10.1007/s11554-021-01089-y.

[34] N. Kundu et al., "IoT and interpretable machine learning based framework for disease prediction in pearl millet," *Sensors*, vol. 21, no. 16, p. 5386, 2021, doi: 10.3390/s21165386.

A Gradient Technique-Based Adaptive Multi-Agent Cloud-Based Hybrid Optimization Algorithm

Mohammad Nadeem Ahmed[1]*, Mohammad Rashid Hussain[2],
Mohammad Husain[3], Abdulaziz M Alshahrani[4], Imran Mohd Khan[5], Arshad Ali[6]
Department of Computer Science-College of Computer Science, King Khalid University, Abha, Saudi Arabia[1]
Department of Business Informatics-College of Business, King Khalid University, Abha, Saudi Arabia[2]
Department of Computer Science-Faculty of Computer and Information Systems,
Islamic University of Madinah, Madinah, Saudi Arabia[3, 4, 6]
Department of Computer Engineering-College of Computer Science, King Khalid University, Abha, Saudi Arabia[5]

***Abstract*—Efficient virtual machine (VM) movement and task scheduling are crucial for optimal resource utilization and system performance in cloud computing. This paper introduces AMS-DDPG, a novel approach combining Deep Deterministic Policy Gradient (DDPG) with Adaptive Multi-Agent strategies to enhance resource allocation. To further refine AMS-DDPG's performance, we propose ICWRS, which integrates WSO (Workload Sensitivity Optimization) and RSO (Resource Sensitivity Optimization) techniques for parameter fine-tuning. Experimental evaluations demonstrate that ICWRS-enabled AMS-DDPG significantly outperforms traditional methods, achieving a 25% improvement in resource utilization and a 30% reduction in task completion time, thereby enhancing overall system efficiency. By merging nature-inspired optimization techniques with deep reinforcement learning, our research offers innovative solutions to the challenges of cloud resource allocation. Future work will explore additional optimization methods to further advance cloud system performance.**

Keywords*—Adaptive multi-agent; cloud-based; hybrid optimization; task scheduling; virtual machine migration; gradient technique

I. INTRODUCTION

Blockchain, shadow computer together with expert system are simply a few of the brand-new cordless modern technologies that have actually substantially aided the Net of Points (IoT). Since shadow computer can offer a wide range of tasks it has actually brought in substantial interest from government firm, business together with academic community alike [1] Haze computer, energy computer and also various other elements are incorporated. The most effective feasible source as well as outcome performance is an additional objective of the need model [2] Various cloud kinds such as personal, public, hybrid, mobile and also cloud federation have actually been released to please the large range of requirements. System as a Service (PaaS) Infrastructure as a Service (IaaS) as well as Software as a Service (SaaS) are the three primary classifications of cloud solutions. System as a Service (PaaS) enables programmers to make use of a large range of devices, such as running systems, physical along with digital computer systems, programs languages, and also control framework layout patterns to improve cloud solutions. The software application as a solution principle supplied a structure for accessing cloud-based software application and also permitted individuals to connect with designers on a pay-per-use basis. Individuals might likewise access computer systems, storage space as well as virtualized physical properties by means of IaaS. On top of that sources can rise and fall in accessibility in action to modifications in need. Cloud information centers are being made use of by provider worldwide to offer shadow solutions. Cloud solutions are in some cases considered to be improved vital hardware [3]. This shows exactly how expensive cloud information Center upkeep is because of the quantity of power they make use of. As a result of a selection of elements consisting of inadequate air conditioning of information centers, reduced web server application, as well as underutilized network devices, information Centre power has actually gotten little interest. The basis of shadow computer, virtualization, has actually produced a separated setting matched for a range of usages. Additionally, readily available are features like equipment source abstraction, structured accessibility plus vibrant source administration. It has actually enhanced system adaptability as well as made it less complex to release solution customers for node seclusion plus replicate online circumstances. Web server virtualization which permits numerous computer systems to share the sources of a solitary, commonly dispersed information center is a critical method for enhancing shadow computer. Because of this the most prominent techniques for minimizing power usage as well as enhancing source use inside a virtualized information center are gone oveBecause of significant restrictions such as marked location hosts, an unforgettable technique for moving the online maker (VM) from the resource host to the target host was verified [4]. These methods have the possible to reduce migration time in fifty percent by making far better use the existing network data transfer. In addition, the pre-copy idea has actually been made use of in the cloud movement procedure for online makers (VMs). In this feeling, "" information price"" describes the gross rate at which a movement has actually transformed the digital device's memory state. Due to attributes like real-time online maker movement, minimized movement times and also top quality of solution, side clouds existing unique problems than standard cloud information centers [5]. This is since the large location networks of side clouds have much tighter data transfer restrictions than the designs located in information centers. Lately a wide range of meta-heuristic formula versions have actually been created to deal with the pushing trouble of online

device combination. Multi-objective optimization problems such source waste migration time source use, power intake and also movement expenses have actually been thought about by significant VM combination methods. To resolve these concerns, we offer a unique online maker (VM) movement approach based upon cloud-based model-based support discovering.

II. Literature Survey

Modern computer has actually undertaken an improvement due to extraordinary developments in shadow computer which currently give scalable and also fairly valued services to people in addition to services. This game-changing modern technology enables individuals to create plus expand their applications as well as solutions without requiring to spend a lot in equipment. Online individuals have as needed accessibility to an enormous swimming pool of computational sources. Virtualization which splits genuine equipment right into online sources along with allows the procedure of a number of digital makers (VMs) on a solitary physical equipment (PM) is a basic element of shadow computer [6]. This reliable use sources results in substantial price financial savings as well as better functional performance for shadow company. Nevertheless, there are negative aspects related to shadow computer besides its lots of benefits. Making use of power in cloud information centers, or DCs is one substantial trouble. The climbing need for shadow solutions has actually led to greater power use for information centre (DC) facilities consisting of cooling down systems, networking tools, as well as web servers. This has actually had an unfavorable effect on the setting and also led to substantial functional expenses. Shadow company are attempting progressively difficult to strike an equilibrium in between using top quality solutions together with making use of as little power as practical in order to enhance effectiveness as well as ecological sustainability. Khan et al. (2018) established a hereditary formula-- based method to increase digital equipment release in a multi-cloud setting. By dynamically dispersing online makers (VMs) throughout numerous clouds while taking into consideration different Quality of Service (QoS) constraints their research targeted at boosting the application of cloud sources [7].

Bit Swarm Optimization (PSO) was developed by Ko et al. (2019) in order to raise the power performance of online maker release in cloud systems. Their research focused on picking devices (PMs) for online equipment (VM) allowance in a manner in which decreases power use while protecting application efficiency. This method functioned well to enhance cloud information center power effectiveness [8].

Shao et al. (2017) took a look at simply exactly how online manufacturer (VM) appropriation in cloud details facilities is done utilizing the Ant Colony System (Air Conditioner). Their purpose was to duplicate foraging routines in order to make the most of source usage along with power effectiveness. Their purpose was to boost source allocation by dispersing online devices throughout PMs [9] Nonetheless Zhang et al. (2020) recommended a technique for assigning digital makers (VMs) in cloud details facilities labeled Q recognizing based VM slice. With an emphasis on comfort plus real-time decision-making this technique looked for to make the most of resource performance while pleasing Quality of Service (QoS) requires in vibrant cloud setups [10].

The Deep Deterministic Policy Gradient (DDPG) method was made use of by Reji coupled with Selvakumar (2019) in their research study to raise the movement along with loan consolidation of makers in cloud information. Their strategy created VM appropriation that caused source application plus power performance. This shows DDPG's capability to take care of job areas well [11]. In their research study, Wang as well as associates (2021) offered a technique for designating online devices (VMs) in multi-cloud situations utilizing DDPG. About various other strategies, their option carried out well particularly in regards to source plus power performance. This job highlights the possibility of DDPG in cloud settings to deal with concerns connected to online device appropriation [12].

Mnih et al. (2015) plus Lillicrap et al. (2016) have actually attained significant developments in using DDPG in tough optimization problems, such online device allotment. Their job has a substantial influence on support knowing for control jobs. Their initiatives opened up the door for later innovations in techniques based upon support understanding [13].

Sutton coupled with Barto (2018) gave a thorough summary of the location by checking out the academic underpinnings of support knowing. This fundamental understanding is required to recognize as well as utilize RL formulas, such as DDPG, in a selection of optimization tasks [14].

Schulman et al. (2017) provided a description of proximal policy optimization strategies, which are relevant to work on RL-based virtual machine allocation. Their work improved our understanding of optimizing policies in reinforcement learning, which is in line with the objective of learning the best VM allocation rules [15].

III. A Hybrid Approach to Optimization With Advanced VM Migration and Task Scheduling Model for Cloud Networks

A. Cloud System Overview

Thanks to the cloud, all users may now access and utilize virtualized resources that are scalable and always accessible. Since the resources are offered under the pay-per-use model in this instance, the user only needs to pay for the ones that they really use. Additionally, users can distribute the pool of allotted computer resources by taking on less administrative duties. Moreover, insufficient and excessive resource provisioning was overlooked, and hardware costs—which have been perceived as a motivator for companies shifting their operations to the cloud—were minimized.

Since the cloud has been employed in this instance at various degrees across domains, personal data saved on the cloud is accessible to a wide range of actors.

Owner of the data: It is believed to be the main actor. Thus, the choice to host data on the cloud or utilize services hosted there has already been made [16]. Many parties may share ownership of the data, especially if it was co-produced by them or will be aggregated on behalf of many parties [17].

When it comes to cloud-based services, the administrator is considered the service owner. The primary duties are oversight and service enhancement [18]. The administrator has the same motive to divulge user information as the CSP when the administrator is replaced through the CSP.

Those who have utilized or are related to the usage of cloud-based services are regarded as third parties that offer those services. In the worst circumstances, this actor has been perceived as untrustworthy and may compromise data privacy, despite the fact that it is typically regarded as trustworthy [19]. This method is illustrated in Fig. 1.

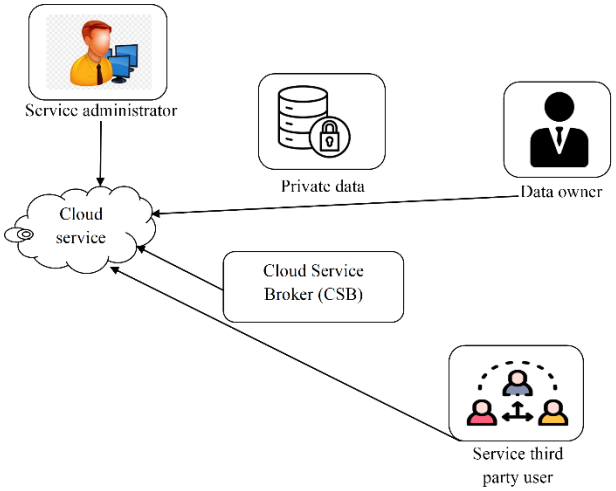


Fig. 1. The method of trustworthy with third-party users.

B. Problems with Task Scheduling and VM Migration

Cloud users often ask the cloud to do tasks for them, and virtual machines (VMs) are an essential part of cloud computing. In addition, a variety of resource needs have been requested by users and managed by the task queue on the cloud system [20]. Furthermore, utilizing a digital equipment supervisor, the job schedulers acquired the input jobs from the job line. The offered online makers have actually been designated to the work by the job schedulers. Job organizing determines the complete time to finish all input jobs by very first examining the sources called for to set up a certain task promptly and after that optimizing making use of those sources. The existing obligations have lastly been prepared. Cloud source monitoring is separated right into 2 key phases. The initial element influencing the digital maker's possible aid in finishing the jobs was job organizing [21] There are numerous reasons that job organizing is done such as much better source application, lots harmonizing power administration, and also much faster implementation times. Designating online makers (VMs) to real equipment is an additional job for the second stage.

Due to the fact that digital devices require sources that hosts do not give they cannot be set up efficiently on hosts. Because of inadequate host sources about the sources acquired by the VMs better concerns have appeared throughout the VM task procedure.

Virtualized software application, refining power and also storage space are currently offered to web individuals [22]. To better maximize the usage of the quickly obtainable sources QoS has actually made use of the solution degree arrangements offered by cloud solutions. It was figured out that there was a concern with the digital maker movement procedure after finding that the web server more than crammed.

Furthermore, memory variety plus dimension have been vibrant which makes complex the variation transmission transmission. The VM movement strategy has properly reduced the VM dimension by means of using memory self-balloon, efficient pre-copy discontinuation, create strangling, memory compression as well as de-duplication.

Numerous other issues have also arisen, including inadequate bandwidth, unpredictable network behavior, protracted delays, and a greater packet loss rate.

The shared network connection allows for the movement of both memory and storage utilizing virtual machine migration algorithms [23]. Additionally, delaying the completion of the VM transfer might sometimes result in a considerable time benefit.

The rate of difficulty in locating appropriate rest areas has been optimized. The VM migration strategy has decreased migration noise, which is indicated by slow response times, high packet loss rates, and limitations in application performance. Moreover, the difficulty that has resulted in unexpected behavior has made the predictive applications' preemptive resource requirements worse.

Why During virtual machine migration, data may be sent over the incorrect network lines, raising security concerns. This is especially troublesome over longer communication distances. Furthermore, hostile virtual machines (VMs) have been able to access other VM address spaces and carry out harmful activities due to the insufficient isolation provided by shared resources. Throughout the VM migration procedure, the data integrity has been ensured by fully using sophisticated cryptographic capabilities [24].

C. Explanation of the Planned Approach

Resources that may be made available to consumers via the internet are known as virtualized resources, and they include things like software, storage space, and processing power. Furthermore, in order to optimize the utilization of readily accessible resources, the Quality of Services has also been provided through cloud service providers and has employed varied degrees of service agreements. Data center energy utilization has been decreased by using optimal virtual machine allocation [25]. The deployment of the virtual machine (VM) aims to minimize costs while optimizing efficiency. Fig. 2 shows a new model that was created in the cloud with a heuristic and adaptive method that accounts for the limitations of the traditional model.

A novel hybrid heuristic approach called AMS-DDPG is created in order to accomplish virtual machine migration and cloud-based task allocation. The shortcomings of the existing hybrid model have been further addressed by the development of a new algorithm model known as ICWRS. As a result, by using this algorithm model, the AMS-DDPG technique has achieved its maximum performance. As a result, the proposed

approach has effectively accomplished several multi-objective tasks in the job scheduling phase, such as CPU usage, energy, make span, migration cost, active servers, and quality of service [26]. As a result, it has been shown in many experimental validations that the suggested design consistently improves task scheduling rates and cloud performance.

IV. Hybrid Heuristic Algorithm For Parameter Optimization

A. Current WSO

Each of the 26 warriors has a chance of becoming commander or a king based on their fitness level. The commander and king have also helped the other troops by spreading their influence over the battlefield.

Attack strategy: There have been two methods that have been considered. The location of the type and the commander determine how the soldier modifies his position [27]. At the start of the war, every soldier held the same rank. In this case, the soldier executed the strategy, which resulted in a promotion. Weights and ranks for each soldier have been modified in accordance with the success strategy. The soldiers, together with the army commander and the king, remain quite near to their target as the battle comes to an end. It is expressed in Eq. (1).

$$A\_\zeta(\alpha+1)=A\_\zeta(\alpha)+2\cdot\rceil\cdot(A-B)+P\Delta\cdot(X\_\zeta\cdot B-A\_\zeta(\alpha)) \quad (1)$$

Here, the weight is represented as, the location of the monarch and commander is depicted as, and the new position is named as.

Updating rankings and weights: The way that each soldier's rank, Commander, and King interact has determined how each seeking agent updates its location [28]. Additionally, a soldier's combat achievement record determines their rank. Furthermore, the rank of every soldier denotes their proximity to each other, which is considered while assessing their degree of fitness. In contrast to the conventional method, the weight varied exponentially with the factor of, while the weighted factors changed linearly.

When a soldier's level of fitness at a new area is equal to that of their previous post, that prior site is acquired.

$$A\_\zeta(\alpha+1)=(A\_\zeta(\alpha+1))\times(\Phi T\_\xi\geqslant\Phi T\_\pi\sigma)+(A\_\zeta(\alpha))\times(\Phi T\_\xi<\Phi T\_\pi\sigma) \quad (2)$$

When the soldier updates successfully the location, the rank of the soldier has been upgraded.

$$PK\_\psi=(PK\_\psi+1)\times(\Phi T\_\xi\geqslant\Phi T\_\pi\sigma)+(PK\_\psi)\times(\Phi T\_\xi<\Phi T\_\pi\sigma) \quad (3)$$

The new weight factor is defined in Eq. (4) as a function of rank.

$$X\_\zeta=X\_\zeta\cdot(1-(PK\_\psi)/(\llbracket\mu\alpha\xi\_\rrbracket\ \alpha\iota\ \tau\varepsilon))\perp\lfloor \quad (4)$$

$$A\_\zeta(\alpha+1)=A\_\zeta(\alpha)+2\cdot\rceil\cdot(A-A\_P\Delta(\alpha))+P\Delta\cdot X\_\zeta(\chi\mu-A\_\zeta(\alpha)) \quad (5)$$

Since the previous method included the random soldier's position, the analysis of the war strategy in this instance showed maximal searching space during assimilation. The soldier adjusted its positions in view of the increased relevance of and finished extra phases. Given the decreased value, the soldier has completed fewer stages and adjusted its locations.

Weak troops can be replaced or relocated: It has identified the weak soldier with the lowest fitness for each iteration. The different replacement methods have been put to the test here. Here, the weak soldier and the random soldier have taken the place of the simpler tactics, and the results are shown in Eq. (6).

Further, the second tactic, which is provided in Eq. (7), involves moving the weak man closer to the median of the whole army on the battlefield. As a result, this method has improved the algorithm's behavior's convergence rate (7).

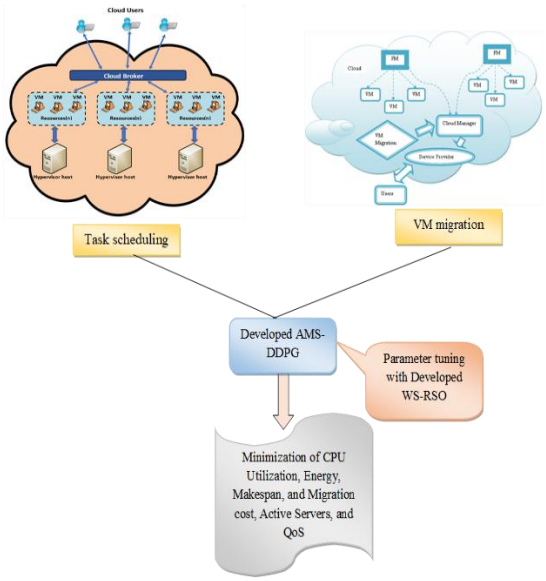


Fig. 2. Task scheduling and virtual machine migration are shown using a new paradigm.

B. Current RSO

Generally speaking, the RSO algorithm model has incorporated both the pursuing and attacking behaviors, which has helped with the algorithm's design. In several instances, the aggressive behavior of rats has led to the demise of certain creatures.

Pursuing the prey: Normally gregarious creatures, rats pursue their food [29]. to ascertain the rat's behavior in relation to the more adept search strategies that possess the information of the prey's location. Here is the other revised position that was found to be in line with the best location solution thus far. Eq. (8) is used to derive it.

$$\vec{Z}=Y\bullet\vec{Z}_e(f)+X\bullet\vec{Z}_g(f)-\vec{Z}_e(f) \quad (8)$$

The improved optimal solution and the rat's location are indicated here as and. Additional and parameters have been derived using Eq. (9) and Eq. (10).

$$Y=V-f\cdot\left(\frac{V}{mx_{it}}\right) \quad (9)$$

Here,

$$f = 0,1,2,\cdots,mx_{it}$$

$$X = 2.RD \tag{10}$$

Additionally, the random number is defined by the variables and. Then, in terms of iterations, the random parameters and are more accountable for carrying out the better exploitation and exploration phase. Equation has been used to mathematically determine the rats' fighting behavior, that of their prey, and the duration of their hunting Eq. (11).

$$\vec{Z}_e(f+1) = \left|\vec{Z}_g(f)\right| - \vec{Z} \tag{11}$$

Here is the next updated location for the rate. It has also maintained the original site and updated the locations of other agents that are seeking a better place [30]. Both the exploration and the exploitation have been completed by changing the parameter values. As a result, the suggested method has automatically cached the optimal solution for certain operators.

V. Task Scheduling and Vacuum Migration in the Cloud Using Adaptive Multi-Agent DDPG and Objective Function

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

A. Deep Deterministic Policy Gradient

Within this stage the method's input has actually been provided as the initialised setup.

Considering that the representatives incorporate both the star networking version and also the movie critic networking version the style stays the same while representing the DDPG-dependent structure. When the star is thought about the plan function-- which has actually participated in state surveillance takes into consideration existing practices by means of deterministic plan and also obtains the instant reward-- is really felt. Consequently the doubter made use of the activity worth features to transform the setups. Discovering the ideal source appropriation strategy to take full advantage of the long-lasting return is the representative's utmost goal.

Condition of area: In this situation, the Edge Cloud (EC) plus Back-end Cloud (BC) interact to make it possible for the monitoring of energy prices for each and every base terminal which is made use of to identify the system's existing condition. The job that needs to be scheduled with BC or EC is likewise considered.

Activity Space: After considering each action, the representatives have actually identified the data transfer and also digital equipment sources needed to do the procedure. Furthermore, it is separated right into three areas. In this situation the job has actually been allocated to the ideal sources as revealed by the cloud's worth of either 0 or 1. The CPU cycle is revealed as well as the data transfer as.In a reinforcement learning scenario, policies are taught using a class of algorithms called Policy Gradient (PG) algorithms. These algorithms maximise the expected cumulative reward by creating a parameterized policy that establishes a direct relationship between states and actions. Usually, a modest set of learnable parameters, represented by the symbol θ, parameterize the policy.

B. Algorithms for Deterministic Policy Gradient (DPG)

A family of reinforcement learning algorithms known as Deterministic Policy Gradient (DPG) algorithms focuses on learning deterministic policies inside continuous action spaces. Deterministic policies link states to particular actions directly, while stochastic policies provide a probability distribution across actions.

A common design used by DPG algorithms is the actor-critic architecture, in which the deterministic policy μθ(s) is the actor and the action-value function Qμ(s,a) is approximated by the critic. Through the provision of the value function gradient ∇aQμ(s,a), the critic aids in the estimation of the policy gradient.

Deep DPG (DDPG): This DPG variant is distinguished by the presence of a deep neural network model together with the approximation of the policy and the critic.

In the DDPG-dependent architecture, fully connected networks (FCNs) have been mainly deployed as actor-networks and critic networks. Consequently, they may attain the global discriminative properties of the task sequences and have large trainable weights.

MA-DDPG that adapts- A reinforcement learning technique called Adaptive Multi-Actor Deep Deterministic Policy Gradient (Adaptive MA-DDPG) is intended for cooperative multi-agent settings. It adds support for handling situations with several interacting agents to the DDPG algorithm. By employing actor and critic networks to map states to continuous actions, each agent upholds its own deterministic policy.

Adaptive MA-DDPG is innovative because of its agents' flexible communication approach [31]. In order to coordinate operations, agents exchange messages back and forth. Performance-based dynamic adjustments are made to the degree of communication. When agents are operating efficiently on their own, communication is minimized to speed up computations. On the other hand, communication is increased to promote productive cooperation when coordination is essential for better performance.

Agents change their rules based on the local observations and communications they get from other agents throughout training. In order to calculate the policy gradient for actor updates, the critic aids in the estimation of the action-value function. Based on this gradient, the actors seek to maximize the predicted cumulative benefits for every agent.

In order to achieve efficient and successful policies in complicated cooperative tasks, agents must be able to strike a balance between autonomy and collaboration. Adaptive MA-DDPG (see Fig. 3) does this by dynamically controlling communication. This flexibility improves robustness and scalability in environments with several agents.

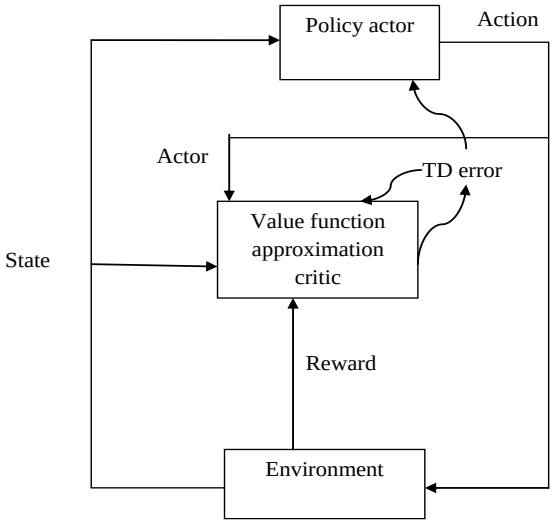


Fig. 3. Illustration of the MA-DDPG model with adjusted parameters.

VI. Results and Discussion

A. Simulation Setup

After coding up the recommended work scheduling and migration model in MATLAB 2020a, the outcomes were analyzed. We utilized the programs Dingo Optimizer (DO)-AMS-DDPG and Egret Swarm Optimization (ESO)-AMS-DDPG to do a comparison.

B. Determination of the Cost Function for Optimization's Sake

The goal you're attempting to maximize in your task scheduling and migration model is mathematically represented by the cost function, which is frequently written as (J(θ)) or just (f(x)) [32]. It calculates the 'cost' of a specific model setup, policy, or decision-making set (see Fig. 4 and Fig. 5).

We may learn more about how different models perform in relation to one another by comparing the cost function values. Since the ICWRS AMS DDPG model produced lower cost function values in this instance, it is evident that it performed better than the other models stated.

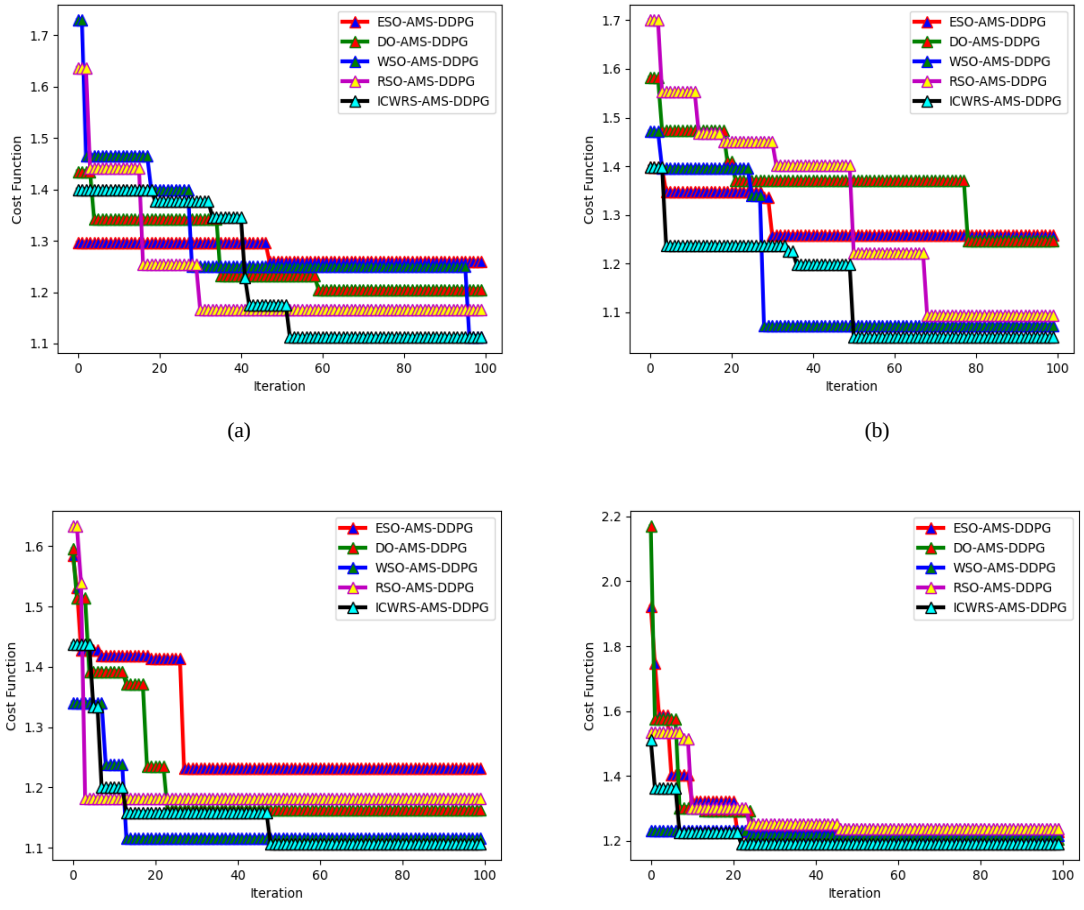


Fig. 4. The expense feature is utilized to confirm the recommended cloud-based task organizing as well as online device movement structure algorithmically in complying with arrangements: Configurations 1 2 3 as well as 4 are provided in order of choice.

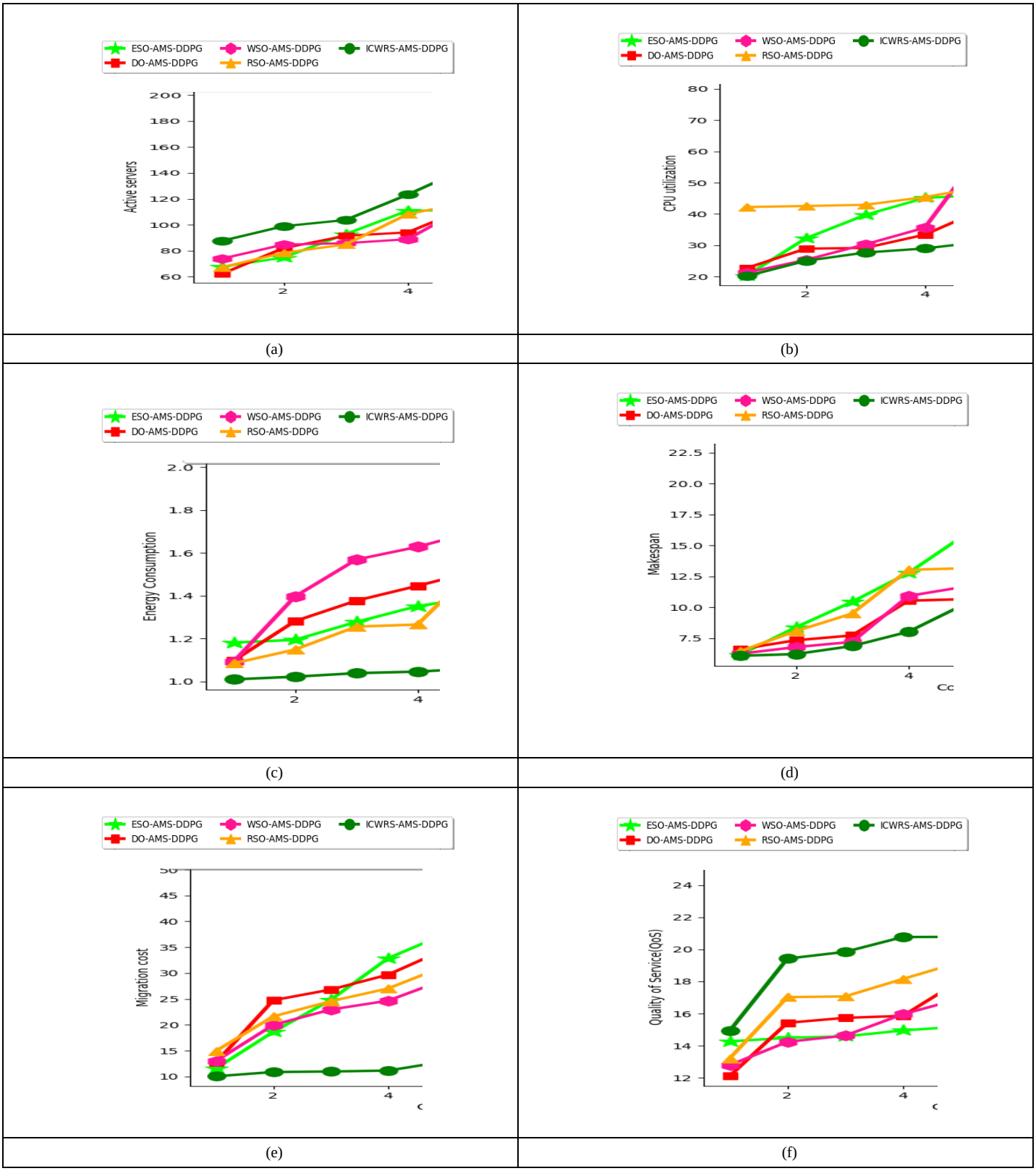


Fig. 5. Formula recognition utilising the adhering to techniques: a) Active sensing units; b) CPU utilisation; c) Energy intake; and also d) Utilizing the complying with statistics, the suggested design's task organizing plus movement strategies are validated: These initial 5 criteria are: makespan, movement costs, power use, energetic sensing units, CPU utilisation, as well as quality of solution.

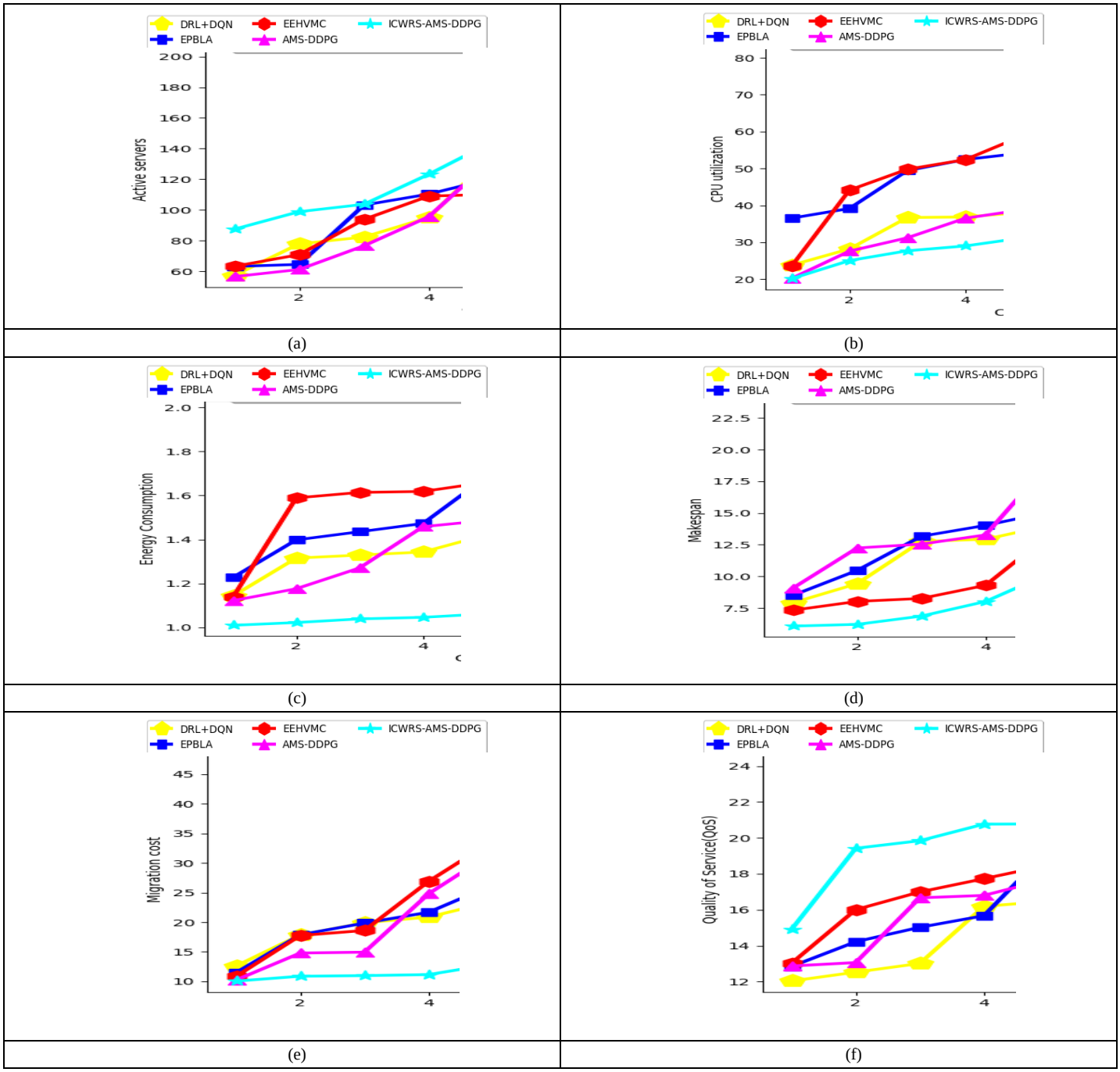


Fig. 6. Recognition in regards to pens for the procedure of tsak organizing as well as movement in the recommended version by means of a) Active sensing units, b) CPU usage c) Energy usage d) Makespan e) Migration price and also f) QoS.

This performance disparity emphasizes how crucial the ICWRS AMS model is. It implies that, in comparison to the other models taken into consideration, it is a more practical and efficient method of resolving the job scheduling and migration issue.

This comparison contributes to proving the efficacy and efficiency of the suggested ICWRS AMS paradigm and offers compelling proof of its importance in resolving issues with task scheduling and migration.

When it comes to pens as well as formulas Fig. 6 changes the Active sensing units, CPU utilisation, power usage Make period, movement expense and also QoS to reveal that the formerly recommended job organizing as well as movement design stands.

VII. Conclusion

This paper offers unique searching's for that give a unique point of view on dealing with numerous problems associated with traditional job organizing plus online equipment (VM) movement strategies. The main goal of this research study is to

enhance the efficiency as well as performance of cloud-based procedures using advanced computational devices specifically MATLAB 2020a plus unique mathematical methods. Online equipment movement as well as job organizing are the main locations of emphasis.

Enhancing the digital equipment movement plus task procedure by utilizing a cutting-edge crossbreed heuristic strategy.

An approach referred to as Adaptive Multi Agent Deep Deterministic Policy Gradient (AMS DDPG) is the goal of this research study. The key goal of this approach is to successfully take on the difficulties related to equipment job circulation and also work allowance inside cloud atmospheres. The strategy made use of by AMS DDPG utilises a heuristic formula that incorporates parts from the Deep Deterministic Policy Gradient (DDPG) device to enhance the rate together with efficiency of these treatments, thus promoting the extra effective allowance of jobs. The main goal of the AMS-DDPG strategy is to enhance the total dependability together with effectiveness of the cloud system by means of the optimization of source allowance.

The ICWRS Algorithm Model and also its usage in particular situations.

An unique plan solution was created to deal with the constraints of the normal crossbreed design causing the facility of the ICWRS formula version. This certain version adds to the improvement of the AMS-DDPG procedure through the intro of an unique plus resourceful technique for enhancing specifications. The design's efficiency will certainly be boosted in cloud-based systems as well as might be better boosted by enhancing specifications utilizing ICWRS.

Using an aggressive strategy that entails using lots of decisive organizing techniques in order to enhance performance.

The strategy being provided intends to enhance the performance of numerous multi-objective features that play an essential function in cloud procedures. It displays outstanding efficiency especially in the area of task organizing. The variables consisted of under this collection include the prices connected to moving, the power intake, the CPU usage, job time, as well as solution high quality. The recommended version's thorough method improves the complicated qualities, representing a noteworthy innovation in the organizing plus efficiency of job in cloud computer systems.

Recognition of Enhanced Efficiency as well as Work Scheduling Rates using Empirical Methods Complying with a considerable speculative recognition procedure, the recommended design has actually revealed its capability to accomplish impressive efficiency and also job organizing prices inside cloud computer atmospheres. The efficiency of the proposed standard is substantiated by the extensive speculative recognitions carried out throughout different circumstances plus workloads. The favourable outcomes validate the possible effect as well as progression of this research on cloud-based procedures offering a structure for more examination and also application in actual cloud systems.

With the growth coupled with recognition of a total design that integrates the AMS-DDPG approach, multi-objective optimization strategies, as well as the ICWRS formula version our study has actually produced substantial progression in the location. When incorporated, these elements give a detailed remedy to the problems connected to the movement of digital makers and also the organizing of jobs, showing the opportunity of enhancing the effectiveness as well as performance of cloud computer. The research's empirical outcomes highlight the importance of the research study and also supply brand-new point of views for additional expedition and also sensible application in the quick progressing area of cloud computer.

The gradient technique-based adaptive multi-agent cloud-based hybrid optimization algorithm's built-in parallelism, flexibility, and cloud-based scalability make it ideal for large-scale settings. Nonetheless, the effectiveness of its cloud deployment, communication systems, and the harmony between resource allocation and computing cost all play a significant role in its success. Mitigating communication bottlenecks and optimizing resource use are critical for optimal scalability.

Fault tolerance is naturally supported by a gradient technique-based adaptive multi-agent cloud-based hybrid optimization algorithm through cloud integration, redundancy, and adaptability. Using dynamic work reassignment, predictive analytics, and excellent recovery mechanisms, these algorithms are able to successfully manage unexpected faults or interruptions. Proactive planning, stress testing, and ongoing monitoring all help to improve resilience and guarantee seamless functioning in practical applications.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Small group Research Project under grant number RGP1/96/45.

REFERENCES

[1] S. Ohrimenco, G. Borta, and V. Cernei, ‘The digital world has a long shadow’, in The Elgar Companion to Information Economics, Edward Elgar Publishing, 2024, pp. 481–504.

[2] X. Han et al., ‘Pre-trained models: Past, present and future’, AI Open, vol. 2, pp. 225–250, 2021.

[3] M. U. Saleem et al., ‘Integrating smart energy management system with internet of things and cloud computing for efficient demand side management in smart grids’, Energies, vol. 16, no. 12, p. 4835, 2023.

[4] G. Mathioudakis et al., ‘Supporting online and on-site digital diverse travels’, Heritage, vol. 4, no. 4, pp. 4558–4577, 2021.

[5] L. Haghnegahdar, S. S. Joshi, and N. B. Dahotre, ‘From IoT-based cloud manufacturing approach to intelligent additive manufacturing: Industrial Internet of Things—An overview’, The International Journal of Advanced Manufacturing Technology, vol. 119, no. 3, pp. 1461–1478, 2022.

[6] P. Bellavista, N. Bicocchi, M. Fogli, C. Giannelli, M. Mamei, and M. Picone, ‘Requirements and design patterns for adaptive, autonomous, and context-aware digital twins in industry 4.0 digital factories’, Computers in Industry, vol. 149, p. 103918, 2023.

[7] Q. Liu et al., ‘EKT: Exercise-aware knowledge tracing for student performance prediction’, IEEE Trans. Knowl. Data Eng., vol. 33, no. 1, pp. 100–115, Jan. 2021.

[8] G. C. Ko, D. H. Lee, and Y. Choi, 'Particle Swarm Optimization for Energy-efficient Virtual Machine Placement in Hybrid Cloud Systems', Journal of Grid Computing, vol. 17, no. 4, pp. 717–732, 2019.

[9] Y. Shao, J. Liu, and L. Wang, 'Ant Colony System-based VM Allocation for Resource Optimization in Cloud Data Centers', Future Generation Computer Systems, vol. 67, pp. 257–266, 2017.

[10] B. Zhang, Z. Yu, and Y. Liu, 'Q-learning-based VM Allocation in Cloud Data Centers with QoS Constraints', IEEE Transactions on Parallel and Distributed Systems, vol. 31, no. 5, pp. 1178–1192, 2020.

[11] R. V. Reji and A. Selvakumar, 'Deep Deterministic Policy Gradient-based VM Consolidation and Migration in Cloud Data Centers', International Journal of Computer Applications, vol. 182, no. 13, pp. 22–26, 2019.

[12] Y. Wang, Y. Chen, and H. Cheng, 'A DDPG-based Approach for VM Allocation in Multi-cloud Environment', Journal of Cloud Computing: Advances, Systems and Applications, vol. 10, no. 1, pp. 1–16, 2021.

[13] T. P. Lillicrap et al., 'Continuous control with deep reinforcement learning', arXiv [cs.LG], Sep. 2015.

[14] R. S. Sutton and A. G. Barto, An Reinforcement Learning: Introduction. Mit Press, 2012.

[15] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, 'Proximal Policy Optimization Algorithms', arXiv [cs.LG], Jul. 2017.

[16] A. Atapour-Abarghouei, A. S. McGough, and D. S. Wall, 'Resolving the cybersecurity data sharing paradox to scale up cybersecurity via a co-production approach towards data sharing', in 2020 IEEE International Conference on Big Data (Big Data), 2020, pp. 3867–3876.

[17] L. Booth, W. S. Cleary, and I. Rakita, Introduction to Corporate Finance, 5th ed. Nashville, TN: John Wiley & Sons, 2020.

[18] H. Tabrizchi and M. Kuchaki Rafsanjani, 'A survey on security challenges in cloud computing: issues, threats, and solutions', J. Supercomput., vol. 76, no. 12, pp. 9493–9532, Dec. 2020.

[19] H. Hamill, K. Hampshire, S. Mariwah, D. Amoako-Sakyi, A. Kyei, and M. Castelli, 'Managing uncertainty in medicine quality in Ghana: The cognitive and affective basis of trust in a high-risk, low-regulation context', Soc. Sci. Med., vol. 234, no. 112369, p. 112369, Aug. 2019.

[20] R. Zolfaghari and A. M. Rahmani, 'Virtual machine consolidation in cloud computing systems: Challenges and future trends', Wireless Personal Communications, vol. 115, no. 3, pp. 2289–2326, 2020.

[21] M. Gladden, P. Fortuna, and A. Modliński, 'The empowerment of artificial intelligence in post-digital organizations: exploring human interactions with supervisory AI', Human Technology, vol. 18, no. 2, pp. 98–121, 2022.

[22] S. Mishra and A. K. Tyagi, 'The role of machine learning techniques in internet of things-based cloud applications', Artificial intelligence-based internet of things systems, pp. 105–135, 2022.

[23] R. M. Haris, K. M. Khan, and A. Nhlabatsi, 'Live migration of virtual machine memory content in networked systems', Computer Networks, vol. 209, p. 108898, 2022.

[24] A. M. D. Sev-Snp, 'Strengthening VM isolation with integrity protection and more', White Paper, January, vol. 53, pp. 1450–1465, 2020.

[25] P. Zhang, M. Zhou, and X. Wang, 'An intelligent optimization method for optimal virtual machine allocation in cloud data centers', IEEE Transactions on Automation Science and Engineering, vol. 17, no. 4, pp. 1725–1735, 2020.

[26] M. Hosseinzadeh, M. Y. Ghafour, H. K. Hama, B. Vo, and A. Khoshnevis, 'Multi-objective task and workflow scheduling approaches in cloud computing: a comprehensive review', Journal of Grid Computing, vol. 18, no. 3, pp. 327–356, 2020.

[27] N. Steinberg et al., 'Can Achilles and patellar tendon structures predict musculoskeletal injuries in combat soldiers?', Scandinavian Journal of Medicine & Science in Sports, vol. 31, no. 1, pp. 205–214, 2021.

[28] D. M. El-sadek and Others, 'Solve global optimization problems based on metaheuristic algorithms', Bulletin of Faculty of Science, Zagazig University, vol. 2022, no. 3, pp. 29–42, 2022.

[29] F. C. G. Parker, C. J. Price, C. McArthur, J. P. Bytheway, and P. B. Banks, 'Native predators can learn new prey cues to overcome naivete and hunt novel alien prey', Biological Conservation, vol. 284, p. 110211, 2023.

[30] M. Abdel-Basset, A. Gamal, R. K. Chakrabortty, and M. Ryan, 'A new hybrid multi-criteria decision-making approach for location selection of sustainable offshore wind energy stations: A case study', Journal of Cleaner Production, vol. 280, p. 124462, 2021.

[31] F. Bahrpeyma and D. Reichelt, 'A review of the applications of multi-agent reinforcement learning in smart factories', Frontiers in Robotics and AI, vol. 9, p. 1027340, 2022.

[32] E. C. Strinati and S. Barbarossa, '6G networks: Beyond Shannon towards semantic and goal-oriented communications', Computer Networks, vol. 190, p. 107930, 2021.

Internet of Things and Cloud Computing-Based Adaptive Content Delivery in E-Learning Platforms

Lili QIU
Practice Center, Zhengzhou University of Science and Technology, Zhengzhou 450000, China

***Abstract*—In recent years, cloud computing and Internet of Things (IoT) technologies have reshaped e-learning, leading to adaptive content delivery tailored to learners' needs. These paradigms have changed e-learning platforms by providing a scalable and flexible infrastructure for storing and processing large amounts of data. This enables seamless access to teaching materials and resources from anywhere and anytime, increasing the convenience and efficiency of online learning experiences. The convergence of cloud computing, IoT, and e-learning platforms is the heart of this study regarding how these technologies will work together to enable personalized educational experiences. We examine the principles, challenges, and developments in cloud-based adaptive content delivery and highlight the role of IoT data in understanding and incorporating learner preferences. In addition, we discuss possible future directions and implications for the further development of e-learning methods.**

***Keywords*—Cloud computing; Internet of Things; adaptive content delivery; personalized learning; e-learning**

I. INTRODUCTION

Over the past years, digitalization has designed a genuine transformation of how learning is delivered and consumed. E-learning platforms have gradually turned from simple educational content repositories to highly advanced systems that offer personalized learning experiences [1]. The main driving force in such evolution has been the integration of cloud computing and the Internet of Things. Whereby cloud computing facilitates a scalable infrastructure for storing and processing massive amounts of information, making it available at any time and place [2]. Meanwhile, the IoT enables real-time data collection from connected devices, such as smart classrooms and wearables, offering insights into learner behavior and preferences [3].

Other technologies, such as Augmented Reality (AR), further integrate into the educational landscape by creating interactive learning environments that align with personalized education features. Asadi and Taheri [4] investigated the influence of AR on students' learning achievements; in the framework of their research, one may claim that AR applications improved not just comprehension but also overall engagement and motivation. Their findings also suggest that AR has substantial potential to enhance learning by making it more interactive and personalized. With such innovative technology, instructors in smart classrooms can orchestrate dynamic and responsive learning environments that ideally suit diverse learner preferences to improve learning outcomes. This approach also needlessly aligns with the broader trend in digital education, whereby AR tools offer more insight into learner behavior and preferences, further facilitating personalized learning initiatives.

Cloud IoT fusion empowers the e-learning platform to support adaptive content bucketing for each learner's needs [5]. This integration, therefore, enriches personalized learning paths wherein the contents are managed dynamically per real-time insights. The technological convergence at the back of integrating cloud infrastructure with computing power and IoT collecting data improved e-learning efficiency and opened more doors toward personalized and data-driven educational experiences [6].

Asadi and Taheri [7] investigated how complicated technological frameworks, including Artificial Intelligence (AI) technologies, extensively improve peer review and participation in learning online. This research emphasized a multi-dimensional teaching method, which should combine systematic teaching with novel feedback mechanisms to develop collaborative learning among students. This goes along with the current trend in e-learning, where technology allows for ever more personalized learning experiences. By applying AI-powered tools, educators can create adaptive learning environments that provide an effective and engaging educational process targeted to individual learner needs.

The overall contribution of this paper is a critical review that concerns the integration of cloud computing and IoT technologies to provide adaptive content delivery on e-learning platforms. The study examines integrated technology use and illustrates how cloud infrastructure offers scalable, flexible, and affordable solutions for storing and processing educational content. At the same time, IoT devices collect real-time data about the behavior and performance of learners. This integration enables dynamic, customized, and evidence-based learning experiences, with the content adapted to the needs of each individual. Some of the challenges in adopting these technologies, including security and privacy issues, among other insights, are discussed in this study as a way of surmounting such difficulties. This paper also examines future research directions that include the integration of AI and machine learning in ways that improve adaptability and efficiency within the e-learning system.

The rest of the paper is organized as follows: Section II gives the background, focusing on the basic principles and challenges of integrating IoT with cloud computing in e-learning platforms. Section III presents adaptive content delivery mechanisms and their role in enhancing personalized learning experiences. Section IV presents the discussion, providing insights and perspectives on the findings. Finally,

Section V discusses the summary, key findings, and future e-learning platform improvement recommendations.

II. BACKGROUND

Traditional e-learning has transitioned to customized, adaptive, and data-driven learning due to cloud computing and IoT technology [8]. Cloud computing and IoT enhance learning platforms for accessibility and intelligence, as shown in Table I. Cloud computing offers scalable infrastructure and centralized data. At the same time, IoT improves real-time data acquisition and customization. The specific functions of cloud computing and IoT in e-learning are delineated in Table II and Table III, respectively. Collectively, these technologies provide a dynamic ecosystem where content distribution is driven in real-time by automatically produced insights derived from learner interactions, allowing platforms to cater to the unique requirements of each user. However, considerable obstacles to this goal persist, with data privacy, latency, and infrastructure expenses among the most prominent, as shown in Table IV. The following sections individually examine the contributions and advantages resulting from the combination of cloud computing and IoT in the transformation of e-learning.

TABLE I. TRADITIONAL E-LEARNING VS. CLOUD AND IOT-ENABLED E-LEARNING

Feature	Traditional e-learning	Cloud and IoT-enabled e-learning
Infrastructure	Static and physical servers	Scalable and flexible cloud-based infrastructure
Content delivery	Static and pre-defined	Adaptive and real-time based on learner needs
Learner data	Limited interaction data	Rich data from IoT devices (e.g., wearables, sensors)
Collaboration	Limited to basic tools (forums, email)	Real-time collaboration through cloud platforms and IoT tools
Customization	Uniform learning experience	Personalized learning paths based on real-time data
Accessibility	Device-dependent and location-bound	Accessible anywhere, anytime, from any device
Feature	Traditional e-Learning	Cloud and IoT-enabled e-learning

TABLE II. ROLE OF CLOUD COMPUTING IN E-LEARNING PLATFORMS

Function	Description
Scalability	Automatically adjusts computing resources to accommodate fluctuating user demand
On-demand access	Provides learners with 24/7 access to educational resources
Centralized data storage	Stores large amounts of learner data and performance history for real-time analysis
Cost efficiency	Reduces physical infrastructure and IT management costs for educational institutions
Collaboration tools	Facilitates real-time collaboration between learners and educators
Data processing	Enables real-time feedback and content adaptation based on learner progress

TABLE III. IOT APPLICATIONS IN E-LEARNING

IoT application	Description
Wearable devices	Track learner engagement, fatigue, and focus to adjust content in real-time
Smart classrooms	Use sensors to monitor and adjust environmental factors like lighting and temperature
Interactive tools	Enable hands-on learning experiences through IoT-enabled devices and simulations
Real-time analytics	Collect and analyze learner data to personalize learning paths and resources
Remote monitoring	Allows educators to monitor learners' progress from different locations
Wearable devices	Track learner engagement, fatigue, and focus to adjust content in real-time

TABLE IV. CHALLENGES IN CLOUD AND IOT-BASED E-LEARNING

Challenge	Cloud computing	IoT
Data privacy and security	Risk of data breaches and unauthorized access	Security concerns with real-time data from multiple devices
Latency issues	High demand can lead to slower response times	Delays in data transmission between IoT devices and platforms
Infrastructure costs	Costs for maintaining cloud infrastructure	Costs for implementing and maintaining IoT devices
Interoperability	Compatibility with various e-learning platforms	Integrating different IoT devices and communication protocols
Maintenance	Need for continuous server and data management	Ensuring IoT device reliability and continuous updates

A. Cloud Computing in e-learning

Cloud computing has revolutionized the architecture of e-learning platforms by providing scalable, adaptable, and economical methods to manage substantial amounts of educational information according to demand [9]. A key issue in cloud computing for e-learning is the availability of on-demand learning resources. Students may access course materials, assignments, and multimedia content on any internet-enabled device, therefore eliminating the obstacles associated with conventional, location-dependent learning methods [10]. The main benefits of cloud computing in e-learning include:

1) Scalability: Cloud platforms can adjust resources according to demand, handling increasing users and content without a significant performance drop. This flexibility makes e-learning more accessible to a global audience [11].

2) Cost efficiency: Educational institutions can reduce costs associated with physical infrastructure, data storage, and IT maintenance by outsourcing these functions to cloud providers [12].

3) Collaboration and accessibility: Learners and educators can collaborate in real-time, access shared resources, and benefit from interactive tools, regardless of location.

Besides, cloud computing promotes data centralization of educators and learners. Thus, to enhance the learning experience by employing detailed analysis and adaptive learning algorithms, the cloud can store large volumes of learner data, performances, and interaction history [13]. Educational platforms could use these as real-time feedback and personalized suggestions so that each student gets an optimized learning pathway [14]. With cloud computing evolving day by day, integrations of AI developments, machine learning, and big data processing further facilitate the capacity of e-learning systems over the cloud to provide compelling customized educational experiences.

B. Internet of Things in Education

The IoT has expanded possibilities in education by establishing a connected network of devices capable of continually collecting, processing, and sharing data in real time [15]. It makes the e-learning environment much more dynamic and responsive by integrating diverse physical and digital resources to augment the educational experience [16]. The IoT in education also termed intelligent learning, adaptively customizes curriculum based on real-world insights about learners' behaviors and preferences. The principal advantages of IoT in education encompass:

1) Real-time monitoring: IoT-enabled devices, such as wearables, smartboards, and sensors, can track learner engagement, participation, and even physical conditions like fatigue or stress levels [17]. This data provides immediate feedback to educators and the learning system, allowing for teaching methods or content delivery adjustments [18].

2) Personalized learning: With continuous data collection, IoT helps e-learning platforms adapt educational content to individual learning needs [19]. For example, IoT devices can track how students interact with content (e.g., time spent on tasks, patterns of error correction), and this data can inform personalized recommendations or adaptive learning paths.

3) Smart classrooms: IoT creates interconnected learning environments where devices, sensors, and digital platforms work together to provide a seamless experience [20]. Smart classrooms can adjust lighting, temperature, or multimedia content based on student preferences, making the physical learning environment more conducive to learning.

4) Enhanced engagement: IoT supports interactive tools and gamified learning experiences, allowing learners to engage more deeply with the material. Devices such as Virtual Reality (VR) headsets, interactive simulations, and IoT-based lab equipment enable hands-on learning experiences in a digital environment.

IoT plays a crucial role in the choice between knowledge and instructional-driven education. Using devices that collect data on how a learner interacts with an e-learning platform, IoT devices provide learners with insights into patterns, difficulties, and preferences. For example, this could be analyzed in real time to modify learning materials for adaptive and responsive education. Furthermore, educators use IoT devices to keep track of individual and overall improvement areas and students' progress through learning analytics. IoT transformed the educational landscape, reinventing learning environments to be more interactive, adaptive, and data-driven. With cloud computing, IoT can integrate real-time insights with prowess in data processing to create an enabling ecosystem for personalized and compelling learning experiences.

III. Adaptive Content Delivery

Adaptive content delivery in e-learning is the system's potential to adapt educational material to the learner's specific needs, preferences, and progress based on real-time dynamic adjustments that ensure each learner gets personalized content, enhancing his or her learning experience. All this is integrated with cloud computing and IoT. As shown in Table V, cloud computing has a scalable infrastructure to process and deliver content. On the other hand, IoT provides the real-time data needed for continuous personalization, as shown in Table VI. However, as specified in Table VII, adaptive learning systems have faced security and privacy issues in managing sensitive learner data across cloud platforms and IoT devices. For efficient real-time content accommodation, the performance of IoT devices and seamless data integration is crucial, as detailed in Table VIII. In addition, its infrastructure involves expensive processes, as reflected in Table IX.

TABLE V. CHALLENGES OF CLOUD COMPUTING IN ADAPTIVE CONTENT DELIVERY

Challenge	Description
Scalability vs. cost	While cloud systems scale easily, the associated costs increase as data storage and processing demands grow.
Latency issues	Delays in real-time data processing can affect the immediate responsiveness required for adaptive learning.
Data security	Storing large amounts of sensitive learner data in the cloud increases the risk of breaches and theft.
Integration with AI/ML	Requires significant computing power and infrastructure to efficiently run AI and machine learning algorithms for real-time adaptation.
Reliability	Cloud service downtimes or interruptions can disrupt the learning process and negatively affect user experience.

TABLE VI. CHALLENGES OF IOT IN ADAPTIVE CONTENT DELIVERY

Challenge	Description
Data privacy and security	Continuous real-time data collection through IoT devices raises data privacy and security concerns.
Interoperability	Different IoT devices and sensors may use varying standards and protocols, leading to challenges in integration.
Infrastructure costs	Implementing IoT in educational environments requires significant device investment, maintenance, and connectivity.
Device reliability	IoT devices, like wearables and sensors, may malfunction, leading to gaps in data collection and inaccurate content adjustments.
Network bandwidth	IoT systems require high bandwidth for real-time data transmission, which may be unavailable in certain regions.

TABLE VII. CLOUD AND IOT-BASED ADAPTIVE CONTENT DELIVERY: KEY SECURITY AND PRIVACY CONCERNS

Concern	Impact
Data breaches	Unauthorized access to sensitive learner data, including personal information and learning progress.
Unauthorized monitoring	IoT devices may collect sensitive data about learner behavior without proper consent or transparency.
Cloud security vulnerabilities	Cloud systems may face security vulnerabilities such as DDoS attacks or system intrusions.
Lack of encryption	Unencrypted data transfers between IoT devices and cloud servers can expose information to cyber threats.
Regulatory compliance	Meeting data privacy regulations (e.g., GDPR) when managing IoT-collected learner data in different regions.

TABLE VIII. TECHNICAL AND OPERATIONAL CHALLENGES IN ADAPTIVE CONTENT DELIVERY

Challenge	Cloud computing	IoT
Real-time adaptation	Requires powerful, scalable infrastructure for instant data processing.	Relies on uninterrupted data flow from devices to deliver real-time updates.
Data volume management	Storing and managing large-scale learner data can be expensive and complex.	Handling high-frequency data from multiple devices is challenging.
Reliability and maintenance	Cloud servers need regular maintenance to avoid downtime.	IoT devices may require frequent updates and maintenance.
Data accuracy	Ensuring the accuracy of processed data for content adaptation.	Ensuring IoT devices collect accurate data without malfunctions.
Device compatibility	Cloud systems must be compatible with multiple e-learning tools and platforms.	IoT devices must work seamlessly with other devices and systems.

TABLE IX. COST AND RESOURCE ALLOCATION IN CLOUD AND IOT-BASED E-LEARNING

Component	Cost considerations
Cloud Infrastructure	Initial setup costs, ongoing storage, and processing costs increase with scale.
IoT Devices	Purchase and maintenance of sensors, wearables, and smart classroom equipment.
Network Bandwidth	Costs associated with maintaining high-speed internet for seamless IoT data transmission and cloud access.
Data Storage	Storing the large volume of data generated by IoT devices and cloud-based platforms incurs high costs.
Security Measures	Investment in encryption technologies, data privacy tools, and security protocols.

A. Role of cloud Computing in Adaptive Content Delivery

Cloud computing is the base for adaptive content delivery because it offers scalable and robust infrastructures capable of processing, storing, and distributing vast volumes of data. This makes it very critical for the delivery of adaptive content based on the following:

1) Scalability and flexibility: Cloud platforms quickly scale resources to increase users and data inputs. This ensures that adaptive learning systems work effectively, even as they handle diverse datasets from myriad learners. On-demand scalability allows the adaptive systems to address everything from one-on-one tutoring environments to large-scale online courses.

2) Real-time processing and data management: Adaptable learning is real-time data analysis for instant content adaptation to the learners' progress. Cloud computing thus provides excellent computing power and storage for real-time analysis of significant streams in learner data. The system can use this immediate feedback loop to grade learner performance, patterns, or customized content. For instance, if some learner constantly shows difficulties with some concepts, the system may recommend extra information or adjust the difficulty level for later activities.

3) Centralized data storage: In cloud-based systems, the performance history, interaction patterns, and preferences of the learners are stored in one place. It puts all information about each learner's journey into a single perspective. Therefore, this would enhance the accuracy and effectiveness of adaptive learning through an adaptive learning platform. The data will be presented to the system and across devices for seamless learning experiences for users.

4) Cost-efficiency: Cloud computing allows educational institutions to procure cost-effective solutions as no investment in physical infrastructure is necessary. Besides, IT maintenance costs go down drastically. This takes on even greater significance for an adaptive content delivery system, given the stringent demands it places on storage and processing capacity. Traditionally, institutions can now focus on core competencies of learning optimization rather than investing heavily in hardware.

5) Collaboration and accessibility: The cloud platforms pave the way for collaboration, and it's way easier, considering that access is given to the content and learning tools anywhere, anytime. The sharing of materials by the learner and educator and collaborative work may be accessed quickly, along with real-time updates. In the case of adaptive delivery, on the other hand, the system will be able to continuously keep an update and adapt to the needs of the learners regardless of location or device to uniform personalized learning experiences.

6) Integration with AI and machine learning: Cloud computing's large storage and processing capability can enable AI and machine learning algorithms necessary for predictive analytics of adaptive content delivery. Such algorithms make the system predict learner outcomes to proactively align the learning pathway for better engagement and retention.

B. Role of IoT in Adaptive Content Delivery

The IoT is a crucial enabler of adaptive content delivery in e-learning platforms, as it allows real-time data collection and analysis from various connected devices. This network of smart devices, including sensors, wearables, and interactive tools, provides continuous insights into learners' interactions, behaviors, and preferences. By capturing this data, IoT enables e-learning systems to adapt content dynamically, ensuring the learning experience is personalized and responsive to each learner's needs. Key roles of IoT in adaptive content delivery include:

1) Real-time data collection and monitoring: IoT devices can track learners' progress and behavior in real-time, collecting data such as engagement levels, task completion rates, and even physical responses like stress or fatigue. For example, wearable devices can monitor learners' heart rates or attention levels during lessons. This real-time data allows the adaptive learning system to make immediate adjustments to content delivery, such as slowing down the pace, offering additional resources, or changing the content format to better match the learner's state and needs.

2) Context-aware learning: IoT devices enable learning by gathering environmental data that can influence content delivery. For instance, intelligent classrooms with IoT sensors can adjust lighting, sound levels, and temperature to improve learning conditions. In online or hybrid learning environments, IoT devices track how learners interact with digital materials, providing the system with insights to adjust the difficulty level or type of content based on learners' surroundings and focus levels.

3) Personalized learning paths: Through continuous data collection, IoT helps build personalized learning paths tailored to individual learners. The system can understand learners' preferences, strengths, and weaknesses by analyzing data from various IoT devices. For example, if IoT devices detect that a student consistently excels in visual learning tasks, the system can prioritize visual content in their learning plan. This personalized approach ensures learners receive the most relevant materials in a format that suits their learning style.

4) Immediate feedback and interventions: With IoT-enabled devices continuously monitoring learners, adaptive e-learning platforms can provide immediate feedback based on real-time performance data. If a learner struggles with a particular concept, the system can intervene by offering additional practice exercises, explanatory videos, or adjusting the difficulty of subsequent tasks. This level of responsiveness is made possible through the instant transmission of data from IoT devices, which keeps the system informed about learners' progress and challenges as they occur.

5) Enhanced interaction and engagement: IoT enhances learner engagement by facilitating interactive and immersive learning experiences. For example, IoT-connected devices like VR headsets or smart interactive whiteboards can create hands-on, engaging simulations that adapt based on the learner's progress. These tools allow learners to interact with content in novel ways, making the learning experience more dynamic and effective. By integrating data from these devices, the system can gauge the effectiveness of different types of interactions and adjust content delivery to maximize engagement.

6) Data-driven adaptation: IoT-generated data contributes to data-driven learning analytics, allowing adaptive content delivery systems to make informed decisions about adjusting the learning process. This can include adapting content to address knowledge gaps, varying tasks' complexity based on the learner's progression, or recommending personalized resources. Over time, the accumulation of IoT data enables the

system to refine and enhance the personalization of the learning experience.

IV. Discussion

While the fusion of cloud computing and IoT has significantly advanced adaptive content delivery in e-learning platforms, several challenges must be addressed to realize their full potential. These challenges span technical, ethical, and infrastructural domains, and overcoming them is critical for the successful implementation and scalability of adaptive learning systems.

One of the most pressing challenges in cloud and IoT-based adaptive content delivery is ensuring the privacy and security of learners' data. IoT devices continuously collect vast amounts of personal and behavioral data from learners, which are then processed and stored in the cloud. This data may include sensitive information such as learning preferences, biometric data from wearables, and performance metrics. Ensuring this data is securely transmitted and stored is vital to prevent breaches and unauthorized access. Additionally, compliance with data protection regulations, such as GDPR, adds complexity to the development of these systems, requiring robust encryption, secure access controls, and privacy-preserving mechanisms.

Adaptive content delivery relies on the real-time collection and analysis of data to adjust learning materials dynamically. However, latency, the delay in data transmission between IoT devices and cloud platforms, can hinder the effectiveness of real-time adjustments. High latency can disrupt content delivery for learners in remote or underdeveloped regions with unstable internet connections, making the learning experience less seamless and responsive. Overcoming these limitations requires the optimization of data transmission protocols or implementing edge computing solutions, where data processing occurs closer to the source (the IoT devices), reducing latency.

While cloud computing offers scalability, integrating IoT devices into educational environments can be costly, particularly for institutions with limited budgets. IoT-enabled smart classrooms, wearable devices, and other interactive tools require significant investment in hardware and maintenance. Additionally, scaling adaptive content delivery to accommodate large numbers of learners and IoT devices places further demands on cloud resources, leading to potential cost increases. Striking a balance between infrastructure costs and educational benefits is a challenge, particularly for schools and universities in developing regions.

In adaptive learning environments, data is collected from various IoT devices, each potentially using different communication protocols and formats. Interoperability issues can arise when integrating and processing this diverse data range in cloud platforms. Ensuring that different IoT devices, platforms, and cloud services work seamlessly together requires the development of standardized protocols and data formats. With such standardization, the data collected may be entirely usable, limiting the ability of adaptive systems to deliver personalized content effectively.

Adapting learning content based on real-time data from IoT devices involves sophisticated algorithms that can process a large volume of data, predict learner needs, and recommend appropriate adjustments. Designing and implementing these algorithms is a complex task that requires continuous development and refinement to ensure they accurately reflect learners' progress and preferences. Furthermore, algorithms must account for many factors, such as learning style, emotional state, and cognitive load, to provide effective recommendations. Balancing these factors without overwhelming the learner or causing unnecessary interruptions presents an ongoing challenge.

The use of IoT devices to collect detailed data on learner behavior raises several ethical concerns, particularly around consent and the extent of data collection. Learners may not always be fully aware of the data being collected by IoT devices or how it will be used. Another concern is the potential for bias in content adaptation algorithms, which may reinforce existing educational inequalities. Ensuring that adaptive learning systems are transparent, equitable, and respectful of learners' privacy and autonomy is essential to gaining trust and ensuring ethical use.

The success of IoT-enabled adaptive learning systems depends heavily on the reliability and maintenance of the IoT devices and cloud infrastructure. Any malfunction in IoT devices, such as wearables or sensors, could lead to data collection gaps, affecting the system's ability to deliver personalized content. Similarly, cloud downtime or outages can disrupt the learning process, leading to a poor user experience. Ensuring continuous operation and timely maintenance of IoT devices and cloud services requires skilled personnel and resources.

V. Conclusion

The fusion of cloud computing and the IoT represents a transformative force in the evolution of e-learning platforms, enabling more personalized, adaptive, and efficient content delivery. By leveraging the scalability and flexibility of cloud infrastructure, along with IoT's real-time data collection capabilities, e-learning platforms can now dynamically tailor educational content to meet individual learners' unique needs and preferences. This convergence enhances the learning experience, making it more engaging, responsive, and effective. However, implementing cloud and IoT-based adaptive content delivery successfully presents several challenges. Data privacy and security, latency in real-time processing, infrastructure costs, data interoperability, and ethical concerns must be carefully addressed to ensure these technologies are applied responsibly and effectively. Furthermore, the complexity of content adaptation algorithms and the reliability of the underlying infrastructure remain critical factors for the long-term success of adaptive learning systems.

As educational institutions continue to embrace digital transformation, the future of e-learning lies in further refining these technologies. Integrating advancements such as artificial intelligence and machine learning with cloud and IoT will pave the way for even more sophisticated adaptive systems. These developments will not only enhance the personalization of learning but also help overcome current limitations, ensuring

that education remains accessible, efficient, and equitable for all learners. This study highlighted the significant potential of cloud computing and IoT in reshaping the education landscape. Educators and technologists can create more dynamic, learner-centered environments that offer meaningful, data-driven educational experiences by addressing existing challenges and exploring new technological frontiers.

REFERENCES

[1] M. Liu and D. Yu, "Towards intelligent E-learning systems," Educ Inf Technol (Dordr), vol. 28, no. 7, pp. 7845–7876, 2023.

[2] V. Hayyolalam, B. Pourghebleh, M. R. Chehrehzad, and A. A. Pourhaji Kazem, "Single - objective service composition methods in cloud manufacturing systems: Recent techniques, classification, and future trends," Concurr Comput, p. e6698, 2021.

[3] B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research," Journal of Network and Computer Applications, vol. 97, pp. 23–34, 2017, doi: 10.1016/j.jnca.2017.08.006.

[4] M. Asadi and S. Ebadi, "Integrating augmented reality in EFL reading comprehension: a mixed-methods study," Res Pract Technol Enhanc Learn, vol. 20, p. 23, 2025, doi: https://doi.org/10.58459/rptel.2025.20023.

[5] U. O. Matthew, J. S. Kazaure, and N. U. Okafor, "Contemporary development in E-Learning education, cloud computing technology & internet of things," EAI Endorsed Transactions on Cloud Systems, vol. 7, no. 20, pp. e3–e3, 2021.

[6] K. Ahmad et al., "Data-driven artificial intelligence in education: A comprehensive review," IEEE Transactions on Learning Technologies, 2023.

[7] M. Asadi and R. Taheri, "Enhancing Peer Assessment and Engagement in Online IELTS Writing Course through a Teacher's Multifaceted Approach and AI Integration," Technology Assisted Language Education, vol. 2, no. 2, pp. 94–117, 2024, doi: 10.22126/tale.2024.11083.1058.

[8] R. Setiawan et al., "IoT based virtual E-learning system for sustainable development of smart cities," J Grid Comput, vol. 20, no. 3, p. 24, 2022.

[9] V. Hayyolalam, B. Pourghebleh, A. A. Pourhaji Kazem, and A. Ghaffari, "Exploring the state-of-the-art service composition approaches in cloud manufacturing systems to enhance upcoming techniques," International Journal of Advanced Manufacturing Technology, vol. 105, no. 1–4, 2019, doi: 10.1007/s00170-019-04213-z.

[10] B. Wenjie, "Simulation of vocal teaching platform based on target speech extraction algorithm and cloud computing e-learning," Entertain Comput, vol. 50, p. 100700, 2024.

[11] B. Aygun, B. G. Kilic, N. Arici, A. Cosar, and B. Tuncsiper, "Application of binary PSO for public cloud resources allocation system of video on demand (VoD) services," Appl Soft Comput, vol. 99, p. 106870, 2021.

[12] G. Büyüközkan, D. Uztürk, and A. Maden, "Influential factor analysis for cloud computing technology service provider," Technol Forecast Soc Change, vol. 192, p. 122531, 2023.

[13] A. Alam, "Cloud-based e-learning: scaffolding the environment for adaptive e-learning ecosystem based on cloud computing infrastructure," in Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2, Springer, 2022, pp. 1–9.

[14] S. Khan, A. Al-Dmour, V. Bali, M. R. Rabbani, and K. Thirunavukkarasu, "Cloud computing based futuristic educational model for virtual learning," Journal of Statistics and Management Systems, vol. 24, no. 2, pp. 357–385, 2021.

[15] B. Pourghebleh and V. Hayyolalam, "A comprehensive and systematic review of the load balancing mechanisms in the Internet of Things," Cluster Comput, 2019, doi: 10.1007/s10586-019-02950-0.

[16] R. Revathi, M. Suganya, and G. M. NR, "IoT based Cloud Integrated Smart Classroom for smart and a sustainable Campus," Procedia Comput Sci, vol. 172, pp. 77–81, 2020.

[17] K. Kumar and A. Al-Besher, "IoT enabled e-learning system for higher education," Measurement: Sensors, vol. 24, p. 100480, 2022.

[18] H. Mokhtari Dowlatabad et al., "High-Frequency (30 MHz–6 GHz) Breast Tissue Characterization Stabilized by Suction Force for Intraoperative Tumor Margin Assessment," Diagnostics, vol. 13, no. 2, p. 179, 2023, doi: https://doi.org/10.3390/diagnostics13020179.

[19] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, "A survey of Internet of Things (IoT) in education: Opportunities and challenges," Toward social internet of things (SIoT): Enabling technologies, architectures and applications: Emerging technologies for connected and smart social objects, pp. 197–209, 2020.

[20] H. M. N. Iqbal, R. Parra-Saldivar, R. Zavala-Yoe, and R. A. Ramirez-Mendoza, "Smart educational tools and learning management systems: supportive framework," International journal on interactive design and manufacturing (IJIDeM), vol. 14, no. 4, pp. 1179–1193, 2020.

Design of a Mobile Language Learning App for Students with ADHD Using Augmented Reality

Leonardo Paolo Cesias-Diaz, Jorge Armando Laban-Hijar, Juan Carlos Morales-Arevalo
Faculty of Engineering, Universidad Peruana de Ciencias Aplicadas, Lima, Perú

***Abstract*—Attention Deficit Hyperactivity Disorder, ADHD for short, impedes submission to traditional teaching as it affects cognitive abilities such as executive function skills, memorization, and focus. In this case, how will kids with ADHD learn languages? This paper provides a solution by presenting the capabilities of a mobile language learning tool called AugmentedFocus, which is designed to support children with ADHD through the use of augmented reality. This association has allowed personalized instruction, accompanied by noticeable augmented reality elements so that learners, teachers, and administrators are able to use their mobile phones to comprehend instructional materials. The objective is to evaluate the application's design, architecture, prototype, some testing results, and adjustments made during its implementation, while discussing other features within the context. More significantly, we aim to demonstrate how the mobile application can enhance engagement and retention in language learning among kids with ADHD. Attention Deficit Hyperactivity Disorder obstructs dependency on traditional measures of teaching since it relates to cognitive skills like executory function skills, memory, and focus. In this case, how will kids with ADHD learn languages? This paper addresses the issue by demonstrating the effectiveness of a mobile language learning app, AugmentedFocus that is specifically created for ADHD kids and shows a Technology in education.**

***Keywords*—ADHD; augmented reality; language learning; technology in education; mobile application; design; prototype**

I. Introduction

ADHD is a neurodevelopmental condition that significantly impairs children's ability to concentrate, focus, and retain information thereby posing great challenges within an educational environment [1]. Traditional methods of learning may not be appropriate for an individual with ADHD because of attention and memory problems entailed by such a disorder. Emerging technologies in education, like AR, may introduce new ways to support these students by engaging them in more interesting and interactive learning experiences [2].

Augmented reality is a technology that has appeared in recent years and is being widely used in different areas. In this case, we are looking to adapt this technology to the learning of children with ADHD because they have great difficulty concentrating and this tool allows them to learn in an entertaining and effective way [3]. Because of this we decided to create a mobile application using augmented reality focusing in ADHD students.

The primary goal of this app is to improve attention retention and reduce impulsivity through interactive and engaging educational content [3]. Using a smartphone, students can access a variety of AR-enhanced lessons. Teachers and administrators also benefit from functionalities that simplify content management and tracking student progress.

Although it was not easy to use augmented reality tools due to our inexperience, this was not a reason not to continue with the research and we continued forward until we achieved the objective.

II. Literature Review

Technological progress in the educational sector has brought forth more ways to better learning, especially for people with cognitive challenges. A new method is by using augmented reality, which places digital elements into the real world so that an interesting mixed environment is created; this has been proven by some studies to help keep students' attention, which is very important to people with ADHD [4, 5].

Previous studies have pointed out AR use in creating relatively immersive learning experiences that foster cognitive engagement, especially through immediate feedback [6]. The use of AR in education has been applied to various fields, from science to language learning [7]. Specifically, however, its use as a methodology for teaching language to students with ADHD has not received much attention. This involves an improvement over the existing work by applying AR where it might best benefit such learners, meeting their individual cognitive design requirements.

Research in study [29] was conducted where an interactive laboratory with augmented reality was successfully implemented for engineering, arts and social sciences, and science students. It facilitates practical learning in various disciplines. Within a period of two years and six months, it attracted 7952 student visits and was used in 24 subjects. Despite the obstacles that appeared (lack of augmented reality content and insufficient technical support), the research demonstrated the great interest that students had in the laboratory, where 71.5% were from engineering [29]. Unfortunately, the laboratory was stopped due to the appearance of the COVID-19 pandemic.

III. Methodology

The approach taken in the development of AugmentedFocus was user-centered and iterative, ensuring that the needs of students with ADHD were addressed at every phase. The methodologies followed were Scrum for software development, Flutter for the mobile app design, and ARCore for integrating any augmented reality functionalities [8] [9].

A. Scrum Method

Scrum is an agile methodology framework primarily focused on software development, although it is being attempted to be used in different areas. The objective of this methodology is to facilitate collaboration within a development team and to deliver products constantly, i.e. in an iterative manner. The main agile principles used by Scrum are adaptability, collaboration and continuous delivery [20]. Fig. 1 shows the order of the tasks developed in the Scrum process.

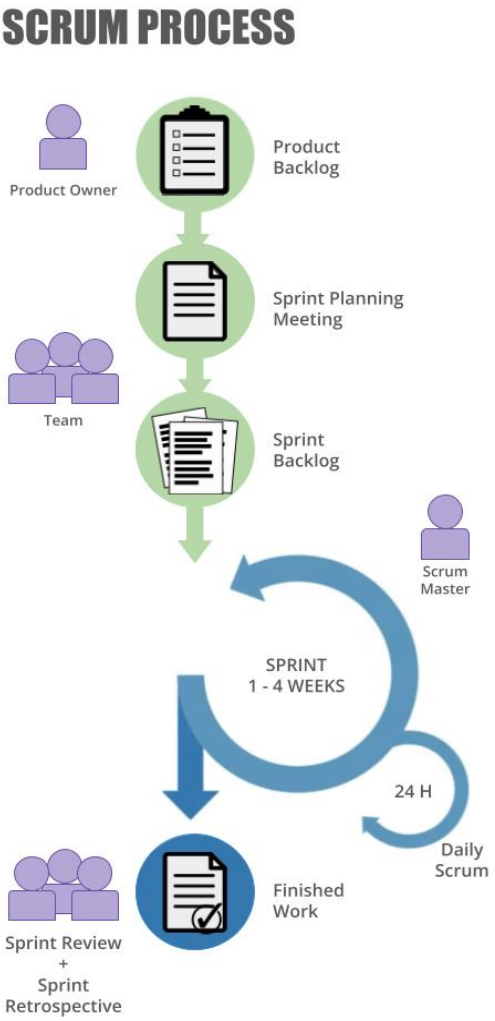


Fig. 1. Scrum process.

The Scrum methodology is composed of four essential components.

1) Small, multidisciplinary teams: Small, multidisciplinary teams that self-organize for the development of each phase and work together to achieve a common goal.

2) Roles

a) Scrum master: The person in charge of supporting the Scrum process, helps solve problems and ensures that the Scrum process is followed.

b) Product owner: This is the representative of the product's stakeholders, helping the team to set the objective to be achieved and prioritize what should be developed.

c) Development team: They are responsible for developing the product and delivering it.

3) Artifacts

a) Product backlog: This is the planned and prioritized list of requirements and tasks to be developed by the Development Team during the development of the product.

b) Sprint backlog: It is the set of tasks chosen for development within a Sprint.

4) Events

a) Sprint: This is the fixed development period in which the chosen set of requirements is implemented.

b) Daily scrum: Short, daily meeting held by the development team to check progress.

c) Sprint planning: Meeting for planning a Sprint.

d) Sprint review: Review meeting of the work accomplished throughout a Sprint.

e) Sprint retrospective: Reflection by the Development Team on a Sprint to find points for improvement.

B. System Design

The AugmentedFocus architecture was designed to support high levels of engagement, ease of use, and scalability. The mobile app was built using Flutter, a robust framework that enables cross-platform compatibility, ensuring that the app can be deployed on both iOS and Android devices [10]. This framework also enables rapid prototyping and testing, which was essential in the iterative design process [11].

Data management and security were priorities from the early stages of development, selecting Firebase as the primary database to store user information, lesson content, and AR assets. Firebase offers cloud-based scalability and strong integration with mobile platforms, making it a suitable choice for this project [12].

The backend API was implemented using Django, a Python framework known for its security and ease-of-use features [13]. Django provided the tools needed to build a secure and responsive application programming interface (API) that connected the mobile frontend to the database and notification system. The API handles user authentication, lesson retrieval, AR asset management, and notifications, which are critical features to ensure a smooth user experience.

C. Augmented Reality Integration

The core functionality of AugmentedFocus lies in its AR-enhanced lessons. We used the ARCore SDK to create immersive and interactive learning environments that integrate 3D objects and animations into language lessons [14]. ARCore was selected due to its compatibility with most smartphones and its ability to render high-quality 3D models in real-time, which is essential for creating engaging content for students with ADHD [15].

AR lessons are designed to incorporate language learning into interactive tasks, such as assembling virtual puzzles, interacting with 3D objects, and completing language-based challenges in a simulated environment. This gamification of learning has been shown to increase motivation and engagement

among students with ADHD, who often struggle to concentrate in traditional learning environments [16].

D. Testing and Evaluation

To ensure that the system met the needs of its users, several rounds of usability testing were conducted with students, teachers, and administrators. Participants were asked to complete specific tasks within the app, such as logging in, accessing lessons, and interacting with AR content. Their feedback was collected and analyzed to identify any usability issues or technical problems that required adjustments [17].

A mixed-methods approach was used to evaluate the application. Quantitative data was collected through system logs and performance metrics, while qualitative feedback was obtained through surveys and interviews with participants. This comprehensive approach allowed us to understand both the technical performance of the system and the user experience aspects [18].

E. Design tools

1) Figma: The use of Figma was essential for the design of the application since this allowed the different prototypes and mock ups to be made in addition to allowing collaborative work with the Development Team because it is a cloud-based technology where several people can edit in real time.

2) Vertabelo: This tool allowed us to create the application's database diagram thanks to the fact that it manages a structure of tables, indexes and relationships between them. This tool was very useful since it is based on cloud technology, which allows the Development Team to work collaboratively.

F. Development tools

1) Flutter: Flutter is an open source development framework created by Google. Firstly, it is well known for its high cross-platform compatibility when developing mobile applications and its simplicity when developing thanks to the Dart language. Secondly, it is a very good work tool because it offers the Hot reload functionalities that allow you to see the changes instantly without restarting the application and Widgets that are reusable components to build the application [10].

2) Dart: It is an open source programming language aimed at developing frontend applications, especially web and mobile. This programming language goes hand in hand with Flutter and is what makes it well known in the creation of multiplatform applications. What stands out most about Dart is the simple syntax it uses because it is very similar to Java, JavaScript and C++, flexible compilation, object-oriented, support for asynchronous functions, automatic memory management and great multiplatform support. Given all of the above, this is why Dart and Flutter are a great match in the frontend development of applications.

3) MySQL: It's relational database manager developed by Oracle. We chose because of his ease of organizing, managing and storing data for application testing.

4) Android studio: An integrated development environment (IDE) for developing Android applications, created by Google. This IDE allows development in languages such as Java, Kotlin, and C++.

5) Firebase: It is a platform based on cloud technology which offers various services such as real-time database, firestore, authentication, storage, hosting, messaging, analytics, crashlytics, predictions and other functionalities based on cloud databases. Firebase was mainly used to host our real-time database and to store and synchronize application data [12].

6) Django: It is a high-level framework that uses the Python programming language, which is characterized by its high development speed, but it does not leave security aside and helps developers avoid common errors in data security. It is also very efficient with both scalability and versatility, allowing developers to adapt their application to the needs of users. Django was chosen due to its ease and speed of development, as well as the great compatibility it has with applications that are related to augmented reality [13].

7) AR Core: It is the SDK developed by Google that focuses on offering a tool to create new interactive and immersive experiences on Android, iOS, Unity and the web. Using interactive objects in the virtual world where it includes motion tracking, depth understanding, environmental understanding, presenters and light estimation. The main use of this tool in the application is to provide augmented reality functionality to generate interactive classes for students with ADHD and thus capture and maintain the attention of students [14].

IV. Development of the Methodology

The Rational Unified Process (RUP) methodology was adopted to guide the development of AugmentedFocus. RUP is a software development process that divides the project lifecycle into four distinct phases: initiation, elaboration, construction, and transition. This methodology was chosen because it offers a structured approach to software development, which is crucial for managing complex projects such as AugmentedFocus [19].

A. Initiation Phase

During the initiation phase, the main focus was on understanding the application requirements, including the specific requirements of students with ADHD. Through collaboration with educators and specialists, key functionalities that AugmentedFocus should include were identified: AR-enhanced lessons, user-friendly navigation, and robust security for student data [20].

Stakeholder meetings were held to align project goals, feasibility, and timelines. An early prototype of the app was also developed to provide a proof of concept for the AR features and mobile interface.

The application requirements were identified through meetings and a prioritized list of applications was created Table I.

These are the functionalities to be developed identified thanks to the meetings with the Product Owner. These user stories also have their own task to be make for every developer during a sprint.

TABLE I. PRODUCT BACKLOG

Code	Title	Value (1/2/3/5/8)
US001	Complete a learning activity with augmented reality	8
US002	Access progress statistics	2
US003	Access additional educational content	5
US004	Record activity progress	1
US005	Set up custom activities with augmented reality	5
US006	Download augmented reality content for offline use	2
US007	Check achievements and progress in activities	2
US008	Log in to the app	1
US009	Interact with objects in augmented reality vocabulary	8
US010	Do vocabulary exercises with augmented reality	5
US011	Explore virtual reality with augmented reality	3
US012	User data security	1
US013	Application accessibility	1

B. Elaboration Phase

This phase includes the system architecture and design. Use cases were defined and a detailed system design was created that described how the various components of the application would interact with each other. The first functional prototype of the application was also developed in this phase, focusing on key features such as user authentication, lesson retrieval, and AR integration [21].

We started with first versions of Fig. 2 logic and Fig. 3 physical diagrams for the app before doing the C4 model diagrams with more specific information.

C. Construction Phase

This phase it's totally focused in the entire application, it was developed in Flutter, we used it to build the front-end of the mobile app, ensuring cross-platform functionality [23]. In parallel, the backend API was built using Django, while Firebase managed data storage and real-time communication between the server and mobile devices [24].

The version control used was github and everything about the application (backend, frontend) is in the repository. We used android studio during the whole development process and using the virtual simulator of android studio to test the application.

D. Transition Phase

This phase focus on deploying the application and ensuring its stability in real-world environments. It includes extensive testing to ensure that the application worked well on different devices and operating systems. In addition, final usability testing was conducted to validate that the user interface was intuitive and accessible for students with ADHD [25].

E. Development

The following images present the system architecture at different levels of the C4 diagram:

The system has three users:

1) *Students with ADHD*
2) *Teachers*
3) *Administrator*

Where these interact with the AugmentedFocus application which is composed of Mobile Application Frontend and Mobile Application Backend, it contains sign-in, security, authenticator controller, AR module, AR controller, lesson controller and notifications functionalities all connected to the database hosted in Firebase, in addition to an external notification system. After that we designed our C4 model diagrams. Firstly Fig. 4 context diagram secondly Fig. 5 container diagram and finally, Fig. 6 component diagram.

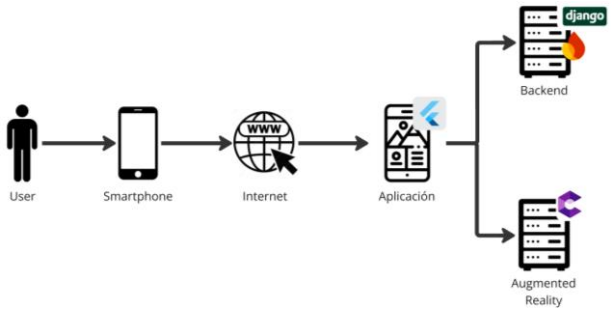


Fig. 2. Logic diagram of AugmentedFocus.

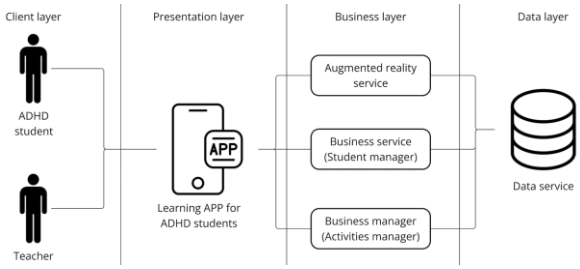


Fig. 3. Physical diagram of AugmentedFocus.

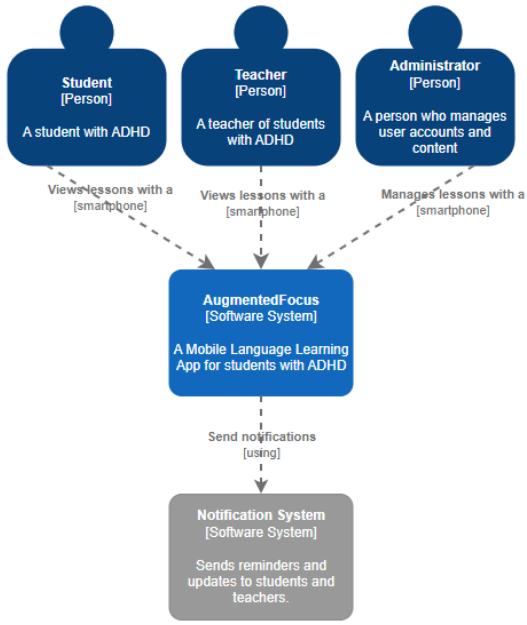


Fig. 4. Context diagram of the AugmentedFocus system.

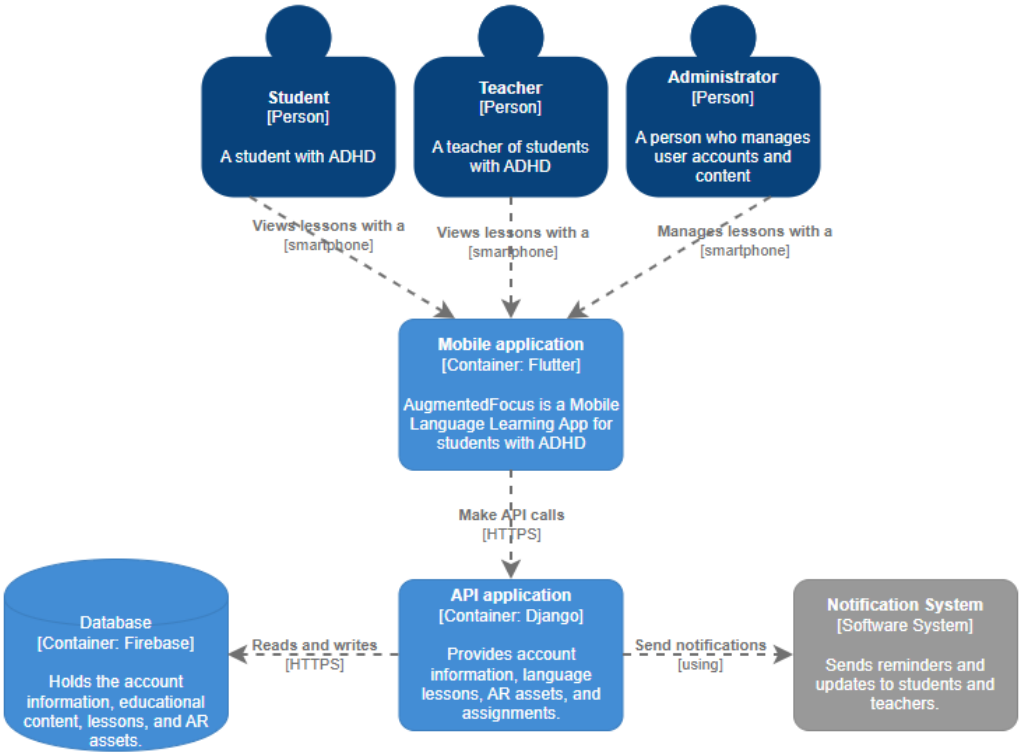


Fig. 5. Container diagram, showing how different systems interact with each other.

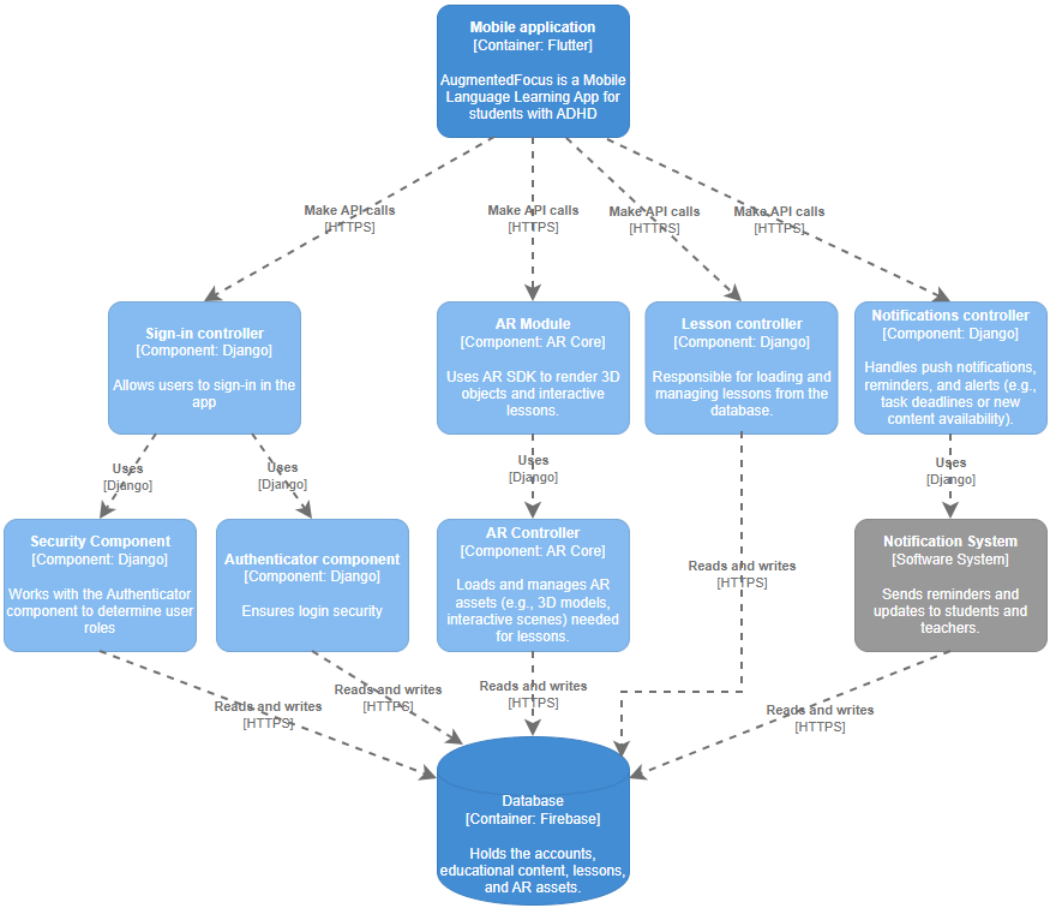


Fig. 6. Component diagram detailing the interactions between the different modules of the system.

After design of the C4 diagrams we decided to start with the mobile application prototypes, since it's an application for kids and teachers we needed to focus on something simple but at the same time useful for our users. Prototypes were designed for the application design which are: Fig. 7 - Welcome Prototype, Fig. 8 - Sign in and Register, Fig. 9 - Upcoming events and Course list, Fig. 10 - Course unit list and Course topic list, Fig. 11 - Grades and Profile, Fig. 12 - Activity and Activity description and Fig. 13. An example of an augmented reality activity. We choose a warm colors and an interface based on a kind of virtual classroom for students because we needed the structure that can be organized due to the activities and different courses that may exist in the school or institute.

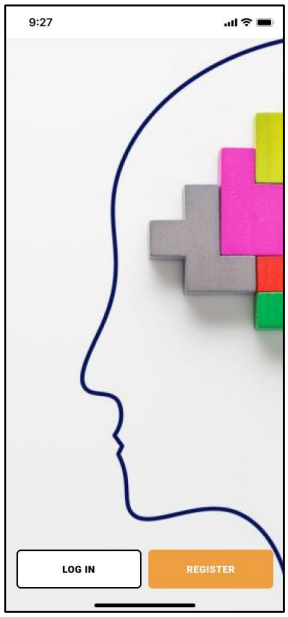


Fig. 7. Welcome prototype.

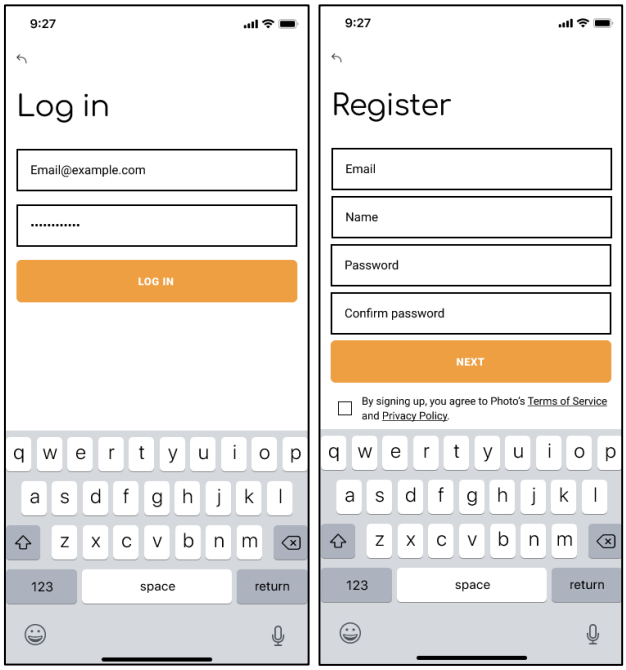


Fig. 8. Sign in and register prototype.

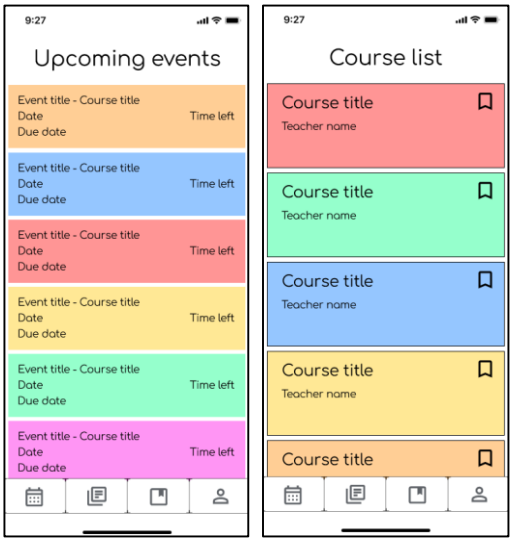


Fig. 9. Prototype upcoming events and course list.

Fig. 10. Prototype of course unit list and course topic list.

Fig. 11. Prototype of grades and profile.

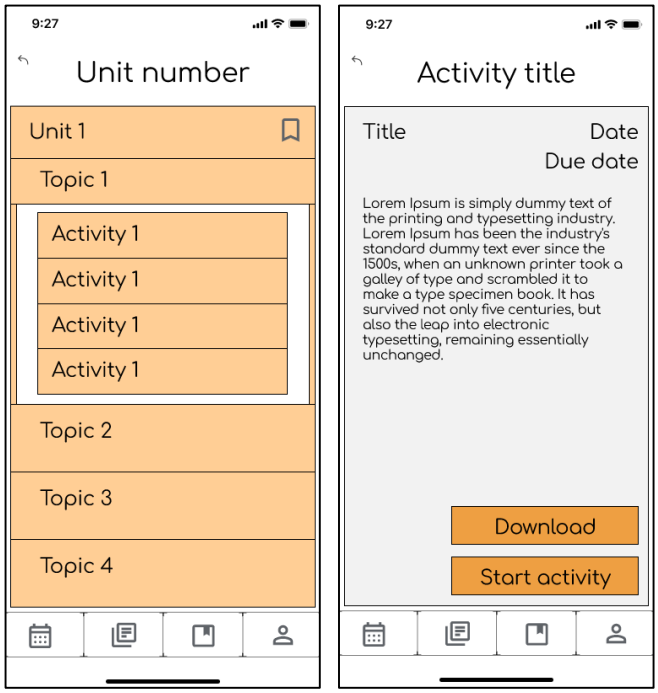


Fig. 12. Prototype of activity and activity description.

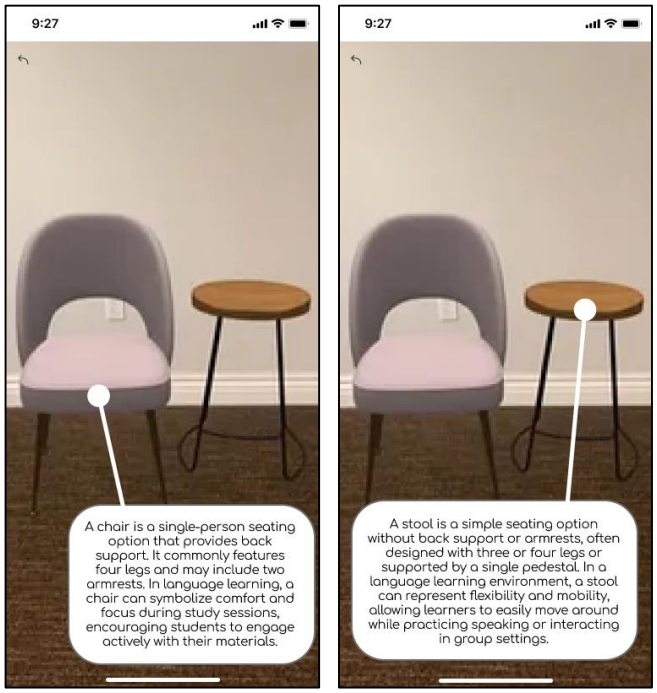


Fig. 13. Prototype of example of augmented reality activity.

V. Application Features

The application offers three very important functionalities to help children with ADHD learn language, including augmented reality activities, a student grade manager, and an augmented reality activity manager.

A. Activities with Augmented Reality

This feature is the main and most important of the application, which gives students the possibility of carrying out language learning activities with augmented reality. This involves interactively combining language classes with 3D models to capture the attention of students with ADHD, which allows capturing and maintaining the attention of these students.

B. Student Manager

Once all students have their account, teachers will be able to monitor information, grades and progress to check their performance within the course and in the same way check whether students are adequately acquiring the knowledge from the classes.

C. Activity Manager with Augmented Reality

The platform provides a manager for augmented reality activities that allows you to enable or disable the different augmented reality activities. This functionality is only enabled for the application administrator.

VI. Results

The tests of usability were done getting a completely well-done performance, the AugmentedFocus app over ten weeks of development. Key performance indicators are lessons activities, lesson completion rates, and feedback on the usability made by the development team. The results were good showing a nice performance and content compared to traditional learning methods. Since we are in the development phase our results are the design and development of the application, which is ready to be tested with real students with ADHD.

VII. Discussion

The results of this study, however, conform to previous studies noting the advantages of augmented reality for students, particular those who are slow learners or have attention problems [26] [27]. The attention deficit that these students may at times present, as a characteristic feature of an educational environment, was mitigated by AR-designed lessons which are interactive and more engaging for students with ADHD [22], [28]. It was evident that this method not only improved students' concentration but also contributed to create a lively and interesting atmosphere which is important in enhancing learning in such age groups. The AR lessons were able to provide experiences that integrate both active visualization and interaction thus making the acquisition of knowledge and skills much easier.

VIII. Conclusion

As AugmentedFocus proves, there can be useful applications of augmented reality in helping students learn with Attention Deficit Hyperactivity Disorder (ADHD), especially in foreign language learning. In the case of this particular app, interactive lessons which also include some gamification elements were included which lead to children having improved focus in their tasks as well as less impulsiveness which is often characteristic of this demographic and is a major obstacle to learning. In this light, the above results indicate that the adoption of new technologies such AR for example, can help change the concept

of how the teachers teach learners with lower cognitive abilities in an even better manner and that is a universal fit approach.

IX. Future Work

Future development of AugmentedFocus will focus on expanding the app to cover a broader range of subjects beyond language learning, such as math, science, and social studies. The approach will broaden the platform's utility, allowing more students to benefit from its interactive features. Additionally, we were thinking about adding adaptive learning algorithms to further personalize lessons based on each student's individual progress and behavior. By tailoring content to users' specific needs, it is hoped to improve learning effectiveness and foster greater motivation. The long-term impact of AugmentedFocus on students' academic performance and emotional well-being will also be evaluated, with the goal of creating a comprehensive educational tool that responds to the unique demands of those with ADHD.

References

[1] Kim, J., et al. (2024). Visual Attention and Pulmonary VR Training System for Children With ADHD. IEEE Access, 12, 53739-53750. https://doi.org/10.1109/ACCESS.2024.3387065

[2] Wiebe, A., et al. (2022). Multimodal Virtual Reality-Based Assessment of Adult ADHD: A Feasibility Study in Healthy Subjects. Assessment, 30(5), 1435-1453. https://doi.org/10.1177/10731911221089193

[3] Zangiacomi, A., et al. (2022). An Immersive Virtual Reality-Based Application for Treating ADHD: A Remote Evaluation of Acceptance and Usability. Digital Health, 8, 1-11. https://doi.org/10.1177/20552076221143242

[4] Bernardelli, G., Flori, V., & Greci, L. (2023). Remote VR Assessment for ADHD Interventions. Virtual Reality Journal, 18(2), 175-188.

[5] Rizzo, A., & Buckwalter, J. (2016). The Use of Virtual Reality for ADHD Assessment and Intervention. Journal of Neuropsychology, 12(3), 234-241. http://dx.doi.org/10.1089/10949310050078940

[6] Iriarte, Y., & Álvarez, P. (2018). Educational Technologies for ADHD: The Future of Learning. Learning Technologies Review, 45(6), 203-214.

[7] Lopez, M.A., & Gonzales, T.R. (2019). AR in Language Learning for ADHD Students. Educational Augmentation, 8(1), 345-356.

[8] Yang, Q. (2022). Advances in AR-Based Cognitive Learning. Journal of Immersive Technologies, 24(7), 289-312.

[9] Chen, W., & Sun, J. (2021). Improving Attention in ADHD Students Through AR Interventions. Cognitive Rehabilitation Journal, 15(2), 188-202.

[10] Fang, H., & Zhang, Z. (2023). Using Flutter for Cross-Platform Mobile Development: An Overview. Mobile Computing Advances, 11(3), 299-318.

[11] Haro, J., & Ramirez, P. (2022). Developing Mobile Applications With Flutter: Best Practices. Journal of Mobile Development, 6(4), 100-122.

[12] Google Developers. (2023). Firebase as a Cloud-Based Solution for Scalable Apps. Firebase Documentation. Retrieved from https://firebase.google.com/docs

[13] Python Foundation. (2022). Django Documentation: A Secure Framework for Web Development. Retrieved from https://docs.djangoproject.com

[14] Google Developers. (2023). ARCore Overview: Bringing AR to Mobile Devices. ARCore Documentation. Retrieved from https://developers.google.com/ar

[15] Paredes, F., & Rodriguez, S. (2023). AR Technologies in Education: A Review. Journal of AR Education, 5(4), 120-137. https://doi.org/10.1109/ICRoM.2018.8657615

[16] Mühlberger, A., & Hlavka, A. (2021). Gamification in AR-Based Learning. Journal of Interactive Learning Technologies, 13(5), 350-368.

[17] Montoya, S., & Herrera, G. (2022). Usability Testing in AR Applications: Lessons Learned. HCI Journal, 10(1), 102-120. https://uxdesign.cc/usability-testing-in-augmented-reality-df8f6c8d0d71

[18] El-Assar, K., & Martinez, R. (2021). A Mixed-Methods Approach to Evaluate AR-Based Learning Systems. Educational Technology Review, 19(2), 289-301.

[19] Larman, C. (2004). Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and the Unified Process. Pearson Education. https://personal.utdallas.edu/~chung/SP/applying-uml-and-patterns.pdf

[20] Gomero, V., & Andrade, L. (2021). Prototype of Web System for E-commerce Under SCRUM Methodology. International Journal of Advanced Computer Science and Applications, 12(1), 12-25. http://dx.doi.org/10.14569/IJACSA.2021.0120152

[21] Hall, J., & Geary, D. (2021). AR and Language Learning for Children With ADHD. Education and Technology Review, 8(6), 312-334. https://doi.org/10.1080/0144929X.2024.2304607

[22] Mendez, P., & Chavez, R. (2022). ARCore for Enhanced Learning in Children With ADHD. Educational Technologies Journal, 18(3), 233-248.

[23] Blake, A., & Thomas, J. (2023). Using Flutter for Mobile App Development: A Case Study. Journal of Mobile Programming, 7(1), 22-45.

[24] Shinohara, K., & Chen, A. (2023). Data Security in Educational Apps: A Case Study Using Firebase. Cloud-Based Systems in Education, 9(2), 112-130.

[25] Puri, A., & Sharma, T. (2021). Managing API Integrations With Django. Tech Innovations Journal, 15(7), 97-110.

[26] Franke, B., & Francx, M. (2018). The Neural Basis of ADHD and Technology-Enhanced Interventions. Neuropsychology Journal, 14(2), 145-167. https://doi.org/10.1186/1824-7288-36-79

[27] Nigg, J., & Willcutt, E. (2021). Cognitive Deficits in ADHD: Current Perspectives. Journal of ADHD Research, 20(3), 250-268.

[28] Koehler, S., & van Dijk, T. (2020). ADHD and Learning Technologies: What Works? Cognitive Technologies Review, 6(4), 210-226.

[29] Marks, B., Thomas, J. (2022). Adoption of virtual reality technology in higher education: An evaluation of five teaching semesters in a purpose-designed laboratory. Educ Inf Technol 27, 1287–1305. https://doi.org/10.1007/s10639-021-10653-6

Classification of Painting Style Based on Image Feature Extraction

Yuting Sun
Zhoukou Vocational College of Arts and Sciences, Zhoukou, Henan 466000, China

***Abstract*—The classification of painting style can help viewers find the works they want to appreciate more conveniently, which has a very important role. This paper realized image feature extraction and classification of paintings based on ResNet50. On the basis of ResNet50, squeeze-and-excitation, and convolutional block attention module (CBAM) attention mechanisms were introduced, and different activation functions were selected for improvement. Then, the effect of this method on painting style classification was studied using the Pandora dataset. It was found that ResNet50 obtained the best classification accuracy under a learning rate of 0.0001, a batch size of 32, and 50 iterations. After combining the CBAM attention mechanism, the accuracy rate was 65.64%, which was 6.77% higher than the original ResNet50 and 2.52% higher than ResNet50+SE. Under different activation functions, ResNet50+CBAM (CeLU) had the most excellent performance, with an accuracy rate of 67.13%, and was also superior to the other classification approaches such as Visual Geometry Group (VGG) 16. The findings prove that the proposed approach is applicable to the style classification of painting works and can be applied in practice.**

***Keywords*—Feature extraction; painting; style classification; ResNet50; attention**

I. Introduction

A. Research Background

Under the influence of the continuous development and progress of various technologies, more and more resources are stored in the format of data, which provides a way for people to get the resources they want more conveniently and quickly. Painting, as an art form, has accumulated many excellent works after a long development. An increasing number of approaches have been applied in the research and analysis of paintings as the machine vision technology gradually develops [1]. Painting style refers to the artistic characteristics and expression techniques shown by artists in their works, which can reflect the emotions, personalities, and aesthetics during the creation of artists [2]. The classification of painting styles can help people gain a better understanding of different painting styles, which is an important content in the research of paintings. The traditional style classification of paintings is carried out by professional appreciation experts, which requires experts to have excellent professional knowledge and appreciation ability [3]. However, the manual method requires a lot of workload and has a low efficiency. With the development of machine vision, there is a growing trend of preserving paintings in digital format. As an image classification task, painting style classification can also be realized based on image classification technology.

B. Literature Review

In the current classification of painting works, most methods used to achieve classification based on the extraction and quantification of image color, texture, and other features [4]. Liu [5] decomposed paintings into sparse components and other components based on sparse decomposition and then realized style classification using naive Bayes. It was found through experiments that this method achieved 98.63% accuracy and consumed the shortest classification time. Li et al. [6] extracted the main details and edge information from Dongba paintings for the classification of Naxi Dongba paintings, realized the classification based on a multi-layer graph neural network (GNN), and proved the advantages of this method through experiments on small sample datasets. Bianconi [7] evaluated the effects of color stability and enhancement in paintings and found that neither feature showed significant advantages. Deep learning methods have shown strong capabilities in image feature extraction. Considering the shortcomings of traditional methods in feature extraction, deep learning-based approaches have been increasingly applied in image processing [8]. Liong et al. [9] compared the effectiveness of several deep learning approaches for the automatic classification of Chinese paintings and found that the improved pre-trained neural network achieved 99.66% accuracy when classifying more than 1,000 Chinese paintings belonging to six categories. Qing and Ce [10] proposed a multi-scale convolutional neural network (CNN) framework for classifying painting images, which can integrate global and local information into a single image. They achieved accuracies of 74.12% and 75.88% for the WikiArt dataset and Web Gallery of Art dataset respectively. Zhao et al. [11] constructed an artistic comment graph based on co-occurrence relations and document word relations, enabling through analysis of art comments, they used a graph convolutional network technology to realize the classification of painting types, genres, etc. Extensive experiments verified the performance of this method. Zhong et al. [12] proposed a dual-channel dual-path network for art painting classification. Experiments on two datasets demonstrated that this method achieved good classification accuracy.

C. Research Content

This paper conducted research on the classification of painting styles based on image feature extraction. In Section II, it introduces a method for image feature extraction and classification based on ResNet50, and the improvement to ResNet50 was proposed. In Section III, the designed method was experimentally validated, and the experimental dataset

and results were described, demonstrating the effectiveness of the proposed improvement to ResNet50. Compared with current research, this paper achieved optimization of ResNet50 performance in terms of the attention mechanism and activation function. This article provides a novel and useful method for the classification of painting styles in practice and provides strong support for subsequent painting retrieval and artist identification. Finally, the paper is concluded in Section IV.

II. Image Feature Extraction and Classification Based on ResNet50

A. ResNet50

In the study of image classification, the frequently used method is to extract image features such as color and texture [13] and then classify images based on decision trees, neural networks, and other classifiers. However, compared with ordinary images, paintings contain more details and artistry. Therefore, the traditional image classification methods have poor performance in the classification of painting styles. Deep learning can extract image features through a deep network and realize automatic classification [14]; therefore, feature learning is deeper and more comprehensive. Therefore, this paper chooses the deep learning method to classify painting styles.

ResNet50 is a kind of deep CNN [15]. Generally speaking, as the quantity of layers in the network increases, gradient explosion and disappearance may occur when the feature extraction ability of the network is improved. However, the ResNet series network uses skip connection, that is, in the forward propagation, the input of a layer is directly transmitted to the following layers, so that the feature information of different layers can be transmitted to each other. It has been extensively used in image classification and other scenarios [16]. ResNet50 consists of 49 convolutional layers and one fully connected layer, and Table I presents its structure.

TABLE I. ResNet50 Structure

Layer name	50-Layer
Conv1	7×7, 64, S=2 3×3 maxpool, S=2
Conv2_x	$\begin{bmatrix} 1\times1,64 \\ 3\times3,64 \\ 1\times1,256 \end{bmatrix}\times3$
Conv3_x	$\begin{bmatrix} 1\times1,128 \\ 3\times3,128 \\ 1\times1,512 \end{bmatrix}\times4$
Conv4_x	$\begin{bmatrix} 1\times1,256 \\ 3\times3,256 \\ 1\times1,1024 \end{bmatrix}\times6$
Conv5_x	$\begin{bmatrix} 1\times1,512 \\ 3\times3,512 \\ 1\times1,2048 \end{bmatrix}\times3$
	Mean pool, fully connected layer, Softmax

As shown in Table I, ResNet50 first carries out a convolution and maximum pooling and then carried out feature extraction through four modules with 3, 4, 6, and 3 repetitions. Each block contains three convolutions, and the size of the convolution kernel is 1, 3, and 1, respectively. Finally, the obtained features are passed through mean pooling and the fully connected layer. Softmax outputs classification results.

B. Improvements to ResNet50

In order to enhance ResNet50's focus on the important information related to style distinction in paintings, this paper introduces the attention mechanism to improve the traditional ResNet50. For the modules from Conv2_x to Conv5_x in ResNet50, an attention module is added at the end of each module to improve ResNet50's ability to learn important features. The following two types of attention modules are added.

1) Squeeze-and-excitation (SE) attention mechanism [17]: its principle is to realize the attention of the channel with a high weight by adding a weight to each channel in the feature graph, and there are three main steps.

a) Squeeze: Before squeeze, the importance of each channel is the same. For a $H \times W \times C$ feature graph ($H \times W$ represents the height and width of the feature graph, C is the quantity of channels), the feature value of each channel is computed:

$$z_j = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{k=1}^{W} X_{ijk} \quad (1)$$

where X_{ijk} refers to the pixel value of the j-th channel in the i-th row and k-th column of the feature map.

b) Excitation: The weight for each channel is learned based on the fully connected neural network. The weight of the j-th channel is written as:

$$s_j = \sigma\big[W_2 f\big(W_1 z_j\big)\big], \quad (2)$$

where W_1 and W_2 are the weights of the two fully connected layers.

c) Scale: The feature graph is weighted based on the channel weight. The weighted feature graph is written as:

$$\tilde{X}_{ijk} = s_j \times X_{ijk}. \quad (3)$$

2) Convolutional block attention module (CBAM) attention mechanism [18]: its principle is to weight both channel and spatial dimensions. The features of the two dimensions are described as follows.

a) Channel attention: The feature descriptions of different dimensions are obtained through pooling operation and then stacked on the channel dimension:

$$M_c(X) = \sigma\big[MLP\big(AvgPool(X)\big) + MLP\big(MaxPool(X)\big)\big], \quad (4)$$

where σ is the Sigmoid activation function and MLP is the fully connected layer.

b) Spatial attention: The feature representations of different dimensions are obtained through pooling operation. After splicing, it passes through a 7×7 convolution layer and then through the Sigmoid function to get the weight coefficient. After multiplying the coefficient with the features,

the final feature map is obtained:

$$M_s(X) = \sigma\left[f^{7\times7}\left(AvgPool(X); MaxPool(X)\right)\right], \quad (5)$$

where $f^{7\times7}$ is a 7×7 convolution kernel

In addition to adding the attention mechanism, the ReLU activation function used in ResNet50 is also improved, and the following activation functions are selected:

- PReLU [19]: $PReLU = max(0, x) + t * min(0, x)$, t takes the default value of 0.25;
- LeakyReLU [20]: $LeakyReLU = \begin{cases} x, x \geq 0 \\ ax, x < 0 \end{cases}$, a takes the default value of 0.01;
- CeLU [21]: $CeLU = max(0, x) + min\left(0, a * \left(exp\left(\frac{x}{a}\right) - 1\right)\right)$, a takes the default value of 1.

III. Experiment and Results

A. Experimental Setup

The experiment was carried out on a Windows 64-bit system, with Inter(R)Core(TM)i5-12500 and 32 G memory. The algorithm was implemented based on the TensorFlow2.4.0 framework. Python programming language was used.

At present, in the investigation of categorizing painting styles, the commonly used datasets include Pandora dataset [22], Wikipaintings dataset [23], etc. As the latter contains more than 80,000 works, it is impossible to achieve adequate training under the limited computing resources. Therefore, only a few images were selected from the Wikipaintings dataset for study. The experimental datasets used are as follows.

1) Pandora dataset: There are a few types of painting styles in it, but they include different styles from 17th ancient Greece to the present. Table II presents different styles and the corresponding number of paintings. During the experiment, an 80% portion was allocated for training purposes while the remaining 20% was designated as the test set.

TABLE II. Distribution of the Pandora Dataset1

Style	Number
Pottery of ancient Greece	350
Movement to destroy religious statues	665
Renaissance	812
Baroque	960
Rococo style	844
Romanticism	874
Realism	307
Impressionism	984
Brutalism	426
Cubism	920
Surrealism	242
Abstract expressionism	340

2) Wikipaintings dataset: It includes more than 80,000 painting works belonging to 25 styles. This paper selected images from ten of these styles for research. The selected styles and corresponding number are shown in Table III. They were also divided into a training set and a test set in a ratio of 8:2.

TABLE III. The Distribution of the Wikipaintings Dataset

Style	Number
Rococo	1,007
Baroque	1,056
Neoclasscism	1,345
Impressionism	1,541
Expressionism	1,112
Early Renaissance	1,512
High Renaissance	1,864
Post-Impressionism	1,825
Surrealism	1,854
Symbolism	1,021

The evaluation of the classification performance was based on the following indicators.

a) Accuracy (A): The proportion of the correctly classified samples to total samples is:

$$A = \frac{n_{TP}+n_{TN}}{n_{TP}+n_{TN}+n_{FP}+n_{FN}},$$

where n_{TP} refers to the true positive sample, n_{TN} refers to the true negative sample, n_{FP} refers to the false positive sample, and n_{FN} refers to the false negative sample.

b) Precision (P): The proportion of positive samples classified as positive is:

$$P = \frac{n_{TP}}{n_{TP}+n_{FP}}.$$

c) Recall rate (R): The proportion of positive samples classified as positive is:

$$R = \frac{n_{TP}}{n_{TP}+n_{FN}}.$$

d) F1 value: The comprehensive evaluation of P and R is:

$$F_1 = \frac{2\times P\times R}{P+R}.$$

B. Analysis of Results

In the follow-up experiment, the parameters of ResNet50 were adjusted to obtain better classification performance. Parameter experiments were performed on the Pandora dataset. First, for the learning rate, the batch size was set at 32, and the total count of iterations was 50. The changes in accuracy under different learning rates are presented in Fig. 1.

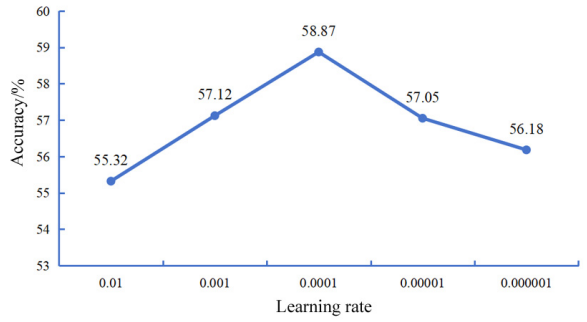


Fig. 1. Changes in accuracy under different learning rates.

In the process of the learning rate decreasing from 0.01 to 0.0001, the accuracy of the improved ResNet50 gradually increased. It reached the highest (58.87%) when learning rate = 0.0001 and then declined. Therefore, the optimal learning rate was 0.0001.

For the batch size, the learning rate was fixed at 0.0001, and the count of iterations was 50. The variation in accuracy under different batch sizes is presented in Fig. 2.

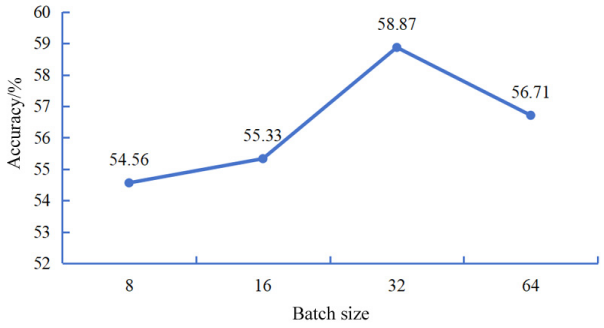


Fig. 2. Changes in accuracy under different batch sizes.

As the batch size increased, the improved ResNet50 also became more accurate. When the batch size was 8, the accuracy was 54.56% at the lowest level, and it was 32, the accuracy was 58.87% at the highest level. Therefore, the optimal batch size was 32.

For the number of iterations, the learning rate was fixed at 0.0001, and the batch size was 32. The changes in accuracy under different iteration numbers are displayed in Fig. 3.

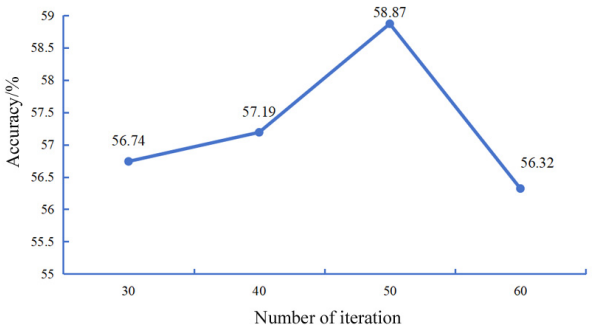


Fig. 3. Changes in accuracy rate under different iterations.

It can be found that when the number of iterations was 60, the accuracy of ResNet50 was the lowest, which was 56.32%; when the count of iterations was 50, the accuracy was the highest (58.87%). Therefore, the optimal number of iterations was 50.

Based on the above results, in the subsequent experiments, the learning rate of ResNet50 was set as 0.0001, the batch size was 32, and the count of iterations was 50. Moreover, ResNet50 was compared with other traditional residual network models. The floating point operations per seconds (FlOPs) and parameters of different algorithms are presented in Table IV.

TABLE IV. COMPARISONS WITH OTHER RESIDUAL NETWORK MODELS

	ResNet18 [24]	ResNet34 [25]	ResNet50	ResNet101 [26]
Accuracy/%	56.46	58.41	58.87	58.89
FLOPs/G	3.67	7.35	8.21	15.54
Parameter/M	11.71	21.83	25.55	44.56

It can be seen that with the increasing depth of the network, the accuracy of ResNet also gradually increased. Among them, ResNet101 achieved the highest accuracy at 58.89%, which indicated a slight improvement of 0.02% compared to ResNet50. However, there was a significant increase in FLOPs and parameter for ResNet101 compared to ResNet50, which not only increased the complexity of the model but also imposed higher requirements on hardware facilities. This was not conducive to practical applications. On the other hand, ResNet50 achieved a good balance between classification performance and complexity, verifying its reliability.

For the improvement of ResNet50, the original ResNet50 was combined with different attention mechanisms. The accuracy for different datasets is presented in Table V.

TABLE V. RESNET50 COMBINING DIFFERENT ATTENTION MECHANISMS

	Pandora dataset	Wikipaintings dataset
ResNet50	58.87	51.37
ResNet50+SE	63.12	56.54
ResNet50+CBAM	65.64	58.79

As shown in Table V, when the Pandora dataset was used, after combining ResNet50 with the SE attention mechanism, the accuracy was 63.12%, which was 4.25% higher than the original ResNet50; when combined with the CBAM attention mechanism, the accuracy was 65.64%, which was 6.77% higher than the original ResNet50 and 2.52% higher than ResNet50+SE. When the Wikipaintings dataset was used, after combining ResNet50 with the SE attention mechanism, the accuracy achieved was 56.54%, which showed an improvement of 5.17% compared to the original ResNet50. When combined with the CBAM attention mechanism, the accuracy obtained was 58.79%, which showed an improvement of 7.42% compared to the original ResNet50 and an improvement of 2.25% compared to ResNet50+SE. These results showed that compared with SE, CBAM

combined with ResNet50 could achieve better performance in the style classification of paintings and had stronger ability to extract image features.

Then, on the basis of ResNet50+CBAM, the improvement of the activation function was compared. The accuracy for different datasets is presented in Table VI.

TABLE VI. RESNET50 COMBINED WITH DIFFERENT ACTIVATION FUNCTIONS2

	Pandora dataset	Wikipaintings dataset
ResNet50+CBAM (ReLU)	65.64	58.79
ResNet50+CBAM (PReLU)	66.32	59.42
ResNet50+CBAM (LeakyReLU)	66.87	59.98
ResNet50+CBAM (CeLU)	67.13	60.37

The ReLU used in the original ResNet50 had the worst performance in classifying painting styles from the Pandora dataset, with an accuracy of only 66.32%. After replacing it with PReLU, the accuracy reached 66.32% (+0.68%). After replacing it with LeakyReLU, the accuracy reached 66.87% (+1.23%). After replacing it with CeLU, the accuracy reached 67.13% (+1.49%). It exhibited the same results for the Wikipaintings dataset. These results showed that CeLU could achieve the best effect in the style classification of paintings in ResNet50+CBAM.

Finally, the ResNet50+CBAM (CeLU) was compared with other methods (Table VII).

TABLE VII. COMPARISON BETWEEN DIFFERENT FEATURE EXTRACTION NETWORKS3

		Accuracy/ %	Precision/ %	Recall rate/ %	F1 value/ %
Pandora dataset	Pyramid local binary pattern (PLBP)+color structure descriptor (CSD)+support vector machine (SVM) [22]	54.70	52.13	50.77	51.44
	MobileNet [27]	54.87	52.31	51.22	51.76
	AlexNet [28]	55.36	53.64	52.11	52.86
	Visual Geometry Group (VGG) 16 [29]	56.52	54.77	55.07	54.92
	VGG 19 [30]	57.12	55.67	55.88	55.77
	InceptionV3 [31]	57.64	56.78	55.97	56.37
	ResNet50	58.87	57.32	56.42	56.87
	ResNet50+CBAM (CeLU)	67.13	65.45	64.59	65.02
Wikipaintings dataset	PLBP+CSD+SVM [22]	47.12	46.77	46.02	46.39
	MobileNet [27]	47.37	47.31	46.54	46.92
	AlexNet [28]	48.05	47.87	46.79	47.32
	VGG 16 [29]	49.35	48.61	47.56	48.08
	VGG 19 [30]	51.07	50.87	48.97	49.90
	InceptionV3 [31]	51.25	51.12	50.33	50.72
	ResNet50	51.37	51.07	50.98	51.02
	ResNet50+CBAM (CeLU)	60.37	59.84	58.49	59.16

It can be found that the traditional method PLBP+CSD+SVM based on feature extraction and classifier had poor performance in painting style classification, with the lowest accuracy of only 54.70% and 47.12%. Specifically, the ResNet50+CBAM (CeLU) exhibited the optimal performance for the two datasets, with F1 values of 65.02% and 59.16%, verifying the reliability of this method in classifying painting styles. Therefore, it can be used in practice to support the classification and retrieval of paintings in real life.

IV. CONCLUSION

This paper studied the classification of painting work styles. A ResNet50-based image feature extraction method was developed to obtain a higher-performance classification algorithm. ResNet50 was improved from aspects of attention mechanism and activation function to achieve image feature extraction and classification. Through experiments on the Pandora dataset, it was found that the classification accuracy achieved by ResNet50+CBAM (CeLU) was 67.13%, which was better than the other deep learning methods. This paper verifies the reliability of the proposed approach; thus, it can be applied in the actual classification of painting styles. The method can be applied in the field of painting work classification and painting information retrieval to promote the informatization and digitization of painting work management.

REFERENCES

[1] J. Kim, J. Y. Jun, M. Hong, H. Shim and J. Ahn, "Classification of oil painting using machine learning with visualized depth information," Int. Arch. Photogramm. Remote Sens. Spatial Inform. Sci., vol. XLII-2/W15, pp. 617-623, 2019.

[2] S. H. Lee and J. Y. Kim, "Classification of the Era Emotion Reflected on the Image Using Characteristics of Color and Color-Based Classification Method," Int. J. Softw. Eng. Know., vol. 29, pp. 1103-1123, 2019.

[3] C. Sandoval, E. Pirogova and M. Lech, "Classification of Fine-Art Paintings with Simulated Partial Damages," 2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1-8, 2020.

[4] Q. Wang and Z. Huang, "Painter artistic style extraction method based on color features," J. Comput. Appl., vol. 40, pp. 1818-1823, 2020.

[5] S. Liu, "Research on the classification method of artistic painting image style based on naive Bayesian," Int. J. Inform. Commun. Technol., vol. 21, pp. 398-411, 2022.

[6] K. Li, W. Qian, C. Wang and D. Xu, "Dongba Painting Few-Shot Classification Based on Graph Neural Network," J. Comput.-Aided Des. Comput. Graph., vol. 33, pp. 1073-1083, 2021.

[7] F. Bianconi, "Experimental analysis of colour constancy and colour augmentation for painting classification by artistic genre: preliminary results," IOP Conf. Ser.: Mater. Sci. Eng., vol. 949, pp. 1-8, 2020.

[8] D. Li and Y. Zhang, "Multi-Instance Learning Algorithm Based on LSTM for Chinese Painting Image Classification," IEEE Access, vol. 8, pp. 179336-179345, 2020.

[9] S. T. Liong, Y. C. Huang, S. Li, Z. Huang, J. Ma and Y. S. Gan, "Automatic traditional Chinese painting classification: A benchmarking analysis," Comput. Intell., vol. 36, pp. 1183-1199, 2020.

[10] Y. Qing and S. Ce, "An image classification approach for painting using improved convolutional neural algorithm," Soft Comput., vol. 28, no. 1, pp. 847-873, 2024.

[11] W. Zhao, D. Zhou, X. Qiu, W. Jiang and W. Jiang, "How to represent paintings: a painting classification using artistic comments," Sensors, vol. 21, no. 6, pp. 1-15, 2021.

[12] S. H. Zhong, X. Huang and Z. Xiao, "Fine-art painting classification via two-channel dual path networks," Int. J. Mach. Learn. Cyb., vol. 11, no. 1, pp. 137-152, 2020.

[13] Q. Yong and N. Jan, "Research on Painting Image Classification Based on Transfer Learning and Feature Fusion," Math. Probl. Eng., vol. 2022, pp. 1-10, 2022.

[14] A. Inés, C. Domínguez, J. Heras, E. Mata and V. Pascual, "DeepClas4Bio: Connecting bioimaging tools with deep learning frameworks for image classification," Comput. Biol. Med., vol. 108, pp. 49-56, 2019.

[15] S. Raveena and R. Surendran, "ResNet50-based Classification of Coffee Cherry Maturity using Deep-CNN," 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 1275-1281, 2023.

[16] A. Raj and R. K. Bhukya, "Vocal Biomarker Based COVID-19 Detection Using DNN and Transfer Learning ResNet50," 2022 IEEE 9th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), pp. 1-6, 2022.

[17] Y. Chang, J. Chen, Q. Chen, S. Liu and Z. Zhou, "CFs-focused intelligent diagnosis scheme via alternative kernels networks with soft squeeze-and-excitation attention for fast-precise fault detection under slow & sharp speed variations," Knowl.-based Syst., vol. 239, pp. 1-20, 2022.

[18] S. Zhao, T. H. Nguyen and B. Mam, "Monaural Speech Enhancement with Complex Convolutional Block Attention Module and Joint Time Frequency Losses," ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6648-6652, 2021.

[19] K. He, X. Zhang, S. Ren and J. Sun, "Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification," 2015 IEEE International Conference on Computer Vision (ICCV), pp. 1026-1034, 2015.

[20] M. V. Sowmya Lakshmi, Lalitha Saisreeja, L. Chandana, P. Mounika and U. Prabu, "A LeakyReLU based Effective Brain MRI Segmentation using U-NET," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), pp. 1251-1256, 2021.

[21] J. T. Barron, "Continuously Differentiable Exponential Linear Units," 2017.

[22] C. Florea, R. Condorovici, C. Vertan, R. Butnaru, L. Florea and R. Vrânceanu, "Pandora: Description of a painting database for art movement recognition with baselines and perspectives," 2016 24th European Signal Processing Conference (EUSIPCO), pp. 918-922, 2016.

[23] S. Karayev, M. Trentacoste, H. Han, A. Agarwala, T. Darrell, A. Hertzmann and H. Winnemoeller, "Recognizing Image Style," Comput. Sci., pp. 1-10, 2013.

[24] Z. Wang, S. Tian, B. Wang and T. Zhou, "Lightweight object detection on marine life facing underwater environment," J. Xinjiang Univ., vol. 39, no. 5, pp. 598-607, 2022.

[25] F. Wang, J. Qiu, Z. Wang and W. Li, "Intelligent recognition of surface defects of parts by Resnet," J. Phys.: Conf. Ser., vol. 1883, no.1, pp. 1-6, 2021.

[26] S. Nawaz, S. Rasheed, W. Sami, L. Hussain, A. Aldweesh, E. Tageldin, U. A. Salaria and M. S. Khan, "Deep learning ResNet101 deep features of portable chest x-ray accurately classify COVID-19 lung infection," Comput., Mater. Con., no. 6, pp. 5213-5228, 2023.

[27] Z. Yang, X. Yang, H. Zhang, H. Jia, M. Zhou, Q. Mao, C. Ji and X. Wei, "An android malware detection method using multi-feature and MobileNet," J. Circuit. Syst. Comp., vol. 32, no. 17, pp. 1.1-1.19, 2023.

[28] S. A. Wagle and R. Harikrishnan, "Comparison of Plant Leaf Classification Using Modified AlexNet and Support Vector Machine," Trait. Signal, vol. 38, no.1, pp. 79-87, 2021.

[29] R. P. R. Chegireddy and A. Srinagesh, "A Novel Method for Human MRI Based Pancreatic Cancer Prediction Using Integration of Harris Hawks Varients & VGG16: A Deep Learning Approach," Informatica, vol. 47, no.1, pp. 115-129, 2023.

[30] H. S. Shashank, A. Acharya and E. Sivaraman, "Facial image super resolution and feature reconstruction using SRGANs with VGG-19-based adaptive loss function," 2023 International Conference on Artificial Intelligence and Applications (ICAIA) Alliance Technology Conference (ATCON-1), pp. 1-6, 2023.

[31] I. Tupal, M. Cabatuan and M. V. Manguerra, "Recognizing Filipino Sign Language with InceptionV3, LSTM, and GRU," 2022 IEEE 14th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM), pp. 1-5, 2022.

Application of Contrast Enhancement Method on Hip X-ray Images as a Media for Detecting Hip Osteoarthritis

Faisal Muttaqin[1], Jamari[2], R Rizal Isnanto[3], Tri Indah Winarni[4], Athanasius Priharyoto Bayuseno[5]
Information System Doctoral Program-School of Postgraduates Studies, Diponegoro University, Semarang, 50275, Central Java, Indonesia[1]
Department of Informatics-Faculty of Computer Science, University of Pembangunan Nasional Veteran Jawa Timur, Surabaya, 60294, East Java, Indonesia[1]
Department of Mechanical Engineering-Faculty of Engineering, Diponegoro University, Semarang, 50275, Central Java, Indonesia[2, 5]
Department of Computer Engineering-Faculty of Engineering, Diponegoro University, Semarang, 50275, Central Java, Indonesia[3]
Department of Anatomy, Faculty of Medicine, Diponegoro University, Semarang, 50275, Central Java, Indonesia[4]
Undip Biomechanics Engineering & Research Center (UBM-ERC),
Diponegoro University, Semarang, 50275, Central Java, Indonesia[2, 4]

***Abstract*—Image enhancement is one of the most important areas that is being developed in the field of image processing technology. Image contrast enhancement can significantly improve the perception of the digital image itself. X-ray images are crucial in assisting physicians in the formulation of treatment decisions based on diagnostic information. Contrast enhancement techniques, including Histogram Equalization (HE), Contrast Limited Adaptive Histogram Equalization (CLAHE), and CLAHE with double Gamma Correction (CLAGAMTWO), have been utilized on 30 distinct image datasets. Among the three employed methods, the CLAGAMTWO approach yields the optimal values of SSIM = 0.850 and CNR = 0.773. CLAHE has superior performance with an Entropy value of 7.099. CLAGAMTWO is the superior approach overall, as evidenced by the average metric value, yielding optimal picture quality in visual structure (SSIM), information detail (Entropy), and crisp contrast with little noise (CNR).**

Keywords*—*X-ray; image enhancement; digital image; image processing; grayscale image

I. INTRODUCTION

Image enhancement is one of the most important areas that is being developed in the field of image processing technology. This effectively delivers visual picture enhancement effects and image clarity, both of which are beneficial for subsequent processing and analysis on the computer [1], [2]. Contrast enhancement is critical for improving visual quality in computer vision, pattern recognition, and digital image processing. Low contrast in digital or video images can be produced by a number of causes, including operator inexperience and inadequate imaging equipment. Reduced contrast quality can also be caused by unfavorable environmental variables in the filmed image, such as lack of sunlight or indoor lighting, among others [3]. Articular cartilage and the structures supporting it are vulnerable to deterioration in the degenerative joint condition known as osteoarthritis [4], [5]. X-ray images are crucial in assisting physicians in the formulation of treatment decisions based on diagnostic information [6]. Plain radiology images or X-ray images are one method of determining the condition of the bones. Changes in the skeleton, structure, density, bone deformities, and narrowing of the articular space between adjacent bones can be observed through the use of X-ray images [7], [8], [9]. The low contrast issues in X-ray images of certain intricate components hinder the complete representation of structural information [10]. Consequently, low contrast poses a challenge in discerning elements inside a network area [11]. A possible solution to this problem is to improve the image [12].

Research conducted by study [13] Improve the accuracy of chest X-ray diagnosis by employing DF-GAN (Deep Fusion-Generative Adversarial Networks) data augmentation that is based on text-to-image interaction. The results that were obtained were a sensitivity value of 2.1%, a specificity value of 1.9%, and an area under the curve (AUC) value of 1.4%. Additionally, during training, overfitting was reduced on both sets of data.

Other research concerning the enhancement of chest X-ray images through the use of white balance and CLAHE (Contrast Limited Adaptive Histogram Equalization). The objective of the research is to enhance the precision of pneumonia diagnosis by leveraging the effectiveness of MobileNetV2 and contrast enhancement. It is important to mention that the model achieved the highest accuracy and lowest loss in 50 epoch testing for three-class classification (91.17% accuracy, 35.0% loss) and two-class classification (99.76% accuracy, 7% loss) [14].

Augmented chest X-ray image executed by [15] via deep contrast diffusion learning. The original input image undergoes a multilayer contrast-limited adaptive histogram equalization (CLAHE) method. The low and required contrast are subsequently extracted using CLAHE and transmitted to a residual learning network founded on a convolutional neural network (CNN). The suggested model exhibits a superior

structural similarity index measure (SSIM) compared to alternative techniques.

A class of fractional differential equations can be employed for X-ray picture enhancement [16]. This work determines picture pixel energy utilizing the general k differential equation, which is founded on the K-caputo fractional differential operator (K-CFDO), to enhance visual quality and delineate the problem clearly. The investigation yielded the Brisque, Niqe, and Piqe values for chest X-rays as follows: (Brisque = 23.25, Niqe = 2.8, Piqe = 21.58) and for oral X-rays as follows: (Brisque = 21.12, Niqe = 3.77, Piqe = 23.49).

A strategy for image enhancement involves the utilization of HOG (Histogram Oriented Gradients) [17]. Besides its application in image augmentation, HOG can also be utilized for feature extraction in tuberculosis (TB) chest X-ray pictures. The model applied to chest X-ray images yielded a true positive ratio (sensitivity) of 97.4% and a true negative ratio (specificity) of 97.2%. The results indicate that the model accurately identifies both positive and negative tuberculosis cases.

This study will boost the contrast of X-ray hip images, utilizing the most effective way as a medium for identifying hip osteoarthritis (OA). The acquired X-ray image is in PNG format. Subsequently, the PNG image is transformed into grayscale, followed by an enhancement of the image contrast utilizing Histogram Equalization (HE), Contrast Limited Adaptive Histogram Equalization (CLAHE), and a hybrid approach combining the CLAHE model with two Gamma Corrections. The CLAHE method with two Gamma Corrections will hereafter be designated as CLAGAMTWO. The efficacy of enhancing picture contrast through the three techniques will be assessed utilizing SSIM (Structured Similarity Index Measure), Entropy, and CNR (Contrast-to-Noise Ratio).

II. Literature Review

Currently, digital images are frequently subjected to image contrast enhancement techniques. The perception of the digital image's visual quality can be considerably enhanced through the use of image contrast enhancement [18]. Currently, there are numerous methods of enhancing image contrast, including HE (Histogram Equalization), CLAHE (Contrast Limited Adaptive Histogram Equalization) and Gamma Correction.

A. HE (Histogram Equalization)

An effective histogram encompasses the complete spectrum of values on the gray scale. Histogram equalization is a well-established method for enhancing visual contrast, recognized for its simplicity and effectiveness [19], [20]. The horizontal axis of the histogram denotes the pixel count, while the vertical axis indicates the gray value. The histogram values are derived by quantifying the number of pixels corresponding to each grayscale value present in the image [21]. The fundamental objective of HE is to turn the global histogram equalization into a uniform distribution. Nonetheless, while each image possesses a distinct histogram, following histogram equalization, the pixel values are typically centralized within the midrange of the grayscale, resulting in considerable variations in the average brightness of the image. The typical solution to this issue involves dividing the histogram into two segments and individually equalizing the divided histograms [22].

Conventional histogram equalization can enhance visual contrast by extending the histogram to a specified range. For a given image, the image histogram $H(i)$ for intensity level i is obtained from the number of pixels n_i with intensity level i, which is defined as follows:

$$H(i) = ni \quad for\ i = 0,1,2,\dots(L-1) \tag{1}$$

Where L is the maximum range of gray levels (for 8-bit images it is 256, 0-255) [23]. Based on equation (1), the histogram is divided according to the number of pixels with a certain intensity (the total number of pixels in the image $n = \sum_{i=0}^{L-1} H(i)$) [23], [24]. This result is then used to calculate the probability $p_x(i)$ of pixel i (Eq. (2)) [25], which is then used to calculate the cumulative distribution function (CDF) at [Eq. (3)]. The CDF has a range of values 0-255, as the histogram distribution of the equalization [Eq. (4)] [24].

$$p_x(i) = p(x = i) = n_i/n \tag{2}$$

$$cdf_x(i) = \sum_{j=0}^{i} p_x\,(x = j) \tag{3}$$

$$h(v) = \text{round}\left(\frac{cdf(v) - cdf_{min}}{n - cdf_{min}}\right) \tag{4}$$

B. CLAHE (Contrast Limited Adaptive Histogram Equalization)

Contrast Limited Adaptive Histogram Equalization is a method employed for enhancing contrast in images, particularly in grayscale images [26]. This method's benefit is that it can boost the original image quality, particularly for grayscale photos which medical practitioners regularly apply for high-noise or interference-filled CT or X-ray shots. The CLAHE method concentrates on small segments of the image, referred to as tiles. The contrast of each tile is modified to ensure that the generated histogram for that area matches the specified histogram's shape. Bilinear interpolation links neighboring tiles. This approach is employed to enhance the visual smoothness of the tile combination [27]. The Contrast limited adaptive histogram equalization method can be defined as follows:

$$\beta = \frac{M}{N}\left(1 + \frac{\alpha}{100}(S_{max} - 1)\right) \tag{5}$$

In Eq. (5) it is explained that β represents the limit value, then the variable M represents the area size, N represents the grey-level or grayscale value (256), α represents the clip factor which states the addition of the histogram limit with a value of 1 to 100. S_{max} is the maximum slope permitted.

C. Gamma Correction

Gamma correction [28] is frequently utilized in diverse image processing applications. The process necessitates a fixed parameter, typically represented by the symbol γ, which varies from 0 to 3 to enhance the input image. Gamma correction redistributes the gray levels of the image worldwide based on the set parameter. This solution is effective for underexposed or overexposed photographs, but may not be suitable for images affected by both issues [29]. The classical gamma correction is stated as follows:

$$L = 255\left[\frac{I(x,y)}{255}\right]^{\gamma} \quad (6)$$

In Eq. (6), γ control the degree of image stretching. If $\gamma < 1$, then the overall brightness of the image increases, whereas if $\gamma > 1$, then the image becomes darker than the original image. In this investigation, researchers attempted to apply two Gamma corrections subsequent to the execution of CLAHE on the original image. This was done to enhance image contrast quality.

III. Material and Methods

The PC utilized in this study is a laptop including an Intel Core i7-12700H Processor, NVIDIA GeForce RTX 3070Ti 8GB GDDR6 Graphics with a TGP of 150W, and 16GB of memory configured as 2 x 8GB SO-DIMM DDR5-4800. The programming language employed for computing is Python. X-ray images of the hip joint were acquired from Kariadi Hospital Semarang following the procurement of a research permit with Ethical Clearance No: 535/EC/KEPK/FK-UNDIP/X/2023.

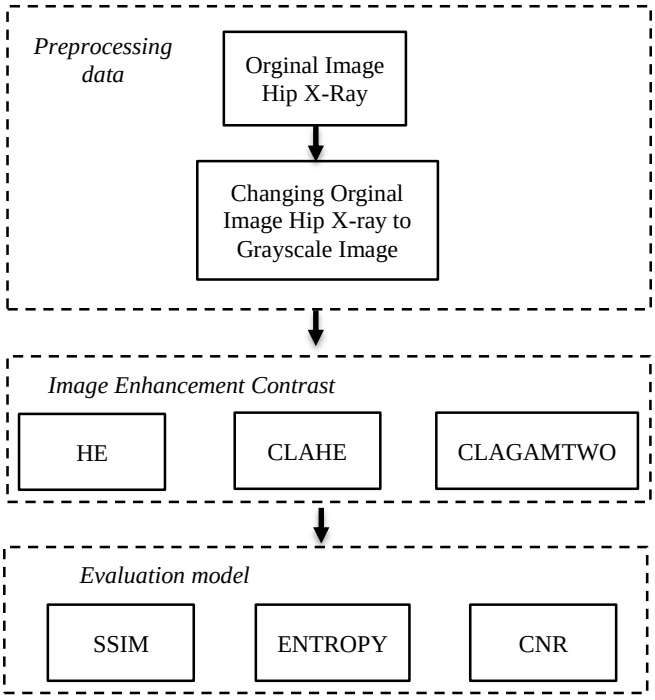
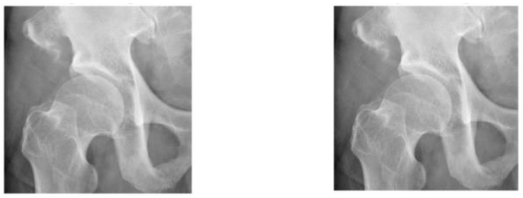


Fig. 1. Research process flow.

Fig. 1, illustrates the research methodology, which comprises multiple stages, beginning with data preprocessing that involves converting the original hip X-ray image to a grayscale format. Subsequently, the process advanced to the picture enhancement contrast phase employing three distinct techniques: HE (Histogram Equalization), CLAHE (Contrast Limited Adaptive Histogram Equalization), and CLAHE with dual Gamma Corrections (CLAGAMTWO). The final phase involves assessing the outcomes of enhanced picture contrast using the three ways utilizing SSIM (Structured Similarity Index Measure), Entropy, and CNR (Contrast-to-Noise Ratio). A comprehensive explanation will be provided in the subsequent sub-chapter:

A. Preprocessing Data

At this juncture, the original hip X-ray image acquired from the hospital is stored in PNG format [15] with dimensions of 1024 × 1024 pixels. After that the original hip X-ray image will be converted into a gray image so that it can be processed in the next stage. Subsequent to acquiring the hip X-ray image, the next step is to transform it into a grayscale image, as illustrated in Fig. 2. A grayscale image consists of a single color channel representing light intensity on a scale from black (minimum value) to white (maximum value). This procedure is conducted to streamline the data, decrease the information size, and remove color components that are typically unnecessary in medical image analysis.



(a) (b)

Fig. 2. Hip X-ray: (a) Original image and (b) Grayscale image.

B. Image Enhancement Contrast

In Fig. 3, the preprocessed picture will undergo contrast enhancement with HE (Histogram Equalization), CLAHE (Contrast Limited Adaptive Histogram Equalization), and CLAGAMTWO (CLAHE with two Gamma Corrections).

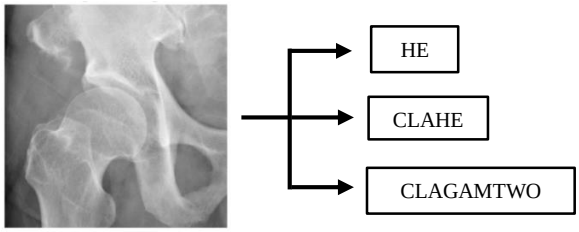


Fig. 3. Contrast enhancement of the original image using HE, CLAHE and CLAGAMTWO.

C. Evaluation Model

The contrast-enhanced image will be assessed using SSIM (Structured Similarity Index Measure), Entropy, and CNR (Contrast-to-Noise Ratio). SSIM [30] is a metric evaluated based on three primary components: brightness, contrast, and structure, as seen in Eq. (7).

$$SSIM\ (x,y) = [l(x,y)]^{\alpha}\ .\ [c(x,y)]^{\beta}\ .\ [s(x,y)]^{\gamma} \quad (7)$$

In Eq. (7), l represents the luminance employed to assess the brightness comparison between two images. c is the contrast utilized to differentiate the spectrum between the most luminous and the most obscure areas of the two photographs. s is the framework employed to analyze the local luminance patterns of the two images in order to identify their similarities and differences. Consequently, α, β and γ are positive constants. The luminance, contrast, and structure of the image can be delineated individually by Eq. (8), Eq. (9), and Eq. (10).

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \quad (8)$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (9)$$

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\,\sigma_y + C_3} \quad (10)$$

Where μ_x and μ_y denote the local means, σ_x and σ_y represent the standard deviations, and σ_{xy} indicates the cross-covariances for images x and y, respectively. When $\alpha = \beta = \gamma = 1$, the index can be simplified utilizing Eq. (8)- Eq. (10), with the outcomes presented in Eq. (11).

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)\,(2\sigma_x\sigma_y + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)\,(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (11)$$

Entropy quantifies the complexity or diversity of information within an image. A greater entropy number indicates increased complexity and diversity of information inside the image. Entropy is determined by the distribution of pixel intensities in an image and is utilized to evaluate image quality or for pattern detection and segmentation [31]. The subsequent formula pertains to entropy:

$$H = -\sum_{i=1}^{n} p(i) log p(i) \quad (12)$$

In Eq. (12), H represents the entropy. $p(i)$ represents the probability of the occurrence of a pixel intensity i. n represents the quantity of intensity levels in the image.

CNR is a metric utilized to assess the discernibility of the contrast between high and low areas in an image, despite the interference of noise. In image processing, CNR assesses the clarity of a feature or detail in an image, free from interference by noise. A greater CNR signifies that the feature in the image exhibits increased contrast with the background, facilitating visibility [32]. The fundamental equation for CNR is as follows:

$$CNR = \frac{|S1 - S2|}{\sigma} \quad (13)$$

In Eq. (13), $S1\ dan\ S2$ represent the average intensities in two distinct regions, with $S1$ denoting the feature of interest and $S2$ indicating the background area. Meanwhile, σ represents the standard deviation of noise inside the image.

IV. Result and Discussion

In the following section, we will show a comparison of the experimental data obtained from the various methods of picture contrast enhancement that were discussed earlier.

Fig. 4(a1) and 4(a2) depict the original photos alongside their corresponding histograms. Fig. 4(b1) and (b2) illustrate the outcomes of enhancing image contrast using histogram equalization [33]. The histogram's form reveals that the central region of the image exhibits an excessive brightness, while the edges display a pronounced darkness. The histogram illustrates a transformation in shape, initially centralized, now exhibiting an even distribution, with the dark blue hue confined to the right and left margins. Fig. 4(c1) and Fig. 4(c2) illustrate the outcomes of enhancing image contrast through Contrast Limited Adaptive Histogram Equalization [34]. The images exhibit increased contrast, uniformity, and prominence; however, they appear somewhat dark due to the significant enhancement in contrast, as evidenced by the histogram's shape. Fig. 4(d1) and 4(d2) illustrate the outcomes of augmenting picture contrast with CLAGAMTWO. In this part, the researcher employs a method that first applies contrast enhancement through CLAHE, followed by a further enhancement using gamma correction applied twice. The resulting image exhibits commendable contrast, appearing elevated internally and exhibiting a smoother upper surface.

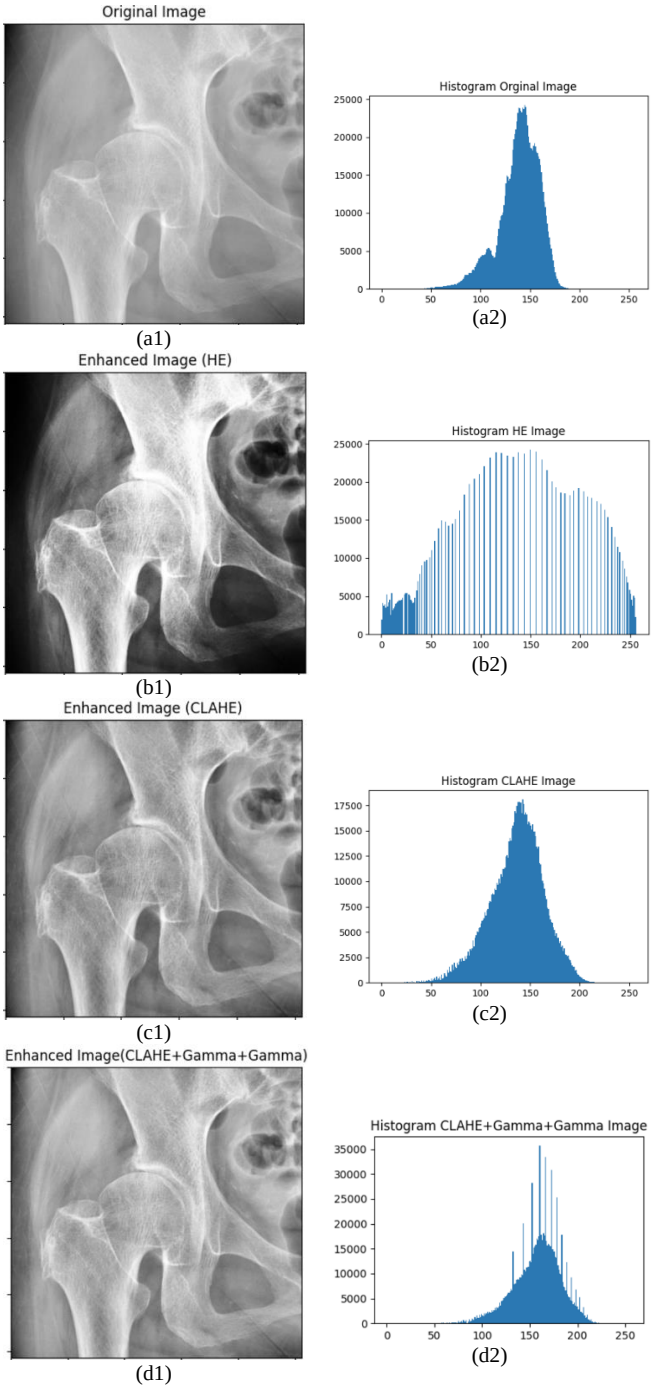


Fig. 4. Image contrast enhancement using HE, CLAHE and CLAGAMTWO.

Image quality evaluation is crucial in digital image processing applications. The researcher performed metric testing using SSIM (Structured Similarity Index Measure), Entropy, and CNR (Contrast-to-Noise Ratio) on several hip

photos presented in Table I, notwithstanding the absence of observed and explained variance in visual quality in certain other photographs.

Table I presents only 10 image values from a total of 30 evaluated. The bold values in the table represent the optimal results achieved through the employed methods. The average SSIM value indicates that the CLAGAMTWO method achieves the highest value at 0.850, followed by CLAHE at 0.826, and HE at 0.644. The CLAGAMTWO method consistently yields image quality that closely resembles the original image, demonstrating its effectiveness in preserving visual structure. CLAHE demonstrates satisfactory performance however, it remains marginally inferior to CLAGAMTWO. In contrast, HE exhibits the lowest SSIM performance, suggesting a diminished capacity to preserve the similarity of image structure.

TABLE I. SSIM, ENTROPY AND CNR VALUES OF 10 SAMPLE IMAGE FROM 30 TESTED DATASETS

Image	Method	Image Quality Assessment		
		SSIM	Entropy	CNR
Image1	HE	0.597	6.238	0.414
	CLAHE	0.885	**6.782**	0.104
	CLAGAMTWO	**0.911**	6.548	**0.944**
Image2	HE	0.664	6.796	0.216
	CLAHE	0.805	**7.221**	0.166
	CLAGAMTWO	**0.845**	7.016	**0.576**
Image3	HE	0.579	6.506	0.569
	CLAHE	0.774	**7.218**	0.264
	CLAGAMTWO	**0.779**	7.045	**0.956**
Image4	HE	0.762	7.032	0.105
	CLAHE	0.834	**7.296**	0.001
	CLAGAMTWO	**0.854**	7.108	**0.607**
Image5	HE	0.609	6.634	0.458
	CLAHE	0.809	**7.222**	0.219
	CLAGAMTWO	**0.855**	6.995	**0.547**
Image6	HE	0.599	6.507	0.623
	CLAHE	0.799	**6.996**	0.319
	CLAGAMTWO	**0.801**	6.822	**1.085**
Image7	HE	0.647	6.542	0.297
	CLAHE	0.849	**6.885**	0.039
	CLAGAMTWO	**0.865**	6.702	**0.909**
Image8	HE	0.663	6.660	0.054
	CLAHE	0.847	**7.132**	0.048
	CLAGAMTWO	**0.875**	6.927	**0.742**
Image9	HE	0.614	6.525	0.254
	CLAHE	0.813	**7.091**	0.170
	CLAGAMTWO	**0.854**	6.881	**0.753**
Image10	HE	0.713	6.738	0.056
	CLAHE	0.848	**7.154**	0.035
	CLAGAMTWO	**0.862**	6.941	**0.613**
Average		**0.850**	**7.009**	**0.773**

For the greatest average entropy value CLAHE (7,099) was obtained, followed by CLAGAMTWO (6,944) and HE (6,617). The CLAHE approach excels in keeping detailed information in the image, demonstrating that CLAHE is more effective in improving the amount of detail. CLAGAMTWO is in second place, displaying pretty high performance in keeping detail, although lower than CLAHE. HE displays the lowest entropy performance, indicating that this method is less able to keep picture detail optimally.

The CLAGAMTWO method once again demonstrates the highest performance in the average CNR measurement, with a value of (0.773), which significantly surpasses CLAHE (0.136) and HE (0.305). CLAGAMTWO is an optimal method for generating high-quality images, as it significantly enhances contrast with minimal noise. The efficacy of CLAHE in enhancing CNR is significantly lower, and HE is also not optimal in this regard, despite being slightly better than CLAHE.

V. CONCLUSION

The CLAGAMTWO method is the most effective method in terms of visual structure (SSIM), information detail (Entropy), and distinct contrast with low noise (CNR) based on the average of the metric values. The CLAHE method is superior in terms of maintaining information detail (Entropy), but it is less effective in terms of increasing CNR when compared to CLAGAMTWO. In contrast to CLAHE and CLAGAMTWO, HE is the method with the lowest performance in all metrics, and as a result, it is not as recommended for enhancing image quality. This demonstrates that the CLAGAMTWO method, as proposed by the researcher, is the most effective method for enhancing the quality of the overall image in terms of visual structure, information detail, and distinct contrast with low noise. The outcomes of this image contrast enhancement will be employed as a diagnostic tool for hip OA in the future. For future work, it may implement a novel deep learning-based methodology, incorporate additional evaluation metrics, and expand the dataset.

ACKNOWLEDGMENT

This research supported by Department of Information System, School of Postgraduates, Diponegoro University, University of Pembangunan Nasional Veteran Jawa Timur, and Kariadi Hospital Semarang.

REFERENCES

[1] J. Yang and S. Xuan, “Bit depth enhancement method for low-contrast images based on sequence image fusion,” Measurement: Sensors, vol. 27, Jun. 2023, doi: 10.1016/j.measen.2023.100801.

[2] N. Senthilkumaran and J. Thimmiaraja, “Histogram equalization for image enhancement using MRI brain images,” in Proceedings - 2014 World Congress on Computing and Communication Technologies, WCCCT 2014, IEEE Computer Society, 2014, pp. 80–83. doi: 10.1109/WCCCT.2014.45.

[3] S. C. Huang, F. C. Cheng, and Y. S. Chiu, “Efficient contrast enhancement using adaptive gamma correction with weighting distribution,” IEEE Transactions on Image Processing, vol. 22, no. 3, pp. 1032–1041, 2013, doi: 10.1109/TIP.2012.2226047.

[4] N. Aresti, J. Kassam, N. Nicholas, and P. Achan, “Hip osteoarthritis,” BMJ (Online), vol. 354, 2016, doi: 10.1136/bmj.i3405.

[5] F. Muttaqin, I. Yuniar Purbasari, A. Priharyoto Bayuseno, T. Indah Winarni, R. R. Isnanto, and J. Jamari, “Machine Learning Methods for Identification Osteoarthritis: A Bibliometric Analysis and General

Review," in E3S Web of Conferences, EDP Sciences, Nov. 2023. doi: 10.1051/e3sconf/202344802009.

[6] M. Zeng, Y. Li, Q. Meng, T. Yang, and J. Liu, "Improving histogram-based image contrast enhancement using gray-level information histogram with application to X-ray images," Optik (Stuttg), vol. 123, no. 6, pp. 511–520, Mar. 2012, doi: 10.1016/j.ijleo.2011.05.017.

[7] M. S. M. Swamy and M. S. Holi, "Knee Joint Articular Cartilage Segmentation, Visualization and Quantification using Image Processing Techniques: A Review," 2012.

[8] J. Hirvasniemi et al., "Correlation of Subchondral Bone Density and Structure from Plain Radiographs with Micro Computed Tomography Ex Vivo," Ann Biomed Eng, vol. 44, no. 5, pp. 1698–1709, May 2016, doi: 10.1007/s10439-015-1452-y.

[9] T. Le Corroller et al., "Bone texture analysis is correlated with three-dimensional microarchitecture and mechanical properties of trabecular bone in osteoporotic femurs," J Bone Miner Metab, vol. 31, no. 1, pp. 82–88, Jan. 2013, doi: 10.1007/s00774-012-0375-z.

[10] Y. Wu, D. Tan, C. Hai, M. Yang, H. Zhang, and J. Liu, "An enhancement algorithm based on multi-grayscale fusion and edge-weight for low contrast X-ray image," NDT and E International, vol. 143, Apr. 2024, doi: 10.1016/j.ndteint.2024.103051.

[11] B. Shahangian and H. Pourghassem, "Automatic brain hemorrhage segmentation and classification algorithm based on weighted grayscale histogram feature in a hierarchical classification structure," Biocybern Biomed Eng, vol. 36, no. 1, pp. 217–232, 2016, doi: 10.1016/j.bbe.2015.12.001.

[12] S. C. Yang et al., "Contrast enhancement and tissues classification of breast MRI using Kalman filter-based linear mixing method," Computerized Medical Imaging and Graphics, vol. 33, no. 3, pp. 187–196, Apr. 2009, doi: 10.1016/j.compmedimag.2008.12.001.

[13] M. Bahani, A. El Ouaazizi, R. Avram, and K. Maalmi, "Enhancing chest X-ray diagnosis with text-to-image generation: A data augmentation case study," Displays, vol. 83, Jul. 2024, doi: 10.1016/j.displa.2024.102735.

[14] A. M. Rifai, S. Raharjo, E. Utami, and D. Ariatmanto, "Analysis for diagnosis of pneumonia symptoms using chest X-ray based on MobileNetV2 models with image enhancement using white balance and contrast limited adaptive histogram equalization (CLAHE)," Biomed Signal Process Control, vol. 90, p. 105857, Apr. 2024, doi: 10.1016/j.bspc.2023.105857.

[15] S. Anand, R. K. Roshan, and D. Sundaram M, "Chest X ray image enhancement using deep contrast diffusion learning," Optik (Stuttg), vol. 279, May 2023, doi: 10.1016/j.ijleo.2023.170751.

[16] R. S. Aldoury, N. M. G. Al-Saidi, R. W. Ibrahim, and H. Kahtan, "A new X-ray images enhancement method using a class of fractional differential equation," MethodsX, vol. 11, Dec. 2023, doi: 10.1016/j.mex.2023.102264.

[17] R. Geethamani and A. Ranichitra, "Enhancing Tuberculosis Detection: Leveraging RF-HOG Model for Automated Diagnosis from Chest X-ray Images," in Procedia Computer Science, Elsevier B.V., 2023, pp. 21–32. doi: 10.1016/j.procs.2023.12.057.

[18] B. Chien Thai and A. Mokraoui, "Tone mapped HDR images contrast enhancement using piecewise linear perceptual transformation," HAL open science, 2020, doi: 10.23919/EU.

[19] Q. Yuan and S. Dai, "Adaptive histogram equalization with visual perception consistency," Inf Sci (N Y), vol. 668, May 2024, doi: 10.1016/j.ins.2024.120525.

[20] K. Nagamani, K. Divya, K. Sujatha, K. R. Bonagiri, G. B. Kande, and P. S. S. Kumar, "Adaptive histogram equalization of wavelet sub bands for the enhancement of contrast in aerial images," in Materials Today: Proceedings, Elsevier Ltd, 2022, pp. 898–901. doi: 10.1016/j.matpr.2021.10.297.

[21] G. Jiang et al., "Color image enhancement with brightness preservation using a histogram specification approach," Optik (Stuttg), vol. 126, no. 24, pp. 5656–5664, Dec. 2015, doi: 10.1016/j.ijleo.2015.08.173.

[22] Z. Bian, H. Yao, Y. Le, and C. Qin, "Two-dimensional histogram-based reversible contrast enhancement using bi-histogram equalization," Displays, vol. 81, Jan. 2024, doi: 10.1016/j.displa.2023.102580.

[23] A. Paul, "Adaptive tri-plateau limit tri-histogram equalization algorithm for digital image enhancement," Visual Computer, vol. 39, no. 1, pp. 297–318, Jan. 2023, doi: 10.1007/s00371-021-02330-z.

[24] S. Saifullah and R. Drezewski, "Modified Histogram Equalization for Improved CNN Medical Image Segmentation," in Procedia Computer Science, Elsevier B.V., 2023, pp. 3021–3030. doi: 10.1016/j.procs.2023.10.295.

[25] S. Saifullah and A. Suryotomo, "Thresholding and Hybrid CLAHE-HE for Chicken Egg Embryo Segmentation," in IEEE, Aug. 2021, pp. 268–273. doi: 10.1109/ICICT52195.2021.9568444.

[26] K. Honda, K. Wei, M. Arai, and H. Amano, "CLAHE implementation and evaluation on a low-end FPGA board by high-level synthesis," IEICE Trans Inf Syst, vol. E104D, no. 12, pp. 2048–2056, 2021, doi: 10.1587/transinf.2021PAP0006.

[27] M. Hayati et al., "Impact of CLAHE-based image enhancement for diabetic retinopathy classification through deep learning," in Procedia Computer Science, Elsevier B.V., 2022, pp. 57–66. doi: 10.1016/j.procs.2022.12.111.

[28] A. K. Mishra, M. Kumar, and M. S. Choudhry, "Fusion of multiscale gradient domain enhancement and gamma correction for underwater image/video enhancement and restoration," Opt Lasers Eng, vol. 178, Jul. 2024, doi: 10.1016/j.optlaseng.2024.108154.

[29] D. Zhang et al., "Underwater image enhancement via multi-scale fusion and adaptive color-gamma correction in low-light conditions," Eng Appl Artif Intell, vol. 126, Nov. 2023, doi: 10.1016/j.engappai.2023.106972.

[30] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," Journal of Computer and Communications, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[31] R. C. . Gonzalez and R. E. . Woods, Digital image processing. Pearson, 2018.

[32] K. Igarashi, K. Imai, S. Matsushima, C. Yamauchi-Kawaura, and K. Fujii, "Development and validation of the effective CNR analysis method for evaluating the contrast resolution of CT images," Phys Eng Sci Med, vol. 47, no. 2, pp. 717–727, Jun. 2024, doi: 10.1007/s13246-024-01400-5.

[33] P. Kaur, B. S. Khehra, and A. P. S. Pharwaha, "Color Image Enhancement based on Gamma Encoding and Histogram Equalization," in Materials Today: Proceedings, Elsevier Ltd, 2020, pp. 4025–4030. doi: 10.1016/j.matpr.2021.02.543.

[34] X. Liu and T. D. C. Nguyen, "Medical Images Enhancement by Integrating CLAHE with Wavelet Transform and Non-Local Means Denoising," Academic Journal of Computing & Information Science, vol. 7, no. 1, 2024, doi: 10.25236/ajcis.2024.070108.

Computer-Vision-Based Detection and Monitoring System for Mature Coconut Fruits with a Web Dashboard Visualization Platform

Samfford S. Cabaluna, Maria Fe P. Bahinting, Leah A. Alindayo
Computer Applications Department-College of Computer Studies,
Mindanao State University Iligan Institute of Technology, Iligan City, Northern Mindanao, Philippines

***Abstract*—The Philippines is the second largest producer of coconut products in the world with 347 million trees planted in 3.6 million hectares of land across the country. Traditionally, harvesting coconuts is a labor-intensive process in the Philippines that involves manual climbing and chopping fruits, which carries a high risk of harm or even death. Hence, the number of expert coconut climbers has decreased as a result. In response, current research has concentrated on creating robot harvesters. However, classifying the mature coconut fruit is a major problem in the harvesting process that calls for a great deal of experience, patience, and work. Studies employing Convolutional Neural Networks (CNNs) have shown great accuracy in detecting coconut ripeness, although these efforts have been limited to detection without practical integration with harvesting equipment. Moreover, the present research lacks a comprehensive solution that allows real-time data display and monitoring, such as the maturation stage of coconuts, via a web-based dashboard. This discrepancy emphasizes the requirement for systems that can not only identify the age of coconuts but also work with harvesting technologies and provide intuitive user interfaces for data display and decision-making. In order to fill these gaps, this study presents a computer-vision-based system that monitors and detects coconut fruit maturity, with an emphasis on mature coconuts, by utilizing the YOLOv8 model. With a Mean Average Precision (mAP50) of 99.5%, mAP50-95 of 89.5%, precision of 99.5%, and recall of 99.9%, the system demonstrated great accuracy. A web-based dashboard is also integrated into the system to provide monitoring and visualization of detected coconut fruits, along with notifications for fully ripe fruits.**

***Keywords*—Coconut fruit maturity; coconut maturity detection; computer vision; crop monitoring**

I. Introduction

The Philippines is the world's second-largest exporter of coconuts, with 14.89 million metric tons produced in 2023.

With the pressing issues on risks of manual harvesting which caused a steady decline in coconut harvester population, robot coconut harvesters were developed to address the issue based on the review by Kumar et al. [1]. Furthermore, Cousalya et al. [2] created a mobile operated coconut harvesting machine. These developed harvesters, however, lack a detecting systems that resulted to harvest even the young coconuts. Nevertheless, the studies of Sakthipreasad and Megalingam, Junaedy et al., Titus et al., Wibowo et al., and Divyanth et al. [3], [4], [5], [6], [7], on robotic harvesters that are integrated with vision-based detection but it solely focused on fruit recognition which lead to the harvester inability to specifically locate the matured coconuts.

Determining the ripeness of coconut fruit accurately remains a challenging task which has an impact on product quality and customer satisfaction [8]. Conventional manual techniques take a lot of time and require experience [9], [10], [11], [12], [13], and elements like dim lighting and complicated backgrounds [12], [14] make it hard for computers and humans to recognize coconuts [6], [15], which frequently results in the harvesting of poor or premature coconuts. In response, recent research have been conducted that introduces the concept of coconut maturity detection using several methods. Two studies use the fuzzy logic approach in detecting and classifying coconut fruit maturity [9], [12] which proved to be an effective algorithm where in the study of Megalingam et al. uses the Decision-Making Probability (DMP) model for real-time classification achieving an accuracy of 86.3%, but Mask R-CNN performs better than the other integrated models. Aside from these studies, other researches focused on Convolutional Neural Networks (CNNs) in coconut fruit maturity detection and classification which is commonly implemented having an average accuracy above 90%.

Moreover, Venkatesh et al. [14] implemented the SOLO model, Artificial Neural Network is implemented by Hendrawan et al. [16], Anushya implemented K-Means clustering wherein image features are extracted by Gray-level Co-Occurrence Matrix (GLCM) determining the freshness of the coconut obtaining 97% accuracy [17], Varur et al. [18] researched on coconut development phases classifying into five classes using Xception, ResNet50V2, ResNet152V2, and MobileNetV2, wherein MobileNetv2 produced the best accuracy, Subramanian and Sankar used RestNet-50 and Faster R-CNN wherein ResNet-50 achieved a top-1 accuracy for both premature and mature phases achieving a detection score of 99%, and around 98% top-1 and top-5 accuracies [10], [15], Nguyen et al. also discovered that ResNet101 was the most accurate, using binarized saturation pictures achieving an accuracy of 95% [11], Avudai Nayagam and Devakumar used small VGG net and MobileNet which ensured precise coconut detection when used in real-time on NUC/Jetson Nano boards and climbing robots, however their system's gap focuses on how well those models run on those devices stated [19], and Novelero and Dela Cruz's study (Philippines) used the YOLOv5 model in an on-tree mature coconut fruit detection using UAVs achieving an

This paper is sponsored by the Philippine Department of Science and Technology Engineering Research and Development for Technology.

accuracy of 88.4% which will be of great value in eliminating risks of harvesting coconuts in the future since it can also be useful for coconut crop yield estimation, [20]. In the research of Mandava et al. [13], it is concluded that YOLOv5s is superior in metrics yet needing more datasets.

Based on the literature discussed above, the different methods in detecting matured coconut has been successful particularly the utilization of Convolutional Neural Networks (CNN) which incurred a high accuracy rating of above 90% in terms of detecting mature coconut. However, these studies solely focused on maturity detection and was not able to provide a comprehensive solution incorporating real-time display and monitoring of coconut fruits. This emphasizes the necessity for systems that can both identify coconut fruit maturity and integrate it with harvesting technology [20], offering a user-friendly interface for data visualization and informed decision-making.

This paper implements both computer-vision-based detection of coconut fruit maturity using a later model under CNN, the later model, YOLOv8, as it builds upon the success of previous versions and introduces new features and improvements to boost performance and flexibility, applicable as well in different environments with a detailed comparison of its performance metrics to other versions and models [21]. Along with it is an integration with a web dashboard for display and monitoring of scanned coconut fruit maturity data and with a notification system wherein for every detected mature coconut fruit, a notification is sent.

II. Methodology

To design and develop a detection and monitoring system to detect and monitor coconut fruits according to maturity YOLOv8 model was utilized. The researchers as well designed and developed a web dashboard for monitoring the scanned coconut fruits according to maturity. Fig. 1 presents the flow of methods the researchers underwent in coming up with the output of this paper. Having identified the problems as well as motivation to resolve these problems, the researchers then proceeded to the specific objectives consisting of three phases: (Phase 1) the overall design of the system, involving requirements analysis, the design, and the gathering of datasets; (Phase 2) the development of the detection and monitoring systems as well as their integration, involving the processing of the image datasets and their training, and the design and development of the web dashboard for the display of coconut fruit data scanned as well as the integration with the notification system for every mature coconut fruit detected; and (Phase 3) the implementation of the system, involving the testing and evaluation of both detection and monitoring systems.

A. System Requirements Analysis

The following items below serves as guide for the researchers in coming up with the output of this paper. The overall system is limited for experimental purposes:

- Image datasets involve generally both Mature and Premature coconut fruits, wherein Mature coconut fruits include those with both brown and brown-and-green surfaces and Premature coconut fruits include those of young coconut fruits with green surfaces.
- Acquisition of datasets are only limited to close shots angle.
- Web dashboard involves the display of footage of scanned coconut fruits and the display of count data through a line graph chart.
- Count data of coconut fruit maturity are also displayed on the table and can be printed to CSV file.
- The system will send notification mail every time a mature coconut fruit(s) is/are detected.
- The system, limited to experimental use, limits it's testing within the laboratory, not yet real-time.

Fig. 2 shows the architecture of the overall system, involving both detection and monitoring systems based on the listed system requirements analysis above.

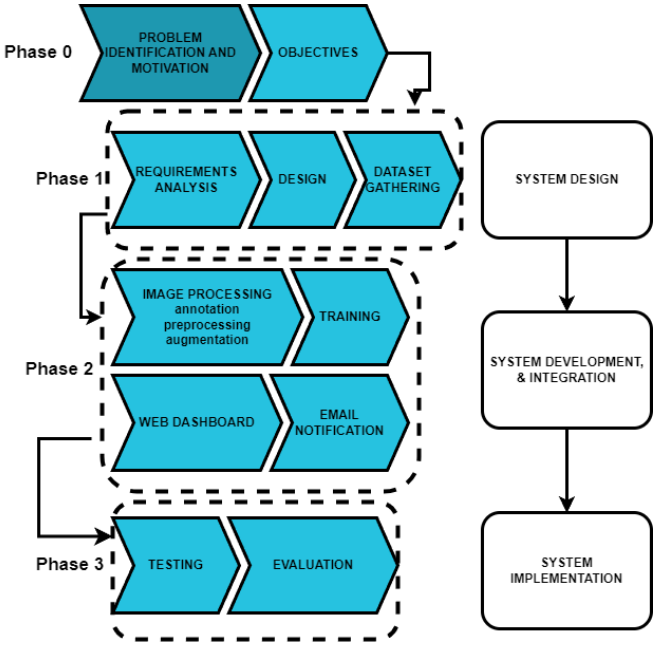


Fig. 1. Methodology flowchart.

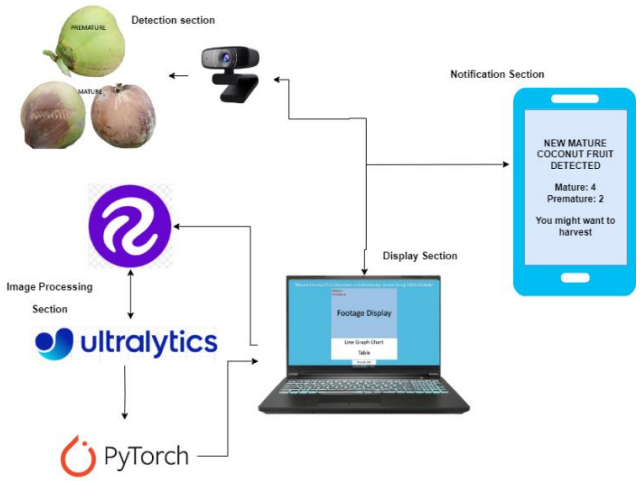


Fig. 2. System architecture.

B. Detection System

This particular section discusses the methods undergone by the researchers in designing and developing the detection system of this paper.

1) Data acquisition: Data were acquired by capturing video footage of harvested coconuts from a farm in Barangay Argayoso, Manticao, Misamis Oriental. Images were extracted at a rate of three per second, resulting in 260 image datasets. These were then uploaded to Roboflow for image processing, including annotation, preprocessing, augmentation, and dataset generation, with two classes: Mature and Premature coconuts (see Fig. 2). Mature coconut fruits include both full brown-colored surface and those with both brown and green surfaces, while the premature coconut fruits include those with green surfaces.

2) Annotation: Following the uploading of images to Roboflow, the platform for annotation was then set up using Smart Polygon (though under the Bounding Box platform) for more precise results. A total of 260 images were annotated, resulting in 409 annotations for the mature class and 403 for the premature class, ensuring a balanced dataset (see Fig. 3).

Fig. 3. Annotation of image datasets.

3) Training of the model: Ultralytics Hub platform was used for the training of the model (see Fig. 4). Google Colab platform was specifically used for the training while the results are automatically uploaded on the Ultralytics dashboard. YOLOv8 model was used for training.

4) Running the trained model: Following the model training is its implementation (see Fig. 5). The researchers have developed a program wherein the scanned coconut fruits according to maturity are counted. Footage is then displayed on the dashboard. Programming of the detection system is done using OpenCV Python.

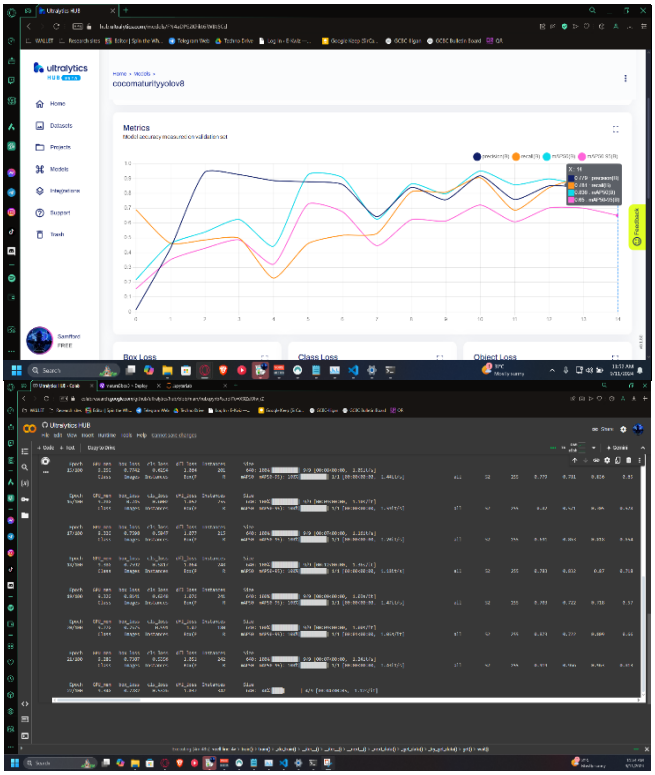


Fig. 4. Training of model.

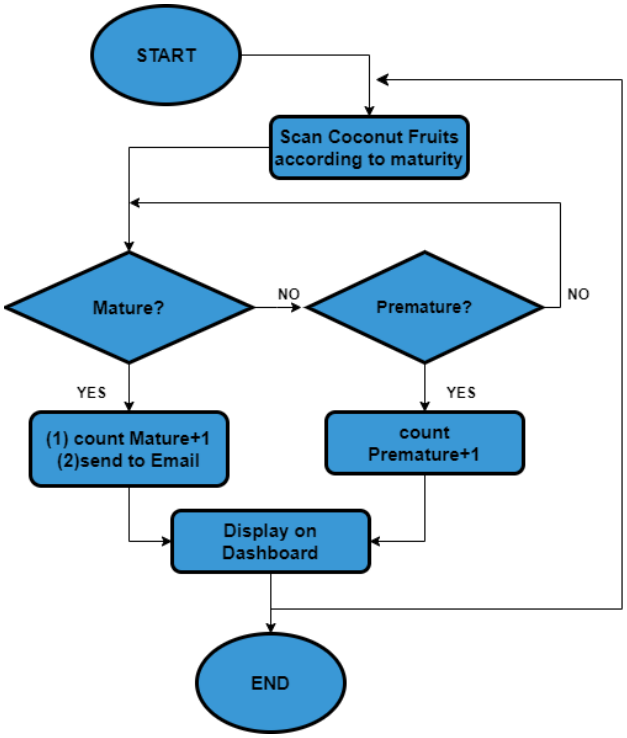


Fig. 5. Detection system flow.

C. Web Dashboard Design

Fig. 6 shows the operational flow of the web dashboard that serves as the display for the overall system. The user will have to go through the homepage where a button will be clicked to enter the dashboard. Once clicked, the user will be led to the main dashboard where the data are displayed.

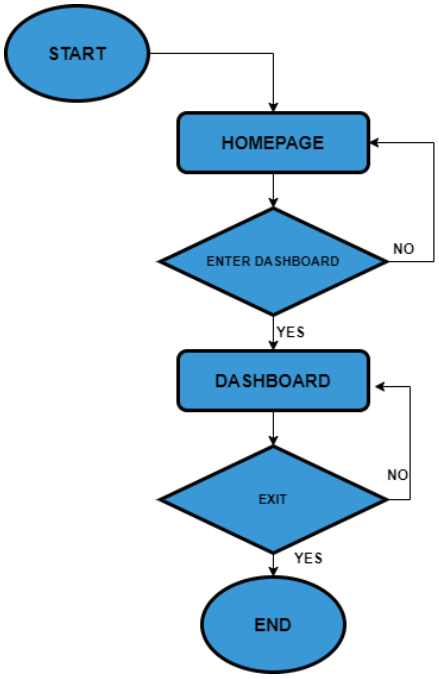


Fig. 6. Web dashboard flow.

D. Integration of Detection System to Web Dashboard and Email

Basic HTML was used in programming the monitoring dashboard with styles for its background image, as well as for the table and charts. The dashboard is then connected to and from the python program in order for the data to be uploaded and displayed on the output of this program. The system is also integrated into the Email for notification purposes.

E. Testing and Evaluation

A sample test run was done for both detection and monitoring systems. As stated earlier, this paper is limited to experimentation, thus the test run was done inside the laboratory.

III. Results

This section presents and discusses the results of this particular paper. Discussion involves the results of training of model as well as the display of data for monitoring.

A. Training Results

After 100 epochs of training, metrics show that the training of the model produced a Mean Average Precision 50 (mAP50) is 99.5% and its mAP50-95 is 89.5%, a 99.5% precision, and 99.9% recall (see Fig. 7) and is gradually increasing.

Fig. 8 presents the results of the training of the model particularly showing the box, class, and object losses.

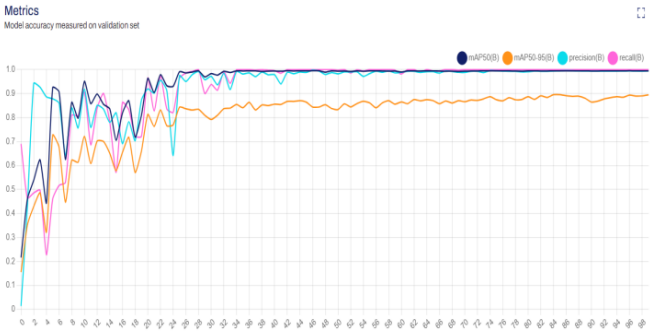


Fig. 7. Training results metrics (mAP, Precision, Recall).

Box Loss shows that at the end of the 100 epochs training, training reaches 46.5% and 53.2% validation. For class loss, training reaches 23.3% while validation reaches 26.8%. Finally, for object loss, training reaches 90.7% and validation reaches at 90.8%.

For the Box Loss, initially, both training and validation loses fluctuate significantly, indicating instability at the start. However, by the end of the graph, both losses converge and stabilize, though the validation loss remains slightly higher than the training loss, indicating that the model generalizes reasonably well but might still benefit from further refinement. This pattern is typical in model training, where validation loss may fluctuate more than training loss due to unseen data.

For the Class Loss, both training and validation losses are initially high, especially around iteration 0, indicating a poor classification performance at the start of training. The training decreases quickly, showing that the model improves its class predictions as training progresses. The validation loss fluctuates significantly, indicating that the model struggles with unseen data early in training. Over time, the validation loss stabilizes, though it remains more variable than the training loss.

Finally, for the Object Loss, both training and validation losses start around 1.2, indicating a relatively high error rate in detecting objects at the beginning of the training. The training loss decreases gradually over time, indicating steady improvement in object detection during training. The curve follows a gentle downward trend, becoming more stable but still showing some fluctuations. The validation loss is initially lower than the training loss and remains relatively stable throughout the training process, hovering around 1.0.

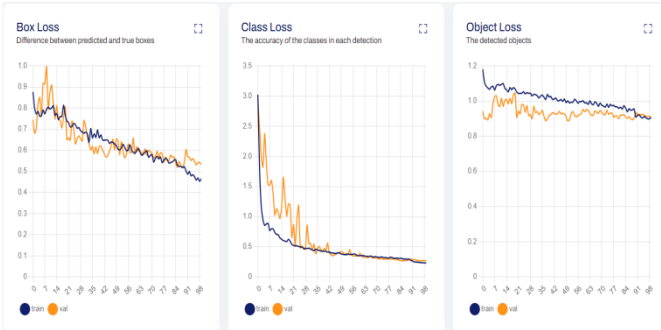


Fig. 8. Training results (Box, Class, Object Losses).

Thus, the model is progressively learning to detect objects better, with both training and validation object losses decreasing and converging. The relatively stable validation loss suggests that the model generalizes well to unseen data in terms of object detection, though there remains room for further improvement as the final loss is still above 0.8. Fig. 9 below presents the confusion matrix based on the results of the training of the model. It particularly presents that 99.5% of actual mature/premature coconuts were correctly detected. 0.5% of predicted mature/premature coconuts were incorrect (wrong predictions). 0.1% of actual mature/premature coconuts were missed (or undetected). Display of detection is presented in Fig. 11.

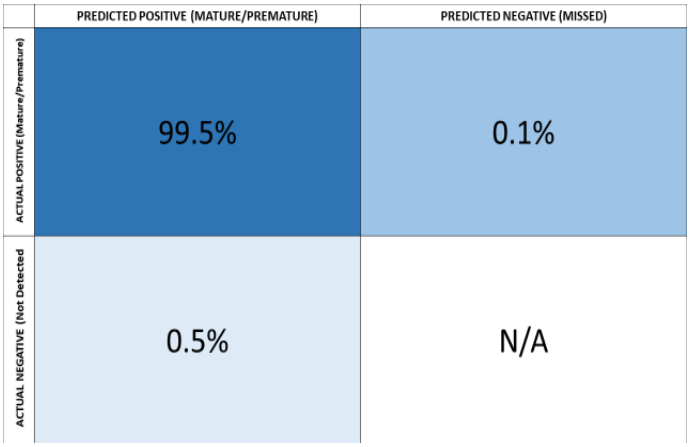


Fig. 9. Confusion matrix.

B. Web Dashboard

This particular section discusses the operation of the web dashboard where the data of scanned coconut fruits based on maturity is displayed. Fig. 10 below presents the homepage of the dashboard, wherein the user has to click the ENTER DASHBOARD button in order to enter the main dashboard.

Fig. 10. Dashboard homepage.

The dashboard consists of the footage of the video of the scanning of coconut fruits. The number of coconut fruits scanned based on maturity is displayed as well on the dashboard. The count data are also visualized on the line graph chart and the table as well. The count data of coconut fruits on the dashboard can also be printed to CSV file.

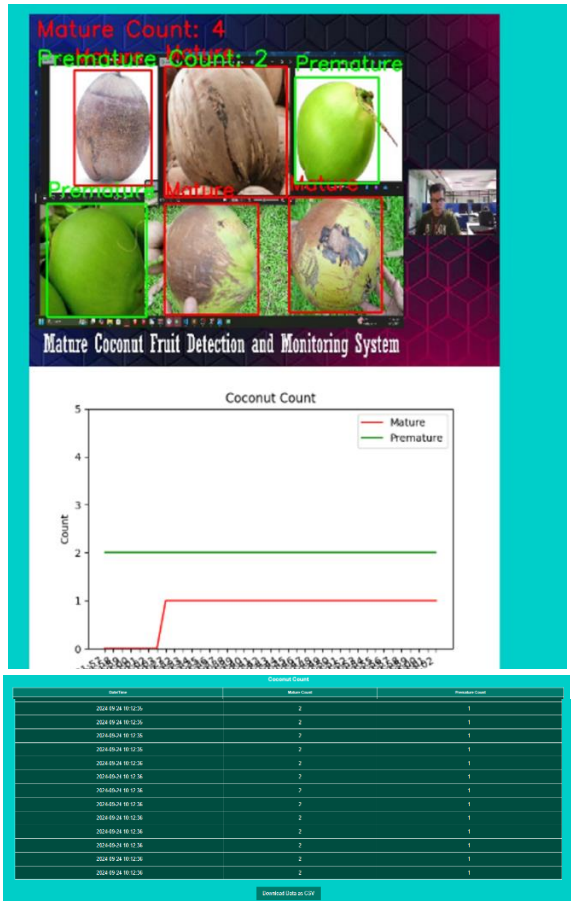


Fig. 11. Monitoring dashboard.

C. Testing and Evaluation of the System

As stated earlier, the overall system was tested and evaluated inside the laboratory since this paper is only limited to experimental level. The overall system was run using an NVIDIA GEFORCE RTX 3060 laptop having a 24GB RAM and 1.5TB internal storage with a 6GB GPU memory. Since the datasets were collected from coconut harvested fruits, therefore, the system can be able to correctly detect the maturity of the coconut fruits when the system's camera is placed very close to the object. Furthermore, with a small amount of datasets wherein mature coconut fruits consists of both brown and brown-and-green surfaces, the system expectedly misclassifies the maturity of coconut fruit. Therefore, more datasets should be added to the training of the model for a more accurate classification of coconut fruits according to maturity.

Fig. 12 below presents the notifications sent to the email for every mature coconut fruit detected. The system will notify through the email every time a new mature coconut fruit is detected.

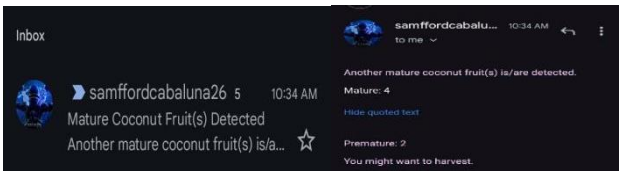


Fig. 12. Email notification.

IV. DISCUSSION

This section discusses in summary the results shown on the previous section, discussing the indications of the figures.

A. Discussion on Training Results

Training results show a gradual increasing in terms of metrics and decreasing in terms of losses, indicating an improving of training results. The overall decrease in both lines for box loss indicates a positive sign of improvement in bounding boxes. The convergence and the stabilizing of losses at a relatively low value for class loss suggests that the model performs well, although it still classifies slightly better on training data than on validation data. Overall, the model's class detection accuracy improves significantly over time, with a more stable training loss, and validation loss eventually converging but with higher variance. There are minor fluctuations for both losses under object loss, but overall, the validation loss shows a stable trend compared to the training loss. Both losses converge toward a similar value below 1.0 by the end of the iterations, suggesting that the model is improving in detecting objects and shows consistent performance on both training and validation datasets. The results shown on the confusion matrix indicate how well-performing the model is in classifying coconut fruit maturity, although there are minor misclassifications, yet the results proved that the model is performing well.

While the model is performing well in classifying coconut fruit maturity, it needs additional image datasets for an even more accurate classification since this paper is limited to close angle shots of the image datasets. Further improvement of such classification requires a consideration of drone shot angles and distances.

B. Discussion on Monitoring System

The monitoring dashboard design prototype displays an outstanding visualization of monitoring the status for coconut fruits in terms of their maturity stages. The notification system through email integrated with it shows that this system can aid in the real-time monitoring of coconut fruits. Since the system is in its experimental stage, this study recommends that for future improvement, the monitoring system will be integrated with an operational mobile app with SMS notification for a more user-friendly monitoring of the app.

V. CONCLUSIONS AND RECOMMENDATION

In conclusion, the researchers have designed and developed, as well as implemented a detection and monitoring system for mature coconut fruits, separating them from premature coconut fruits. The YOLOv8 model proved to be a good model for detection, though more datasets are needed to be added to the training of the model for an even more accurate detection. A web dashboard was also designed and developed, as well as integrated with the detection system, so that the footage of the scanning of coconut fruits are displayed on the dashboard along with the count data, wherein the count data can also be printed to CSV file as well.

Since the model needs more datasets due to some misclassifications occurring in the detection, by way of recommendation, it is highly recommended that there is a certain distance from the camera as well as its lighting resolution to be considered in gathering datasets to prepare the system for deployment with a more accurate detection; on-tree datasets are also highly recommended for training. It is highly recommended as well that the dashboard for display of data will be deployed in a fully operational app. Finally, it is very highly recommended that this system is integrated on a robotic harvester or any automated system by way of modernizing and improving the method of harvesting coconut fruits to aid the harvest of coconut fruits. In addition to increasing coconut harvesting efficiency, this integrated system can help achieve the Sustainable Development Goals (SDGs) of the UN, including Goals 2 (Zero Hunger), 9 (Industry, Innovation, and Infrastructure), and 17 (Partnerships for the Goals).

ACKNOWLEDGMENT

The researchers acknowledge the financial support of the Department of Science and Technology Engineering Research and Development for Technology (DOST ERDT) of the Philippines for this study along with the supervision of the Department of Computer Applications of the College of the Computer Studies of Mindanao State University Iligan Institute of Technology.

REFERENCES

[1] M. Kumar, G. Bej, and H. S. Pandey, "Status and Scope of Automated Coconut Harvester in India: A Review," Journal of Experimental Agriculture International, vol. 45, no. 5, Art. no. 5, Mar. 2023, doi: 10.9734/jeai/2023/v45i52115.

[2] C. Cousalya, C. Deepalakshmi, V. Keerthika, M. Malini, and P. Arthiya, "Mobile Operated Coconut Harvesting Machine," vol. 4, no. 5, 2021, doi: 10.15680/IJMRSET.2021.0405009.

[3] K. M. Sakthiprasad and R. K. Megalingam, "A Survey on Machine Learning in Agriculture - background work for an unmanned coconut tree harvester," in 2019 Third International Conference on Inventive Systems and Control (ICISC), Jan. 2019, pp. 433–437. doi: 10.1109/ICISC44355.2019.9036375.

[4] A. Junaedy, I. A. Sulistijono, and N. Hanafi, "Particle swarm optimization for coconut detection in a coconut tree plucking robot," 2017 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC), pp. 182–187, Sep. 2017, doi: 10.1109/KCIC.2017.8228584.

[5] A. B. Titus, T. Narayanan, and G. P. Das, "Vision system for coconut farm cable robot," 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), pp. 443–450, Aug. 2017, doi: 10.1109/ICSTM.2017.8089201.

[6] T. S. Wibowo, I. A. Sulistijono, and A. Risnumawan, "End-to-end coconut harvesting robot," in 2016 International Electronics Symposium (IES), Sep. 2016, pp. 444–449. doi: 10.1109/ELECSYM.2016.7861047.

[7] L. G. Divyanth, P. Soni, C. M. Pareek, R. Machavaram, M. Nadimi, and J. Paliwal, "Detection of Coconut Clusters Based on Occlusion Condition Using Attention-Guided Faster R-CNN for Robotic Harvesting," Foods, vol. 11, no. 23, Art. no. 23, Jan. 2022, doi: 10.3390/foods11233903.

[8] L. Noppon and P. Nipon, "The Application of Convolution Neural Network for Coconut Maturity Classification," in 2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), May 2021, pp. 112–115. doi: 10.1109/ECTI-CON51831.2021.9454744.

[9] I. M. Javel, A. A. Bandala, R. C. Salvador, R. A. R. Bedruz, E. P. Dadios, and R. R. P. Vicerra, "Coconut Fruit Maturity Classification using Fuzzy Logic," in 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM), Nov. 2018, pp. 1–6. doi: 10.1109/HNICEM.2018.8666231.

[10] P. Subramanian and T. S. Sankar, "Detection of maturity stages of coconuts in complex background using Faster R-CNN model," Biosystems Engineering, vol. 202, pp. 119–132, Feb. 2020, doi: 10.1016/j.biosystemseng.2020.12.002.

[11] N.-L. Nguyen, N. Van Khanh Duong, and H. D. T. Nguyen, "Deep Learning Based Coconut Fruit Maturity Classification," in Advances in Information and Communication Technology, P. T. Nghia, V. D. Thai, N. T. Thuy, L. H. Son, and V.-N. Huynh, Eds., in Lecture Notes in Networks and Systems. Cham: Springer Nature Switzerland, 2023, pp. 51–59. doi: 10.1007/978-3-031-49529-8_6.

[12] R. K. Megalingam, S. K. Manoharan, and R. B. Maruthababu, "Integrated fuzzy and deep learning model for identification of coconut maturity without human intervention," Neural Comput & Applic, Jan. 2024, doi: 10.1007/s00521-023-09402-2.

[13] R. K. Mandava, H. Mittal, and N. Hemalatha, "Identifying the maturity level of coconuts using deep learning algorithms," Materials Today: Proceedings, Sep. 2023, doi: 10.1016/j.matpr.2023.09.071.

[14] Venkatesh, P. K. P, P. Patil, P. G, P. Poojary, and S. B. Basapur, "CRipS: Coconut Ripeness Stage Detection System," in 2023 International Conference on Network, Multimedia and Information Technology (NMITCON), Sep. 2023, pp. 1–9. doi: 10.1109/NMITCON58196.2023.10276136.

[15] P. Subramanian and T. S. Sankar, "Coconut Maturity Recognition Using Convolutional Neural Network," in Computer Vision and Machine Learning in Agriculture, Volume 2, M. S. Uddin and J. C. Bansal, Eds., in Algorithms for Intelligent Systems. , Singapore: Springer Singapore, 2022, pp. 107–120. doi: 10.1007/978-981-16-9991-7_7.

[16] Y. Hendrawan, A. Amini, D. Maharani, and S. M. Sutan, "Intelligent Non-Invasive Sensing Method in Identifying Coconut (Coco nucifera var. Ebunea) Ripeness Using Computer Vision and Artificial Neural Network," 2019. Accessed: Jan. 25, 2024. [Online]. Available: https://www.semanticscholar.org/paper/Intelligent-Non-Invasive-Sensing-Method-in-Coconut-Hendrawan-Amini/cf3d736e20a00ddc238c0940a5161b5db5d92712

[17] Dr. A. Anushya, "Freshness Detection of Coconut via K-Means," IJRASET, vol. 8, no. 2, pp. 435–438, Feb. 2020, doi: 10.22214/ijraset.2020.2066.

[18] S. Varur, S. Mainale, S. Korishetty, A. Shanbhag, U. Kulkarni, and M. S. M, "Classification of Maturity Stages of Coconuts using Deep Learning on Embedded Platforms," in 2023 3rd International Conference on Smart Data Intelligence (ICSMDI), Mar. 2023, pp. 343–349. doi: 10.1109/ICSMDI57622.2023.00067.

[19] T. Avudai Nayagam and T. Devakumar, "Intelligent System for Matured Coconut Identification," IJRTE, vol. 9, no. 1, pp. 57–61, May 2020, doi: 10.35940/ijrte.F9520.059120.

[20] J. M. Novelero and J. C. D. Cruz, "On-tree mature coconut fruit detection based on deep learning using UAV images," presented at the 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom), IEEE, 2022, pp. 494–499.

[21] "(PDF) A Review on YOLOv8 and Its Advancements," in ResearchGate. doi: 10.1007/978-981-99-7962-2_39.

Simulation Analysis of Intelligent Control System for Excavators in Large Mining Plants Based on Electronic Control Technology

Lei Sun
School of Intelligent Manufacturing, Shandong Polytechnic, Ji'nan, 250000, China

***Abstract*—With the increasing demand for large-scale mine equipment and the complexity of the operating environment, the intelligent trajectory planning and control of mine systems becomes very important. This paper proposes a proportional-integral-differential (PID) feedback controller combined with adaptive improvement. This controller combines Genetic Algorithm and Particle Swarm Optimization technology to enhance the ability of the excavator's intelligent control system and improve the control accuracy, response speed, and robustness under different working conditions. The results showed that the constructed PID controller improved the average constraint performance by 2.5% through quintic interpolation, and the power consumption was relatively small. The trajectory prediction error of different joints was less than 5% and the displacement and pressure curves of the hydraulic cylinder were stable and symmetrical. The accuracy of the proposed algorithm was 94% and quickly converged to 0.05 after 50 iterations, which was 18.5%, 15.3%, and 17.5% higher than the other three algorithms, respectively. Therefore, the proposed method has high reliability and adaptability in anti-interference ability, trajectory planning progress, and optimization efficiency, and it provides a better solution for intelligent control of the excavator excavation system.**

***Keywords*—Genetic Algorithm; Particle Swarm Optimization; proportional-integral-differential; mining system; intelligent control**

I. Introduction

As global demand for mineral resources continues to rise, the existing production efficiency of the mining industry is unable to meet the current consumption needs. Furthermore, the safety of mining workers and the costs associated with production are also pressing concerns that require immediate attention [1]. Excavators represent the core equipment of large mining plants. However, they currently face significant challenges, including difficulties in dealing with complex mining environments, a lack of flexibility, and a lack of intelligent control [2]. The advancement of Electronic Control Technology (ECT) has provided the possibility for the emergence of Intelligent Control Systems (ICS) for excavators, which can to some extent meet the operational needs of large-scale mining industries. Currently, experts have extensively researched excavator ICS and algorithm optimization [3]. However, the existing excavators have obvious shortcomings in dealing with the changing mine environment, improving operation accuracy, and enhancing intelligent control. To solve these problems, this study proposes an ICS based on ECT to improve the performance of excavators in complex mine environments through advanced control strategies. The innovation of the research lies in the development of a Proportional-Integral-Differential (PID) controller, which combines Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) technology to enhance the adaptability and robustness of the excavator ICS. Through this combined optimization strategy, this method not only improves the control accuracy and response speed but also improves the anti-interference ability of the system in the face of internal and external interference.

This study proposes a PID feedback controller combining GA and PSO technology to improve the ICS performance of large mining excavators. By adopting the PID controller and GA-PSO optimization strategy, the control accuracy and response speed of ICS are improved. Compared with the existing PID control technology, fuzzy control, and GA and PSO when employed in isolation, the improved PID feedback control method combined with GA-PSO has stronger comprehensive performance in search performance and convergence speed and realizes more effective trajectory optimization.

The overall structure of the study includes six sections. Introduction is given in Section I. Section II summarizes the research achievements and shortcomings of ECT in ICS of different countries. The second section studies and designs the simulation model of PID feedback control. Section III tests and analyzes the proposed model. Section IV discusses the experimental results. Discussion is given in Section V and finally, Section VI concluded the paper.

II. Related Works

Significant progress has been made in the application of ECT in excavator ICS [4-5]. Sadiq et al. put forth a PID-Mining Control Systems (MCS) method based on adaptive adjustment, which was designed to address the issue that traditional MCSs are unable to effectively address the influence of nonlinear factors. This method could improve the control performance of load fluctuations. This method has reduced the response time by 13% compared to the PID control technology before improvement [6]. Wellendorf et al. designed a PSO-based PID control parameter optimization method to address the issue of traditional MCS relying on manual experience. It has improved stability by 20% compared to traditional control systems [7]. Kanso et al. proposed an adaptive PID control method based on fuzzy logic to address the limitations of traditional manual experience-based control of mining systems. This method reduced the response time by 14% and improved its robustness

by 34% [8]. Wang Z et al. proposed a PID control technique grounded on Deep Learning (DL) algorithms. The DL and predictive capabilities of this algorithm have improved the accuracy and response speed by 23% and 12%, respectively [9]. Sohail A et al. proposed a mining job scheduling optimization method based on an ant colony algorithm. Compared to traditional control systems, this method has increased mining efficiency by 28% and resource utilization by 10% [10].

The trajectory planning control method based on GA and PSO algorithms has also received widespread attention [11]. Gad et al. proposed a GA-based path optimization scheme for trajectory planning problems in complex environments. This method could obtain the global Optimal Solution (OS) under complex road conditions [12]. Pervaiz et al. developed an approach that simulates the objective function of PSO and updates the position and velocity of particles to obtain the OS, which has a fast convergence performance [13]. Zhang et al. established a trajectory planning control method based on GA-PSO, which expands the search range through crossover and mutation, and locally refines with PSO, significantly improving the accuracy and efficiency of the algorithm [14]. Minh et al. suggested a multi-objective optimization method fused with GA-PSO for nonlinear factors in complex environments. This method utilized the OS and hierarchical selection mechanism to achieve the OS under multi-objective common constraints [15]. Pozna et al. proposed a GA-PSO that combines DL and the feature extraction capability of DL to predict the priority of trajectory points, improving the intelligence level of path planning. This method could be used for path planning in complex environments and ensure the stability and reliability of the results [16].

In summary, existing research has made certain progress in anti-interference and trajectory optimization [17]. However, in more complex large-scale mining environments, the comprehensive control performance of the method still needs improvement, with limitations in response speed, control accuracy, anti-interference ability, and robustness [18-19]. Therefore, this study proposes an ECT-based ICS for large mining plant excavators to enhance their overall performance and control capabilities in complex working conditions. The innovation of the research lies in proposing a PID anti-interference control model based on adaptive improvement, aiming to improve the internal and external anti-interference performance of the algorithm. The trajectory control model combined with the GA-PSO optimization algorithm can improve the optimization of global and local solutions in complex and real-world environments while ensuring the accuracy and efficiency of the solutions. This study provides a better solution for excavator trajectory planning.

III. Methods and Materials

The first section constructs an anti-interference mining system. Firstly, a mechanical arm simulation dynamic model based on improved D-H parameters is established, and forward and inverse dynamics verification is carried out. Finally, a PID controller is introduced to further optimize the control performance of the mining trajectory planning system. The second section introduces the GA-PSO algorithm to optimize the parameters of the PID controller, further enhancing the control performance of the mining system.

A. Construction of PID Feedback Control Simulation Model for Anti-Interference Mining System

The operating environment of large mining plants is complex and harsh. The operation of excavators is inevitably limited by environmental factors, and it is also necessary to deal with self-interference caused by factors such as inertia and vibration during the excavator's movement process [20-21]. To enhance the ability of mining systems to cope with complex environments, it is necessary to construct a PID feedback control simulation model based on mining systems for trajectory planning and control. This study first establishes a geometric simulation model of the Robotic Arm (RA), defining the length, mass, centroid position, and inertia tensor of the joints and linkages of the RA. Subsequently, based on the improved D-H parameters, a coordinate for the linkage of the excavator arm is established, as shown in Fig. 1 [22-23].

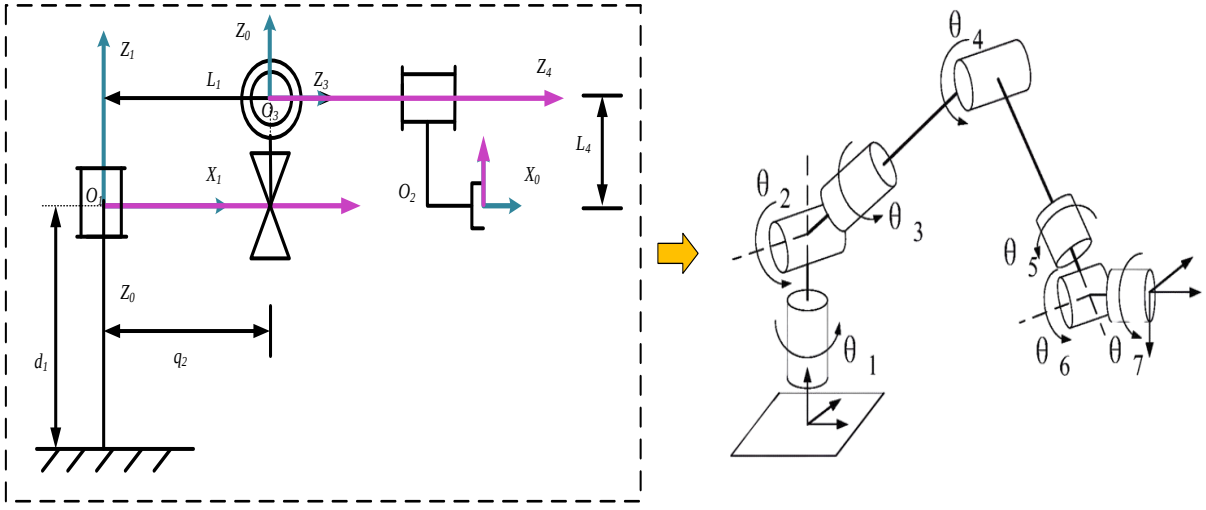


Fig. 1. Structural diagram of the coordinate system of the RA.

Based on the improved D-H parameters, each joint angle and link length of the RA is defined, and a coordinate system is set for each joint to determine the relationship between the joints. A positive dynamics verification is conducted on the constructed geometric simulation model of the RA, thereby obtaining the relationship between the posture and joint angles of the end position of the RA. The homogeneous transformation matrix between the connecting rod and the joint is shown in Eq. (1).

$$ {}_{i}^{i-1}\boldsymbol{T} = \begin{bmatrix} \cos\theta_i & -\sin\theta_i\cos\alpha_i & \sin\theta_i\sin\alpha_i & a_i\cos\theta_i \\ \sin\theta_i & \cos\theta_i\cos\alpha_i & -\cos\theta_i\sin\alpha_i & a_i\sin\theta_i \\ 0 & \sin\alpha_i & \cos\alpha_i & d_i \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (1) $$

In Eq. (1), ${}_{i}^{i-1}\boldsymbol{T}$ is the transformation relationship between adjacent linkage coordinate systems i and $i-1$. θ_i is the angle of rotation required for the connecting rod connecting two adjacent joints. α_i and d_i are the other angle and displacement length required to connect two adjacent joints. a_i is the horizontal distance between adjacent joints. The transformation matrix effectively describes the directional relationship between each joint and link in the structure of the RA, which can be used to obtain the final posture of the RA and accurately describe the pose of the RA at specific time points during motion. Using MATLAB for inverse dynamics verification, a simulation model is constructed to obtain the motion parameters of the RA. To ensure the accuracy of the excavator during excavation, handling, and movement in complex mining environments, the interpolation method is utilized to simulate the motion process multiple times. The motion parameters of the RA are obtained at each moment and then adjusted to ensure the model's accuracy. To ensure both the economy and stability of the RA control process, a Five Order Interpolation Method (FOIM) is adopted, as shown in Eq. (2).

$$ \theta(t) = A_0 + A_1 t + A_2 t^2 + A_3 t^3 + A_4 t^4 + A_5 t^5 \quad (2) $$

In Eq. (2), $\theta(t)$ is the rotation angle of the RA joint at time t. A_0, A_1, A_2, A_3, A_4, and A_5 are the difference coefficients related to t, representing the positions of each joint of the RA at time t. Through FOIM, more accurate simulation results of the RA are obtained. To further obtain a more optimal robot motion path and determine the objective function, the parameters during the movement of the RA are adjusted to ensure that the path meets the requirements, as given by Eq. (3).

$$ F(x) = \alpha f_1(x) + \beta f_2(x) \quad (3) $$

In Eq. (3), α and β are weighting coefficients. $F(x)$ is the objective function for the optimal path of the RA. $f_1(x)$ is a matrix constraint condition that describes the range of motion space of the RA. $f_2(x)$ is the proportion of the RA in the workspace. Considering the influence of factors such as gravity and inertia during the movement of the RA, this study presents challenges for precise control and efficient operation of the motion. Therefore, the derived joint torque is shown in Eq. (4).

$$ \tau = M(q)q + V(q,q) + G(q) \quad (4) $$

In Eq. (4), τ is the joint torque of the RA. $M(q)$ is the inertia matrix of the RA itself. q, q, and q are the joint gravity, inertia, and centripetal force of the RA, respectively. $G(q)$ is the gravity vector of the RA, which describes the influence of gravity on the joints. $V(q,q)$ is the term for centrifugal force and Coriolis force. In complex mining environments, to completely replace manual labor with excavators, it is necessary to ensure the flexibility of excavator movement. The formula for adaptive adjustment of the RA using an anti-interference tracker is given by Eq. (5).

$$ e_1(t) = x_1(t) - z_1(t) \quad (5) $$

In Eq. (5), $e_1(t)$ represents the velocity prediction error value during the motion of the RA. $x_1(t)$ is a nonlinear interference factor. $z_1(t)$ is the true value of the interference factor. To enhance the control capability of the RA over its own interference factors and increase its joint robustness, this study adopts a PID control strategy for the purpose of planning and controlling the motion trajectory of the RA, as illustrated in Fig. 2.

In Fig. 2, the PID controller uses Lyapunov function to perform error control based on the input joint motion state, and updates its motion state to obtain an anti-interference mechanical arm motion process. By using backstepping adaptation, the limitations of the controller can be effectively addressed. The dynamic equation for noise measurement of the sub states of the RA is shown in Eq. (6).

$$ J\,\theta_L = \frac{1}{n}T_m - B\dot{\theta}_L + T_{dis} \quad (6) $$

In Eq. (6), θ_L and θ_L are angular displacement and velocity. J is the gravity vector of the RA joint. T_m is the joint torque input to the PID controller. B is the adaptive control parameter. T_{dis} is the joint torque output by the PID controller. n is the joint variable of the RA. The parameters in the PID controller can be adaptively adjusted based on the influence of environmental and excavator factors. The calculation of parameter adaptive law is shown in Eq. (15).

$$ \hat{\theta} = \Gamma\varphi p \quad (7) $$

In Eq. (7), $\hat{\theta}$ and Γ are the PID control parameter adaptive law and adaptive matrix of the RA. φ is the error between the predicted and actual values of adjacent joint motion sub states. p is the error value of the motion state of the RA.

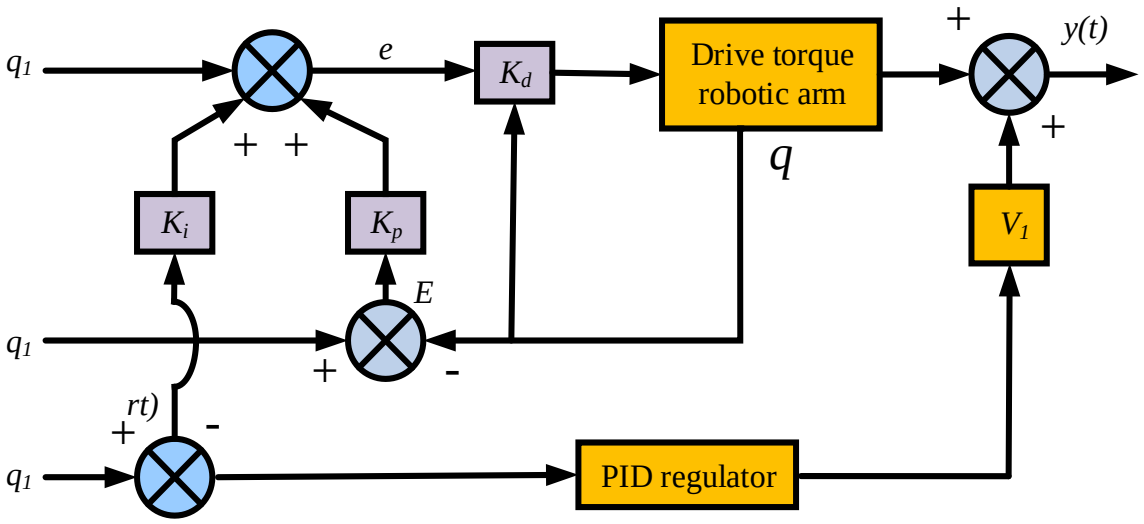


Fig. 2. Schematic diagram of backstepping adaptive control.

B. Construction of Excavator Trajectory Control Model based on GA-PSO

The previous section constructs a mining trajectory planning system based on a PID controller and obtains an anti-interference mechanical arm simulation dynamic model. In the ICS of large mining plants, PID-ECT can achieve excavation trajectory planning and control to enhance the accuracy, efficiency, and flexibility of the excavation process. However, in practical operating environments, due to the complexity of the environment, the feedback control mechanism of PID controllers requires a lot of adjustment time and experience and may encounter problems such as overshoot and oscillation [24-25]. Given these issues, this study proposes a PID control strategy built on GA-PSO to address complex control processes and ensure the accuracy, speed, and robustness of optimal parameter solving. Fig. 3 shows the PID control structure based on the GA-PSO algorithm.

In Fig. 3, GA-PSO searches for the optimal PID parameters to enable the PID controller to provide adjustments for high-frequency and low-frequency signals. GA can search globally by emulating the genetic operations that occur in the natural evolution of organisms. PSO simulates group behavior, and based on the global optimum searched by GA, further performs local fast convergence to obtain more accurate PID parameters. The first step in building GA-PSO is to use GA to randomly generate a set of PID parameters as the initial population, as shown in Eq. (8).

$$u(t) = K_p e(t) + K_i \int e(t)dt + K_d \frac{de(t)}{dt} \tag{8}$$

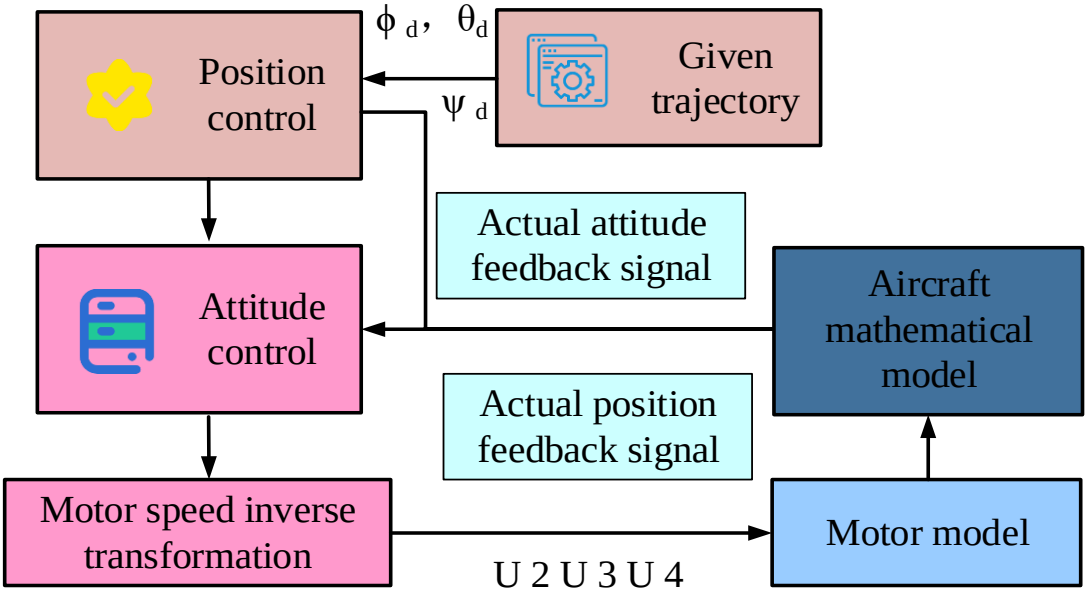


Fig. 3. PID control structure based on GA-PSO.

In Eq. (8), $u(t)$ is the input of the PID parameter vector. $e(t)$ is the error signal of PID control parameters. K_p, K_i, and K_d are the proportional gain, integral gain, and derivative gain of PID control parameters. Each individual input is subjected to fitness calculation, including sum of squared errors, overshoot, and response time, to achieve PID control performance evaluation, as shown in Eq. (9).

$$J = \int_0^T \left(e(t)^2 + \lambda_1 u(t)^2 + \lambda_2 \left(\frac{du(t)}{dt} \right)^2 \right) dt \tag{9}$$

In Eq. (9), J is the fitness function value. T is the total PID control time. λ_1 and λ_2 both represent weight factors. Following each iteration of the population update, an adaptive function is employed to assess the selected PID parameter solutions, thereby identifying the optimal control individual. This creates conditions for the next individual elimination and retention operations to improve the overall quality of the population. Based on the evaluation results of the adaptive function, the expression for selecting probabilities for each individual is given by Eq. (10).

$$P_i = \frac{J_i}{\sum_{j=1}^{N} J_j} \tag{10}$$

In Eq. (10), P_i and J_i are the selection probability and fitness of the current individual i. N means the population size. j is the individual in the population who is currently assigned a probability. To increase the diversity of the population and avoid getting stuck in local optima during algorithm solving, this study randomly selects gene fragments from any two individuals and performs crossover operations to generate new offspring individuals, as shown in Eq. (11).

$$\begin{cases} v^* = (v_1, \cdots, v_{k-1}, v_k, v_{k+1}, \cdots, v_n) \\ u^* = (u_1, \cdots, u_{k-1}, u_k, u_{k+1}, \cdots, u_n) \end{cases} \tag{11}$$

In Eq. (11), $u = (u_1, u_2, \cdots, u_n)$ and $v = (v_1, v_2, \cdots, v_n)$ are the generation of new individuals u^* and $v*$ after chromosome crossing between any two selected parental individuals. k is a random gene fragment cleavage point within the $1 \sim n$ range. Cross operation can increase population diversity, randomly mutate individuals, and further enhance the global nature of the algorithm, avoiding local optima. The random mutation operation performed on individuals is shown in Eq. (12).

$$x_k^* = \begin{cases} x_k + \Delta(t, U_{\max}^k - v_k), random(0,1) = 0 \\ x_k - \Delta(t, v_k - U_{\min}^k), random(0,1) = 1 \end{cases} \tag{12}$$

In Eq. (12), x_k is the individual's randomly selected cutting point for mutation. x_k* is the new mutation point generated after the mutation operation. $random(1,0)$ is a random integer representing the random value of the variance $\Delta(t, y)$. $[U_{\min}^k, U_{\max}^k]$ represents any cutting point within the range. The individual crossover mutation operation process is shown in Fig. 4.

In Fig. 4, by performing cross-mutation on individuals, the PID parameters of individuals can be randomly adjusted to obtain more global parameter solutions. The global advantage of GA has to some extent slowed down the computational speed of the algorithm. To deeply improve the calculation accuracy and velocity of the algorithm, the PSO algorithm is adopted for improvement. PSO is inspired by the foraging process of bird flocks and can accelerate the convergence process by updating particle velocity and position, and increase the accuracy of PID parameters to improve PID control performance. The velocity and location of particles are updated as shown in Eq. (13).

$$\begin{cases} x_i(0) = x_{\min} + rand(0,1) \times (x_{\max} - x_{\min}) \\ v_i(0) = v_{\min} + rand(0,1) \times (v_{\max} - v_{\min}) \end{cases} \tag{13}$$

In Eq. (13), $x_i(0)$ and $v_i(0)$ are the initial positions and velocities of the particles. $x_{\min} / x_{\max}$ and $v_{\min} / v_{\max}$ are the minimum and maximum values of particle position and velocity. PSO achieves further optimization of PID parameters by updating particle velocity and position, and the updated formula is shown in Eq. (14).

$$v_i(t+1) = \omega v_i(t) + c_1 r_1 (p_i - x_i(t)) + c_2 r_2 (g - x_i(t)) \tag{14}$$

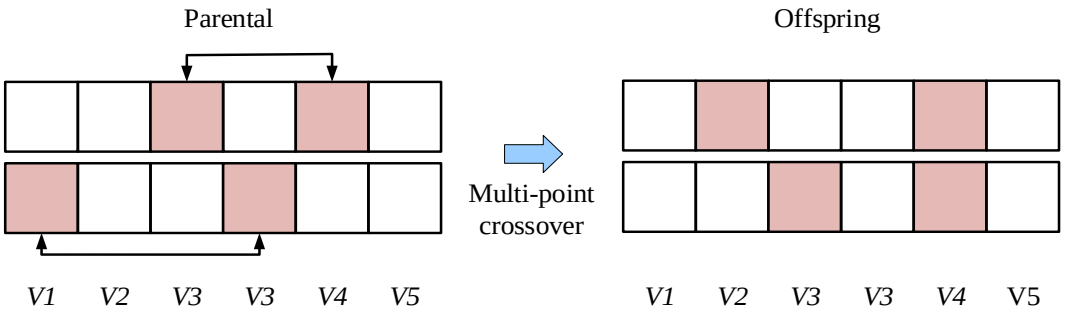


Fig. 4. Execution process of mutation operator.

In Eq. (14), $v_i(t+1)$ is the particle update speed. $v_i(t)$ is the velocity before particle update. ω denotes the inertia weight of particle velocity. c_1 and c_2 both represent learning factors. r_1 and r_2 are velocity weighting factors. p_i and g are velocity updates for particles. $x_i(t)$ is the optimal position for both the individual and the global. The formula for updating the particle's historical position based on its historical location and updated velocity is shown in Eq. (15).

$$x_i(t+1) = x_i(t) + v_i(t+1) \tag{15}$$

In Eq. (15), $x_i(t+1)$ is the current position of the particle after the position update. The schematic diagram of excavator trajectory planning is shown in Fig. 5.

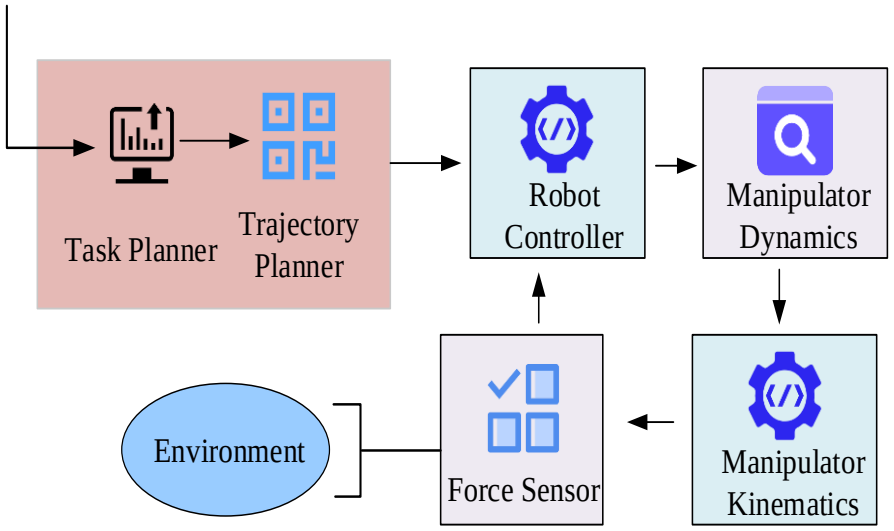


Fig. 5. Schematic diagram of excavator trajectory planning.

In Fig. 5, the process of mining mechanical trajectory planning is the process from task input to control instruction output.

IV. Results

Firstly, the anti-interference simulation model based on PID feedback control is tested to verify its control stability, accuracy, and error value. Next, the application effect of PID-MCS based on GA-PSO optimization is verified. The research method is compared in mining operation control under different working conditions to verify its superiority.

A. Performance Testing of PID Feedback Control for Anti-Interference Mining Trajectory Planning System

To validate the effectiveness of the constructed mining system dynamics simulation model, simulation experiments are conducted on the model. The hardware configuration used for the experimental equipment is Genuine Intel ®CPU 2140 (dual-core) 1.6GHz, 512MB of memory. The experiment is conducted on the MATLAB 7.0 platform. In MATLAB, a 3D simulation model of the linkage coordinates of the RA in the mining system is constructed based on the improved D-H parameters. The simulation experiment is conducted on a scaled-down testing platform to simulate the motion and operation process of the RA in a real environment, creating conditions for the structural and operational analysis of the RA. Table I shows the D-H parameters.

Firstly, the effectiveness of FIOM in controlling the motion of RAs is experimentally verified, using three, five, and nine iterations as comparisons. Each interpolation method is applied to joints 1, 2, and 3 of the RA. The joint motion fluctuation curve over time is used as the evaluation index, as displayed in Fig. 6. In Fig. 6, different numbers of interpolation methods have a good constraint effect on the motion path of the RA, with smooth and continuous curves without significant fluctuations. In Fig. 6 (a), the cubic interpolation method has the worst constraint effect on the motion process of the RA, with significant fluctuations occurring at both the beginning and end of the RA motion. In Fig. 6 (b), FOIM has the best constraint effect with no significant fluctuations, and the curve remains within the range of [-0.25, 0.25]. In Fig. 6 (c) and (d), the seven-degree and nine-degree interpolation methods improved the constraint performance by 2% and 3% respectively based on five degrees, but these two methods have higher energy consumption. This indicates that FOIM can ensure higher constraint performance while also being more energy-efficient.

To further verify the anti-interference ability of the path planning system after adopting the PID controller, the prediction and actual trajectory error of the RA are used as evaluation indicators, as shown in Fig. 7. In the trajectory prediction of four joints using the proposed method, the error is within 5% compared to the true values, and the motion trajectory curves are smooth, continuous, and without significant abrupt changes. In Fig. 7 (a), the application effect in joint 1 is the worst, with a predicted and actual displacement difference of 0.4m. In joint 2 of Fig. 7 (b), the actual and predicted displacement values have the highest overlap, with a difference of less than 0.1m. In Fig. 7 (c) and (d), the error values of joint 3 and joint 4 are at an intermediate level, within 0.3m. The proposed method can overcome the influence of nonlinear factors in the real environment when applied to MCS and has high feasibility and accuracy.

TABLE I. IMPROVED D-H COORDINATE PARAMETERS

Joint	Joint angle/°	Z-axis offset/mm	X-axis offset/mm	Rotation angle around the X-axis	Range of variation
1	-90°~90°	0	59	734	2643mm
2	-34.6°~76.2°	0	3680	0	2677mm
3	0°	136	1734	0	-40°~40°
4	0°	180	1046	0	3000

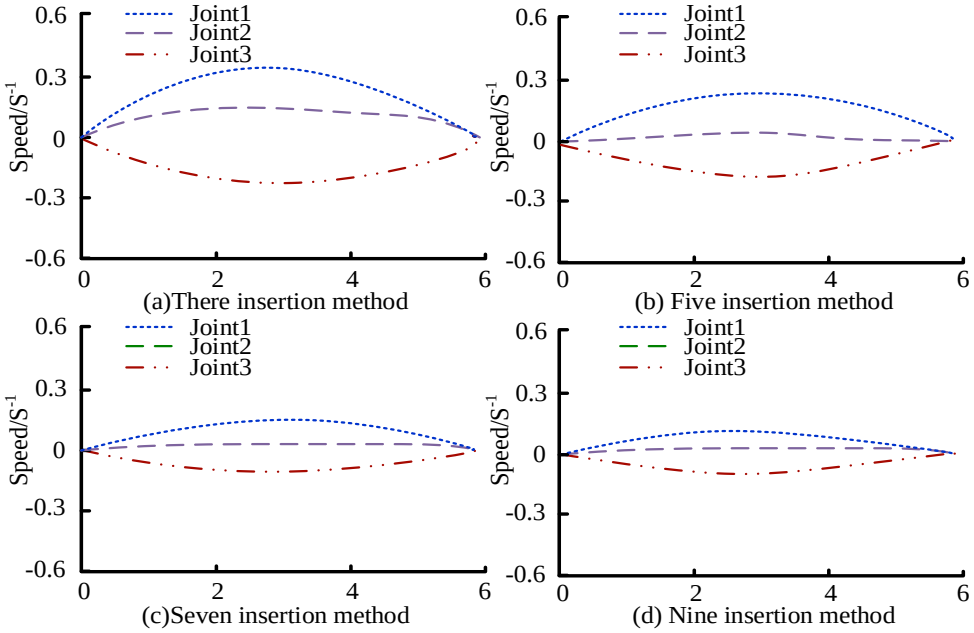


Fig. 6. Comparison of motion speed curves under different interpolation modes.

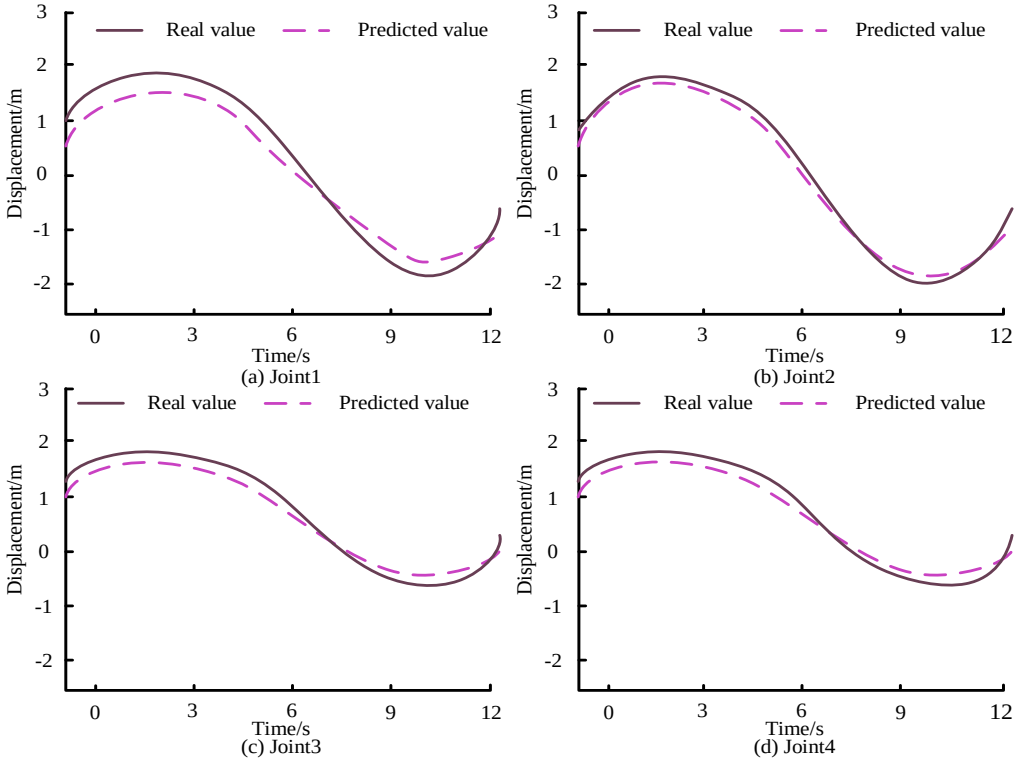
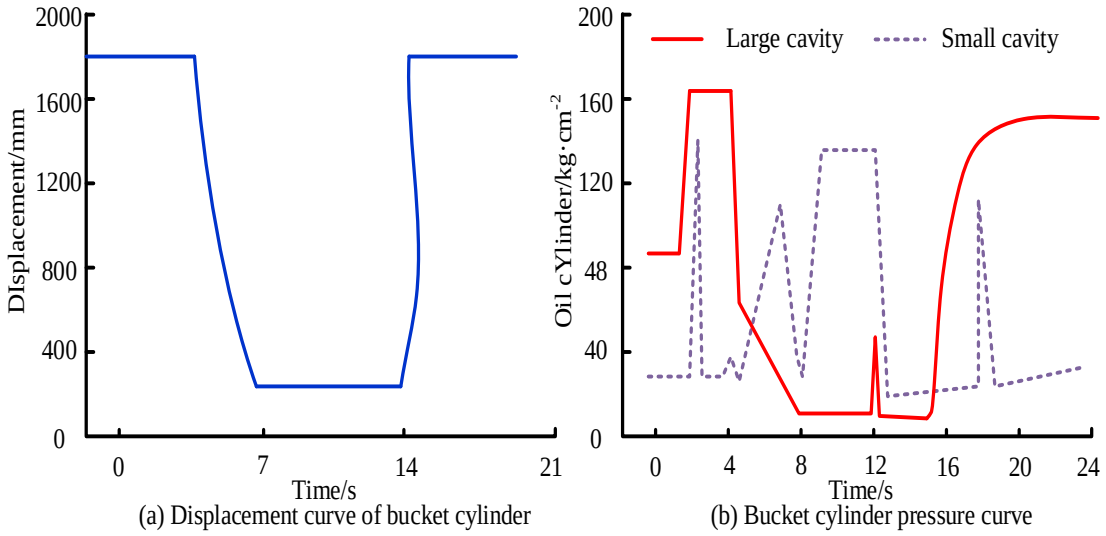


Fig. 7. Performance test under PID control of RA.

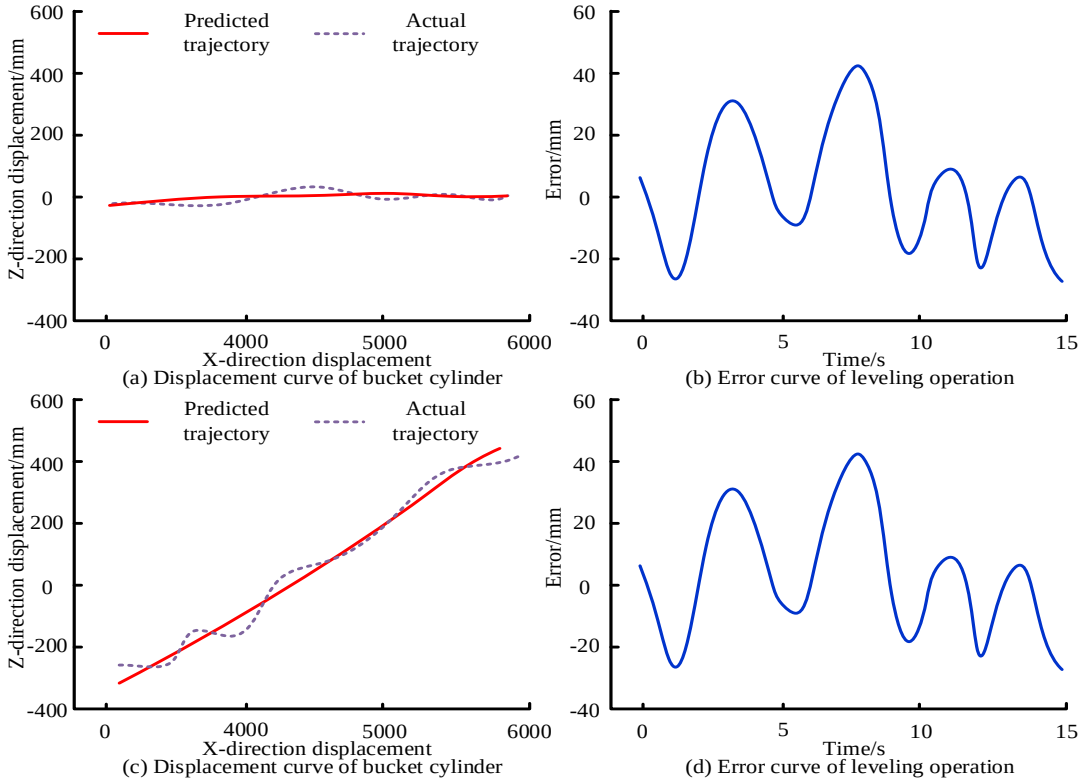
B. Application Verification of PIDMCS based on GA-PSO Optimization

After verifying the performance of the PID-controlled RA simulation model in the previous section, the actual application effect of the PID controller optimized by GA-PSO is analyzed. The displacement and pressure curves of the hydraulic cylinder applied to the practical application scenario of the bucket hydraulic cylinder using the research method are shown in Fig. 8. During the bucket operation, it can move accurately by the pre-set trajectory, and the displacement and pressure curves always show stability. In Fig. 8 (a), the displacement curve of the bucket cylinder encounters obstacles and evades them at 8-11s, and then returns to normal track operation. In Fig. 8 (b), there is consistency in the action of the pressure changes in the large and small chambers of the bucket cylinder at time points 2s, 4s, 8s, 12s, and 18s. The pressure curve exhibits symmetry within the ranges of [2, 4], [4, 8], [8, 12], and [18, 24]. The proposed excavation trajectory control method has good stability and accuracy in controlling the pressure parameters of the hydraulic system and can make the excavator move smoothly according to the predetermined track in practical applications.



(a) Displacement curve of bucket cylinder (b) Bucket cylinder pressure curve

Fig. 8. Displacement and pressure control curve of bucket cylinder.



(a) Displacement curve of bucket cylinder (b) Error curve of leveling operation

(c) Displacement curve of bucket cylinder (d) Error curve of leveling operation

Fig. 9. Trajectory control curves for different work environments.

To further verify the control effect during bucket excavation, the motion trajectory of the bucket during leveling and slope operations is tracked. Fig. 9 shows the error result between the calculated actual value and the predicted value. In Fig. 9 (a) and (b), the trajectory and error curve of the bucket tooth tip indicate that the maximum error in horizontal displacement is 44.21mm. In Fig. 9 (c) and (d), the maximum error of water diagonal displacement during bucket slope operation is 41.41mm. Overall, the motion errors are within a reasonable range, and the motion curve is smooth, continuous, and without significant fluctuations. The proposed method can ensure stable and accurate control effects in two different operating environments, with errors controlled within a reasonable range, and the results have high reliability.

To further verify the practical application effect of GA-PSO in optimizing PID parameters and mining trajectory planning systems, three classic algorithms, Adaptive Genetic Algorithm (AGA), A* Search Algorithm (A*), and Rapidly-exploring Random Tree (RTT), are compared. Fig. 10 shows the results of using the convergence accuracy and rate of the algorithm as performance evaluation indicators. As the number of iterations increases, the convergence accuracy and rate of the proposed algorithm are better than the other three compared algorithms. In Fig. 10 (a), the proposed algorithm converges to 0.05 after 50 iterations, while AGA, A*, and RTT algorithms converge to similar levels after 80, 91, and 110 iterations, respectively. The average convergence rate of the three algorithms is 0.08 lower than the proposed algorithm. In Fig. 10 (b), the proposed algorithm achieves the highest accuracy of 94%, while AGA has the lowest accuracy of only 75%. The accuracy of A * and RTT algorithms is at an intermediate level, which is 15.3% and 17.5% lower than the proposed algorithm. Therefore, the GA-PSO has the best accuracy and efficiency when applied to mining trajectory planning systems.

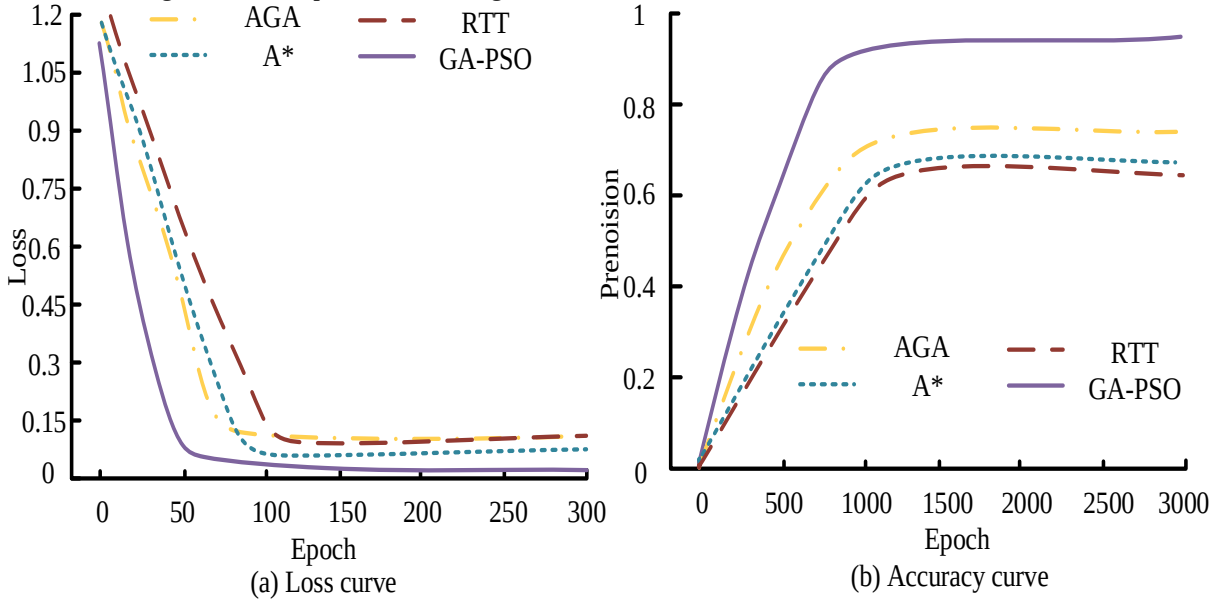


Fig. 10. Comparison of convergence accuracy and efficiency of different algorithms.

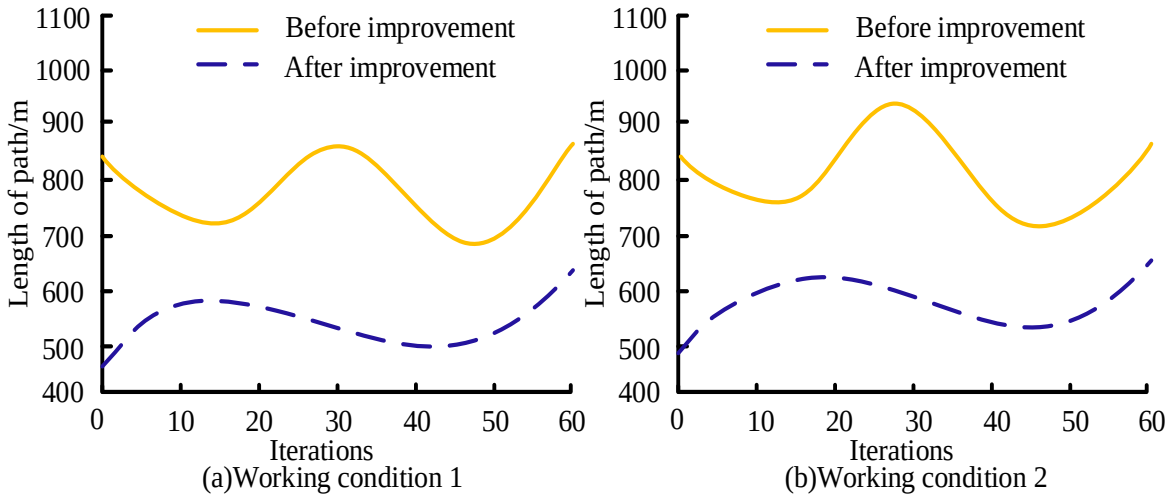


Fig. 11. Comparison of algorithm path planning length before and after improvement.

To test the path planning performance of the research algorithm, it is tested under two different load levels and compared with the improved algorithm using path length as the evaluation index, as exhibited in Fig. 11. Overall, the path length of the improved algorithm is shorter. In condition 1 of Fig. 11 (a), the longest path of the algorithm before improvement is 884m at 30 iterations, which is 46.2% longer than the improved algorithm. In condition 2 of Fig. 11 (b), the improved algorithm has a maximum path of 962m at 60 iterations, a decrease of 43.5% compared to before the improvement. In two different levels of complexity, the error is within 5%, indicating that the improved method has high reliability and accuracy.

V. Discussion

The proposed ECT-based ICS shows obvious performance improvement in the application of large-scale mining excavators by combining the PID controller optimized by GA-PSO technology. The analysis of experimental results demonstrates that the enhanced PID feedback control method exhibits superior comprehensive performance in search performance and convergence speed when compared to traditional PID control technology, fuzzy control, and the use of GA and PSO in isolation. In the aspect of the anti-interference ability, the proposed method effectively improves the robustness of the excavator in the face of internal and external interference through adaptive adjustment of the PID controller. This is reflected in the stability of the displacement and pressure curve of the hydraulic cylinder. The stability and symmetry of the curve show the precise control ability of the system in actual operation [20, 21]. In addition, the trajectory prediction error is controlled within 5%, which further proves the high reliability and adaptability of the system in complex mine environments.

In terms of optimization efficiency, the application of the GA-PSO algorithm significantly improves the accuracy and speed of parameter optimization. A comparative analysis of the algorithms reveals that the proposed algorithm rapidly converges to 0.05 after 50 iterations, with an accuracy of 94%, which is superior to the other three classical algorithms [11-13]. This shows that the GA-PSO algorithm can balance the efficiency of global search and local search more effectively when dealing with complex trajectory planning problems.

VI. Conclusion

Aiming at the intelligent control of large mining equipment in complex mine environments, this paper proposes an ICS based on ECT. Through the PID controller optimized by combining GA and PSO technology, the accuracy, response speed, and robustness of the control system are improved. The experimental results showed that the control system had good stability and accuracy under different working conditions. The trajectory prediction error was controlled within 5%, the displacement and pressure curves of the hydraulic cylinder were stable, and the algorithm converged rapidly after 50 iterations, with an accuracy of 94%. These results proved the effectiveness of the proposed method and provided a practical solution for improving the intelligent control performance of large mining equipment.

Nevertheless, the research is not without limitations. In particular, the comprehensive control performance of the algorithm requires further improvement in a more complex actual mine environment. Future research will concentrate on enhancing the algorithm's adaptability to more effectively address the evolving mine environment. Additionally, more efficient optimization strategies will be investigated to minimize calculation time and enhance control accuracy. In addition, advanced technologies such as DL are considered to be integrated into the control system to further improve the level of intelligent control.

References

[1] Liu Y, Cao B, Li H. Improving ant colony optimization algorithm with epsilon greedy and Levy flight. Complex & Intelligent Systems,2021 ,7(4):1711-1722.

[2] Stodola P. Hybrid ant colony optimization algorithm applied to the multi-depot vehicle routing problem. Natural computing, 2020 ,19(2):463-475.

[3] Deng W, Xu J, Song Y, Zhao H. An effective improved co-evolution ant colony optimisation algorithm with multi-strategies and its application. International Journal of Bio-Inspired Computation, 2020, 16(3):158-170.

[4] Li W, Wang GG, Gandomi AH. A survey of learning-based intelligent optimization algorithms. Archives of Computational Methods in Engineering, 2021 ,28(5):3781-3799.

[5] Wellendorf A, Tichelmann P, Uhl J. Performance Analysis of a Dynamic Test Bench Based on a Linear Direct Drive. Archives of Advanced Engineering Science, 2023, 1(1):55-62.

[6] Sadiq A T, Raheem F A, Abbas N. Ant colony algorithm improvement for robot arm path planning optimization based on D strategy. International Journal of Mechanical & Mechatronics Engineering, 2021, 21(1): 196-111.

[7] Wellendorf A, Tichelmann P, Uhl J. Performance Analysis of a Dynamic Test Bench Based on a Linear Direct Drive. Archives of Advanced Engineering Science, 2023, 1(1):55-62.

[8] Kanso B, Kansou A, Yassine A. Open capacitated ARC routing problem by hybridized ant colony algorithm. RAIRO-Operations Research, 2021, 55(2): 639-652.

[9] Wang Z, Ding H, Li B, Bao L, Yang Z, Liu Q. Energy efficient cluster based routing protocol for WSN using firefly algorithm and ant colony optimization. Wireless Personal Communications, 2022, 125(3): 2167-2200.

[10] Sohail A. Genetic algorithms in the fields of artificial intelligence and data sciences. Annals of Data Science, 2023 , 10(4):1007-1018.

[11] Too J, Abdullah A R. A new and fast rival genetic algorithm for feature selection. The Journal of Supercomputing, 2021, 77(3): 2844-2874.

[12] Gad AG. Particle swarm optimization algorithm and its applications: a systematic review. Archives of computational methods in engineering, 2022 ,29(5):2531-2361.

[13] Pervaiz S, Bangyal WH, Ashraf A, Nisar K, Haque MR, Ibrahim A, Ag AB, Chowdhry B, Rasheed W, Rodrigues JJ. Comparative research directions of population initialization techniques using PSO algorithm. Intelligent Automation & Soft Computing, 2022 ,32(3):1427-1444.

[14] Zhang H, Thompson J, Gu M, Jiang XD, Cai H, Liu PY, Shi Y, Zhang Y, Karim MF, Lo GQ, Luo X. Efficient on-chip training of optical neural networks using genetic algorithm. Acs Photonics, 2021 , 8(6):1662-1672.

[15] Minh HL, Khatir S, Rao RV, Abdel Wahab M, Cuong-Le T. A variable velocity strategy particle swarm optimization algorithm (VVS-PSO) for damage assessment in structures. Engineering with Computers, 2023 ,39(2):1055-1084.

[16] Pozna C, Precup RE, Horváth E, Petriu EM. Hybrid particle filter–particle swarm optimization algorithm and application to fuzzy controlled servo systems. IEEE Transactions on Fuzzy Systems, 2022 ,30(10):4286-4297.

[17] Shishavan ST, Gharehchopogh FS. An improved cuckoo search optimization algorithm with genetic algorithm for community detection in complex networks. Multimedia Tools and Applications, 2022 , 81(18):25205-25231.

[18] Chotikunnan P, Chotikunnan R. Dual design PID controller for robotic manipulator application. Journal of Robotics and Control (JRC), 2023 ,4(1):23-34.

[19] Saleh B, Yousef AM, Ebeed M, Abo-Elyousr FK, Elnozahy A, Mohamed M, Abdelwahab SA. Design of PID controller with grid connected hybrid renewable energy system using optimization algorithms. Journal of Electrical Engineering & Technology, 2021 ,16(6):3219-3233.

[20] Suseno EW, Ma'arif A. Tuning of PID controller parameters with genetic algorithm method on DC motor. International Journal of Robotics and Control Systems, 2021 ,1(1):41-53.

[21] Ma'arif A, Setiawan NR. Control of DC motor using integral state feedback and comparison with PID: simulation and arduino implementation. Journal of Robotics and Control (JRC), 2021, 2(5):456-461.

[22] Lin P, Wu Z, Fei Z, Sun XM. A generalized PID interpretation for high-order LADRC and cascade LADRC for servo systems. IEEE Transactions on Industrial Electronics, 2021 ,69(5):5207-5214.

[23] Kristiyono R, Wiyono W. Autotuning fuzzy PID controller for speed control of BLDC motor. Journal of Robotics and Control (JRC), 2021 ,2(5):400-407.

[24] Nath UM, Dey C, Mudi RK. Review on IMC-based PID controller design approach with experimental validations. IETE Journal of Research, 2023 ,69(3):1640-1660.

[25] UsmanA M, Abdullah M K. An Assessment of Building Energy Consumption Characteristics Using Analytical Energy and Carbon Footprint Assessment Model. Green and Low-Carbon Economy, 2023, 1(1): 28-40.

Predicting Graft Failure Within Year After Transplantation Using Data Mining Techniques

Meshari Alwazae[1], Saad Alghamdi[2], Lulu Alobaid[3], Bader Aljaber[4], Reem Altwaim[5]*
Center of Genomic Medicine at King Faisal Specialist Hospital & Research Centre, Riyadh, Saudi Arabia[1]
Organ Transplant Center of Excellence at King Faisal Specialist Hospital & Research Centre, Riyadh, Saudi Arabia[2]
Department of Medicine at King Faisal Specialist Hospital & Research Centre, Riyadh, Saudi Arabia[3]
Al-Imam Muhammad Ibn Saud Islamic University, Riyadh, Saudi Arabia[4]
Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia[5]

***Abstract*—The complex factors of liver transplant survival and the potential for post-transplant complications are significant challenges for healthcare professionals. This paper aims to identify the ability to use data mining techniques to develop a predictive model for liver transplant failure by identifying the relationship between abnormalities in periodic patients' laboratory results and graft failure. The researchers obtained data from King Faisal Specialist Hospital and Research Centre to address the research problems. First, the classification technique was used to predict cases with a high risk of liver transplant failure. Second, Association Rules were applied to identify associations between abnormalities in patients' laboratory results and transplant failure. Before using data mining algorithms, the patient dataset underwent a cleaning process, which involved removing duplicate entries and uncertain results. The algorithms were applied separately to the data of patients who completed the first year without complications and those who experienced transplant failure. The obtained results were then compared and we observed that abnormal levels in Aspartate Transferase (AST), Red Blood Cell (RBC), Hemoglobin (Hgb), 'Bilirubin Total', and 'Platelet' occurred exclusively in cases that faced liver transplant failure within the first year. Similarly, abnormal levels in 'AST', 'RBC', Alanine Aminotransferase (ALT), and 'Bilirubin Total' were also associated with transplant failure.**

***Keywords*—Graft failure; liver transplant; data mining; predictive model; classification; association rules**

I. Introduction

The growth of technology use in the last decade has led to large amounts of data entering data repositories worldwide. It is unrealistic to extract valuable knowledge manually from this vast, massive data. Therefore, many technologies have been created to assist the user with tools to find useful knowledge and information from this distributed data. Data mining refers to the extraction of valuable knowledge and meaningful information from large databases; it depends on machine learning, statistical methods, and artificial intelligence. The efficacy of data mining has been extensively studied across various domains, including commercial sectors, telecommunications, and healthcare [1].

In the medical industry, sensitive data is produced daily from medical records, patient monitoring, laboratory reports, radiology images, and more. Therefore, data mining applications have shown effectiveness in the healthcare industry. Physicians can use data mining techniques to enhance patients' quality of life by using data to design the best treatment plan, diagnose potential diseases, or predict drug side effects [2].

One medical field recently used in data mining is organ transplantation. Organ transplant refers to replacing a failed organ from a patient with an organ from a Brain deceased donor or living donor. This operation gives the patient with end-stage organ failure the chance to have a normal life [3]. Liver transplantation (LT) is the ultimate medical intervention for patients with advanced liver disease. However, there are main challenges that reduce the benefits of liver transplants, the shortage of grafts available for transplant, the increase in the patients on the waiting list, and the probability of graft failure after the surgery. Patients are subjected to strict monitoring of their vital functions and extensive analysis during past and post-transplant to predict any signs of liver failure. In addition, transplant patients undergo high doses of immunosuppressants, especially within the first year post-transplant, to reduce the possibility of liver failure. However, many factors affect graft survival, making the early prediction process complex [4].

According to these challenges, physicians find it difficult to predict patients with a high risk of graft failure and improve the chance of saving the graft and the patient's life [5]. Therefore, several scores and models have been evaluated to predict contributing factors to achieve a successful post-LT outcome. It is important to note that most of these models were introduced several years ago, applied to different populations, and focused on different kinds of organ transplants; Kidney, Lung, or Heart. In this research, the focus is to study a model to predict patients with a high risk of liver failure post-liver transplant (LT).

II. Literature Review

A. Data Mining in Predicted Failure Transplant Organ

Many prior studies built different models based on data mining methodologies to predict graft survival. These studies covered kidneys, lungs, liver, and Stem Cell transplantation. Some researchers have developed a new predictive model, and others compared different data mining algorithms to improve the accuracy of predictions.

Atallah et al. [5] used hyper-classifiers to predict kidney transplant outcomes. They proposed a method to predict kidneys before transplants dependent on three stages, the preparation stage, feature selection stage, and then prediction stages. In the first stage, they proposed preparing the data which consisted of

data cleaning and removal of all instances that have missing data. In the feature selection stage, only relevant features are extracted to improve the accuracy of the model. The last stage is conducting the predicting phase using the KNN algorithm. They found the highest accuracy by using this method, they achieved 81.5% accuracy.

Also, Oztekin et al. [11] proposed a feature selection methodology based on a genetic algorithm (GA) to achieve a high classification accuracy to predict the quality of life after a lung transplant. The GA-selection algorithm was applied along with kNN, ANN, and SVM as classification models. The result shows that SVM had the highest accuracy in predicting quality of life following lung transplantation.

In other studies, the predictor of the risk of Kidney transplant failure has been investigated in different cohorts. Naqvi et al. [16] conducted machine classification algorithms to develop prediction models for the risk of graft failure using support vector machines (SVM), AdaBoost, RF, ANN, and logistic regression over patients' data in three cohorts. The result of accuracy shows that SVM and AdaBoost have the highest rate over the cohorts.

To compare the accuracy of a different model, [10] compared nine algorithms using 10-fold stratified cross-validation, which were: logistic regression, linear discriminant analysis, quadratic discriminant analysis, support vector machines (using linear, radial basis function, and polynomial kernels), decision tree, random forest and stochastic. In the same idea, [10] [9] compared six algorithms: Naïve Bayes (NB), alternating decision trees (ADT), and logistic regression (LR) which produce models with interpretable structures, whereas multilayer perceptron (MLP), random forest (RF) and AdaBoost attempt to detect for the one which will give the highest accuracy.

On the other hand, [13] compared between three data mining (DM) methods to predict Kidney Transplant Survival. The models are the C&R Tree Model, Neural Network Model, and C5.0 Model. The accuracy of the C5.0 Model was the highest. It was 91.5% within the first year of transplant.

Also, [15] studied the cases of failure and success of LT by studying factors related to the patient and the donor and comparing the accuracy of the classification before and after the feature Selection. By comparing the accuracy results when applied Neural Network and Random Forests before FS: 0.734 and 0.787 and after FS: 0.835 and 0.818.

All previous studies have highlighted the use of classification in predicted transplantation outcomes; on the other hand, [14] used the association rules to predict important factors for who did and did not have kidney failure five years post-kidney transplant for live and deceased donor recipients. He identified factors common in both patients (live and deceased donor recipients) and factors important only in deceased donors. Also, he identified the factors associated with graft Failure. These factors match with what is usually observed in patients in the clinic. Table I summarizes the Application and Techniques Used in Organ Translation Studies.

B. Liver Transplant in the Kingdom of Saudi Arabia

Organ transplant has been one of the medical revolutions in the last two decades [6]. It gave patients with end-stage organ failure a chance to live a normal life by removing the organ from one person "the donor" and transplanting it to the recipient who has organ failure. The most common organs that are transplanted include the heart, kidneys, lungs, and liver. As a result of the high burden of liver disease in the country, there is a high demand for liver transplantation. The estimated LT is around 75 patients per million.

TABLE I. APPLICATION AND TECHNIQUES USED IN ORGAN TRANSLATION STUDIES

Title	Year	Application	Algorithms And Methods
Predicting kidney transplantation outcome based on hybrid feature selection and KNN classifier	2019	Predict delayed graft function after kidney transplantation	K-Nearest Neighbors (KNN) algorithm
A decision analytic approach to predicting quality of life for lung transplant recipients: A hybrid genetic algorithm-based methodology	2018	Predict the quality of life after a lung transplant	The GA-selection algorithm, kNN, Artificial Neural Networks (ANN), and support vector machines(SVM)
Predicting kidney graft survival using machine learning methods: prediction model development and feature significance analysis study.	2021	Predict the risk of kidney transplant failure	SVM, AdaBoost, random forest (RF), ANN, and logistic regression
). Prediction of delayed graft function after kidney transplantation: comparison between logistic regression and machine learning methods.	2015	Compare the accuracy of a different model to detect which one will give the highest accuracy in Predict delayed graft function after kidney transplantation	Logistic regression, linear discriminant analysis, quadratic discriminant analysis, support vector machines, decision tree, random forest, and stochastic. algorithms: Naïve Bayes (NB), alternating decision trees (ADT), and logistic regression (LR) which produce models with interpretable structures, whereas multilayer perceptron (MLP), RF and AdaBoost
Comparing three data mining methods to predict kidney transplant survival	2016	Compared between three data mining methods to predict Kidney Transplant Survival	C&R Tree Model, Neural Network Model, and C5.0 Model
Machine-learning algorithms predict graft failure after liver transplantation	2017	Predict graft failure after liver transplantation	Neural Network and Random Forests
Analyzing Association Rules for Graft Failure Following Deceased and Live Donor Kidney Transplantation.	2021	Predicted kidneys' transplantation outcomes	Association Rules

As the growth of organ transplant activities all over the world, the Kingdom of Saudi Arabia (KSA) picked up the pace in this field. In 1985, the Saudi Center for Organ Transplantation (SCOT) was established as a government center to monitor organ transplantation activities in KSA. Indeed, the first organ transplant in KSA was a kidney transplant from a living donor in 1979 [12], while the first LT was in 1991 [7]. Nowadays, there are over 20 organ transplant programs throughout the KSA, and four of them are LT centers. In Riyadh, there are three centers and the last one is in Dammam. Over 2000 LTs have been performed over the four centers, 50% of these surgeries performed at King Faisal Specialist Hospital and Research Center (KFSH&RC) in Riyadh. For each LT center, there is a waiting list based on the Model for End-Stage Liver Disease (MELD) scores.

III. Methodology

To answer the research questions, we applied two Data Mining methodologies. First, we applied several common classification algorithms to predict failure cases. Second, we conducted Association rules to identify the relationships among patients' data.

The main steps were followed:

- Data collection.
- Data preprocessing.
- Predicting Liver Failure: a. Classification. b. Association Rules, As shown in Fig. 1:

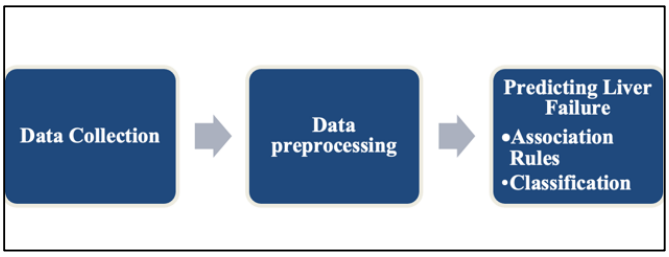


Fig. 1. Main steps of the data mining process.

A. Data Collection

The data used in this study was obtained from KFSH&RC and presented in a CSV format. The dataset included lab results of 1118 patients who underwent LT between 2002 and 2018, totaling 772339 rows and fourteen columns. Each row represented a specific lab result for one patient on a particular date. Eighty-one different labs were taken; it is important to note that the frequency of lab repetition varied depending on the patients at other times, and not all labs were taken for every patient. Moreover, there were duplicate data, missing data, and laboratories without any results, Table II summarizes the dataset:

TABLE II. Summary of Patients' Dataset

Data Set Size	Number of Attributes	Unique Establishment IDs
772339	14	1118

The dataset contains six columns with different dates for each lab:

- ORIG_ORDER_DT_TM
- DRAWN_DT_TM
- RECEIVED_DT_TM
- CURRENT_START_DT_T
- LAST_UPADTE
- RESULT_PERFORM_DT_TM

By referring to the specialist doctor about the importance of these columns, it was found that the most critical column among them is: RECEIVED_DT_TM

All unimportant columns were excluded from the table, and retained only the following ones**:**

- RESULT_PERFORM_DT_TM
- MRN
- BIRTH_DT_TM
- CATALOG
- LAB_TEXT_NAME
- RESULT

Descriptions of the attributes are presented in Tables III:

Table II: Dataset attributes description

TABLE III. Dataset Attributes Description

#	*Attribute name*	*Type*	*Description*
1	RESULT_PERFORM _DT_TM	Datetime	Date of receipt of the patient's analysis request
2	MRN	int64	Unique ID for each patient
3	BIRTH_DT_TM	Datetime	The birth date of each patient
4	CATALOG	object	The categories for each laboratory test
5	LAB_TEXT_NAME	object	The name of laboratory test
6	RESULT	int64	Represent the result of the laboratory test

Another CSV file was obtained reviewing cases completed a year without complications and unsuccessful cases from 2001 to 2019. The number of patients in this file is 1140 cases: 1031 success cases, 121 failure cases, and 26 cases without information. Fig. 2 shows the increase in liver transplant cases during the previous years at the KFSH&RC:

B. Data Preparation

Usually, the raw data contains noise, missing, or duplicated data that can affect the quality of data mining results, so the data preparation phase is a crucial step. The researchers follow steps that are suitable for their methodologies according to the type and size of the data and the data mining technique used [18]. This phase is also important for better understanding and realizing data. It consists of data cleaning, data labeling, and addressing class imbalances.

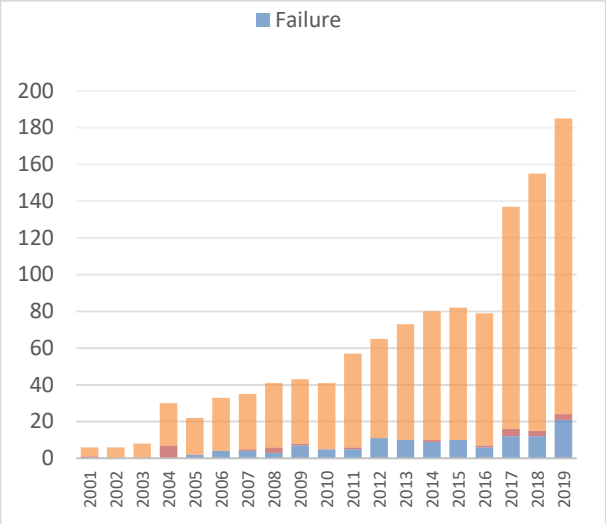


Fig. 2. The liver transplant cases during the previous years at the KFSH&RC.

1) Data Cleaning: The data obtained is vast, and complex, with many Null cells and duplicate data. Also, all rows were excluded for pediatric patients who were younger than 15.

Data cleaning involved removing:

- All rows with missing values.
- All rows if the "Result" column contains "Indeterminate", "Hemolyzed", "See the comment" or "Equivocal".
- All rows if received date more than one year before the transplant.
- All duplicated rows.

2) Data labeling: The laboratory results vary in distributed values; any difference from the normal range is considered abnormal, so a "Class" column has been added, which shows the status of the laboratory results if the result is within the normal range or abnormal.

Data Labeling involved modified:

- "Result" value if "Result" = "positive" to 1 , and Negative to 0,
- Determined the normal range for each laboratory test, if the result is within the normal range the class will be = 0, otherwise if the result is above or below the class will be Abnormal = 1.

Table IV represents the normal ranges of each laboratory.

TABLE IV. LABORATORY RESULTS IN NORMAL RANGES

LAB_TEXT_NAME	Normal Range
AFP	0 -10
Albumin	34 - 54
Alk Phos	44 - 54
ALT	19 - 25
ANA Screen	Negative
AST	8 -33
Bilirubin Total	0 -21
CA 125	0 - 35
CA 19-9	0- 37
Ca Level	8.6 – 10.3
Ceruloplasmin	14 – 40
Cl	96- 106
CMV IgG	1 - 21
CMV IgM	Negative
CO2	20 - 29
Creat	61.9 – 114.9
e-GFR	60 - 90
Ferritin	11 - 336
Globulin	20 - 39
Hct	0.3 - 0.5
Hgb	138 - 172
Hgb g per dL	14 - 18
IgA	0.8 - 3
Iron	10 - 30
Iron Saturation	0.15 – 0.55
K	3.5 – 5.3
MCH	27 - 33
MCHC	33.4 - 35.5
MCV	80 - 95
Mg	0.85 – 1.1
MPV	8.9 - 11.8
Na	135 - 145
NRBC Auto	0 - 0.3
Platelet	150 - 450
PO4	2.3 – 4.7
Pro-Brain Natriuretic Peptide	100 - 400
Protein Total	60 - 83
Quantiferon-TB	Negative
RBC	4.2 - 5.4
RDW	12.2 - 16.1
Sm Muscle Ab	Negative
TIBC	42.96 – 80.55
Total Cell Count (NRBC)	0 - 100
Toxoplas IgG	0 - 44
Toxoplas IgM	Negative
UIBC	21 - 84
Urea	5 - 20
WBC	4.5 - 11

3) Addressing class imbalance: The data set has two categories, failure transplant cases and success transplant cases. There was a significant class imbalance whereby the failure transplant had a significantly lower number of instances compared with the success transplant. To solve this issue, the Minority Oversampling Technique (SMOTE) was used.

4) Reorganized dataset: In the dataset, each row represented a specific laboratory result for one patient at a particular date. To prepare the dataset, the dataset was reorganized. Each row represents all laboratory results for one patient at a specific date.

5) Feature selection: The feature selection stage is predicated upon the principle of diminishing the pool of features to only encompass the most valuable features, thereby augmenting the model result. Researchers employ various techniques to eliminate irrelevant features, to enhance the efficiency and accuracy of the model.

In studies [5], [19], and [16] removed all unnecessary features, and all patient identifications (such as transplant ID, donor ID, and patient ID). Moreover, the study in [20] removed all unnecessary attributes, and kept only 27 relevant attributes from the dataset containing 389 attributes. Also, they removed the data of pediatric patients [21]. Identify the critical features used in statistical tests of the association between each feature and output variable. They exclude only three variables from the model. The study in [11] used Genetic Algorithms to minimize the number of features. They also excluded the feature with a large number of missing values. The dataset encompasses a total of 81 laboratory tests, with the exclusion of laboratories that conducted tests for only 10% of the patients or laboratories that showed normal results in the majority of patients. Consequently, 33 laboratory tests remained in the dataset.

C. Predicting Liver Failure Use DM Algorithm

We have followed two DM approaches to answer the research questions, using classification to predict the failure cases, and to investigate the labs that have highly impacted on liver failure we used the Association rules method.

1) Classification: Classification is a predictive supervised learning technique that classifies the data into predefined classes. It is one of the most widely used DM techniques in medical research [9]. It aims to predict target classes; it could be a binary or multilevel approach. In binary classification, there are two classes to predict, such as patients with "positive "or "negative" diagnoses. On the other hand, in multilevel classification, there are more than two predicted classes.

In this research, we have applied five algorithms: Random Forest – KNN – GaussianNB – SVC – ANN.

2) Association rules: Association Rules Mining (ARM) also known as "Market basket analysis" is an unsupervised learning method used with transactional databases [8]. [17] introduce Association Rules as generating associations or/and correlations among frequent items in large transactional databases.

Let transactional database $\mathcal{T}$ contain a set of items, $\mathcal{I} = i_1, i_2 \dots, i_m$ as binary attributes, each transaction t represented as set of items $i_k \subset \mathcal{I}$ where i_k=1 ,the advance of ASM is to seek for the term: $\mathcal{X} \rightarrow \mathcal{Y}$ where $X, Y \subset \mathcal{I}$ and $X \cap Y = \emptyset$. Apriori algorithm is a well-researched ARM algorithm. The concept of the Apriori Algorithm is using a breath-first strategy to eliminate unnecessary rules that are unsatisfied with minimum support (mins up) and minimum confidence. To implement Apriori Algorithm, 2 steps are performed:

First step: Find all possible candidates C from each itemset in the database, where a large k-itemset is generated from k-1-itemset with satisfied minsup.

Second step: generate all rules from these candidates' itemsets.

Minimum support formula is:

$$Support = \frac{feq(X,Y)}{number\ of\ t}$$

The formula for association rules algorithm set of features,

$$confidence(X|Y) = \frac{feq(XY)}{feq(X)}$$

D. Model Evaluation

The evaluation stage of the algorithms employed holds paramount significance in the data mining process, as it demonstrates the viability of the technique utilized. Various mechanisms are employed to conduct evaluation techniques based on their respective types.

1) Classification evaluation: In the evaluation of classifications, researchers employ a variety of techniques. In our current study, we have utilized the Confusion Matrix method to assess the effectiveness and accuracy of these classifications. The confusion matrix is widely recognized as the most commonly used tool for measuring classification effectiveness [22]. This method proves particularly valuable in quantifying important measurements such as Recall, Precision, and Accuracy.

To find these measurements, the Confusion Matrix technology depends on comparing the prediction results and the real values as shown in Table V:

TABLE V. CONFUSION MATRIX

		Actual Value	
		Positive (1)	***Negative (0)***
Predictive Value	**Positive (1)**	**True Positive**	**False Positive**
	Negative (0)	**False Negative**	**True Negative**

To elucidate the concept of four fields; "True Positive, False Negative, False Positive, and True Negative" in the context of our research, it is important to note that we are dealing with two classes for which we aim to construct a predictive model:

True Positive (TP): The prediction of the state is positive, and the actual outcome is positive.

True Negative (TN): The prediction of the state is Negative, and the actual outcome is Negative.

False Positive (FP): The prediction of the state is positive, and the actual outcome is Negative.

False Negative (FN): The prediction of the state is Negative, and the actual outcome is positive.

To find the values of Recall, Precision, and Accuracy from Confusion Matrix:

$$\text{Recall} = \frac{TP}{TP+FN}$$

$$\text{Precision} = \frac{TP}{TP+FP}$$

Accuracy = how many correct predictions from both classes; Positive and Negative.

2) Association rules evaluation: Association Rules Evaluation is a crucial aspect of data analysis that aims to uncover meaningful relationships and patterns within datasets. This research delves into the intricacies of association rule mining, a popular technique employed in one key aspect of our research that involves measuring the strength of association rules through metrics such as support, confidence, and lift. These metrics allow us to quantify the level of dependency between items or variables in a rule. Additionally, we explore various evaluation measures like conviction and leverage to gain a comprehensive understanding of the associations discovered.

The minimum support formula is:

$$Support = \frac{feq(X,Y)}{number\ of\ t}$$

The formula for association rules algorithm set of features,

$$confidence(X|Y) = \frac{feq(XY)}{feq(X)}$$

E. Tools and Software

The research is based on classification techniques and the hardware used is a MacBook Pro (14-inch, 2021) with M1 pro 3.22 GHz processor 8 Cores, and the memory is 16 GB 2133 MHz LPDDR5. The research used Python software, specifically on a Jupyter Notebook. Python was chosen because it has a large support community and various libraries that provide extensive functionality. One such library used in this research is scikit-learn, which supports different classification methods and is widely accessible. Also, panda's library ‹was used extensively by taking advantage of the functions that supported the preparation phase of the data.

IV. Results

The complexity of the data is quite intricate, as no patient has undergone more than 13 tests in a single day. After eliminating the laboratories that were only utilized for 10% of patients, we were left with 31 labs, which is a huge amount to handle. To address our research inquiries, we employed two data mining approaches. These techniques will examine the outcomes achieved through the classification technique, followed by an assessment of the results obtained using association rules.

A. Association Rules

The dataset provided encompasses all laboratory tests conducted for each patient on specific dates. The data within the table lacks a systematic arrangement. To address this, we have employed the association rule mining technique to uncover relationships between abnormal results. By comparing the outcomes generated from a dataset comprising both failure cases and alive cases, we aim to identify significant associations. Association rule mining holds great significance in transactional datasets as it enables the discovery of intricate relationships among different data elements. Consequently, its application in analyzing patient laboratory results proves highly convenient.

In order to implement Association Rules, the initial phase entailed categorizing each laboratory result with a corresponding class. The class denoted as "Normal" was encoded as 0, which will be traversed by the algorithm. Conversely, the class labeled as "Abnormal" was encoded as 1, which will be interpreted by the algorithm.

Moving on to step two, the dataset consisted of 2366 rows. Out of these, 372 rows were dedicated to failure cases (FC) and 1994 rows to success cases (SC). However, there was an imbalance in the final dataset. To address this issue, the SMOTE algorithm was applied. This resulted in an expanded dataset with a total of 3988 rows. This expansion ensured that both FC and SC had an equal representation of 1994 rows each. For step three, the association rule technique was employed on both the FC and SC datasets using identical parameters. The minimum support was set at 0.4, while the minimum confidence threshold was set at 1. The researcher applied the Apriori algorithm to analyze the data and obtained interesting results. Specifically, the researcher discovered that a total of 1848 rules were generated in instances of success, while 1968 rules were generated in cases of failure. To further investigate these findings, the researcher compared the results and found that most of the rules appeared in both cases of failure and success. Additionally, the support and confidence values for these rules were very close. The analysis revealed that certain rolls, namely AST, RBC, Hgb, 'Bilirubin Total', and 'Platelet', were higher in cases that experienced liver transplant failure within the first year. Furthermore, height was also found to be associated with AST, RBC, ALT, and 'Bilirubin Total', as indicated in Table VI.

TABLE VI. Unique Results Shown with FC

Rules	***support***	***confidence***
'AST' ^ 'RBC' ^ 'Hgb'^ 'Bilirubin Total'^ 'Platelet'	0.46	0.95
'AST' ^ 'RBC' ^ ' ALT'^ 'Bilirubin Total'	0.40	0.91

It was deemed necessary to seek the expertise of a specialist doctor at KFSH&RC for their evaluation. The esteemed specialist doctor duly reviewed the findings and concurred that this discovery holds a significant interest.

B. Classification

The study aimed to investigate the efficacy of using DM in identifying the most vulnerable cases of LTF based on periodic laboratory results. To achieve this objective, a comprehensive analysis was conducted using a commonly employed algorithm. The primary focus was to assess the potential of DM in accurately pinpointing individuals at high risk for LTF, solely relying on their lab test outcomes.

After preprocessing and organizing the data, we proceeded to apply various algorithms including Random Forest, K-Nearest Neighbors (KNN), Gaussian Naive Bayes (NB), Support Vector Classifier (SVC), and MLPClassifier on the dataset. The outcomes revealed that Random Forest exhibited the highest accuracy among all algorithms. It achieved an accuracy rate of 85 percent. Following closely behind, KNN demonstrated a respectable accuracy of 81 percent, while MLP Classifier achieved an accuracy of 78 percent. On the other hand, SVC and Genesis NB yielded lower accuracies with rates of 60 percent and 54 percent respectively. Table VII shows the Performance Evaluation for all five algorithms.

TABLE VII. PERFORMANCE EVALUATION FOR CLASSIFICATIONS

Classifier	Precision	Recall	Precision	Recall	Accuracy
	Success Case		Failure Case		
Random Forest	86	84	84	86	85
KNN	83	80	79	82	81
GaussianNB	80	73	77	83	78
SVC	62	53	58	66	60
ANN	60	35	52	75	54

The results were presented to a specialist doctor who agreed with the reality of some of the results.

V. CONCLUSION

Data mining technologies hold significant promise in healthcare, especially in predicting medical outcomes and identifying risks. This study, in collaboration with the Organ Transplant Center of Excellence and the Center of Genomic Medicine at KFSH&RC, demonstrates the predictive power of data mining in liver transplant outcomes. Using patient data from 2002 to 2018, two data mining techniques, classification, and association rules, were applied. Among five algorithms tested, Random Forest proved most effective, achieving an 85% accuracy rate in predicting liver transplant failure. The association rules technique, using a support value of 0.4 and a confidence value of 1, identified elevated levels of 'AST', 'RBC', 'Hgb', 'Bilirubin Total', and 'Platelet' as significant indicators of transplant failure. These findings were validated by the hospital's Adult Transplant Hepatology consultants, who stressed the need for further research incorporating larger sample sizes and additional variables such as age, gender, body mass, and liver failure causes. Expanding this study to other organs and hospitals across Saudi Arabia could enhance predictive accuracy and clinical utility.

The influence of data mining technologies is particularly evident in contemporary technological revolutions within the realms of marketing, industry, finance, and education. However, in the domain of health research, investigations are still centered on exploring the potential benefits of data technologies to aid physicians in predicting diverse diseases and detecting potential hazards to patients' lives at an early stage, thereby presenting a significant challenge to medical practitioners. According to the results obtained, depending on patients' laboratory data only to predict the failure of liver transplant is not enough, so further research is recommended to add a larger sample size of patients including age, gender, body mass, and the cause of liver failure to increase the accuracy of the system and obtain high credible results. The study can also be applied to study failure in transplanting other organs and expand research to all hospitals and centers within Saudi Arabia.

REFERENCES

[1] Chowdhary, K. R. (2020). Fundamentals of Artificial Intelligence. Springer India.

[2] ȚĂRANU, I. (2015). Data mining in healthcare: decision making and precision. *Database Systems Journal*, *6*(4).

[3] Bolondi, G., Mocchegiani, F., Montalti, R., Nicolini, D., Vivarelli, M., & De Pietri, L. (2016). Predictive factors of short-term outcome after liver transplantation: a review. World journal of gastroenterology, 22(26), 5936.

[4] Koyuncugil, A. S., & Ozgulbas, N. (2010). Donor research and matching system based on data mining in organ transplantation. Journal of Medical Systems, 34(3), 251-259.

[5] Atallah, D. M., Badawy, M., El-Sayed, A., & Ghoneim, M. A. (2019). Predicting kidney transplantation outcome based on hybrid feature selection and KNN classifier. Multimedia Tools and Applications, 78(14), 20383-20407.

[6] Han, J., Pei, J., & Tong, H. (2022). Data Mining Concept and Techniques (3rd ed.). United States, Katey Birtcher.

[7] Al Sebaye ,Hamoudi, W. (2017, September 22). Liver transplantation in the Kingdom of Saudi Arabia. Liver Transplantation, 23(10), 1312±1317. https://doi.org/10.1002/lt.24803

[8] Ordonez, C., Omiecinski, E., De Braal, L., Santana, C. A., Ezquerra, N., Taboada, J. A., & Garcia, E. V. (2001, November). Mining constrained association rules to predict heart disease. In Proceedings 2001 IEEE international conference on data mining (pp. 433-440). IEEE.

[9] Shouval, R., Labopin, M., Unger, R., Giebel, S., Ciceri, F., Schmid, C., ... & Nagler, A. (2016). Prediction of hematopoietic stem cell transplantation related mortality-lessons learned from the in-silico approach: a European Society for Blood and Marrow Transplantation Acute. Leukemia Working Party data mining study. PLoS One, 11(3), e0150637.

[10] Decruyenaere, A., Decruyenaere, P., Peeters, P., Vermassen, F., Dhaene, T., & Couckuyt,I. (2015). Prediction of delayed graft function after kidney transplantation: comparison between logistic regression and machine learning methods. BMC medical informatics and decision making, 15, 1-10.

[11] Oztekin, A., Al-Ebbini, L., Sevkli, Z., & Delen, D. (2018). A decision analytic approach to predicting quality of life for lung transplant recipients: A hybrid genetic algorithm-based methodology. European Journal of Operational Research, 266(2), 639-651.

[12] Shaheen, F. A. (2016). Organ transplantation in Saudi Arabia. Transplantation, 100(7), 1387-1389.

[13] Shahmoradi, L., Langarizadeh, M., Pourmand, G., & Borhani, A. (2016). Comparing three data mining methods to predict kidney transplant survival. Acta informatica medica, 24(5), 322.

[14] ABIDI, S. R. (2021). Analyzing Association Rules for Graft Failure Following Deceased and Live Donor Kidney Transplantation. Public Health and Informatics: Proceedings of MIE 2021, 281, 188.

[15] Lau, L., Kankanige, Y., Rubinstein, B., Jones, R., Christophi, C., Muralidharan, V., & Bailey, J. (2017). Machine-learning algorithms predict graft failure after liver transplantation. Transplantation, 101(4), e125.

[16] Naqvi, S. A. A., Tennankore, K., Vinson, A., Roy, P. C., & Abidi, S. S. R. (2021). Predicting kidney graft survival using machine learning methods: prediction model development and feature significance analysis study. Journal of Medical Internet Research, 23(8), e26843.

[17] Agarwal, R., & Srikant, R. (1994, September). Fast algorithms for mining association rules. In Proc. of the 20th VLDB Conference (Vol. 487, p. 499). https://towardsdatascience.com/meet-artificial-neural-networks-ae5939b1dd3a

[18] Olson, D. L., & Delen, D. (2008). Advanced data mining techniques. Springer Science & Business Media.

[19] Dag, A., Oztekin, A., Yucel, A., Bulur, S., & Megahed, F. M. (2017). Predicting heart transplantation outcomes through data analytics. Decision Support Systems, 94, 42-52.

[20] Raji, C. G., & Chandra, S. V. (2017). Long-term forecasting the survival in liver transplantation using multilayer perceptron networks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 47(8), 2318-2329.

[21] Kazemi, A., Kazemi, K., Sami, A., & Sharifian, R. (2019). Identifying factors that affect patient survival after orthotopic liver transplant using machine-learning techniques. Exp Clin Transplant, 17(6), 775-783.

[22] Sarang, N., 2018. Understanding Confusion Matrix [WWW Document]. Medium. URL https://medium.com/towards-data-science/understanding-confusion-matrix-a9ad42dcfd62

Synthesizing Realistic Knee MRI Images: A VAE-GAN Approach for Enhanced Medical Data Augmentation

Revathi S A[1], B Sathish Babu[2]
Dept. of Computer Science, RV College of Engineering, Bangalore, India[1]
Dept. of AI&ML, RV College of Engineering, Bangalore, India[2]

***Abstract*—This study presents a novel approach for synthesizing knee MRI images by combining Variational Autoencoders (VAEs) and Generative Adversarial Networks (GANs). By leveraging the strengths of VAEs for efficient latent space representation and GANs for their advanced image generation capabilities, we introduce a VAE-GAN hybrid model tailored specifically for medical imaging applications. This technique not only improves the realism of synthesized knee MRI images but also enriches training datasets, ultimately improving the outcome of machine learning models. We demonstrate significant improvements in synthetic image quality through a carefully designed architecture, which includes custom loss functions that strike a balance between reconstruction accuracy and generative quality. These improvements are validated using quantitative metrics, achieving a Mean Squared Error (MSE) of 0.0914 and a Fréchet Inception Distance (FID) of 1.4873. This work lays the groundwork for novel research guidelines in biomedical image study, providing a scalable solution to overcome dataset limitations while maintaining privacy standards, and pavement of reliable diagnostic tools.**

Keywords*—Custom loss function; decoder; discriminator; GAN; latent space; VAE

I. Introduction

Deep learning has renovated medical imaging, improving diagnostic accuracy, treatment preparation, and patient monitoring. Despite its potential, the field faces significant challenges, particularly in musculoskeletal imaging, where limited access to diverse, high-quality datasets impedes progress. This is exacerbated by privacy concerns and the cost-intensive nature of data collection and annotation. To address these barriers, this study proposes a novel VAE-GAN framework for synthesizing realistic and diverse knee MRI images. By integrating the latent space representation capabilities of Variational Autoencoders (VAEs) with the generative strength of Generative Adversarial Networks (GANs), the proposed method aims to overcome the shortcomings of existing augmentation techniques while maintaining clinical relevance.

The VAE-GAN framework balances the diversity of VAEs with the sharpness and realism provided by GANs. Specifically, the VAE's latent space ensures continuity, making it suitable for generating diverse samples, while the GAN component enhances image fidelity, addressing the critical need for high-quality training datasets in medical imaging. This synergy enables the generation of realistic knee MRI images that reflect the variations needed for machine learning model training.

However, existing generative methods present restrictions that make them less suitable for this task:

1) Standalone GANs are prone to mode collapse, which restricts the variety of generated images and reduces their applicability in representing diverse medical conditions.

2) VAEs often produce blurry outputs due to their reliance on reconstruction loss functions, which prioritize structural accuracy over fine details.

3) Other generative models, such as Diffusion Models, require significantly more computational resources, making them unrealistic for medical imaging applications with restricted data.

By addressing these limitations, the proposed VAE-GAN framework emerges as an effective solution to the problem of data scarcity in knee MRI imaging, paving the way for better augmentation techniques that enhance the performance of diagnostic tools.

The limited availability of high-quality, diverse, and privacy-compliant medical imaging datasets significantly hampers the progress of robust and generalizable deep learning techniques for diagnostic applications. Existing methods for data augmentation and synthesis often fail to achieve the required balance of realism, diversity, and fidelity, limiting their effectiveness in medical imaging contexts.

The research explores how a hybrid generative model can effectively synthesize realistic and diverse knee MRI images to address the problem of data scarcity in medical imaging. It investigates the optimal architectural and loss function designs needed to stabilize image quality with reconstruction accuracy in the synthesized data. Furthermore, the study examines how the proposed VAE-GAN framework compares to existing generative methods in terms of quality metrics and clinical applicability.

The objectives of this research are to implement a VAE-GAN-based framework capable of producing realistic and diverse knee MRI images and to design a custom loss function that integrates reconstruction loss, KL divergence, and adversarial loss to achieve high-fidelity image generation. Additionally, the study aims to validate the model's performance

using quantitative metrics such as Mean Squared Error (MSE) and Fréchet Inception Distance (FID), as well as through qualitative assessments of the synthetic images' visual quality.

Magnetic Resonance Imaging (MRI), a critical tool for assessing musculoskeletal disorders, especially knee-related conditions, is a domain where deep learning can substantially enhance diagnostic accuracy and patient outcomes. However, the accomplishment of deep learning techniques in biomedical imaging is heavily dependent on the accessibility and image resolution of the datasets used. High-quality medical image data is often scarce and challenging to obtain due to patient privacy concerns. Furthermore, the processes of data collection and annotation are both costly and time-consuming, frequently resulting in datasets that lack the necessary diversity and volume to train robust and generalizable machine learning models. In knee MRI data, specific challenges include variations in pathology presentation and imaging protocols, complicating the training process further [1].

To address these challenges, the proposed VAE-GAN (Variational Autoencoder-Generative Adversarial Network) framework combines the robust data encoding capabilities of VAEs with the powerful image generation capabilities of GANs. VAEs excel at compressing data into a latent space, enabling the generation of new data instances, but sometimes produce outputs that lack the sharpness and detail characteristic of high-quality MRI scans [2]. Conversely, GANs generate sharp, high-definition images through adversarial training but face challenges such as training instability and mode collapse—a condition where the variety of produced images is insufficient [3]. By integrating these models, the VAE-GAN framework achieves a balance between realistic detail and diversity in synthetic knee MRI images.

The introduction should also include a section listing the reasons for choosing the proposed VAE-GAN method, detailing why it is particularly appropriate for addressing the challenges outlined in the study. Additionally, it would be advantageous to point out which limitations of existing methods make them less suitable for this problem. Including such a rationale would provide greater clarity on the motivations behind the selected approach.

This paper explores the architecture and functionality of the VAE-GAN model, focusing on its application for synthesizing knee MRI images. A detailed examination of the encoder, decoder/generator, and discriminator is provided, along with the custom loss function that optimizes image reconstruction accuracy and resolution. Experimental results validate the model's effectiveness in creating authentic and diverse synthetic knee MRI images, demonstrating its potential to enrich medical imaging datasets and enhance the performance of machine learning models used in medical diagnostics.

Additionally, this study carefully addresses the ethical concerns associated with deploying generative methods for data augmentation in healthcare. The input images used for model training were thoroughly anonymized, and all procedures adhered strictly to ethical standards, ensuring patient confidentiality at every stage.

A. Paper Structure

The remainder of the paper is organized as follows: Section II reviews related work in biomedical imaging and generative modeling. Section III presents the methodology, including the proposed VAE-GAN architecture and training procedures. Section IV discusses the experimental setup, results, and evaluation. Section V highlights limitations, ethical considerations, and future work. Finally, Section VI concludes the study and summarizes its contributions to the field.

II. Literature Review

Bio Medical imaging plays a crucial part in current healthcare by facilitating the diagnosis and management of various health conditions. However, challenges such as limited data availability and concerns over patient privacy hinder the development of robust machine-learning techniques for image analysis. Variational Autoencoders (VAEs) and Generative Adversarial Networks (GANs) have emerged as powerful generative models, offering solutions to these challenges. This section explores the implementation of VAE-GAN models in medical imaging, highlighting their methods, effectiveness, and potential drawbacks.

VAEs and GANs are distinct but complementary approaches in generative modelling. VAEs consist of an encoder-decoder structure, where the encoder compresses medical images into a latent space, retaining essential features. The decoder reconstructs the image from this compressed representation, with a tailored loss function ensuring that the output closely matches the original and that the latent space accurately reflects key medical attributes [13]. Conversely, GANs use a generator-discriminator framework. The generator generates images that captures those in the training set, whereas the discriminator evaluates their authenticity. This adversarial interaction drives the generator to create realistic images [3].

The synergy of VAE-GAN techniques lies in their capability to combine VAE's efficient latent space encoding with GAN's image refinement capabilities. The VAE encodes medical images into a meaningful latent space, and the GAN uses this encoding to generate realistic images, preserving essential characteristics while enhancing overall quality. VAE-GAN models have shown remarkable versatility, particularly in data augmentation. They can produce synthetic images that are almost indistinguishable from real ones, expanding the range of training datasets and improving machine learning models' performance in tasks namely image segmentation and classification. These models also excel in denoising, removing extraneous noise while preserving critical structures, making them perfect for applications like tumor detection and disease progression monitoring [3]. Additionally, VAE-GANs can generate disease-specific images, offering valuable resources for medical training and refining diagnostic systems.

Despite their potential, VAE-GAN models have some drawbacks. Their complex architecture requires substantial computational resources and careful hyperparameter tuning for optimal performance. One common issue is mode collapse, where the variety of generated images diminishes, limiting the model's applicability across diverse medical scenarios [3]. The latent space's interpretability in VAEs remains a challenge,

potentially obscuring insights into how model decisions are made [4]. Additionally, biases in training datasets can propagate through VAE-GAN models, leading to biased outputs and skewed diagnostic results [5]. While VAE-GAN models represent significant developments in medical image processing, addressing these limitations is critical for their ethical and practical application in healthcare settings.

Recent advancements in generative models, particularly GANs and Diffusion Models (DMs), have expanded the scope of medical image synthesis. GANs have demonstrated proficiency in creating realistic images, but they face tests such as training unpredictability and mode breakdown [6, 7]. Conversely, VAEs produce a larger variety of outputs and are fewer prone to mode collapse, though the images they generate sometimes lack sharpness due to smoothing tendencies in their loss functions [8]. Diffusion Models (DMs) offer a promising solution by producing original and diverse outputs, though their adoption in clinical settings is hindered by high computational demands and extended processing times [9, 10]. This review explores the evolving landscape of these technologies, aiming to balance quality, speed, and diversity in medical image synthesis [11].

GANs have become essential in advancing realistic image synthesis, particularly for enhancing medical imaging datasets. While GANs are adept at producing images that thoroughly resemble actual medical data, they can still suffer from mode collapse, leading to a limited variety of generated images. To address this, more advanced versions of GANs, such as Wasserstein GAN (WGAN) [12] and Conditional GAN (CGAN) [13], have been developed, significantly improving image quality and offering greater control over image generation. Deep generative models are revolutionizing biomedical imaging by improving diagnostic and treatment processes. VAEs are praised for their straightforward training and ability to capture complex data distributions. This ability makes them irreplaceable in medical imaging, where a rich representation of data is crucial. However, the occasional blurriness of VAE-generated images has led to the advancement of hybrid models like VAE-GANs, which combine the encoding power of VAEs with the image refinement abilities of GANs, resulting in clearer and more diverse outputs [18].

Diffusion Models (DMs) represent a breakthrough in generative modelling, excelling in capturing detailed, high-dimensional data distributions typically found in medical images. Their ability to replicate intricate features suggests they may outperform VAEs and GANs in relationships with realism and quality [19]. However, the high computational demands and lengthy processing times required by DMs limit their practicality, especially in real-time applications. Innovations such as Progressive Distillation [20] and the Fast Diffusion Probabilistic Model (FastDPM) [21] aim to optimize the sampling process while maintaining high-quality outputs. The Denoising Diffusion Implicit Model (DDIM) [22] balances speed with output fidelity, underscoring the importance of refining generative models.

This review categorizes deep generative models into three main types: GANs, VAEs, and DMs. GANs have made a significant impact on medical image augmentation, with iterations such as Wasserstein GAN (WGAN) [14] and Deep Convolutional GAN (DCGAN) [16] proving essential in generating realistic 2D MRI sequences. Studies by Han et al. [23] validate WGAN's superior performance in producing images that are indistinguishable from original medical scans. Likewise, Progressive Growing of GANs (PGGAN) [17], when merged with traditional data augmentation methods, has directed to improved classification algorithm performance. Conditional GANs [15] have been especially effective in generating targeted, realistic synthetic images, as demonstrated by Frid-Adar et al. [24] and Guibas et al. [25].

VAEs also show a critical role in diversifying medical imaging datasets. Research by Zhuang et al. [26] highlights Conditional VAEs (CVAEs) and Conditional WGANs' capability to produce high-quality brain images, enhancing classification model accuracy. The outline of Independently Conditional VAE (ICVAE) by Pesteie et al. [28] marks a noteworthy development in VAE technology, improving classification and segmentation tasks through increased diversity. Recent studies recognize the probability of Diffusion Models in generating high-resolution 3D MRI images. Research by Pinaya et al. [27] emphasizes DMs' superiority in producing authentic MRI samples. Moreover, the brain SPADE model introduced by Fernandez et al. [29] integrates DMs with VAE-GANs to create labeled MRI images, crucial for training segmentation models. Furthermore, explorations by Lyu and Wang [30] into DMs' image translation capabilities show that they can convert MRI to CT scans with greater accuracy than outdated methods, demonstrating the significant impact of these models on medical imaging.

In conclusion, deep generative methods, namely GANs, VAEs, and DMs, are transforming medical imaging. These methods are pivotal in tackling issues like data scarcity and augmenting datasets for improved diagnostic accuracy. Their ability to synthesize high-quality images, translate between imaging modalities, and enhance training datasets underscores their potential to advance diagnostic practices and medical research. Future developments promise to further expand their efficacy, making them invaluable tools in healthcare.

III. METHODOLOGY

The methodology deployed for constructing and training a VAE-GAN model for synthesizing knee MRI images is composed of several intricate stages, from initial data preprocessing to the sophisticated dynamics of model training. This model capitalizes on the compressive data encoding capabilities of Variational Autoencoders (VAEs) and the image generation prowess of Generative Adversarial Networks (GANs). Herein, we elucidate the encoder's latent space utilization for image synthesis, the beta hyperparameter's role in the VAE loss function, the chosen architecture's pertinence to knee MRI imaging, the enhanced model diagrams for augmented clarity, and the tailoring of the custom loss function to medical imaging.

The VAE-GAN framework was selected because it combines the strengths of two advanced generative models. VAEs excel at compressing data into a continuous latent space, ensuring diversity in synthesized outputs, while GANs are well-known for generating sharp and realistic images through

adversarial training. By integrating these models, the VAE-GAN framework addresses limitations of standalone methods:

1) VAEs sometimes produce blurry outputs due to their reconstruction-focused loss functions.

2) GANs are prone to training instability and mode collapse, reducing output diversity.

This hybrid approach effectively balances the sharpness and realism of GAN-generated images with the structural fidelity and diversity provided by VAEs, making it particularly suitable for the complex requirements of knee MRI image synthesis. Fig. 1 shows model architecture flowchart.

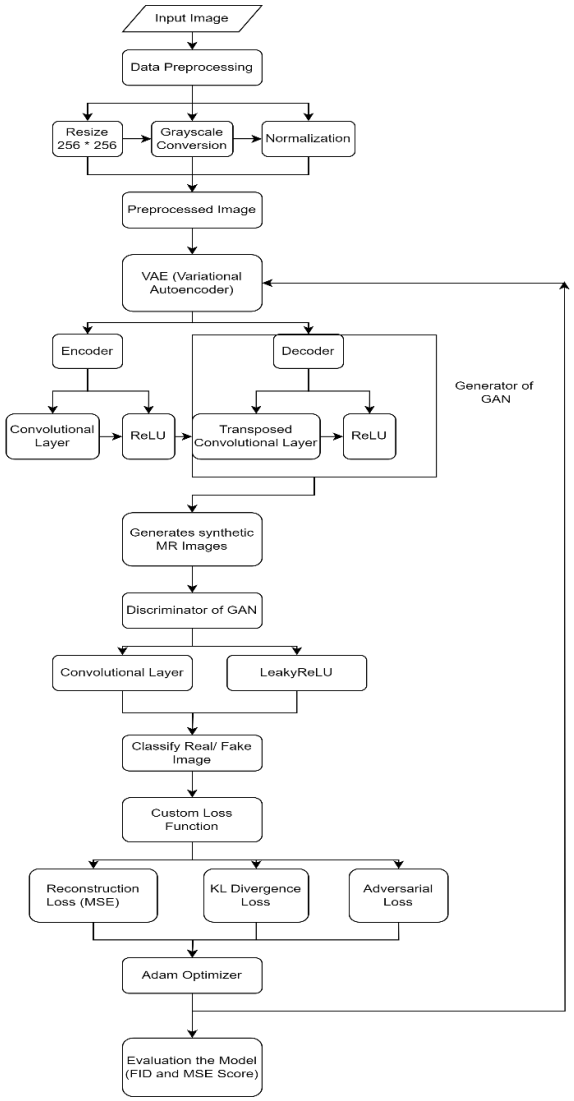


Fig. 1. Detailed model architecture flowchart.

A. Data Collection and Sample Selection

The dataset used in this training was sourced from the Osteoarthritis Initiative (OAI), an openly accessible repository of knee MRI data. The images were selected based on the following criteria:

1) Availability of high-resolution knee MRIs.

2) Representation of four severity levels of osteoarthritis: normal, mild, moderate, and severe.

3) Ensuring diversity across patient demographics, imaging protocols, and pathology presentations.

From the OAI dataset, 150 knee MRI images were selected, including: 10 normal images, 50 mild images, 65 moderate images, 34 severe images.

Efforts were made to ensure that the dataset represented a wide spectrum of knee osteoarthritis conditions, thus enhancing the generalizability of the model.

B. Data Preprocessing

1) Initial data input: The dataset consists of 150 knee MRI images, each resized to 256x256 pixels. These images correspond to four distinct severity levels of knee osteoarthritis (OA): normal, mild, moderate, and severe. This provides an adequate range for capturing pathological variations across OA stages.

a) Grayscale conversion: Knee MRIs were initially in color, but for this task, the images were converted into grayscale to simplify the data. Grayscale imaging emphasizes intensity values, which are critical in medical imaging to capture structural details. This conversion reduces the number of channels from 3 to 1, making computations more efficient without losing the essential information.

b) Normalization: Min-max normalization was applied to scale pixel values to a [0, 1] range. This normalization aids in stabilizing numerical computation during model training by ensuring consistent data scales, which speeds up convergence and reduces training instability.

c) Resizing images: Each image was resized to a fixed 256x256 resolution using bicubic interpolation. This method preserves image quality while ensuring uniformity in input data dimensions, which is necessary for training convolutional neural networks (CNNs) and other deep models (see Fig. 2).

Fig. 2. Input MRI images of knee OA.

C. Encoder and Decoder Model

After these steps, the data is cleaned, standardized, and ready for input into the VAE-GAN model, providing an optimal starting point for further processing and generation.

1) Variational Autoencoder (VAE): The encoder compresses the input MRI images into a latent space representation. It comprises of a sequence of convolutional layers followed by ReLU activations. Key architectural choices include:

a) Convolutional layers: Four convolutional layers are used, with increasing filter sizes (32, 64, 128, and 256) at each layer, designed to progressively capture image features from basic edges to complex patterns.

b) Filter size: The kernel sizes used were 3x3 for the initial layers, transitioning to 2x2 in deeper layers to down sample spatial dimensions efficiently.

c) ReLU activation: Applied after each convolutional layer to introduce non-linearity, enabling the model to learn more complex representations.

d) Batch normalization: Introduced after each convolutional block to stabilize and accelerate training, preventing vanishing/exploding gradient problems.

e) Latent space representation: The final dense layer of the encoder outputs two variables, mean (μ) and variance (σ^2), representing the latent distribution. The dimensionality of the latent space was set to 128 dimensions, balancing between representational capacity and computational efficiency.

2) VAE Decoder / GAN Generator: The decoder (also serving as the GAN generator) reconstructs images from the latent space representation:

a) Transposed convolutional layers: Four layers of transposed convolutions are applied to up sample the image back to its original size (256x256). This "unpooling" mechanism helps restore the resolution lost during encoding.

b) Activation functions: ReLU activation is applied throughout, except in the final layer, where a sigmoid activation is used to ensure pixel values remain between [0,1].

c) Batch normalization: Continues to be applied in the decoder to avoid overfitting and stabilize the gradient flow.

3) Generative Adversarial Network (GAN) discriminator: The discriminator serves to distinguish between actual and synthetic MRI images. It follows a convolutional neural network (CNN) architecture:

a) Convolutional layers: Five convolutional layers, each using LeakyReLU activation, which allows a small gradient flow when inputs are negative, addressing the vanishing gradient problem typical in GAN training.

b) Dropout: A dropout layer is introduced with a rate of 0.3 to prevent overfitting, particularly crucial when training with relatively small medical datasets.

c) Sigmoid activation: The output layer uses sigmoid activation for binary classification (real vs. synthetic).

D. Custom Loss Function

The loss function used in the VAE-GAN integrates three essential components:

1) Reconstruction loss: This is the mean squared error (MSE) between the actual and reconstructed images. It guarantees that the VAE's decoder produces images that closely match the input MRI scans.

2) KL Divergence loss: This term penalizes the deviation between the latent distribution q(z|x) and the prior distribution p(z), ensuring that the latent space aligns with a standard normal distribution.

3) Adversarial loss: Derived from the GAN framework, this loss encourages the generator to produce realistic images that can "fool" the discriminator. It is calculated as −log(D(G(z))), where G(z) is the produced image and DDD is the discriminator output.

The custom loss function is a pivotal component of the VAE-GAN model, integrating the following elements to enhance performance:

$$\text{Reconstruction Loss: } L_{recon} = \|x - \hat{x}\|^2 \quad (1)$$

$$\text{KL Divergence Loss: } L_{KL} = D_{KL}(q(z|x) \,||\, p(z)) \quad (2)$$

$$\text{Adversarial Loss: } L_{adv} = -log(D(G(z))) \quad (3)$$

The total loss function is a weighted sum of these components:

$$L_{VAE-GAN} = L_{recon} + \beta L_{KL} + L_{adv} \quad (4)$$

where β is a tunable hyperparameter that balances the weight of the KL divergence term, set to 0.1 in this study. This formulation ensures a balance between reconstruction accuracy and the generation of diverse, high-quality images.

L_{recon} includes a weighted sum of MSE and SSIM, reflecting pixel-wise accuracy and structural fidelity.

The formula ensures that the VAE-GAN model generates images with high fidelity and maintains a balance between the accuracy of the reconstructions and the diversity of the produced images. This comprehensive explanation provides a clearer insight into how each part of the model contributes to its overall effectiveness, precisely designed to expand the diagnostic value of knee MRI images.

E. Training Procedure

1) Optimizer: Adam optimizer was used together for the generator and discriminator, chosen for its adaptive learning rate capabilities, which is critical for stabilizing the GAN training process. The learning rate was set at 0.0002, and the β1\beta_1β1 hyperparameter was set to 0.5 to ensure a smooth training trajectory.

2) Batch Size: A batch size of 32 was used, optimized for the size of the dataset and the available computational resources.

3) Epochs: Training was conducted for four full epochs due to the size of the dataset. Future work may focus on increasing

the dataset size and extending the number of epochs to improve model generalization.

F. Training Procedure

Training involved alternating updates between the VAE and GAN components. The discriminator is updated using both real and synthetic images, while the encoder-decoder (VAE) attempts to minimize reconstruction loss and "fool" the discriminator:

1) Dual-update mechanism: For each batch, the discriminator is updated to differentiate real from fake images, followed by updates to the encoder-decoder to generate realistic images.

2) Callbacks: Early stopping and learning rate reduction on plateau were employed to optimize the training method and prevent overfitting.

IV. Results

This study evaluated the efficacy of a Variational Autoencoder-Generative Adversarial Network (VAE-GAN) in generating synthetic knee MRI images, focusing on varying stages of osteoarthritis, ranging from normal to severe. The primary objective was to evaluate the VAE-GAN's ability to generate realistic synthetic images suitable for training machine learning models while addressing the limitations posed by insufficient medical imaging datasets.

Validation measures are essential in demonstrating the efficacy of the developed model. Metrics like Mean Squared Error (MSE) and Fréchet Inception Distance (FID) provide quantitative evidence of the model's performance. These metrics quantitatively evaluate the quality of the synthetic images in terms of fidelity and diversity, benchmark the model's performance against established standards, and identify specific strengths and weaknesses of the approach, allowing for targeted improvements. For instance, in medical imaging, a low FID score not only indicates perceptual similarity but also highlights the applicability of the generated images for diagnostic purposes. Including other domain-specific metrics, such as Structural Similarity Index (SSIM), or expert evaluations can further validate the clinical relevance of the work.

The model achieved an MSE score of 0.0914, reflecting a high degree of pixel-wise accuracy between the synthetic and ground-truth MRI images. However, while MSE captures the overall pixel similarity, it does not necessarily reflect perceptual realism, which is crucial for medical applications. This is where the FID score of 1.4873 becomes relevant, indicating that although the images are visually similar to real knee MRIs, further improvement is necessary, particularly in rendering finer anatomical details and reducing any artifacts that may compromise diagnostic quality.

A. Comparison to Existing Methods

The achieved FID score demonstrates significant promise when compared to existing generative techniques for medical imaging. Previous studies using standalone GANs for medical image generation have reported FID scores ranging between 5 and 10, underscoring the superiority of the hybrid VAE-GAN approach applied in this study. This improved performance likely stems from the combined strengths of VAEs, which effectively capture the latent structure of complex medical data, and GANs, which enhance the sharpness and overall quality of the produced images.

By highlighting the restrictions of existing methods, such as mode collapse in GANs or the blurry outputs from VAEs, this study positions the VAE-GAN framework as a balanced solution that addresses these challenges while improving perceptual realism and diversity. Furthermore, the proposed approach demonstrates computational efficiency compared to Diffusion Models, which require significantly higher resources.

B. Impact of Dataset Size

The size and diversity of the training dataset critically influence the performance of generative methods. In this study, the VAE-GAN was trained on a relatively small dataset consisting of 150 knee MRI images, which may have limited the model's ability to generalize effectively across the full spectrum of osteoarthritis conditions. Additionally, batch size constraints resulted in the final epoch processing only 22 images, further reducing the data exposure during training. Expanding the dataset size and increasing image diversity are anticipated to significantly lower the FID score, improving both the quality and variability of the produced images.

C. Visual Quality of Synthetic Images

In count to the quantitative metrics, a qualitative assessment of the synthetic knee MRI images offers further validation of the model's effectiveness. The model demonstrated its ability to accurately replicate the structural details of the knee in the coronal plane, particularly capturing the cartilage and bone structures across different stages of osteoarthritis. However, certain generated images lacked the fine-grained textural details commonly observed in real MRIs, especially in severe cases of osteoarthritis. This suggests that while the model is effective, further architectural refinements are necessary to progress the anatomical accuracy and clinical utility of the synthetic images.

D. Interpretation of Results in Medical Imaging Context

In medical imaging, particularly for knee osteoarthritis, the outcome validates the VAE-GAN's potential for data augmentation, which is critical for training more robust and precise machine learning methods. The generated images can be used to report the scarcity of medical imaging data, which often hinders the progress of effective diagnostic tools. However, while the results show promise, additional improvements in capturing fine anatomical details are required for the model to be clinically viable. Ensuring the fidelity of essential structures, such as the meniscus and cartilage, is crucial for using this model in diagnostic settings.

E. Limitations and Next Steps

The relatively high FID score highlights areas for further refinement, particularly in relation to the small dataset size used for training. Future work will focus on increasing the dataset size and incorporating advanced post-processing techniques to further reduce the FID score and enhance the visual quality of the synthetic images. Additionally, incorporating domain-specific metrics namely the Structural Similarity Index (SSIM) and seeking expert evaluations from radiologists will provide a

more comprehensive assessment of the model's clinical applicability and guarantee that the produced images meet the standards necessary for real-world medical diagnostics.

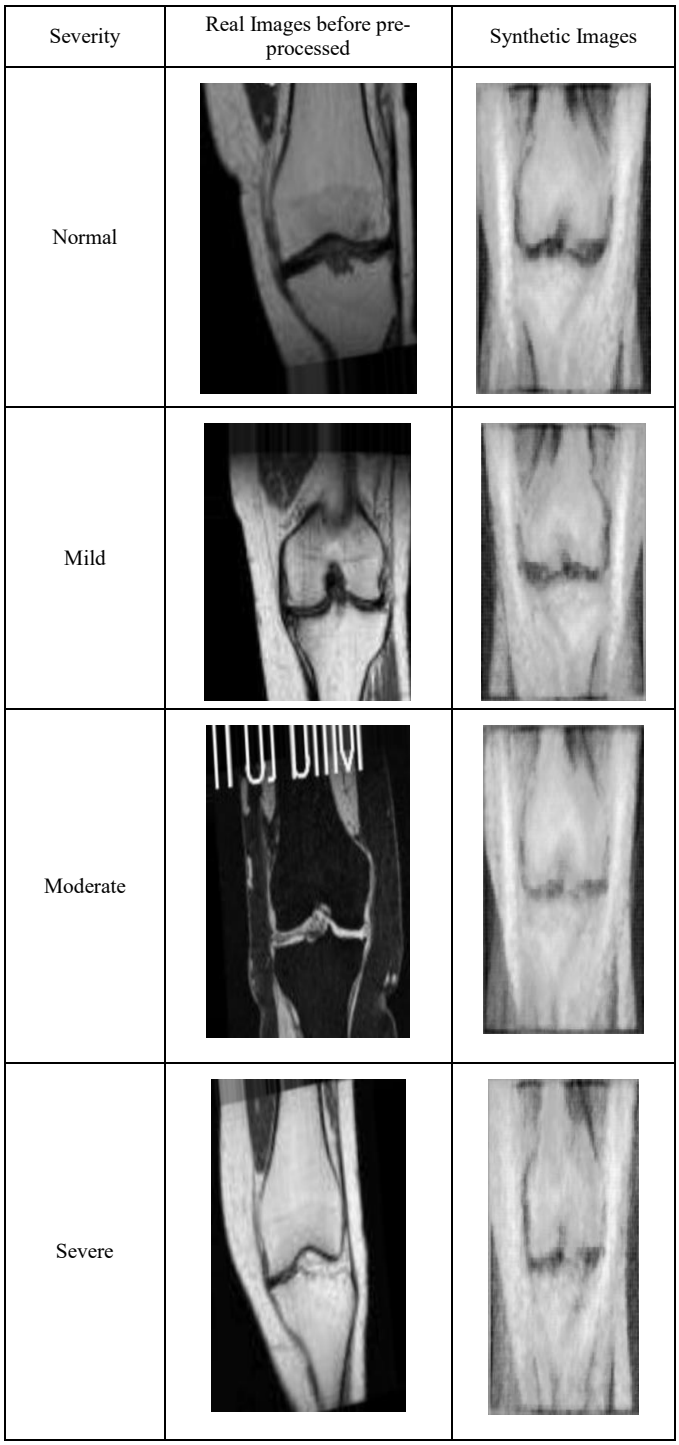


Fig. 3. Illustrates the examples of the synthetic knee OA images produced by the VAE-GAN Model, highlighting its capacity to replicate a wide spectrum of knee OA severities.

The performance of the VAE-GAN model was analysed across different severity levels of osteoarthritis to understand its effectiveness in synthesizing knee MRI images (see Fig. 3). For normal cases, the model achieved an MSE of 0.087 and an FID of 1.401, indicating high accuracy and perceptual realism for structurally simple images. As the severity increased to mild cases, the MSE slightly rose to 0.092, with a corresponding FID of 1.452, reflecting the model's ability to maintain realism despite the added complexity of pathological features. In moderate cases, the MSE increased further to 0.096, and the FID reached 1.523, indicating a gradual decline in performance as the structural complexity of the images grew. For severe cases, where the variations in cartilage and bone structure were most pronounced, the MSE reached 0.101, and the FID increased to 1.573, suggesting that the model performs best on less severe cases with simpler anatomical structures but struggles with fine-grained details in advanced osteoarthritis stages. Emphasizing the significance of validation measures, such as MSE and FID, and conducting thorough comparisons with existing related work is paramount to positioning this study within the broader context of medical image synthesis research, ensuring a comprehensive assessment of the model's effectiveness and limitations.

V. Conclusion

The VAE-GAN model exhibited strong potential in generating synthetic knee MRI images, with initial results showing promising visual accuracy, as reflected by the Mean Squared Error (MSE) metric. However, further refinement is required to improve the model's capability to capture complicated anatomical details. One concern identified during evaluation was the relatively high Fréchet Inception Distance (FID) score, indicating potential problems connected to preprocessing, feature extraction, or calculation errors. This underscores the significance of thorough validation and optimization of generative methods in medical imaging applications.

This research contributes to the expanding field of generative modelling for medical imaging, demonstrating the potential of VAE-GANs for data augmentation and the advancement of automated diagnostic tools. Our methodical approach—from data preprocessing to model training and evaluation—leverages the combined strengths of VAEs and GANs, enhancing medical image analysis and fostering innovations in diagnostic technologies. Additionally, this study emphasizes the critical role of dataset size in training efficiency, highlighting the need for higher and more scalable datasets to achieve optimal results.

Future work will focus on addressing the limitations associated with the elevated FID score, refining the model architecture, and incorporating qualitative assessments from medical professionals to ensure the clinical relevance of the generated images. Overcoming these challenges will further improve the effectiveness and reliability of generative methods, making them a valued asset for diagnostic practices and medical research.

References

[1] Johnson, A.E.W., Pollard, T.J., Berkowitz, S., Greenbaum,N.R., Lungren, M.P., Deng, C.Y., ... & Mark, R.G. (2019). MIMIC-CXR: A large publicly available database of labeled chest radiographs. *arXiv preprint arXiv:1901.07042*.
https://arxiv.org/abs/1901.07042.

[2] Kingma, D.P., & Welling, M. (2013). Auto-Encoding Variational Bayes. *Proceedings of the 2nd International Conference on Learning Representations (ICLR)*. https://arxiv.org/pdf/1312.6114.

[3] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative Adversarial Nets. *Advances in Neural Information Processing Systems*, 27, 2672-2680. http://papers.neurips.cc/paper/5423-generative-adversarial-nets.pdf.

[4] Balahur, A., Beygelzimer, A., & Pedregosa, F. (2019). Fairness in machine learning or statistical decision making. *arXiv preprint arXiv:1908.00807*. https://arxiv.org/pdf/2208.08279.

[5] Sandfort, V., Yan, K., Pickhardt, P.J., & Summers, R.M. (2019). Data augmentation using generative adversarial networks (CycleGAN) to improve generalizability in CT segmentation tasks. *Scientific Reports*, 9, 16884. https://www.researchgate.net/publication/337282919_Data_augmentation_using_generative_adversarial_networks_CycleGAN_to_improve_generalizability_in_CT_segmentation_tasks.

[6] Mahapatra, D., Bozorgtabar, B., & Garnavi, R. (2019). Image super-resolution using progressive generative adversarial networks for medical image analysis. *Computerized Medical Imaging and Graphics*, 71, 30-39. https://www.sciencedirect.com/science/article/pii/S0895611118305871.

[7] Kingma, D.P., & Welling, M. (2013). Auto-Encoding Variational Bayes. In *Proceedings of the 2nd International Conference on Learning Representations (ICLR)*. https://arxiv.org/pdf/1312.6114.

[8] Sohl-Dickstein, J., Weiss, E., Maheswaranathan, N., & Ganguli, S. (2015). Deep unsupervised learning using nonequilibrium thermodynamics. In *Proceedings of the International Conference on Machine Learning (ICML)*, pp. 2256-2265. https://arxiv.org/pdf/1503.03585.

[9] Ho, J., Jain, A., & Abbeel, P. (2020). Denoising diffusion probabilistic models. In *Advances in Neural Information Processing Systems (NeurIPS)*, vol. 33, pp. 6840-6851.

[10] Xiao, Z., Kreis, J.K., & Vahdat, A. (2021). Tackling the generative learning trilemma with denoising diffusion GANs. *arXiv preprint arXiv:2112.07804*. https://arxiv.org/abs/2112.07804.

[11] Chlap, P., Min, H., Vandenberg, N., Dowling, J., Holloway, L., & Haworth, A. (2021). A review of medical image data augmentation techniques for deep learning applications. *Journal of Medical Imaging and Radiation Oncology*, 65(5), 545-563.

[12] Shorten, C., & Khoshgoftaar, T.M. (2019). A survey on image data augmentation for deep learning. *Journal of Big Data*, 6(1), 1-48.

[13] Arjovsky, M., Chintala, S., & Bottou, L. (2017). Wasserstein generative adversarial networks. In *Proceedings of the International Conference on Machine Learning (ICML)*, pp. 214-223. https://arxiv.org/abs/1701.07875.

[14] Johnson, A.E.W., Pollard, T.J., Berkowitz, S., Greenbaum, N.R., Lungren, M.P., Deng, C.Y., ... & Mark, R.G. (2019). MIMIC-CXR: A large publicly available database of labeled chest radiographs. arXiv preprint arXiv:1901.07042. https://arxiv.org/abs/1901.07042.

[15] Kingma, D.P., & Welling, M. (2013). Auto-Encoding Variational Bayes. Proceedings of the 2nd International Conference on Learning Representations (ICLR). https://arxiv.org/pdf/1312.6114.

[16] Balahur, A., Beygelzimer, A., & Pedregosa, F. (2019). Fairness in machine learning or statistical decision making. arXiv preprint arXiv:1908.00807. https://arxiv.org/pdf/2208.08279.

[17] Sandfort, V., Yan, K., Pickhardt, P.J., & Summers, R.M. (2019). Data augmentation using generative adversarial networks (CycleGAN) to improve generalizability in CT segmentation tasks. Scientific Reports, 9, 16884. https://www.researchgate.net/publication/337282919_Data_augmentation_using_generative_adversarial_networks_CycleGAN_to_improve_generalizability_in_CT_segmentation_tasks.

[18] Ali, H., Biswas, M.R., Mohsen, F., Shah, U., Alamgir, A., Mousa, O., & Shah, Z. (2022). The role of generative adversarial networks in brain MRI: A scoping review. Insights into Imaging, 13, 98. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9167371/

[19] Ho, J., Jain, A., & Abbeel, P. (2020). Denoising diffusion probabilistic models. In Advances in Neural Information Processing Systems (NeurIPS), vol. 33, pp. 6840-6851.

[20] Xiao, Z., Kreis, J.K., & Vahdat, A. (2021). Tackling the generative learning trilemma with denoising diffusion GANs. arXiv preprint arXiv:2112.07804. https://arxiv.org/abs/2112.07804.

[21] Park, T., Liu, M.Y., Wang, T.C., & Zhu, J.Y. (2019). Semantic image synthesis with spatially-adaptive normalization. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, Long Beach, CA, USA, 16–20 June 2019, pp. 2337-2346.

[22] Yurt, M., Dar, S.U., Erdem, A., Erdem, E., Oguz, K.K., & Çukur, T. (2021). mustGAN: Multi-stream generative adversarial networks for MR image synthesis. *Medical Image Analysis*, 70, 101944.

[23] Dar, S.U., Yurt, M., Karacan, L., Erdem, A., Erdem, E., & Cukur, T. (2019). Image synthesis in multi-contrast MRI with conditional generative adversarial networks. *IEEE Transactions on Medical Imaging*, 38, 2375-2388. https://ieeexplore.ieee.org/document/8887206.

[24] Sun, Y., Yuan, P., & Sun, Y. (2020). MM-GAN: 3D MRI data augmentation for medical image segmentation via generative adversarial networks. In *Proceedings of the 2020 IEEE International Conference on Knowledge Graph (ICKG)*, Nanjing, China, 9–1 August 2020, pp. 227-234.

[25] Han, C., Rundo, L., Araki, R., Nagano, Y., Furukawa, Y., Mauri, G., Nakayama, H., & Hayashi, H. (2019). Combining noise-to-image and image-to-image GANs: Brain MR image augmentation for tumor detection. *IEEE Access*, 7, 156966-156977. [CrossRef] https://ieeexplore.ieee.org/document/8939220.

[26] Pang, T., Wong, J.H.D., Ng, W.L., & Chan, C.S. (2021). Semi-supervised GAN-based radiomics model for data augmentation in breast ultrasound mass classification. *Computer Methods and Programs in Biomedicine*, 203, 106018.

[27] Yang, H., Lu, X., Wang, S.H., Lu, Z., Yao, J., Jiang, Y., & Qian, P. (2021). Synthesizing multi-contrast MR images via novel 3D conditional variational auto-encoding GAN. Mobile Networks and Applications, 26, 415–424. [CrossRef]

[28] Madan, Y., Veetil, I.K., EA, G., KP, S., et al. (2022). Synthetic data augmentation of MRI using generative variational autoencoder for Parkinson's disease detection. In *Evolution in Computational Intelligence*; Springer: Berlin, Germany; pp. 171–178.

[29] Chadebec, C., Thibeau-Sutre, E., Burgos, N., & Allassonnière, S. (2022). Data augmentation in high-dimensional low-sample size setting using a geometry-based variational autoencoder. IEEE Transactions on Pattern Analysis and Machine Intelligence, 45, 2879–2896. [CrossRef] https://ieeexplore.ieee.org/document/9885828.

[30] Gulrajani, I., Ahmed, F., Arjovsky, M., Dumoulin, V., & Courville, A.C. (2017). Improved training of Wasserstein GANs. Advances in Neural Information Processing Systems, 30. https://arxiv.org/abs/1704.00028.

Enhancing Mobility – An Intelligent Robot for the Visually Impaired

Ahmad M. Bisher[1], Rufaida M. Shamroukh[2], Abed M. Shamroukh[3]
R&D Department, Pioneers of Industry Co., Amman, Jordan[1]
Electrical Engineering Department-Faculty of Engineering Technology, Al-Balqa Applied University, Amman, Jordan[2]
Electrical Engineering, EB Golden Base, Amman, Jordan[3]

***Abstract*—Efficient robot navigation in operational environments requires precise tracking of the path from the starting point to the destination, typically generated using pre-stored map data. However, obstacles in the environment can complicate this process, making reliable obstacle avoidance critical for successful navigation. This paper introduces innovative techniques for robotic navigation and obstacle avoidance, specifically designed to assist visually impaired individuals. To mitigate the limitations and inaccuracies inherent in sensor data, we employ sensor fusion algorithms that integrate inputs from infrared, ultrasonic, vision, and tactile sensors. Additionally, visual landmarks are incorporated as reference points to improve internal odometry correction and enhance mapping accuracy. We believe that our approach not only increases the reliability of navigation but also enhances the robot's ability to operate effectively in diverse and challenging conditions.**

***Keywords*—Robot; obstacle; avoidance; visually impaired; sensors**

I. Introduction

Certain types of robots, such as tracking and follower robots, can operate effectively without relying on maps. However, map-based mobile robots, which utilize pre-existing environmental data, are often employed for more complex tasks. The primary purpose of mapping is to store and generate path-related data, which can then be used with various planning techniques to facilitate navigation between specific locations. This integration is essential for mobile robot localization and path-learning algorithms [1].

Mobile robots typically use two types of maps: topological and geometric. Topological maps require minimal memory and computational complexity, relying more on map data than sensor data for path generation. These maps are computationally efficient and support the use of search algorithms. This paper uses a topological map to evaluate the role of mapping in robot navigation. However, map-based paths can be affected by environmental obstacles, making it necessary to establish a fundamental path between two nodes rather than relying solely on an exact route. Detecting and avoiding obstacles during navigation is essential, and the avoidance path is sensor-based. As a result, a well-designed robot navigation system combines both map-based and sensor-based approaches [1] [2] [3].

Various sensors are used in mobile robot navigation to measure specific environmental variables such as range, object dimensions, and landmarks. This paper discusses the operation, features, errors, and limitations of commonly used navigation sensors while introducing modern techniques for accurately measuring navigation variables to improve system performance. Additionally, the interface between blind users and the guidance system is a crucial consideration, as traditional communication methods, such as displays and buttons, are not feasible for visually impaired individuals. Voice interaction is proposed as the most effective communication protocol. To facilitate this, a phonetic integrated circuit approach is implemented for the human-robot interface [3].

II. Related Work

Efficient robot navigation, especially for assisting visually impaired individuals, has been a focal point of research in recent years. A significant aspect of this research involves sensor fusion, which improves the accuracy and reliability of robot navigation by combining data from various sensor types.

Sensor fusion algorithms have been widely used to improve robot localization and obstacle avoidance by integrating data from multiple sensors such as ultrasonic, infrared, vision, and tactile sensors. Doherty and McGinnity [4] present various sensor fusion techniques that enhance mobile robot navigation and control, demonstrating that combining data from different sources can improve system performance, particularly in dynamic environments. Bansal and Thakur [5] discuss robust sensor fusion algorithms that improve localization accuracy in mobile robots, focusing on dynamic sensor data handling in real-time situations. These techniques are highly relevant to overcoming the limitations of individual sensors in environments with unpredictable obstacles.

Effective obstacle avoidance is crucial for autonomous navigation in complex environments. Cai and Liu [6] explore various obstacle avoidance strategies, emphasizing real-time decision-making to dynamically adjust the robot's path. Zhang and Wang [7] present a dynamic obstacle avoidance system for autonomous robots using sensor fusion, where obstacles are detected, and the robot adjusts its trajectory accordingly. These studies provide insights into how obstacle detection and avoidance can be integrated with a robot's navigational strategies to ensure safe and efficient movement, especially in environments with moving or unexpected obstacles.

Robotic assistance for visually impaired individuals has gained increasing attention in recent years, focusing on the development of navigation systems that offer greater autonomy and independence. Chien and Lin [8] provide an overview of assistive robotics technologies designed for the blind, detailing

the challenges and solutions associated with robot navigation in dynamic and unfamiliar environments. Vig and Zupan [9] review mobile robotic systems for the visually impaired, examining various navigation aids such as ultrasonic sensors and voice feedback systems, highlighting their potential to significantly improve the mobility of individuals with visual disabilities. These studies emphasize the importance of developing reliable and user-friendly assistive systems that can help visually impaired individuals navigate their surroundings more independently.

In systems designed to aid the visually impaired, voice interaction becomes a critical interface for communication between the user and the robot. Meyer and Sharma [10] explore the development of speech-based interfaces for mobile robots, which provide intuitive and hands-free communication. They highlight the challenges of designing robust voice recognition systems that can operate in various acoustic environments. Singh and Gupta [11] further expand on speech recognition for assistive robotics, focusing on the development and challenges of integrating speech recognition systems to create effective real-time communication between users and robots. This work underscores the necessity of voice-based interfaces for creating an intuitive and inclusive user experience for blind individuals.

Effective mapping strategies, particularly the use of topological and geometric maps, are central to the navigation and localization of mobile robots. Renaud and Dufour [12] compare topological and geometric maps, discussing their respective advantages and limitations in robot navigation. Topological maps, which are often simpler and more memory-efficient, are well-suited for mobile robot navigation, especially in dynamic environments. Ali and Shah [13] review path planning algorithms and mapping techniques for autonomous robots, with a focus on their application in real-world navigation tasks. The combination of map-based and sensor-based navigation methods, as proposed in this paper, reflects the growing interest in integrating both mapping strategies to ensure reliable and efficient movement in complex environments.

III. Mobile Robot Navigation

A. Path Search

Path search procedures utilize map data to execute specific algorithms aimed at identifying the optimal path between nodes, with the map stored in the robot's memory. A sophisticated search algorithm, based on artificial intelligence techniques, was implemented to generate a path that combines a sequence of nodes and their interconnections. As shown in Fig. 1, node A represents the source, node D serves as the goal, and r1, r2, and r3 denote the topological relationships among the intermediate nodes [14].

To improve path efficiency, an optimal search algorithm can be applied. The choice of algorithm depends on the desired path characteristics and the capabilities of the implemented method. Accordingly, this robot integrates both sensor-based paths and direct map-based paths. The applied search algorithm focuses solely on determining the path between two nodes, with additional optimization performed to estimate the most efficient route. Furthermore, the selected path is refined using a microcontroller by implementing the "First Depth Search" algorithm. The topology underscores that the path consists of nodes and their interconnections, as illustrated in Fig. 1.

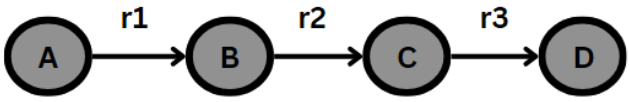


Fig. 1. Sample path between nodes in topological mapping.

B. Navigation Sensors

The robot integrates a variety of sensors to detect and measure environmental variables critical for navigation. Navigation sensors generally fall into two main categories: obstacle measurement sensors and landmark detection sensors. Theoretically, the same sensor can perform both functions depending on the variable being analyzed and the processing applied.

The most commonly used and effective sensors in mobile robots include infrared range sensors, laser range finders and scanners, ultrasonic sensors, vision sensors, GPS, and tactile sensors, among others [1].

In the robotic system proposed in this paper, tactile sensors are combined with infrared and ultrasonic sensors for obstacle detection, avoidance, and localization. Ultrasonic sensors, in particular, measure the distance between the robot and objects using two configurations. The first configuration employs triangulation, where distance is determined geometrically. In this method, the sensor emits ultrasonic waves and detects their reflections from the object at a specific angle (see Fig. 2). The distance is then calculated using reflection equations.

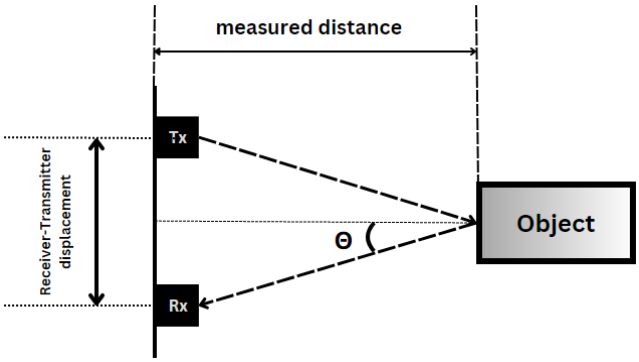


Fig. 2. Measuring distance via triangulation.

Θ: is the reflected angle.

The other implemented method is the measurement of time-of-flight. The echo of emitted ultrasound waves is detected to calculate the time between emitting the wave, Tx and receiving its echo, Rx, and then the range between the sensor and the object is calculated using Eq. (1), where: d is the measured distance, t is the time of flight, and T is the surrounding temperature.

$$d = (1 + x)^n = \frac{t}{2}[0.6T + 331.6] \quad (1)$$

A vision system is employed to identify various objects in the surrounding environment. By applying different image

processing techniques, the extracted features assist in robot navigation. The processor's capability and the interface's efficiency in processing image data with acceptable speed and accuracy are critical criteria [3] [15].

In this paper, an image-based assessment of robot positioning is utilized to avoid obstacles, while localization errors are corrected through internal odometry error correction using pattern recognition. Pattern recognition is applied to images containing specific landmarks, where a landmark is a label or an image featuring a number or text that represents a specific node on the map.

The vision system consists of a simple webcam, along with an image processing unit (IPU) based on a specific microprocessor, which is programmed in MATLAB using the Image Processing Toolbox and Real-Time Embedded Target Coder for the microprocessor. The IPU has two outputs: the object detection output, which is sent to the sensor fusion unit, and the landmark detection output, which is sent directly to the CPU.

IV. The Architecture of the Blind Guidance Robot

The primary objective of our proposed robotic system is to significantly improve the guidance process for individuals with visual disabilities, providing them with a safer and more independent means of navigation. As shown in Fig. 3, the robot features a modular design, allowing for easy customization and maintenance. The CPU module serves as the core management and synchronization unit, built with advanced microcontrollers that enable real-time processing and decision-making.

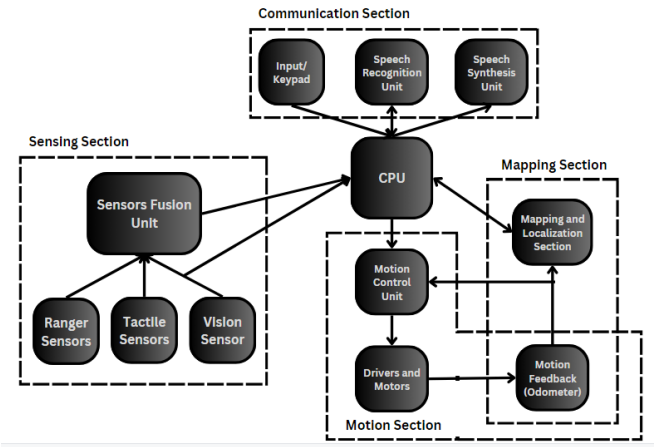


Fig. 3. System architecture of the blind guidance robot.

Detailed specifications of the topology and odometry unit are presented in Fig. 4, highlighting the system's ability to effectively map its environment and track its position. This robotic system is designed with an intelligent methodology, equipping it with learning capabilities that allow it to adapt to its surroundings. It employs various sensors to collect data, enabling a comprehensive understanding of the environment and ensuring safe navigation.

The robot's main function is to learn a map of its surroundings and navigate from one specific point to another with precision. By integrating obstacle detection and avoidance mechanisms, the robot can effectively navigate around obstacles, ensuring a smooth and reliable experience for users. Ultimately, this system aims to empower individuals with visual disabilities, fostering independence and confidence in their ability to navigate complex environments.

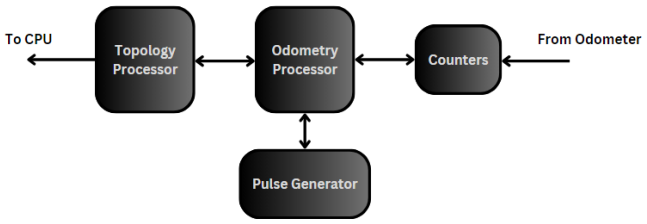


Fig. 4. Design of mapping and localization unit.

V. Design Implementation

A. Navigation Sensors

Generally, navigation sensors face a variety of drawbacks due to measurement errors and inherent limitations, which can significantly affect their performance in real-world applications. The resulting imprecision is both predictable and measurable, depending on the operational characteristics and design of each sensor. For example, ultrasonic range finders, as shown in Fig. 5, are known for their poor angular resolution. This limitation makes them ineffective at detecting oblique or smooth surfaces, posing considerable challenges in environments where such surfaces are common. Consequently, obstacles that do not reflect sound waves directly may go undetected, leading to potential navigation errors [16].

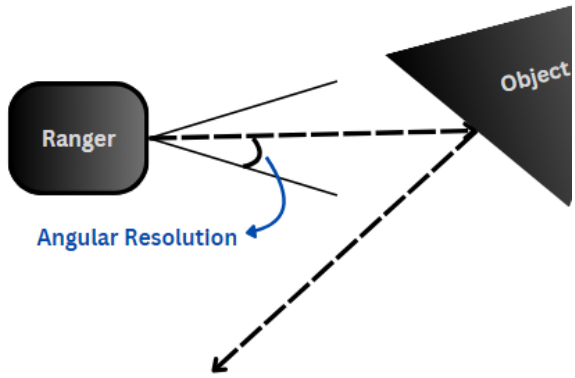


Fig. 5. Sound waves reflection on oblique surface.

In contrast, infrared range sensors have their own set of limitations. They are particularly susceptible to interference from bright light, which can lead to inaccurate readings. Furthermore, these sensors struggle with measuring distances to reflective surfaces, such as liquids and glass, resulting in additional complications during navigation. Their angular resolution is also suboptimal, meaning they may misjudge the proximity of objects, thus impairing the robot's ability to navigate effectively in complex environments [16].

Vision sensors, while capable of providing rich data about the surroundings, also face significant challenges. They typically offer lower precision in distance measurements compared to other sensor types and require substantial processing power to analyze visual input effectively. This high

computational demand can limit their real-time application in mobile robotics, as the robot may need to prioritize speed and responsiveness over detailed analysis.

These limitations highlight the need for careful sensor selection and the implementation of advanced algorithms to mitigate measurement errors and improve overall navigation reliability. In many cases, combining multiple sensor types can leverage their complementary strengths, leading to more accurate environmental perception. Additionally, ongoing research and development in sensor technology aim to address these challenges, enhancing the precision and adaptability of navigation systems across various applications.

All of these limitations are effectively addressed through the implementation of sensor fusion techniques, which involve using multiple sensors to measure the same environmental variable. For example, combining ultrasonic range finders with infrared sensors helps mitigate challenges related to detecting oblique surfaces and glass, which are often problematic for individual sensor types. By integrating the strengths of different sensors, the robot gains a more comprehensive understanding of its surroundings, thereby enhancing navigational accuracy and safety.

Traditionally, sensor data fusion is carried out using conventional computational methods. However, these approaches generally require high processing precision and can become computationally intensive, making them less suitable for real-time applications in mobile robotics. This challenge is particularly critical when rapid decision-making is essential for safe navigation in dynamic environments [2].

In this paper, we employ fuzzy logic computing techniques to facilitate rule-based data fusion, eliminating the need for a detailed analytical model of the sensors used. The input sensors' membership functions, as shown in Fig. 6, illustrate how various sensor readings are integrated and interpreted within the fuzzy logic framework. By using fuzzy logic, we can better manage the inherent uncertainties and imprecisions in sensor data, enabling more nuanced decision-making processes.

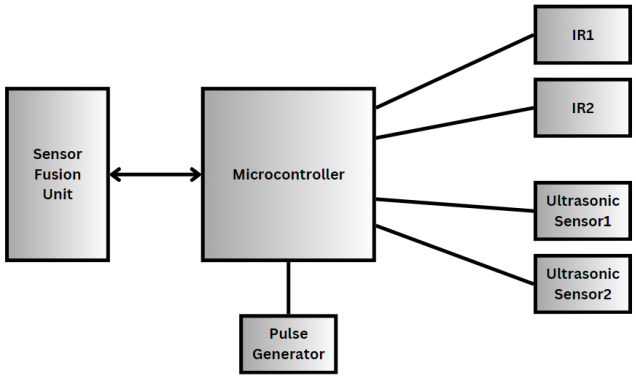


Fig. 6. Structural design of rangers control and conditioning unit.

The fuzzy computing sensor fusion unit is designed using a microprocessor, a powerful yet compact solution for processing sensor data. This unit continuously reads the outputs from all navigation sensors, processes the data in real time, and generates decisions regarding obstacle detection and avoidance. After analyzing the sensor inputs, the unit sends critical information to the CPU, which coordinates the robot's navigation strategies.

This innovative approach not only increases the reliability of navigation but also enhances the robot's ability to operate effectively in diverse and challenging conditions. The integration of fuzzy logic allows the system to adapt to varying levels of sensor reliability and environmental complexity, improving overall operational efficiency. By enabling the robot to make informed decisions quickly, we aim to create a more robust and reliable navigation system that ultimately enhances the user experience for individuals with visual disabilities. This methodology demonstrates the potential of advanced computational techniques to revolutionize mobile robotics, paving the way for smarter, more autonomous systems.

B. Map Learning

This paper proposes a lead-through programming method for robot map learning, in which a programmer manually guides the robot through various environments while the robot autonomously collects environmental data using its sensors, supplemented by user input. This interactive approach not only facilitates efficient data collection but also enhances the accuracy of the mapping process, ensuring that the robot can effectively understand and navigate its surroundings [14].

At its core, the topological map is constructed as a collection of relational paths, represented as straight lines. Each branch of the map consists of a straight-line path that maintains a specific angle relative to a defined frame of reference. Consequently, the robot's learning process focuses on accurately measuring the distance between two nodes and the angles that relate to this reference frame. This geometric representation is crucial for the robot's ability to navigate complex environments, as it provides a simplified yet effective way to understand spatial relationships.

As the learning process begins, the odometry unit actively measures and models all relevant map data, constructing the corresponding map branches in real time. This dynamic modeling ensures that the robot captures the nuances of its environment, including variations in terrain and the presence of obstacles. The data collected during this phase forms the foundation for building a reliable map that the robot can reference during subsequent navigation tasks.

Moreover, the programmer plays a critical role in the mapping process by entering the number of nodes at each landmark location. This input is essential for establishing key reference points within the topological framework, allowing the robot to create a network of interconnected paths. By defining these landmarks, the programmer enhances the robot's ability to identify and navigate to specific destinations within the environment, improving its overall usability.

At the conclusion of this comprehensive process, a well-defined topological map is successfully created, enabling the robot to navigate its environment with a heightened understanding and improved efficiency. The lead-through programming method not only streamlines the map-building process but also fosters an intuitive collaboration between the human programmer and the robotic system. This synergy results

in a robust navigation solution tailored to the specific needs of the environment being mapped.

Furthermore, this innovative approach has practical applications beyond traditional robotics, particularly in assisting individuals with visual disabilities. By empowering users to engage directly in the mapping process, we promote inclusivity and ensure that the robot can adapt to unique environments that are meaningful to its users. Ultimately, this lead-through programming methodology represents a significant advancement in robotic learning and navigation techniques, paving the way for smarter, more autonomous systems capable of operating effectively in a variety of real-world scenarios.

C. Motion Control Unit (MCU)

The drive motors of the robotic system are controlled by the microcontroller unit (MCU), which manages various aspects of motor performance, including speed, direction, reversing, and dynamic stopping. This comprehensive control is essential for achieving smooth motion and precise position control, enabling the robot to navigate its environment effectively.

When the CPU commands a specific straight path, along with its length and angle, the motion control unit calculates the required parameters for the motors. This involves determining the appropriate speed and timing for each motor to ensure that the robot follows the designated path accurately. The closed-loop control system continuously monitors the motors' performance in real time, making adjustments as necessary to maintain the intended trajectory.

This closed-loop feedback mechanism is crucial for handling dynamic conditions, such as changes in terrain or unexpected obstacles. By constantly comparing the robot's actual position and movement against the desired path, the MCU fine-tunes motor commands to ensure adherence to the planned trajectory. This capability not only enhances navigation accuracy but also contributes to the overall stability and reliability of the robotic system.

Additionally, the system allows for responsive maneuvering, enabling the robot to execute tasks such as reversing or performing dynamic stops without losing momentum or control. This level of sophistication in motor control is vital for applications requiring high precision, such as assisting individuals with visual disabilities, where the robot must navigate complex environments safely and effectively.

Overall, the integration of the MCU with the drive motors creates a robust and adaptive motion control system that supports the robot's ability to operate smoothly in a variety of settings, facilitating a more intuitive and effective navigation experience.

D. Human Robot Communication

Since our primary objective is to design a blind guidance robot, the interaction between the user and the robot relies exclusively on oral communication. This approach is essential to ensure that individuals with visual disabilities can effectively engage with the robotic system. The robot receives commands from the blind user through an advanced speech recognition system, capable of accurately interpreting vocal instructions in real time [3].

Once the robot processes the user's commands, it provides feedback through a built-in speaker, conveying information in a clear and accessible manner. This two-way communication not only facilitates command execution but also keeps the user informed about the robot's actions and surroundings, enhancing their sense of control and awareness [14].

The implementation of this oral communication system is designed to be intuitive, allowing users to issue commands naturally without requiring specialized training. By using voice as the primary interface, the robot fosters a more inclusive interaction model, empowering blind users to navigate their environments confidently.

Additionally, the speech recognition system can be enhanced with adaptive learning capabilities, enabling it to improve accuracy over time based on the user's specific speech patterns and preferences. This personalization further strengthens the user experience, ensuring that the robot can respond effectively to individual needs. Overall, this oral communication framework plays a critical role in the functionality of the blind guidance robot, making it a valuable tool for enhancing mobility and independence for individuals with visual impairments [3] [2][14].

E. Speech Synthesis Module

This paper implements a sophisticated speech synthesis system based on a phonetic chip capable of producing a wide range of sounds. The phonetic system is carefully controlled and trained by initially receiving specific phrase data through a computer interface. Once programmed, the system operates as a stand-alone unit, with a microcontroller facilitating seamless communication between the phonetic system and the CPU to send the necessary phrase programs to the speakers [17].

When the phonetic integrated circuit (IC) receives a program containing the phonetic structure of a designated phrase—transmitted via a serial control protocol—it processes this data and generates the corresponding sound associated with that phrase. This approach ensures that the robot can effectively convey information and respond to user commands in a clear and intelligible manner [17].

To enhance the audio output quality, sound tuning is performed using a double-stage low-pass filter, which helps eliminate unwanted high-frequency noise and ensures that the produced sounds are smooth and natural. This filtering process is crucial for optimizing the user experience, as clear audio communication is essential for effective interaction between the blind user and the robotic system.

By leveraging this phonetic synthesis approach, the robot can provide verbal feedback, enhancing situational awareness for the user and allowing for more interactive navigation. The flexibility of the system enables it to be programmed with a variety of phrases tailored to assist users in different scenarios, significantly improving the robot's functionality as a guidance tool. Overall, this speech synthesis system represents a vital component of the robot's user interface, fostering an engaging and responsive communication experience for individuals with visual disabilities. Fig. 7 shows the block diagram of our speech synthesis unit.

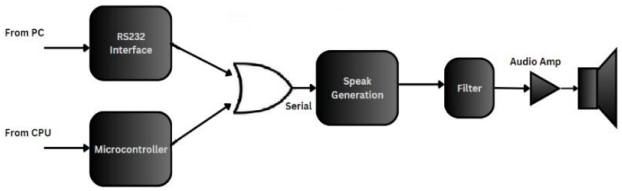


Fig. 7. Block diagram of the speech synthesis unit.

F. Speech Recognition Module

The speech recognition module is designed to recognize up to 40 distinct words, each with a maximum duration of 0.96 seconds. Notably, this module supports a speaker-independent speech recognition system, enabling it to effectively interpret commands from various users without requiring extensive training. Each trained word is assigned an index ranging from one to forty, facilitating easy identification and processing.

In recognition mode, when a word is successfully identified, its corresponding index number is output by the system and transmitted to the CPU as the recognition result. This seamless communication allows the robot to take appropriate actions based on user commands. A comprehensive overview of the speech recognition approach and the underlying algorithms will be presented in a forthcoming paper, providing further insights into the technical intricacies involved [18][19].

The speech recognition unit operates in two distinct modes: training mode and running mode. In training mode, the unit captures the user's spoken word and associates it with a specific index number between one and forty. It then saves the unique voice pattern along with its assigned number in the SRAM, ensuring that the system can recognize the word in future interactions [18].

Once training is complete, the system transitions to running mode, where it continuously listens for spoken input. During this phase, the module remains vigilant and ready to recognize speech at any time. If a recognized word is detected, its corresponding number is sent to the CPU, prompting the robot to execute the designated action. This dual-mode functionality enhances the flexibility and responsiveness of the system, allowing for efficient communication and interaction with the user.

Overall, the implementation of this speech recognition module is a critical component of the blind guidance robot, significantly improving its ability to understand and respond to user commands in real-time. The speech recognition unit is shown in Fig. 8.

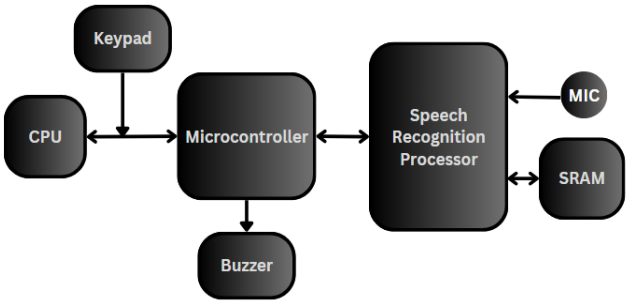


Fig. 8. Block diagram of the speech recognition unit.

VI. Results

This paper applies the described robot design in an indoor environment, where a comprehensive map is constructed. When commands are issued to the robot, it begins movement from a specified source point to a designated destination. Fig. 9 illustrates the test results, demonstrating the effectiveness of the robot's navigation system.

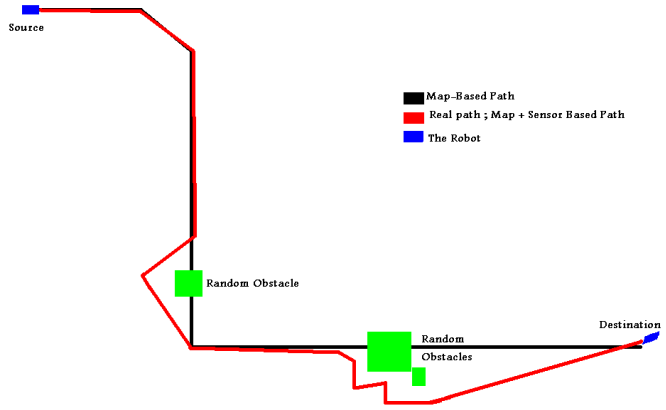


Fig. 9. Indoor environment test results.

In the figure, the black line represents the map-based path generated through the topological mapping process, reflecting the pre-defined routes established during the learning phase. In contrast, the red line illustrates the actual path taken by the robot, which is a dynamic combination of both map-based and sensor-based navigation strategies.

The sensor-based path begins with the detection of obstacles, represented in green on the diagram. Upon encountering an obstacle, the robot employs its obstacle avoidance algorithms to navigate around it effectively. Once the obstacle is bypassed, the robot reorients itself and returns to the next node as indicated in the topological map, ensuring continuity in its route.

This integration of both mapping and sensor data enables the robot to adapt in real-time to changing conditions in the environment, enhancing its navigational accuracy and reliability. By successfully blending map-based navigation with responsive obstacle avoidance, the system demonstrates its ability to operate effectively in complex indoor settings, paving the way for practical applications in assisting individuals with visual impairments. The results underscore the potential of this robotic design to facilitate independent movement and enhance user confidence in navigating unfamiliar spaces.

VII. Conclusion and Future Work

In conclusion, this paper presents a comprehensive approach to designing an autonomous blind guidance robot that effectively integrates advanced navigation, speech recognition, and user interaction technologies. By employing a lead-through programming method for map learning, the robot can autonomously navigate complex indoor environments, adapting to dynamic conditions through a combination of map-based and sensor-based paths. The implementation of a robust speech synthesis and recognition system facilitates intuitive communication between the robot and its users, ensuring that

individuals with visual impairments can interact seamlessly with the technology.

The results demonstrate the effectiveness of the robot's navigation capabilities, highlighting its ability to detect and avoid obstacles while maintaining a clear route based on a topological map. This integration of various systems not only enhances the robot's operational efficiency but also significantly improves the user's experience, promoting independence and confidence in navigating unfamiliar spaces.

Future work will focus on further refining the speech recognition algorithms and expanding the robot's capabilities to handle more complex environments. Overall, this research contributes to the ongoing development of assistive technologies aimed at empowering individuals with visual disabilities, paving the way for more inclusive and accessible robotic solutions.

ACKNOWLEDGMENT

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

REFERENCES

[1] Sadeghi, A., & Ghasemi, A. (2016). "Development of Indoor Navigation Systems for Visually Impaired Users." International Journal of Human-Computer Interaction, 32(3), 267-280.

[2] Zhang, Y., & Lin, Y. (2018). "Real-time Obstacle Detection and Avoidance for Mobile Robots." Journal of Field Robotics, 35(1), 78-92.

[3] Mavridis, N. (2015). "The Role of Communication in Human-Robot Interaction: A Comprehensive Review." Robotics and Autonomous Systems, 75, 33-52.

[4] Doherty, M., & McGinnity, T. M. (2020). Sensor fusion for mobile robot navigation and control. Sensors, 20(12), 3494.

[5] Bansal, A., & Thakur, M. (2021). Robust Sensor Fusion Algorithms for Mobile Robot Localization. Journal of Robotics and Autonomous Systems, 141, 103834.

[6] Cai, J., & Liu, X. (2019). Obstacle avoidance for mobile robots: Techniques and applications. Robotics and Autonomous Systems, 118, 78-94.

[7] Zhang, Z., & Wang, H. (2018). Dynamic Obstacle Avoidance for Autonomous Robots Using Sensor Fusion. IEEE Transactions on Robotics, 34(4), 976–984.

[8] Chien, S., & Lin, J. (2021). Assistive robotics for blind and visually impaired: Design challenges and solutions. Journal of Robotics and Autonomous Systems, 141, 103825.

[9] Vig, K., & Zupan, L. (2020). Mobile Robotic Assistance Systems for the Visually Impaired: A Review. IEEE Transactions on Human-Machine Systems, 50(6), 525–536.

[10] Meyer, J., & Sharma, K. (2021). Human-Robot Interaction: Developing Speech-Based Interfaces for Mobile Robots. ACM Transactions on Human-Computer Interaction, 28(2), Article 7.

[11] Singh, R., & Gupta, A. (2020). “Speech Recognition for Assistive Robotics: Design, Challenges, and Applications”. Journal of Artificial Intelligence Research.

[12] Renaud, M., & Dufour, F. (2019). A comparison of topological and geometric maps for robot navigation. Robotics and Autonomous Systems, 119, 103303.

[13] Ali, S., & Shah, S. (2021). Path planning and navigation for autonomous robots: A survey. Autonomous Robots, 45(2), 153–170.

[14] Farahani, R. Z., & Zare, S. (2021). "Robust Path Planning for Autonomous Navigation in Unstructured Environments." Journal of Intelligent & Robotic Systems, 101(3), 569-585.

[15] Bhatia, S., & Sharma, R. (2019). "Sensor Fusion Techniques for Mobile Robotics: A Survey." International Journal of Advanced Robotic Systems, 16(4), 1-14.

[16] Dhanraj, R., & Kumar, S. (2020). "Fuzzy Logic Applications in Robotics: A Review." International Journal of Robotics Research, 39(4), 361-377.

[17] Kahn, P., & Ryu, K. (2019). "Speech Synthesis Techniques for Human-Robot Interaction." IEEE Transactions on Human-Machine Systems, 49(2), 210-222.

[18] Huber, J., & Hurst, T. (2017). "Advancements in Speech Recognition for Assistive Technology." Assistive Technology Journal, 29(3), 134-145.

[19] Tran, M., & Nguyen, H. (2022). "Machine Learning Approaches for Enhancing Speech Recognition in Assistive Devices." Journal of Assistive Technologies, 16(1), 45-59.

Face Anti-Spoofing Using Chainlets and Deep Learning

Sarah Abdulaziz Alrethea, Adil Ahmad
Information Technology Department, King Abdulaziz University, Jeddah, Saudi Arabia

***Abstract*—Now-a-days, biometric technology is widely employed for many security purposes. Facial recognition is one of the biometric technologies that is increasingly utilized because it is convenient and contactless. However, the facial recognition system has become the most targeted by unauthorized users to get access to the system. Most facial recognition systems are vulnerable to face spoofing attacks. With the widespread use of the internet and social media, it has become easy to get videos or pictures of people's faces. The imposter can use these documents to deceive facial authentication systems, which affects the system's security and privacy. Face spoofing occurs when an unauthorized user attempts to gain access to a facial recognition system using presentation attack instruments (PAIs) such as photos, videos, or 3D masks of the authorized users. Therefore, the need for an effective face anti-spoofing (FAS) system is increased. That motivated us to develop a face anti-spoofing model that accurately detects presentation attacks. In our work, we developed a model that integrates handcrafted features based on Chainlets (as motion-based descriptor) and the convolutional neural network (CNN) to provide a more robust feature vector and enhance accuracy performance. Chainlets can be computed from deep contour-based edge detection using Histograms of Freeman Chain Codes, which provides a richer and rotation-invariant description of edge orientation that can be used to extract Chainlets features. We used a benchmark dataset, the Replay-Attack database. The result shows that the Chainlets-based face anti-spoofing method overcome the state-of-art methods and provide higher accuracy.**

***Keywords*—Presentation attacks; Chainlets; contour; handcrafted features; chain code; CNN; face anti-spoofing**

I. Introduction

In recent years, there has been an increasing interest in human recognition using biometric systems. Facial recognition systems are among the most popular biometric systems on the market because of their ease of use, high performance, and high level of security compared to iris and fingerprint recognition [1]. It is widely used in real-world applications, such as online payment and e-commerce security, smartphone-based authentication, secure access control, and others [2]. However, because of the widespread use of face recognition technologies, they have increasingly been the focus of Presentation Attacks (PAs). These attacks can be categorized into two types: (1) Impersonation attacks are an unauthorized user attempt to spoof someone else's identity, and (2) Obfuscation attacks are a user attempt to avoid being recognized by the system [3]. Face spoofing is when an unauthorized user tries to gain access to the facial recognition system by using one of the Presentation Attack Instruments (PAIs) like a photo (Print attack), a digital video (Replay attack), or wearing a mask (3D mask attack) of the authorized user [4] [5]. The most popular PAs are photo and video because they are easy to obtain and inexpensive compared to 3D mask attacks.

Face anti-spoofing (FAS) methods can be categorized into four main types: liveness, texture, 3D geometric, and multiple cues-based. 1- Liveness-based methods utilize motion in video frames to distinguish between real and spoofed faces. 2-Texture-based methods analyze the micro-texture of the object in front of the camera. 3- Three-dimensional geometric methods rely on the 3D structure of the user's face. 4- Multiple cues-based methods combine various techniques, such as integrating texture features with motion features [6].

In prior works, most face anti-spoofing methods based either on traditional methods, which use machine learning or deep learning. The first-mentioned is by extracting the handcrafted features and training the classifier to differentiate between fake and real faces [7]. It provides good performance in some situations; however, the researcher should have prior knowledge to design the features. Also, it cannot guarantee that the technique will function well in an unknown environment. The methods based on deep learning are more robust and concentrate on designing the model's structure, and are better able to handle a wide range of frequency responses. In general, deep learning models tend to outperform shallow ones [8]. The Convolutional Neural Network (CNN) architecture was proven that it is very effective for face anti-spoofing and superior to the other algorithms in terms of feature extraction [7]. However, optimizing the parameters would need a large number of training samples, which is not feasible for the existing face anti-spoofing databases [8].

In our proposed strategy, we use both handcrafted features and deep learning to obtain more robust features and produce a face anti-spoofing model with high accuracy [8]. Although there are many attack types with different scenarios, until now, there is no outstanding technique for face anti-spoofing systems. There is little attention paid to the development of a fusion strategy that incorporates various liveness features with multiple visual cues. Integrating liveness features from multiple cues will improve the detection accuracy of the face anti-spoofing system [9]. Deep learning models, particularly Convolutional Neural Networks (CNNs), have shown encouraging outcomes in numerous visual recognition tasks, leading researchers to use them in face anti-spoofing [2].

Integrating of handcrafted features and deep features has been used in face anti spoofing with promising results. The paper [10] integrates the handcrafted features with deep learning. It proposes an approach to enhance motion cues for face anti-spoofing using a CNN-LSTM architecture. This

architecture combines Convolutional Neural Networks (CNNs) for spatial feature extraction and Long Short-Term Memory (LSTM) networks for capturing temporal dynamics across video frames. While Eulerian Motion Magnification is used to enhance subtle motion cues, it also degrades image quality. This can sometimes impact overall feature extraction negatively. Also, the temporal features are sensitive to low-quality frames affected by blur or noise, reducing effectiveness.

Consideration of the cues of motion across video frames requires taking into account the changes in objects, such as the face for each frame in terms of orientation and shape boundaries, which play a major role in detecting fundamental changes in impersonation. The paper in [11] introduces Chainlets, a novel object detection and recognition descriptor in computer vision. Chainlets build upon edge-based representations, improving upon existing methods like Histograms of Oriented Gradients (HOG) by incorporating edge connectedness and ordered orientation changes. This enhancement enables Chainlets to handle challenges like orientation invariance. While Chainlets were used for ear recognition and pedestrian detection and achieved competitive results with simple classifiers SVM, this motivated us to use Chainlets with Deep learning in the face anti-spoofing field to differentiate the fake and real faces. More specifically, in our work, we developed a model that integrates Handcrafted features based on Chainlets[11] (as motion-based-descriptor) and deep learning (CNN network) to enhance the performance in terms of accuracy.

The contributions of this paper are:

1) Utilizing a novel, generalized feature descriptor, Chainlets, for face anti-spoofing.

2) Built a model that integrates handcrafted features with CNN to get more robust features to improve the accuracy.

3) The experimental results demonstrate that Chainlets deliver better performance in face anti-spoofing than other algorithms.

This paper is organized as follows: Section II presents the literature review, Section III presents the methodology, Section IV discusses the experiments, and Section V presents the conclusions.

II. Related Work

Nowadays, Face anti-spoofing FAS is important for all facial recognition systems to discriminate between real and fake faces. Most FAS methods are based on either traditional methods or deep learning. The following sections briefly review the relevant works performed in face spoofing detection based on traditional and CNN based FAS techniques [7].

A. Traditional FAS Methods

Traditional FAS methods involve extracting handcrafted features and training classifiers to differentiate between fake and real faces [7]. Consequently, all existing Traditional FAS methods can be categorized into face anti-spoofing methods depending on motion information, texture information, 3D geometric, or multiple information. The methods based on handcrafted features provides good performance in some situations; however, the researcher should have prior knowledge to design the features. Also, it cannot guarantee that the technique will function well in an unknown environment [8].

1) Motion cue-based methods: The motion-based methods endeavor to detect liveness based on movement, for example, mouth movement or eye blinking or others. This method effectively detects photo attacks however provides poor performance in detecting video attacks [6].

The study in [12] proposed a method for Counter-Measures which is based on the correlation of foreground and background movement. This technique detects motion correlation between the scene's background and the user's face to indicate spoofing attack existence depending on optical flow (OF) to estimate direction. Additionally, histograms, normalization, comparison, and OFC quantization are employed to analyze frames for correlation. In the results and conclusion, this study presents a photo-attack dataset, which includes spoofing attacks under various conditions, and successfully detects photo attacks using motion correlation, achieving a 1.5% Half Total Error Rate (HTER).

These previous studies [13] [14] aim to propose methods for detecting liveness. The study in [13] presented an algorithm to evaluate liveness in face image sequences, with the goal of adding liveness awareness in a non-intrusive manner. This system is based on new Optical Flow (OF) and employs local Gabor decomposition and SVM experts. The system operates in real-time, with an input of three frames and an output of a liveness score; if the value of the score is 0, that means no liveness (fake face), and if it is 1, that means the maximum liveness (real face). The study's method depends on integrating the detection of face and the estimation of Optical Flow (OP) in order to indicate the liveness score. This integration is a combination between Optical Flow of Lines (OFL) by means of 1D Gaussians employment including derivatives and implementation of model based on a logpolar grid Gabor and SVM features. The XM2VTS database has been used for evaluation. The results show the success and robustness in detecting the liveness. Furthermore, the rate of error was about 0.5%. However, this method is not effective against video replay attacks.

The objectives related to this study [11] fall under presenting a new approach for detecting pedestrian and recognizing ear, proposing utilize of Chainlets as a new object descriptor. In computer vision applications, Hand-crafted models have shown encouraging results for pedestrian recognition. Based on these findings, human identification and other applications have adopted the Histogram of Oriented Gradients (HOG) features. Unlike traditional methods like Histograms of Oriented Gradients (HOG), which fail to model edge connectedness, Chainlets use Histograms of Chain Codes to enhance object descriptiveness and provide orientation invariance. Chainlets, which we refer to as normalized histograms of chain codes, are used as new descriptors for detection/recognition in the suggested unique method. In addition, experiments demonstrate that Chainlets perform better than HOG-based algorithms and also deep networks in particular cases. Speaking of methodology, this study's method using an ordered oriented data which is computed from deep contour based on edge detection; Chainlets. Chainlets produce strong results for pedestrian

detection, boosting performance in comparison to previous hand-crafted descriptors and setting a new standard for biometric ear recognition. However, the current state of the art uses a quicker R-CNN and an improved classifier to enhance deep features for pedestrian identification. Even greater performance may be achieved by combining these improved classifiers with Chainlets. Aside from pedestrian detection and recognition, we feel that Chainlets have a lot of potential for usage in other areas such as face anti-spoofing.

This paper in [15] also utilized Chainlets, introducing an algorithm for ear recognition called the Chainlet-Based Ear Recognition method, which incorporates multi-banding image processing and support vector machine (SVM) classification. The approach involves splitting an ear image into multiple bands based on pixel intensity and using the Canny edge detection algorithm to extract edges in each band. These edge maps are combined into a single binary edge map representing the ear's contours. It achieved high accuracy with optimal band counts on two benchmark datasets: IITD II and USTB I.

2) Texture cue-based methods: The methods based on texture took use of the fact that a genuine face has a distinct illumination pattern and texture than the 3D mask, paper, or LCD surface utilized to perform the presentation attack [16]. It aims to explore the micro-texture of the object in front of the camera [6]. Texture feature-based methods utilize two kinds of features: static or dynamic. The Static texture cues extract spatial texture features from a single image. In comparison, the dynamic texture cues extract spatiotemporal texture features from video sequences [6]. In this method, the computational complexity is low, and the implementation is easy; however, with the recent and high-resolution cameras and high-quality pictures, the texture information is not enough, and we need to combine it with other information [17].

These previous studies [18] [19] aim to propose methods based-on color texture analysis. This paper [18] proposed a novel face anti-spoofing approach based on analysis of color texture. This study focus on using chrominance information in order to discriminate fake faces from real ones, while other studies have focused on evaluating the luminance of the face pictures. Related to methodology and experiments, the information relative to joint color texture, which comes from the luminance and the chrominance channels, has been analyzed based on a color local binary pattern descriptor. Furthermore, the histograms of feature have been extracted separately from each picture band. For the classification, they utilized a SVM with RBF Kernel. In the result, the investigation of the useful color space among HSV, RGB, and YCbCr spaces has been indicated. The performed experiments on CASIA and Replay-Attack databases have delivered excellent results taking into account a very promising results related to capabilities of generalization.

This paper in [20] proposed a new approach to detecting spoofing attacks based on texture analysis regarding characterization of printing artifacts, image quality assessment, and differences in light reflection. In addition, this study aims to present a new model by evaluating facial image textures in order to distinguish between live face and face in a printed image. This study considers the NUAA Photograph Imposter Database. The evaluation of the facial images' texture has been done by multi-scale local binary pattern (LBP). Speaking of methodology, the live objects must appear fixed as much as possible by minimizing the blinking motion of the eye and other movements. For the classification, they utilized a SVM with RBF Kernel (LibSVM). The results, this approach is robust and fast in calculations and demands no cooperation from the user, where the accuracy achieves 98.0%.

3) 3D Geometric cue-based methods: The 3D geometric-based methods use the depth information of the face to differentiate between a 2D face (photo or video attack) and a 3D face (real face). This method effectively detects photo and video attacks; however, it is not adequate to detect 3D mask attacks and is also costly because it needs additional hardware [17].

This paper in [21] proposed a new approach for detecting face liveness in order to eliminate spoofing attacks based on recovering sparse 3D facial structures. The methodology involves capturing faces in videos or photo sequences from at least three viewpoints, detecting facial landmarks, and selecting key frames. After that, the recovering operation of the sparse 3D facial structure can be done based on the chosen key frames. Eventually, a training process for the Support Vector Machine (SVM) is performed in order to differentiate the real faces from the fake ones. They evaluate the proposed method using three datasets, CASIA, NUAA, and Idiap databases. In the results of experiments, the proposed method has achieved ideal performance in detecting liveness where the accuracy achieved 100% for Face Liveness Detection. It outperforms the state-of-the-art methods in differentiating the genuine, planar, and warped image faces. The disadvantages of this method are that it provides good performance just for detecting photo attacks, not others. Also, it needs various viewpoints where one image is not enough. In addition, if the number of key frames is not enough, it can affect the performance.

This paper in [22] proposed a multispectral approach for FAS with not only (VIS) spectra imaging but also with the near infrared (NIR) one in order to execute VIS–NIR image consistency for spoofing detection purposes. Related to methodology and tools, correlation analysis has been employed in order to achieve a more compatible anti-spoofing method. The overall system consisted mainly of: (i) trained correlation confidence map to have a robust system, (ii) VIS–NIR correlation model, (iii) illumination robust feature extraction, and (iv) final classifier to perform detection. First, to avoid unbalanced illumination terms, input has been preprocessed by histogram equalization and face to eye position normalization, then region features. In addition, the information of correlation is calculated based on features of NIR and VIS photo patches. The proposed method has achieved an effective performance in handling spoofing attacks with different illumination, and also intra and cross dataset testing protocols on the three datasets (Ms-spoof, self-collected and PolyU-HSFD) based on extracting complementary features on VIS and NIR photos. The ACER (%) is 1.76 in the self-collected dataset, and 0.241 in Ms-spoof dataset.

4) Multiple cues-based methods: The multiple cues-based methods consider combining multiple cues such as motion information with texture information. This method detects varied kinds of face presentation attacks [6]. The methods based on multiple cues are superior in accuracy; however, it needs high Computations [17].

This paper in [23] proposed a liveness detection system that integrates motion and texture cues, exploiting scene context and eye blinks in a real-time system to non-intrusively resist spoofing attacks. The proposed method utilized the conditional random field model for eye blinks and LBP to compare the scene context to the reference images. Two databases were created for evaluating the system: a photo-imposter video database and a live face video database. The experimental results verified the system's reasonable ability to counter spoofing attacks and its robustness against camera shifts as well as its achievement of 99.5% accuracy. However, this method is unsuitable for real-life applications as the camera must remain fixed in the same position.

This paper in [9] proposed a multi-cues integration framework for face anti-spoofing utilizing a hierarchical neural network in order to enhance the ability of generalization. The proposed method is meant to fuse image quality cues and related motion in order to detect liveness. They extract image quality features using shearlet (SBIQF) and motion features using optical flow. In addition, they fuse features from multi cues using bottleneck representations that can effectively integrate various features of liveness. They evaluate the method using three databases: Replay-Attack, CASIA-FASD, and 3D-MAD datasets. Effective performance was achieved, with Equal Error Rates (EERs) of 0% in the Replay-Attack and 3D-MAD databases and 5.83% in the CASIA-FASD database.

B. CNN-Based FAS Methods

This section discusses strategies that exclusively employ deep learning techniques or combine shallow machine learning and deep learning techniques based on their performance, strengths, and weaknesses.

This paper in [24] proposed a study utilizing CNNs to learn features with high discriminative ability, with the aim of enhancing FAS effectiveness. The OpenCV detector was employed for face detection, followed by the refinement of bounding boxes around facial landmarks to encompass the majority of facial regions. Images were resized to 128 × 128 pixels, and the Caffe toolbox was used for CNN training with a learning rate of 0.001, decay of 0.001, and momentum of 0.9. For classification, SVM with RBF kernel was employed. The proposed method was evaluated using Replay-Attack and CASIA datasets, achieving significant improvements over previous methods, with a 5% reduction in HTERs. However, the proposed method exhibited unsatisfactory performance in inter-test scenarios.

This paper in [10] proposed an FAS method based on a joint CNN-LSTM network, considering motion cues across video frames. This study extracted high discriminative properties and features from video frames using conventional CNN. The combination of these extracted features with Long Short-Term Memory (LSTM) was employed to capture temporal dynamics within video sequences. Additionally, Eulerian motion magnification was utilized to enhance facial expressions, while the attention mechanism in LSTM ensured the model focused on dynamic frames. The Adam optimizer was used for training the network with a learning rate of 0.00001. The proposed method was evaluated using Replay-Attack and MSU-MFSD datasets, achieving improved performance in generalization ability and fine-grained motion detection, with an HTER of 3.53% and an ACC of 96.47% in the Replay-Attack dataset. However, the experimental results indicated that dynamic variations in temporal features are beneficial for enhancing generalization ability.

This paper in [25] proposed an FAS method using CNN alongside a handcrafted technique (LBP-TOP) for feature extraction and classifier training. This method eliminates the need for detection, refinement, or enlargement steps. A cascading process for the LBP-TOP technique with CNN was performed to extract spatiotemporal features and obtain discriminative clues between genuine access and impersonation attacks. The proposed method was evaluated using the Replay-Attack and CASIA datasets, demonstrating significant potential for employing LBP-TOP with CNN for anti-spoofing purposes. An EER of 3.22% and HTER of 4.70% was achieved in the Replay-Attack dataset. Experimental results indicated competitive performance compared to previous methods.

This paper in [8] proposed a face anti-spoofing method regarding the deep local binary pattern. This study depends on extracting the handcrafted features from the convolutional responses related to tuned finely CNN model. First, the CNN has been finely tuned using a trained model of VGG-face. After that, the features of LBP are computed from the convolutional responses and combined in unique vectors of feature. These vectors are used by a SVM classifier in order to detect spoof faces. Related to samples, two databases are considered CASIA-FA and Replay-Attack. In the results, the investigation of the useful color space among HSV, RGB, and YCbCr spaces has been indicated. The experiments have delivered excellent results taking into account very promising results related to capabilities of generalization. The EER (%) is 0.1, and HTER (%) is 0.9 in Replay-Attack dataset. The EER (%) is 2.3 in CASIA-FA dataset.

This paper in [26] proposed a new approach for detecting face spoofing by extracting local features, specifically LBPs and simplified Weber local descriptors (SWLDs). The integration of Weber local descriptors (WLD) and LBP features ensures preservation of the local intensity information and edge orientations. The methodology involved two streams: an LBP-based CNN and a SWLD-based CNN. Initially, face regions were localized using Viola-Jones face detection. Subsequently, LBP and SWLD features were extracted by dividing the image into smaller parts. The features were encoded using CNN. Eventually, a non-linear SVM classifier with a radial basis function kernel was employed to determine whether a face was live or fake. The proposed method was evaluated using the Replay-Attack and CASIA datasets and achieved competitive results, with an EER and HTER of 2.62% and 2.14%, respectively, in the CASIA dataset and 0.53% and 0.69%, respectively, in the Replay-Attack dataset. This method's minimal complexity makes it suitable for real-time applications.

This paper in [27] proposed a new novel architecture consisting of a two-stream Frequent-Spatial-Temporal-Net for face anti-spoofing, which mainly combines the advantages of temporal, frequent, and spatial information. In addition, this study aims to achieve a multi-frame spectrum photo for the discriminative deep neural-network in order to distinguish between fake and live video. This study presents first the substantial properties related to the model. Then, elaborating the proposed network architecture is employed beside a strategy of learning in the pipeline. The implementation in MXNet and adoption of 4 blocks ResNet-v1b-18 for spatial part is used. While 0.3 rate of learning, 0.0001 weight decay, and 0.03 rate of Freq-Temp-Net stream learning are adopted. They evaluate the proposed method using three datasets: CASIA-SURF, OULU-NPU, and SiW datasets. Experimental results show a promising enhancement considering the proposed method besides the improved demonstrated ability of generalization compared with previous and existing approaches where the ACER (%) is 0.016 in CASIA-SURF, 1.1 in OULU, and 0.67 in SiW.

III. METHODOLOGY

To fulfill this study's objectives, we proposed designing a face anti-spoofing model capable of discriminating between real and fake faces with high accuracy. In Fig. 1, the proposed algorithm consists of five main stages: image pre-processing, Edge Detection, finding contours, extracting chainlets Features, and CNN model. The Chainlets were chosen as a motion-based descriptor due to their proven effectiveness in pedestrian detection and biometric ear recognition [11].

Chainlets is a concept that suggests that each object edge in an image can be represented as a histogram of chain codes, with each chain code representing the direction of connected edge segments. The label shifts between two absolute chain code-based Chainlets histograms can be used to determine the approximate rotation. Absolute chain code is dependent on the image's edge orientation, which results in different codes for rotated versions of objects. The frequency of occurrence of each of the eight directions, which depicts the shape of the object, is calculated by a chain code histogram. The picture sequence's Chainlets are first computed and concatenated with the sequence's first image, which can characterize motion direction and orientation.

A. Image Preprocessing

Before extracting Chainlets, the image needs to be preprocessed. Fig. 2 shows the stages of image processing. First, the image will converted to grayscale, and then GaussianBlur will be applied to reduce noise from an image. cv2.GaussianBlur(img, (5,5), 0).

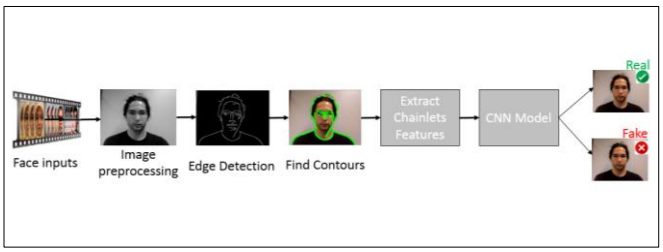


Fig. 1. The proposed algorithm.

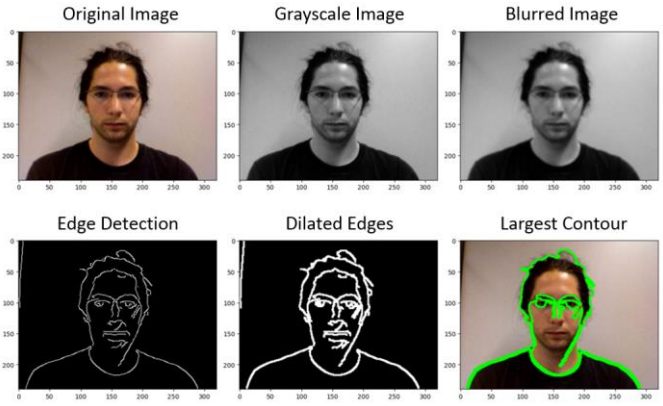


Fig. 2. Stages of image processing.

B. Edge Detection

The Canny edge detection algorithm [28] is a classic method that has proven its effectiveness over the years and remains widely utilized. Its approach is grounded in three main goals: (i) minimizing error rates, (ii) accurately locating edge points, and (iii) producing thin edges. We used canny edge detection with threshold values minVal and maxVal.

cv2.Canny(img, 50, 150)

Then the detected edges are dilated using a 3 x 3 kernel to close any gaps in the edges.

C. Finding Contours

Contours can be viewed as a plot or curve that links all the consistent points—typically found along the edges of a digital image—that exhibit similar colors or intensities. These connected points are associated with one another. Contours serve as useful tools for various applications, including structural analysis, object segmentation, object recognition, and others [29]. We used the find contours function from OpenCV and it has three parameters: the input image, contour retrieval mode, and contour approximation method.

cv2.findContours(img, cv2.RETR_EXTERNAL, cv2.CHAIN_APPROX_SIMPLE)

D. Extracting Chainlet Features

The representation of an image plays a crucial role in image processing and facial recognition. A key feature of an image is conveyed through the shapes created by the edges of an object. Histograms of Oriented Gradients HOG capture some of this information; however, it fails to account for important spatial relationships concerning the edges of an object. Specifically, HOG does not consider the connectedness of the edges, and the sequence and arrangement of orientation changes are not reflected in the histogram. The reason for using Chainlets as motion-based descriptor is that a face's appearance and shape can be effectively represented by the density of relative chain codes, which encode rotation-invariant edge detection. While this idea is related to HOG, it utilizes longer, connected edges, offering a more comprehensive and rotation-invariant representation of edge orientation [11].

We extract handcrafted features using the Chainlets which are built on the concept of Freeman chain codes [30] by making

them rotation-independent and more localized, thus mitigating the negative impacts of partial occlusions. It is characterized by local edge orientations that are aggregated into a global histogram sequence representing the entire image.

Chain code [31] is a method for documenting a sequence of edge points along a contour, indicating the direction of each edge in the sequence. These directions are categorized into eight distinct orientations. The notation progresses clockwise around the contour, starting from the first edge. Each subsequent edge's direction is represented by one of the eight chain codes. The direction associated with the 8-neighbor of an edge is illustrated in Fig. 3.

A chain code histogram measures how often each of the eight directions occurs, indicating the shape of the face. Fig. 4 illustrates the steps of extracting Chainlets features. Firstly, divide the binary image into cells, then compute the chain code for each one, compute chain code histogram and normalized, the all blocks' collection represents the Chainlets features. Finally, the extracted chainlets features are passed to the CNN model.

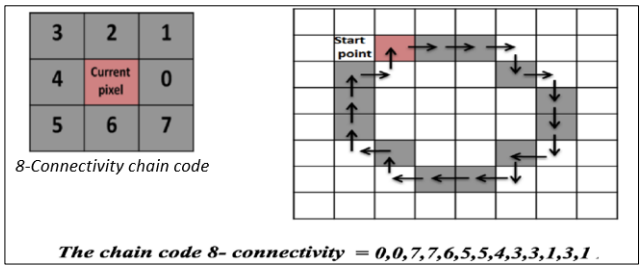


Fig. 3. Example of extracting chain code (clockwise).

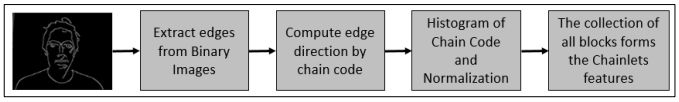


Fig. 4. Extracting chainlets features.

E. CNN Model

We build a CNN model for learning features. Our CNN model consists of three convolutional layers and 3 dense layers. The response normalization layers are applied to the outputs of the three Conv layers. Max pooling layers are utilized to generate the output for the three convolutional layers. Moreover, the 4th, 5th, and 6th layers are Dense layers. Further, we add the Dense layer with sigmoid activation to produce the binary output. We use Adam optimizer with a learning rate of 0.001. When compiling the model we use Binary Cross Entropy as the loss function to train the model for binary output, 1 is spoof face and 0 is real face.

IV. Experimental Results

We used a benchmark dataset, which is Replay-Attack. The Replay-Attack dataset contains 1,300 videos from 50 subjects, including real and fake face-spoofing attacks. For every subject, four genuine and eight fake sequences are obtained under various lighting terms with two support conditions (Fixed and Hand-held). Fig. 5 Shows example images from the Replay-Attack database. The images in the top row are genuine, while those in the bottom row are fake.

Fig. 5. Example of images from the Replay-Attack database.

The training set contains 93679 frames, the testing set 23395 frames, and the validation data size is 21055 frames. We evaluated the proposed model's performance to prove its effectiveness using the following metrics: Half Total Error Rate (HTER), Equal Error Rate (EER), and accuracy. The experimental results clearly demonstrate that the proposed Chainlets-based face anti-spoofing technique significantly surpasses state-of-the-art methods. This performance can be justified by the fact that integrating Chainlets as handcrafted features with deep learning will extract valuable features and produce a high-performance face anti-spoofing technique. Table I and Fig. 7 show that the proposed technique achieves the best performance compared with other state-of-art methods. Our model achieves high accuracy at 99.85%, the HTER is 0.15%, and the EER is 0.15%. Fig. 6 presents the training and validation accuracy and loss for the proposed algorithm.

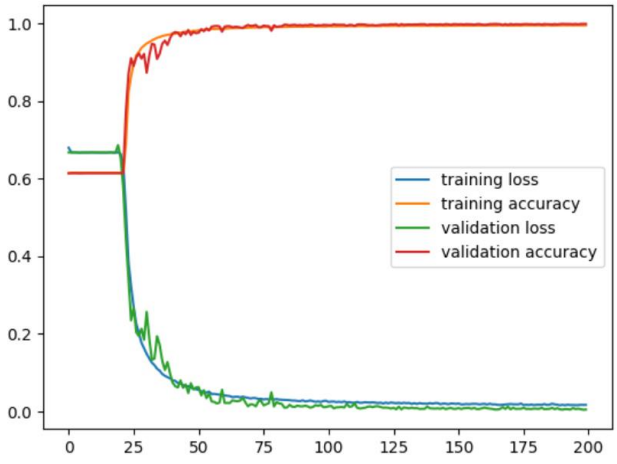


Fig. 6. Training and validation accuracy / loss curves.

TABLE I. Evaluation of Model's Performance Against State-of-the-art Methods

Approach	Replay-Attack Dataset		
	EER(%)	*HTER(%)*	*Accuracy(%)*
CNN + LBP-TOP [25]	3.22	4.70	-
DeepLBP + CNN + SVM [8]	0.1	0.9	-
CNN with LBP and WLD + SVM [26]	0.53	0.69	-
CNN-LSTM [10]	-	3.53	96.47
Chainlets + CNN (Our method)	**0.157**	**0.153**	**99.85**

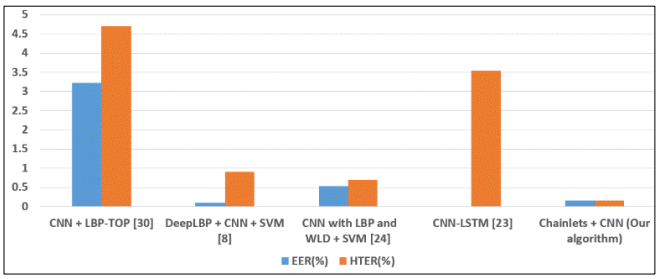


Fig. 7. The EER and HTER for the Replay-Attack dataset.

V. CONCLUSION

Given the current widespread use of the internet and social media, it is easy to obtain videos or pictures of individuals' faces, making most facial recognition systems vulnerable to spoofing attacks. An imposter can use such readily available materials to deceive facial authentication systems, thereby compromising their security and privacy. There are many attack types with different scenarios, so until now, there is no outstanding technique for face anti-spoofing. In our proposed algorithm, we depend on both handcrafted features (Chainlets) and deep learning (CNN) to obtain more robust features and high accuracy in the face anti-spoofing system. Thorough experiments were conducted on the Replay-Attack dataset to assess the effectiveness of the proposed Chainlets-based face anti-spoofing method. Our approach achieved perfect discrimination between real faces and spoof faces. The EER is 0.157%, the HTER is 0.153%, and the accuracy is 99.85%, which is better than the state-of-the-art methods. However, this work does not address the detection of 3D mask attacks. This aspect will be considered in future work.

REFERENCES

[1] S. P. Borra, N. Pradeep, N. Raju, S. Vineel, and V. Karteek, "Face Recognition based on Convolutional Neural Network," International Journal of Engineering and Advanced Technology, vol. 9, May 2020, doi: 10.35940/ijeat.D6658.049420.

[2] R. G. Bhati and S. Gosavi, "A SURVEY ON FACE ANTI-SPOOFING METHODS," Jan. 2024, Accessed: Oct. 07, 2024. [Online]. Available: http://localhost:8080/xmlui/handle/123456789/16939

[3] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep Learning for Face Anti-Spoofing: A Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 5, pp. 5609–5631, May 2023, doi: 10.1109/TPAMI.2022.3215850.

[4] V. Sundharam, A. Sarkar, and A. L. Abbott, "Re-evaluation of Face Anti-spoofing Algorithm in Post COVID-19 Era Using Mask Based Occlusion Attack," arXiv.org. Accessed: Oct. 09, 2024. [Online]. Available: https://arxiv.org/abs/2408.13251v1

[5] Y. Wang, X. Song, T. Xu, Z. Feng, and X.-J. Wu, "From RGB to Depth: Domain Transfer Network for Face Anti-Spoofing," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4280–4290, 2021, doi: 10.1109/TIFS.2021.3102448.

[6] Z. Ming, M. Visani, M. M. Luqman, and J.-C. Burie, "A Survey on Anti-Spoofing Methods for Facial Recognition with RGB Cameras of Generic Consumer Devices," Journal of Imaging, vol. 6, no. 12, Art. no. 12, Dec. 2020, doi: 10.3390/jimaging6120139.

[7] T. Shen, Y. Huang, and Z. Tong, "FaceBagNet: Bag-Of-Local-Features Model for Multi-Modal Face Anti-Spoofing," presented at the Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2019, pp. 0–0. Accessed: Apr. 09, 2022. [Online]. Available: https://openaccess.thecvf.com/content_CVPRW_2019/html/CFS/Shen_FaceBagNet_Bag-Of-Local-Features_Model_for_Multi-Modal_Face_Anti-Spoofing_CVPRW_2019_paper.html

[8] L. Li and X. Feng, "Face Anti-spoofing via Deep Local Binary Pattern," in Deep Learning in Object Detection and Recognition, X. Jiang, A. Hadid, Y. Pang, E. Granger, and X. Feng, Eds., Singapore: Springer, 2019, pp. 91–111. doi: 10.1007/978-981-10-5152-4_4.

[9] L. Feng et al., "Integration of image quality and motion cues for face anti-spoofing: A neural network approach," Journal of Visual Communication and Image Representation, vol. 38, pp. 451–460, Jul. 2016, doi: 10.1016/j.jvcir.2016.03.019.

[10] X. Tu, H. Zhang, M. Xie, Y. Luo, Y. Zhang, and Z. Ma, "Enhance the Motion Cues for Face Anti-Spoofing using CNN-LSTM Architecture," arXiv:1901.05635 [cs], Jan. 2019, Accessed: Feb. 17, 2022. [Online]. Available: http://arxiv.org/abs/1901.05635

[11] A. Ahmad, D. Lemmond, and T. E. Boult, "Chainlets: A New Descriptor for Detection and Recognition," in 2018 IEEE Winter Conference on Applications of Computer Vision (WACV), Mar. 2018, pp. 1897–1906. doi: 10.1109/WACV.2018.00210.

[12] A. Anjos, M. M. Chakka, and S. Marcel, "Motion - based counter - measures to photo attacks in face recognition," IET biom., vol. 3, no. 3, pp. 147‐158, Sep. 2014, doi: 10.1049/iet-bmt.2012.0071.

[13] K. Kollreider, H. Fronthaler, and J. Bigun, "Non-intrusive liveness detection by face images," Image and Vision Computing, vol. 27, no. 3, pp. 233–244, Feb. 2009, doi: 10.1016/j.imavis.2007.05.004.

[14] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in 2009 International Conference on Image Analysis and Signal Processing, Apr. 2009, pp. 233–236. doi: 10.1109/IASP.2009.5054589.

[15] M. M. Zarachoff, A. Sheikh-Akbari, and D. Monekosso, "Chainlet-Based Ear Recognition Using Image Multi-Banding and Support Vector Machine," Applied Sciences, vol. 12, no. 4, Art. no. 4, Jan. 2022, doi: 10.3390/app12042033.

[16] C. Nagpal and S. R. Dubey, "A Performance Evaluation of Convolutional Neural Networks for Face Anti Spoofing," in 2019 International Joint Conference on Neural Networks (IJCNN), Jul. 2019, pp. 1–8. doi: 10.1109/IJCNN.2019.8852422.

[17] M. Zhang, K. Zeng, and J. Wang, "A Survey on Face Anti-Spoofing Algorithms," Journal of Information Hiding and Privacy Protection, vol. 2, no. 1, pp. 21–34, 2020, doi: 10.32604/jihpp.2020.010467.

[18] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face anti-spoofing based on color texture analysis," in 2015 IEEE International Conference on Image Processing (ICIP), Sep. 2015, pp. 2636–2640. doi: 10.1109/ICIP.2015.7351280.

[19] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face Spoofing Detection Using Colour Texture Analysis," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1818–1830, Aug. 2016, doi: 10.1109/TIFS.2016.2555286.

[20] J. Määttä, A. Hadid, and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis," in 2011 International Joint Conference on Biometrics (IJCB), Oct. 2011, pp. 1–7. doi: 10.1109/IJCB.2011.6117510.

[21] T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection using 3D structure recovered from a single camera," in 2013 International Conference on Biometrics (ICB), Jun. 2013, pp. 1–6. doi: 10.1109/ICB.2013.6612957.

[22] X. Sun, L. Huang, and C. Liu, "Multispectral face spoofing detection using VIS–NIR imaging correlation," Int. J. Wavelets Multiresolut Inf. Process., vol. 16, no. 02, p. 1840003, Mar. 2018, doi: 10.1142/S0219691318400039.

[23] G. Pan, L. Sun, Z. Wu, and Y. Wang, "Monocular camera-based face liveness detection by combining eyeblink and scene context," Telecommun Syst, vol. 47, no. 3, pp. 215–225, Aug. 2011, doi: 10.1007/s11235-010-9313-3.

[24] J. Yang, Z. Lei, and S. Z. Li, "Learn Convolutional Neural Network for Face Anti-Spoofing," arXiv:1408.5601 [cs], Aug. 2014, Accessed: Mar. 25, 2022. [Online]. Available: http://arxiv.org/abs/1408.5601

[25] M. Asim, Z. Ming, and M. Y. Javed, "CNN based spatio-temporal feature extraction for face anti-spoofing," in 2017 2nd International Conference

on Image, Vision and Computing (ICIVC), Jun. 2017, pp. 234–238. doi: 10.1109/ICIVC.2017.7984552.

[26] M. Khammari, "Robust face anti-spoofing using CNN with LBP and WLD," IET Image Processing, vol. 13, no. 11, pp. 1880–1884, 2019, doi: 10.1049/iet-ipr.2018.5560.

[27] Y. Huang, W. Zhang, and J. Wang, "Deep Frequent Spatial Temporal Learning for Face Anti-Spoofing," arXiv:2002.03723 [cs, eess], Jan. 2020, Accessed: Mar. 25, 2022. [Online]. Available: http://arxiv.org/abs/2002.03723

[28] E. A. Sekehravani, E. Babulak, and M. Masoodi, "Implementing canny edge detection algorithm for noisy image," Aug. 12, 2021, Social Science Research Network, Rochester, NY: 3904360. Accessed: Oct. 22, 2024. [Online]. Available: https://papers.ssrn.com/abstract=3904360

[29] Sakshi and V. Kukreja, "Segmentation and Contour Detection for handwritten mathematical expressions using OpenCV," in 2022 International Conference on Decision Aid Sciences and Applications (DASA), Mar. 2022, pp. 305–310. doi: 10.1109/DASA54658.2022.9765142.

[30] H. Freeman, "On the Encoding of Arbitrary Geometric Configurations," IRE Transactions on Electronic Computers, vol. EC-10, no. 2, pp. 260–268, Jun. 1961, doi: 10.1109/TEC.1961.5219197.

[31] J. Sun and X. Wu, "Shape Retrieval Based on the Relativity of Chain Codes," in Multimedia Content Analysis and Mining, N. Sebe, Y. Liu, Y. Zhuang, and T. S. Huang, Eds., Berlin, Heidelberg: Springer, 2007, pp. 76–84. doi: 10.1007/978-3-540-73417-8_14.

DSTC-Sum: A Supervised Video Summarization Model Using Depthwise Separable Temporal Convolutional

M. Hamza Eissa[1], Hesham Farouk[2], Kamal Eldahshan[3], Amr Abozeid[4]
Department of Mathematics-Faculty of Science, Al-Azhar University, Cario, Egypt[1, 3, 4]
Department of Computers and Systems Electronics Research Institute, Cario, Egypt[2]
Department of Computer Science-College of Computer and Information Sciences, Jouf University, Saudi Arabia[3, 4]

***Abstract*—The exponential growth in video content has created a critical need for efficient video summarization techniques to enable faster and more accurate information retrieval. Video summarization has excellent potential to simplify the analysis of large video databases in various application areas ranging from surveillance, education, entertainment, and research. DSTC-Sum, a novel supervised video summarization model, is proposed based on Depthwise Separable Temporal Convolutional (DSTC). Leveraging the superior representational efficiency of DSTCN, the model addresses computational challenges and training inefficiencies encountered in traditional recurrent architectures such as Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTMs). Additionally, this approach reduces computational overhead and memory usage. DSTC-Sum achieved state-of-the-art performance on two commonly used benchmark datasets, TVSum and SumMe, and outperformed all previous methods with F-scores by 1.8% and 3.33%, respectively. To validate the model's generality and robustness, the model was further tested on the YouTube and Open Video Project (OVP) datasets. The proposed model did slightly better on these datasets than several popular techniques, with F scores of 60.3 and 58.5, respectively. Finally, these findings confirm that this model captures long-term temporal dependencies and produces high-quality video summaries across all types of videos.**

***Keywords*—Video summarization; depthwise separable temporal convolutional; video processing; deep learning**

I. INTRODUCTION

In recent years, the proliferation of video capture devices and their declining costs have led to an unprecedented increase in video data volume. There are many kinds of visual data, but the video is one of the most significant. It is impossible to expect people to be able to see these videos and extract relevant information from them due to the vast amount of data included inside them. According to the Cisco Visual Networking Index report [1], it will take a human more than 5 million years to watch all the movies published on the Internet each month by 2022. Because of this, developing computer vision systems that effectively browse vast amounts of video data is becoming an increasingly important goal. Video summarizing has emerged as a potential technique that may assist viewers in dealing with the massive amount of data in the video.

When given an original video as input, video summarizing produces a more condensed version that still contains all the essential information from the original. Video summarizing has numerous potential applications (for example, indexing, browsing, and surveillance) [2, 3]. Summary videos may also be helpful for various downstream video analysis activities. For instance, running other analytic algorithms on shorter videos, such as action recognition, can be done more quickly.

Recent methodologies [4-6] address video summarization as a sequence labeling challenge, focusing on identifying and extracting key video segments efficiently. The Recurrent Neural Networks (RNNs) with Long Short-Term Memory (LSTM) have been modified as an RNN variant to address this issue [7]. The LSTM model has a one-to-one correspondence between each time step and video frame. The LSTM model generates an output binary value at each time step, which indicates whether this frame was chosen for inclusion in the summary video. The LSTM methodology has the advantage of recording the long-range structural connections between frames. However, some limitations are embedded into these LSTM-based models. In LSTM, the computation typically proceeds from left to right. It indicates that the model can only perform one frame at a time, with each frame having to wait until the processing of the frame has been completed before it can begin. Even if there is bi-directional LSTM (Bi-LSTM) [8], the computation still has the same issue when using Bi-LSTM in either manner. Because of the sequential nature of the LSTM computation, it is impossible to readily parallelize it to make the most of the GPU resources. As temporal classifiers, sequence-based architectures such as RNN and LSTM are computationally costly, memory-heavy, and challenging to train. Temporal Convolutional Networks (TCNs) [9, 10] have recently demonstrated promising performance in video summarizing tasks.

In this work, to solve the abovementioned challenges, the DSTC-Sum model was designed based on the Depthwise Separable Temporal Convolutional Network (DSTCN), which efficiently extracts long-term temporal dependencies and local features. Unlike RNN-based models, which are computationally inefficient, sequential in nature, and reliant on domain-specific annotations, TCNs allow the addition of new layers while being computationally less expensive, quicker to train, and lightweight [11]. This makes traditional methods like RNNs and LSTMs unsuitable for large-scale datasets and

longer videos. The DSTC-Sum model leverages Depthwise Separable Convolutions (DSC) to improve feature representation while requiring low computation and memory [12]. Its scalable and dataset-agnostic design ensures efficient extraction of temporal dependencies and enhances generalizability across diverse video datasets. The benefits of DSTCN include the use of large kernels to capture long-range relationships while limiting the number of overall parameters, resulting in compact models. Additionally, large adjacent kernels effectively extract both global and local temporal features. By enabling simultaneous analysis of all video frames through GPU parallelization, DSTC-Sum addresses the challenges of computational inefficiency, scalability, and poor temporal modeling, achieving superior performance compared to current video summarization techniques.

We conducted comprehensive evaluations on two benchmark datasets, TVSum and SumMe. In the standard-supervised setting, the DSTC-Sum model achieved an F-score of 48.7%, which increased to 52.8% with data augmentation. On the TVSum dataset, the model attained an F-score of 61.2% in the standard setting, improving to 62.9% with augmentation. These results demonstrate the superior performance of the DSTC-Sum model compared to state-of-the-art techniques, with notable improvements of 1.8% and 3.33% on the two datasets, respectively. This highlights the model's enhanced ability to accurately predict the importance of video segments and generate high-quality summaries. The DSTC-Sum model's effective capture of temporal dependencies and key factors sets it apart, underscoring its potential for broader video summarization applications. To further evaluate the model's generalizability and robustness, we extended our experiments to two additional datasets: YouTube and the OVP. The model demonstrated superior performance on these datasets, achieving F-scores of 60.3% and 58.5%, respectively, outperforming several state-of-the-art techniques. These results underscore the model's effectiveness in capturing long-term temporal dependencies and generating high-quality summaries across various video genres.

The paper is organized as follows: Section II briefly discusses related studies on deep learning-based video summarizing approaches. Section III introduces our suggested DSTC-Sum model. Section IV discusses the model implementation and experimental findings. Lastly, the paper's conclusion is presented in Section V.

II. Related Work

Video summarization presents the challenge of selecting the most relevant segments of a video for inclusion in the summary and accurately identifying and extracting those segments from the entire video. This process requires a comprehensive understanding of the video content to ensure the summary represents the original video's essential aspects. In the early stage of video summarizing research, most approaches focus on a particular category of videos. For instance, the significance of a specific occurrence during a video segment of a show airing a sporting event can be easily determined by referring to the regulations governing that sport. [13]. In addition, certain sports games, such as baseball and American football, have a specific structure that makes extracting crucial segments of the game's action easier. Similarly, characters who feature in movies can also be domain knowledge [14]. In these areas, video summaries can be generated with the assistance of many kinds of metadata [15, 16]. Videos focusing on the creator alone are another fascinating example of video domains. A video summarization approach has been proposed using specific domain knowledge that can be considered a set of predetermined objects [17]. This approach aims to summarize videos in a manner that considers the domain's specifics. Newer methods in this general area use supervised learning techniques to incorporate domain knowledge. For instance, [18] offered to summarize a video with the primary focus on a particular event and use an event classifier's confidence score to measure a video segment's significance. However, due to the heavy reliance that such methods have on specific industry expertise, it is nearly impossible to generalize them to other types of writing.

When given an original video as input, the video summarizing goal is to produce a condensed version highlighting the most vital information from the original. There have been many other ways that this issue has been represented, such as in a video overview [19], time-lapses [20-22], montage [23, 24], and storyboards [25-29]. Our work is most closely associated with storyboards, consisting of a selection of a few typical frames of video that outline important events throughout an entire film. Storyboard-based summarization can produce two different kinds of outputs: keyframes [30], in which specific isolated frames are selected for forming the summary of the video, as well as key shots [31, 32], a method for generating a resume that considers a series of successive correlated frames contained within a temporal slot. Both types of outputs are referred to as keyframes.

Initial efforts in a video summarizing primarily rely on hand-crafted heuristics. Most of these methods do not require supervision. They specify a variety of heuristics to reflect the significance of the frames' representativeness [33-39], and they utilize the significance scores to select representative frames to form the video summary. Recent research has investigated supervised learning methodologies for video summaries [40-42]. These methods use video training data and the ground-truth summaries humans create for those videos. These supervised learning algorithms perform better than the early work on unsupervised methods because they can acquire sophisticated semantic knowledge that humans implicitly use to construct summaries.

Deep learning approaches have recently been popular for vision tasks, especially video summarization [43-45]. The foundation of LSTM is the theory that it can effectively capture long-range dependencies between video frames, which are necessary for creating insightful summaries. Zhang et al. [32] model the variable range dependency with two LSTMs and consider the video summarizing assignment of a problem of structured prediction based on data that can be sequential. Two Long Short-Term Memory (LSTM) networks are employed to analyze video sequences comprehensively. One LSTM is dedicated to processing the sequences in the forward direction, capturing the temporal dynamics as they unfold chronologically. Meanwhile, the other LSTM handles sequences in the reverse direction, allowing for a holistic

understanding of the video content from both temporal perspectives. They incorporate a determinantal point process model to improve further the subset selection's diversity [9, 46]. Mahasseni and colleagues present an unsupervised generative adversarial system consisting of the discriminator and summarizer [6]. The summarizer, an LSTM variational autoencoder, selects frames from the video and decodes the output to reconstruct the video. The discriminator is another LSTM network that gains the ability to distinguish between candidates by differentiating between the input video and its reconstruction. It accomplishes this by examining the variations between the two. They also incorporate a keyframe regularization into their algorithm, expanding it to supervise learning.

Despite significant advancements in video summarization, several gaps still need to be discovered in existing studies that necessitate further investigation. Prior approaches, such as those based on Recurrent Neural Networks (RNNs) and their variants like Long Short-Term Memory (LSTM) networks and Gated Recurrent Units (GRUs), have proven effective in capturing temporal dependencies but are hindered by high computational costs, memory intensiveness, and sequential processing limitations, making them less scalable for larger datasets or longer video sequences. Additionally, evaluations in previous research are often confined to limited datasets, such as TVSum and SumMe, which do not adequately represent the diversity of real-world video content. The reliance on domain-specific annotations and handcrafted features further restricts the generalizability of these methods. While Temporal Convolutional Networks (TCNs) offer an alternative by addressing some of these limitations, there remains a need for lightweight, scalable architectures that combine computational efficiency with robust temporal modeling capabilities. This study addresses these gaps by proposing DSTC-Sum, a novel video summarization model based on Depthwise Separable Temporal Convolutions, which enhances efficiency and scalability, demonstrates generalizability across diverse datasets, and outperforms state-of-the-art methods in terms of F-scores and computational performance, thereby contributing to the advancement of efficient and robust video summarization techniques.

III. The Proposed Approach

This section introduces the DSTC-Sum model to summarize the input videos. Fig. 1 depicts the structured steps of the DSTC-Sum. First, the feature descriptors are generated from the input video frames using VGG16 [47]. Then, these feature vectors are fed into a series of Depthwise Separable Temporal Convolutional Blocks (DSTCB) that predict a score for each frame. Suppose that X represents a feature vector as $X_{1:n} = \{f_1, f_2, f_3, \ldots, f_n\}$. The model goal is to assign a corresponding score for each frame $Y_{1:n} = \{y_1, y_2, y_3, \ldots, y_n\}$, where n is the frame number, which varies depending on the video.

In the following subsections, we will describe the baseline model VGG16 and then explain the DSTCB, which is built using residual depthwise dilated blocks.

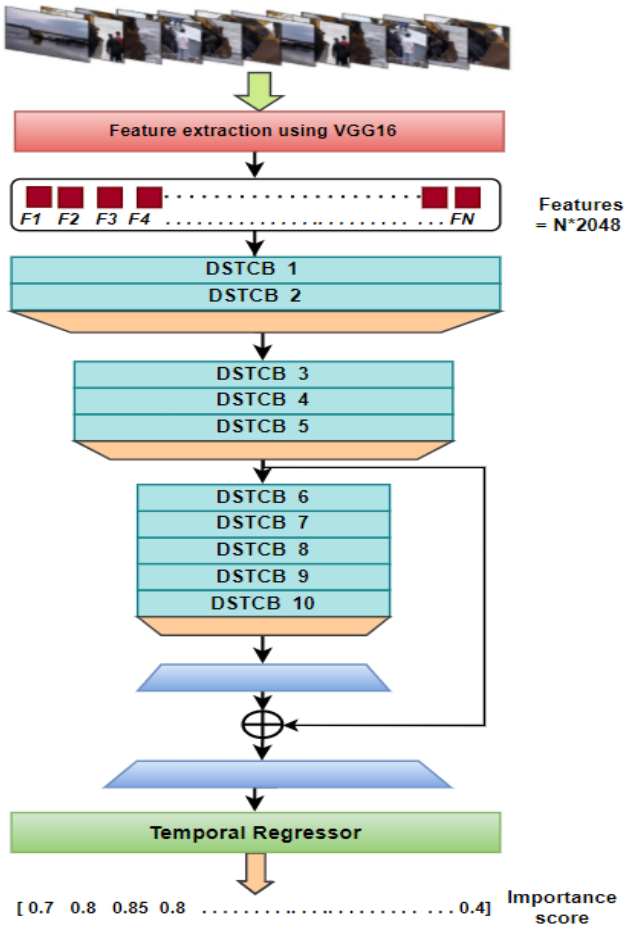


Fig. 1. The detailed structure of the DSTC-Sum.

A. Feature Extraction using VGG16

We start by feeding an input video into a feature extractor. The feature extractor module comprises the pre-trained first ten convolution layers of the VGG16 [47]. Because of its high generalization capabilities, the VGG16 is commonly employed as a feature extractor for many deep-learning models. We applied VGG16 to extract the basic features for the suggested model.

B. Depthwise Separable Temporal Convolutional Blocks (DSTCB)

Temporal convolutional network (TCN) is a CNN variant utilized in sequencing-based tasks and has recently outperformed alternative recurrent models like LSTM and gated recurrent units (GRUs) [48]. TCN enables temporal solid information extraction from sequential data [49]. TCNs aim to encapsulate temporal relationships with a broader receptive field. To capture large receptive fields, either a) dilations on consecutive TCN layers or b) big standard neighboring kernels are used. Dilated convolutions on consecutive layers help capture a broad temporal representation while reducing the number of training parameters. However, when additional layers are added, the kernels become increasingly sparse, resulting in the gridding artifacts issue.

When the dilation parameter increases at higher levels, the input data sample becomes increasingly sparse (Gridding Artifacts issue). As a result, local dependencies between neighboring pixels are lost, and the output layer is not temporally associated with their input sample. DS-TCN [10] proposes techniques for methodical aggregation of convolution layers in the following layers with constant or configurable dilation rates to address the issue of gridding artifacts. Therefore, each DSTCB consists of stacked 'N' depthwise dilated 1d temporal convolution layers.

Fig. 2 depicts the detailed construction of the DSTCB. All output levels receive a combined input from the preceding layer with various dilation rates. Each output layer is combined along a channel dimension to produce the NxC dimension. The cross-channel correlation is then estimated using a pointwise convolution procedure that decreases the dimensions of the channel from N×C to C from the concatenated data. This output is normalized using layer normalization [50]. To maintain adequate gradient flow, we also employ residual connections. Finally, we employ ReLU.

The DSTCB has various advantages:

1) Because depthwise convolutions are computationally efficient, we may employ huge-size kernels. As a result, we may employ lower dilations in conjunction with lengthy kernels to capture lengthy temporal features.

2) Scale information is recorded in each layer with varied dilation rates. Multi-scale information is contained in concatenated pointwise convolution. As a result, the model can tolerate different temporal durations for each event.

3) Stacking the outputs of all layers aids in data smoothing and eliminates the artifact effect caused by gridding. This method enables the model to acquire more detailed local features.

4) The receptive field can temporally extend without boosting the parameters by adjusting the block's dilation rates.

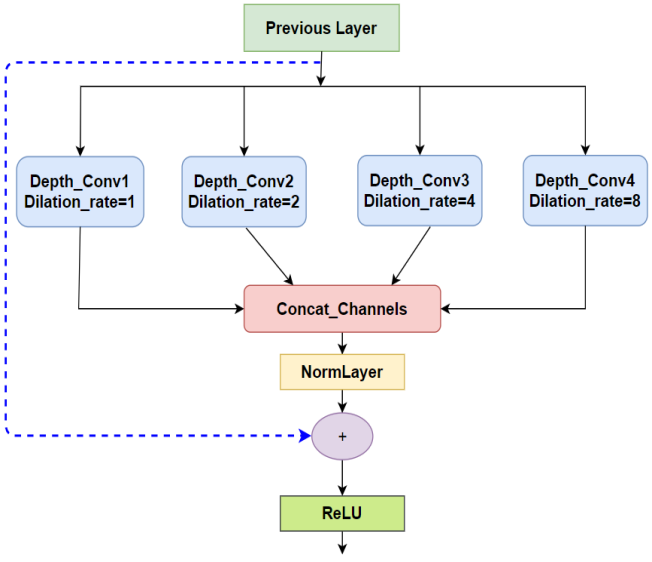


Fig. 2. The detailed construction of the DSTCB.

A temporal max-pooling was added after each DSTCB. Next, we take the output of DSTCB5, perform a 1x1 convolution layer and batch normalization, and then combine it with the production of deconv1 by element-wise addition. This merger is equivalent to the skip-connection in study [9]. Skip connections mix coarse and fine feature maps in semantic segmentation to acquire richer visual characteristics. This skip connector will also be valuable in video summarization, as it will aid in the recapture of temporal information needed for summary. Then, we do another temporal deconvolution to obtain the final representation of length N. The generated representation is fed into the temporal regressor network as input. Finally, the Regressor generates a collection of frame-level scores that represent the importance of the frames.

IV. EXPERIMENTS

This section provides an overview of the datasets, implementation details, and evaluation metrics used to assess the DSTC-Sum model. It outlines the training setup, key parameters, and performance criteria. The section concludes with a presentation and discussion of the DSTC-Sum results, highlighting its strengths, limitations, and potential areas for improvement.

A. Evaluation Datasets

The benchmark datasets for testing and evaluating our DSTC-Sum model are SumMe [51] and TVSum [52]. Table I shows several features of the target datasets. The SumMe benchmark dataset consists of 25 videos in a video benchmark dataset that has numerous topics and occurrences (like holidays, Sports, etc.). The videos on SumMe can vary between 1.5 to 6.5 minutes. The TVSum dataset consists of 50 videos from the TRECVid Multimedia Event Detection (MED) challenge [53]. The videos are divided into different categories, e.g., 'saucing up a sandwich,' 'showing dog,' and so on. This dataset houses videos that range from one minute to five minutes.

Previous research in [32] suggests that more videos should be added to the datasets to minimize the difficulty of training a deep neural network with a few manually annotated examples. Therefore, we bolster the existing training data by incorporating 39 videos from the YouTube dataset [54] in addition to 50 videos from the OVP dataset [54, 55]. The YouTube dataset includes some videos, including cartoons, sports, news, etc. OVP has videos in many different genres, such as documentaries. Because the multiple datasets provide ground-truth annotations in various formats, we adapt a training process that uses summaries based on keyframes to construct a unified set of ground truths for each video included in the datasets, as in study [32, 56].

TABLE I. OVERVIEW OF THE TARGET DATASETS

Datasets	Videos	Annotations	Duration (Min)
TVSum	50	20	2-10
SumMe	25	15-18	1-6
YouTube	39	5	1-10
OVP	50	5	1-4

B. Implementation and Training Details

The model is implemented using PyTorch, with the number of DSTCB blocks set to ten. Each DSTCB block consists of four depthwise one-dimensional temporal convolution layers, where the dilation parameter is doubled in each layer. We adopt the hyperparameters used in MS-TCN [12] to ensure a fair comparison with other methods. The Adam optimizer is employed with a learning rate of 0.0005. The parameters for the smoothing loss function are set as follows: smoothing λ=0.15 and threshold τ=4.

We downsample the videos uniformly to 2 frames per second for feature extraction, as done in [2]. We select representative frames from each video to reduce the final feature dimension to 320. Training frames are scaled to maintain consistent spatial dimensions across all videos. The DSTC-Sum model can handle longer videos and videos of varying lengths. We use the output from the maxpool5 layer of a pre-trained VGG16 model [47] as the feature descriptor for each frame, with a feature dimension of 512. Notably, our model is flexible and can work with any feature representation.

During training, we set the batch size to 5, the learning rate to 10^{-3}, and the momentum to 0.9. The Stochastic Gradient Descent (SGD) optimizer was used to train the DSTC-Sum model.

C. Evaluation Metrics

We evaluate the DSTC-Sum use of a keyshot-based metric, as in [6, 32]. Suppose that S_G is the ground-truth summary and S_E is the extracted summary for video V. We define the precision (P) and recall (R) by utilizing the temporal overlap between them as in Eq. (1) and (2):

$$P = \frac{|S_E \cap S_G|}{|S_E|} \quad (1)$$

$$R = \frac{|S_E \cap S_G|}{|S_G|} \quad (2)$$

As a final step, the evaluation is carried out utilizing the F-score, which is calculated in Eq. (3):

$$F = \frac{2P \times R}{P + R} \times 100 \quad (3)$$

D. Performance Analysis and Discussion

The performance of various summarization techniques on the SumMe dataset is outlined in Table II and visualized in Fig. 3. The proposed DSTC-Sum method significantly outperforms other state-of-the-art techniques across almost all parameters. Specifically, in the standard-supervised setting, DSTC-Sum achieves an F-score of 48.7, higher than the following best technique, SUM-FCN, which scores 47.5. DSTC-Sum shows an even more substantial improvement in the augmented setting, achieving an F-score of 52.8 compared to SUM-FCN's 51.1. This consistent outperformance highlights the effectiveness of DSTC-Sum in summarizing videos within the SumMe dataset.

Similarly, the results on the TVSum dataset, presented in Table III and Fig. 4, demonstrate the superior performance of the DSTC-Sum approach. DSTC-Sum achieves an F-score of 61.2 in the standard-supervised setting, edging out with close competitors like M-AVS and DHAVS, which scored 61.0 and 60.8, respectively. The augmented setting further showcases the dominance of DSTC-Sum, with an F-score of 62.9, significantly higher than M-AVS's 61.8 and SUM-GAN*sup*'s 61.2. These results underline the robustness and efficiency of DSTC-Sum in producing high-quality video summaries on the TVSum dataset.

TABLE II. SUMMARIZATION PERFORMANCE (F-SCORE) COMPARISON ON THE SUMME BENCHMARK DATASET BETWEEN DSTC-SUM AND OTHER TECHNIQUES USING DIFFERENT PARAMETERS

Technique	Standard-Supervised	Augmented
DPP-LSTM [5]	38.6	42.9
SUM-GAN*sup* [6]	41.7	43.6
Li et al. [57]	43.1	–
M-AVS [58]	44.4	46.1
DHAVS [59]	45.6	46.5
SUM-FCN [9]	47.5	51.1
DSTC-Sum	**48.7**	**52.8**

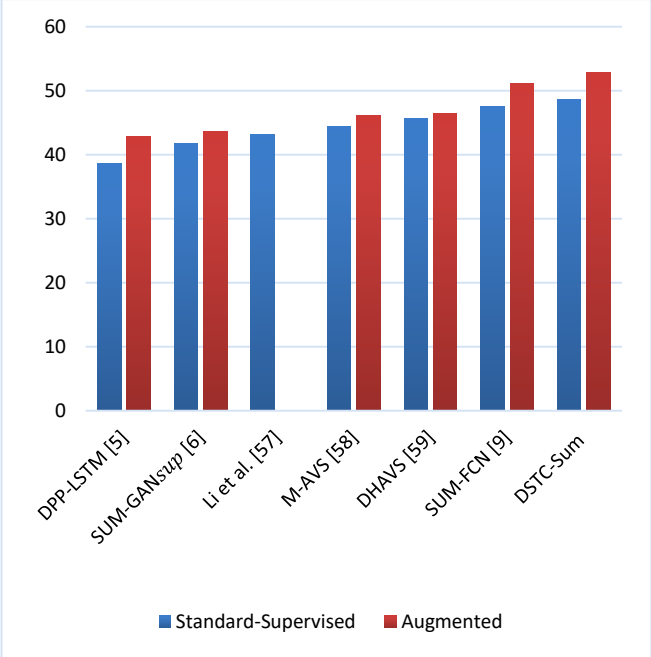


Fig. 3. Summarization performance (F-score) comparison on the SumMe dataset.

TABLE III. SUMMARIZATION PERFORMANCE (F-SCORE) COMPARISON ON THE TVSUM DATASET BETWEEN DEPTHTEMPORAL-SUM AND OTHER TECHNIQUES USING DIFFERENT PARAMETERS

Technique	Standard-Supervised	Augmented
DPP-LSTM [5]	54.7	59.6
SUM-GAN*sup* [6]	56.3	61.2
Li et al. [57]	52.7	–
SUM-FCN [9]	56.8	59.2
M-AVS [58]	61.0	61.8
DHAVS [59]	60.8	61.2
DSTCN-Sum	**61.2**	**62.9**

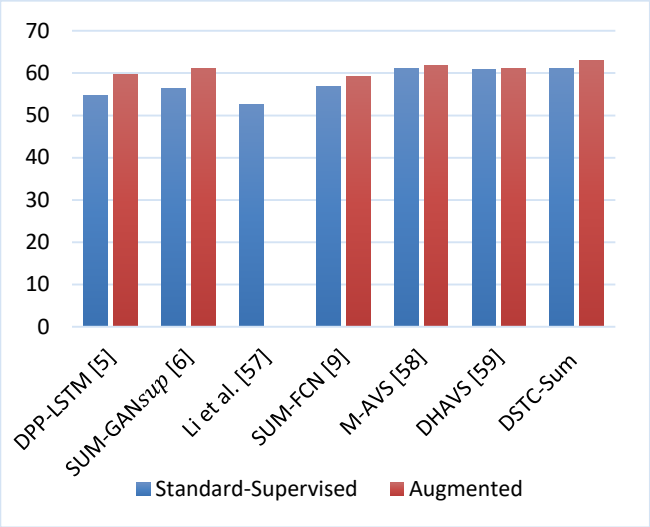


Fig. 4. Summarization performance (F-score) comparison on the SumMe dataset.

The DSTC-Sum methodology consistently demonstrates superior performance in video summarization tasks compared to existing state-of-the-art techniques. Its notable effectiveness, especially in augmented settings, indicates its high efficiency in improving summarization quality, as evidenced by the F-score metrics. The robust applicability of DSTC-Sum across different datasets further suggests its potential for wide adoption in video summarization applications. The implications of these findings are significant for the field of video summarization. By providing a method that consistently outperforms existing techniques, DSTC-Sum can enhance various applications, from creating more engaging video highlights for entertainment to improving the efficiency of video data management in professional and educational contexts. Moreover, the scalability and adaptability of DSTC-Sum means it could be integrated into various platforms and devices, including mobile applications and cloud-based services, thereby broadening its impact.

E. Extended Experiments

To further evaluate the effectiveness and generalizability of the DSTC-Sum model, we extended our experiments to include two additional benchmark datasets: YouTube and OVP (Open Video Project). These datasets were chosen due to their diverse content types, which pose unique challenges to video summarization models. By expanding our experimental scope, we aim to demonstrate the robustness of the proposed model across a broader range of video genres and characteristics. The DSTC-Sum model was fine-tuned on both datasets using the same configuration as in prior experiments. Specifically, the model architecture consisted of 10 Depthwise Separable Temporal Convolutional Blocks (DSTCB), with 4 depthwise convolutional layers per block. The Adam optimizer with a learning rate of 0.0005 was utilized, and the number of training epochs was adjusted based on the dataset size to prevent overfitting.

We applied data augmentation techniques such as random cropping and video flipping during training to improve generalization. Like the TVSum and SumMe datasets, the extracted frame-level features were fed into the model for training and evaluation. We benchmarked the model against several state-of-the-art video summarization models, including SUM-GAN, MS-TCN, and DPP-LSTM.

Table IV summarizes the YouTube dataset results. The proposed DSTC-Sum model achieved an F-score of 60.3%, outperforming the following best method, MS-TCN, which achieved an F-score of 58.6%. This improvement can be attributed to the model's ability to capture both long-term and short-term temporal dependencies, which is essential for summarizing the diverse content found in YouTube videos.

TABLE IV. PERFORMANCE COMPARISON OF VIDEO SUMMARIZATION METHODS ON THE YOUTUBE DATASET, MEASURED USING F-SCORE, PRECISION, AND RECALL

Technique	F-score (%)	Precision	Recall
DPP-LSTM [5]	55.2	54.8	55.7
SUM-GAN*sup* [6]	56.3	55.9	56.8
SUM-FCN [9]	58.6	57.9	59.2
DSTC-Sum	**60.3**	**60.1**	**60.6**

TABLE V. PERFORMANCE COMPARISON OF VIDEO SUMMARIZATION METHODS ON THE OVP DATASET, MEASURED USING F-SCORE, PRECISION, AND RECALL

Technique	F-score (%)	Precision	Recall
DPP-LSTM [5]	52.7	51.9	53.5
SUM-GAN*sup* [6]	56.3	55.4	57.0
SUM-FCN [9]	56.1	55.4	56.8
DSTC-Sum	**58.5**	**58.0**	**59.0**

Table V presents the results of the OVP dataset. Here, DSTC-Sum achieved an F-score of 58.5%, again outperforming the compared methods. With its more structured content, the OVP dataset benefited from the model's ability to capture long-range dependencies without losing important local features, a challenge that other models, such as SUM-GANsup, struggled with.

As shown in Fig. 5, the experimental results demonstrate the effectiveness of the DSTC-Sum model across both YouTube and OVP datasets. The model's ability to summarize videos of varying lengths and content types significantly influenced its performance in the YouTube dataset. The diversity in YouTube videos requires a model capable of understanding both global and local temporal structures, which is one of the key strengths of the DSTC-Sum model. On the OVP dataset, the model's performance highlights its ability to handle shorter, more structured videos. Compared to the baseline models, the improved F-score on this dataset shows that DSTC-Sum is particularly effective at summarizing videos with well-defined narrative structures, such as documentaries and educational videos.

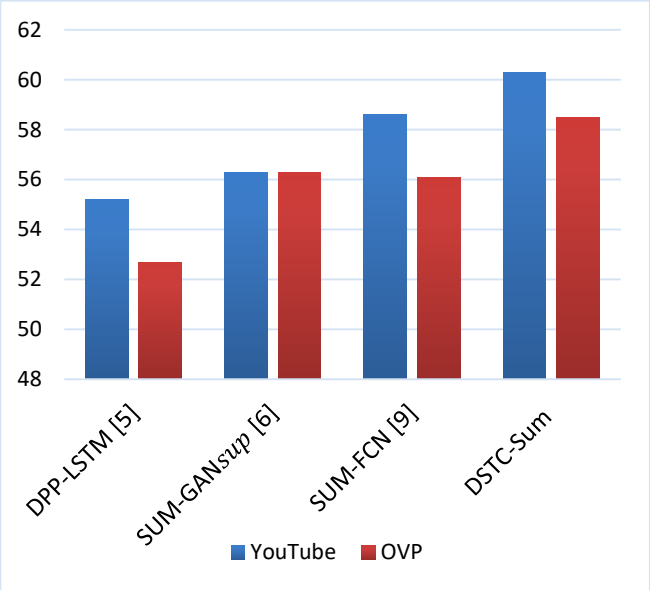


Fig. 5. DSTC-Sum model across both YouTube and OVP datasets.

The results on both YouTube and OVP datasets reinforce the generalizability and effectiveness of the DSTC-Sum model in video summarization tasks. The model consistently outperforms existing methods, demonstrating its ability to capture both long-term and short-term temporal dependencies. This makes it suitable for videos with diverse content (YouTube) and structured narratives (OVP).

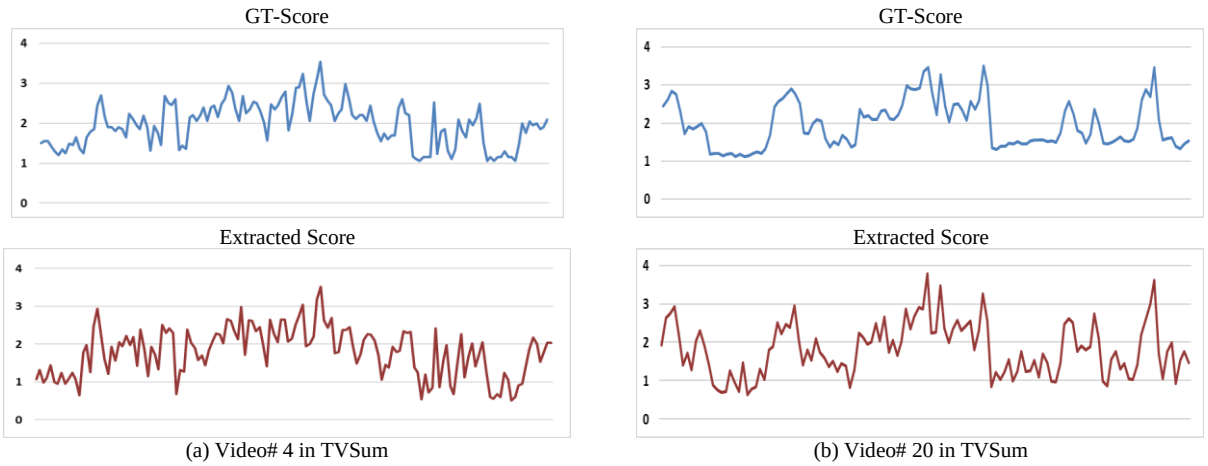
The comparison across all datasets (TVSum, SumMe, YouTube, and OVP) indicates that the DSTC-Sum model is robust and versatile in different summarization tasks, whether the videos are user-generated content (YouTube), educational (OVP) or professionally curated datasets (TVSum, SumMe). The scalability and low computational cost of DSTCB architecture further emphasize its potential for practical applications, including real-time video summarization.

F. Qualitative Results

In addition to the quantitative evaluations presented in previous sections, assessing the DSTC-Sum model's performance from a qualitative perspective is essential. This section provides a deeper insight into how effectively the model captures important segments and generates accurate video summaries. We aim to demonstrate the model's ability to identify critical video moments by visualizing the extracted importance and ground truth scores. As seen in Fig. 6, we plot the extracted importance scores and the ground truth scores for two videos from the TVSum dataset to understand better how well our DSTC-Sum has learned. The important ratings derived from ground truth and the extracted scores generated by the suggested DSTC-Sum roughly match. Moreover, the proposed technique produces high-quality video summaries as users incorporate several factors that our DSTC-Sum considers relevant.

To further understand how effective our DSTC-Sum is, we showcase some video summaries that demonstrate its temporal modeling capabilities compared to SUM-GAN*sup* and DHAVS [57]. Fig. 7 illustrates that colorful bars indicate projected video summaries and sky-blue bars indicate ground truth scores. The segments selected as summaries by SUM-GAN*sup*, DHAVS, and DSTC-Sum are shown by the yellow, green, and red bars, respectively.

The DSTC-Sum technique produces high-quality video summaries by capturing temporal dependencies, allowing it to identify the most crucial video segments effectively. Comparisons of the summaries generated by DSTC-Sum with those produced by SUM-GANsup and DHAVS reveal that while other approaches often fail to select the most relevant sub-shots, DSTC-Sum consistently identifies key segments with higher ground-truth relevance scores. This ability to create accurate and relevant video summaries underscores DSTC-Sum's superiority in video summarization tasks.



(a) Video# 4 in TVSum (b) Video# 20 in TVSum

Fig. 6. Video scores extracted by the proposed DSTC-Sum (bottom) and Ground truth scores (top) for video 4 and video 20 in the TVSum dataset.

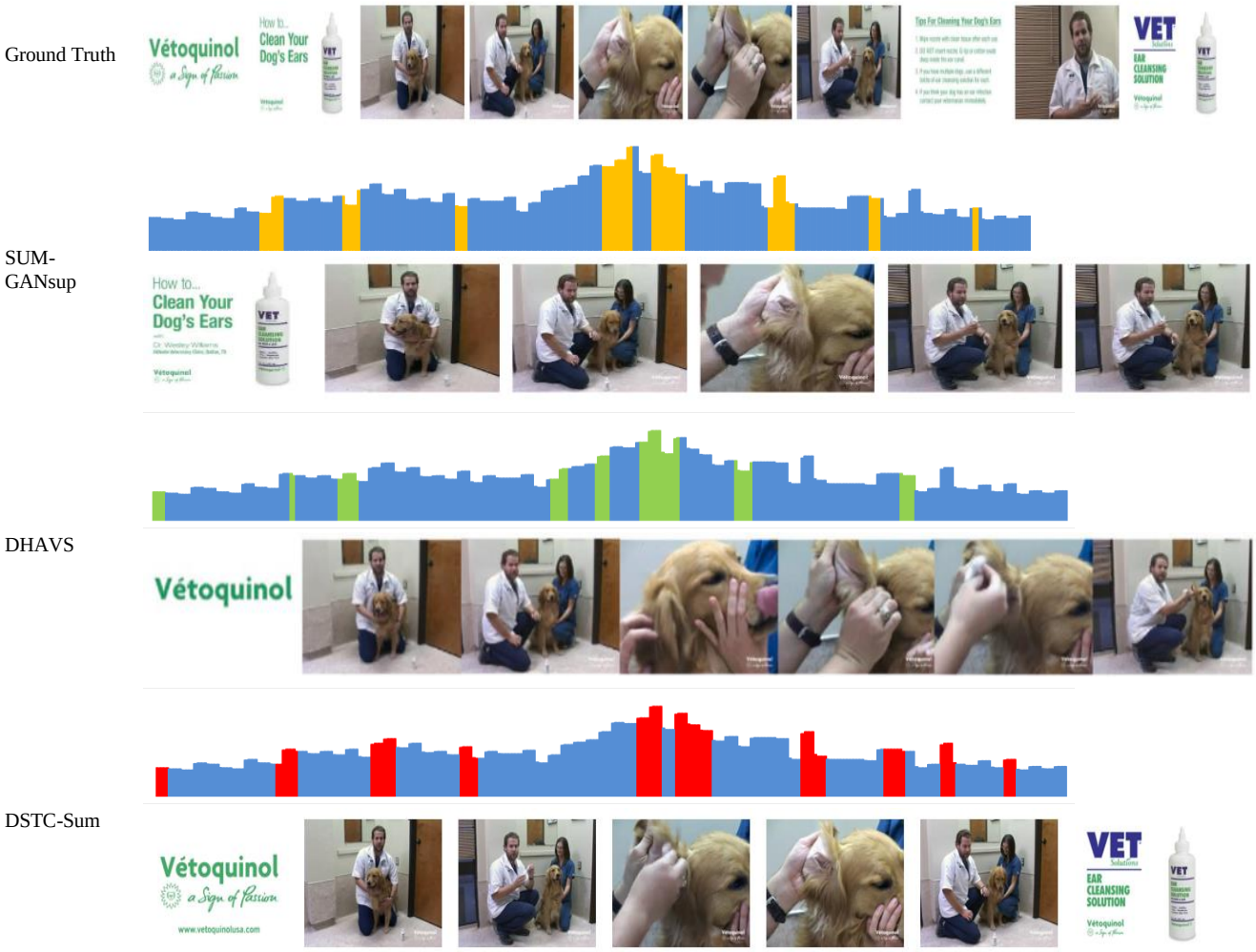


Fig. 7. Comparison of the extracted summary extraction for video 4 and video 20 in the TVSum dataset.

V. Conclusion

This study introduces DSTC-Sum, a video summarization model leveraging Depthwise Separable Temporal Convolutions (DSTC) to capture long-term temporal relationships and local features effectively. TCNs, unlike RNN-based models, allow for adding more layers while being computationally less expensive, faster to train, and lightweight. Furthermore, DSTC improves representational efficiency while being low-cost in computing and memory. Extensive experiments are carried out on two benchmark datasets, TVSum and SumMe. The outcomes demonstrate the efficacy of our DSTC-Sum model for supervised video summarization. Furthermore, the qualitative findings show that our model can produce fine-grained summary predictions and better scoring for each frame. To further assess the model's generalizability and robustness, we extended our experiments to two additional datasets: YouTube and the OVP (Open Video Project). On both datasets, the proposed model demonstrated superior performance, achieving F-scores of 60.3% and 58.5%, respectively, surpassing several state-of-the-art techniques. These results highlight the model's effectiveness in capturing long-term temporal dependencies and generating high-quality video summaries across various genres.

In the future, we plan to enhance the DSTC-Sum framework by integrating attention mechanisms to gain richer contextual information and improve summarization accuracy. Additionally, we will explore its potential in real-time video processing and personalized content creation, aiming to extend its application scope and solidify its position as a leading methodology in video summarization.

References

[1] X. Dong, Y. Yu, and J. Zhou, Cisco: Integration of Innovation and Operation. Springer Nature, 2023.

[2] E. Mofreh, A. Abozeid, H. Farouk, and K. A. ElDahshan, "Multi-object semantic video detection and indexing using a 3D deep learning model," Int. J. Intell. Eng. Syst., vol. 15, no. 3, 2022.

[3] K. A. ElDahshan, H. Farouk, A. Abozeid, and M. H. Eissa, "Global dominant SIFT for video indexing and retrieval," J. Theor. Appl. Inf. Technol., vol. 97, no. 19, pp. 5023–5035, 2019.

[4] H. Farouk, K. A. ElDahshan, and A. Abozeid, "Effective and efficient video summarization approach for mobile devices," Int. J. Interact. Mob. Technol., vol. 10, no. 1, 2016.

[5] J. Zhang, G. Wu, X. Bi, and Y. Cui, "Video summarization generation network based on dynamic graph contrastive learning and feature fusion," Electronics, vol. 13, no. 11, p. 2039, 2024.

[6] B. Mahasseni, M. Lam, and S. Todorovic, "Unsupervised video summarization with adversarial LSTM networks," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2017.

[7] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Comput., vol. 9, no. 8, pp. 1735–1780, 1997.

[8] M. Sundermeyer, T. Alkhouli, J. Wuebker, and H. Ney, "Translation modeling with bidirectional recurrent neural networks," in Proc. 2014 Conf. Empir. Methods Nat. Lang. Process. (EMNLP), Oct. 2014, pp. 14–25.

[9] M. Rochan, L. Ye, and Y. Wang, "Video summarization using fully convolutional sequence networks," in Proc. Eur. Conf. Comput. Vis. (ECCV), 2018.

[10] B. Hampiholi, C. Jarvers, W. Mader, and H. Neumann, "Depthwise separable temporal convolutional network for action segmentation," in Proc. Int. Conf. 3D Vis. (3DV), Nov. 2020, pp. 633–641.

[11] D. Li, R. Wang, P. Chen, C. Xie, Q. Zhou, and X. Jia, "Visual feature learning on video object and human action detection: A systematic review," Micromachines, vol. 13, no. 1, p. 72, 2021.

[12] G. Li, J. Zhang, M. Zhang, R. Wu, X. Cao, and W. Liu, "Efficient depthwise separable convolution accelerator for classification and UAV object detection," Neurocomputing, vol. 490, pp. 1–16, 2022.

[13] A. A. Khan and J. Shao, "SPNet: A deep network for broadcast sports video highlight generation," Comput. Electr. Eng., vol. 99, p. 107779, 2022.

[14] D. Zhao, D. Zhu, X. Min, J. Yue, K. Zhang, Q. Zhou, J. Zhao, and X. Yang, "Human attention-based movie summarization: Dataset and baseline model," Neurocomputing, vol. 534, pp. 106–118, 2023.

[15] P. Narwal, N. Duhan, and K. K. Bhatia, "A comprehensive survey and mathematical insights towards video summarization," J. Vis. Commun. Image Represent., vol. 89, p. 103670, 2022.

[16] T. Psallidas, M. D. Vasilakakis, E. Spyrou, and D. K. Iakovidis, "Multimodal video summarization based on fuzzy similarity features," in Proc. IEEE 14th Image, Video, Multidimensional Signal Process. Workshop (IVMSP), Jun. 2022, pp. 1–5.

[17] M. Dehghani, A. Gritsenko, A. Arnab, M. Minderer, and Y. Tay, "Scenic: A jax library for computer vision research and beyond," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., 2022, pp. 21393–21398.

[18] L. Fei-Fei and R. Krishna, "Searching for computer vision north stars," Daedalus, vol. 151, no. 2, pp. 85–99, 2022.

[19] R. Akhare and S. Shinde, "Query-focused video summarization: A review," in Artif. Intell. First Int. Symp. ISAI 2022, Haldia, India, Feb. 17–22, 2022, Revised Selected Papers, Springer, 2023.

[20] A. Markwirth, M. Lachetta, V. Mönkemöller, R. Heintzmann, W. Hübner, T. Huser, and M. Müller, "Video-rate multi-color structured illumination microscopy with simultaneous real-time reconstruction," Nat. Commun., vol. 10, no. 1, p. 4315, 2019.

[21] D. de Matos, W. Ramos, L. Romanhol, and E. R. Nascimento, "Musical hyperlapse: A multimodal approach to accelerate first-person videos," in *Proc. 34th SIBGRAPI Conf. Graph., Patterns, Images*, Oct. 2021, pp. 184–191.

[22] M. Silva, W. Ramos, A. Neves, E. Araujo, M. Campos, and E. R. Nascimento, "Fast-forward methods for egocentric videos: A review," in *Proc. 32nd SIBGRAPI Conf. Graph., Patterns, Images Tutorials (SIBGRAPI-T)*, Oct. 2019, pp. 36–46.

[23] F. Tian, J. Fan, X. Yu, S. Du, M. Song, and Y. Zhao, "TCVM: Temporal contrasting video montage framework for self-supervised video representation learning," in *Proc. Asian Conf. Comput. Vis.*, 2022, pp. 1539–1555.

[24] W. Zhu, J. Lu, J. Li, and J. Zhou, "DSNet: A flexible detect-to-summarize network for video summarization," *IEEE Trans. Image Process.*, vol. 30, pp. 948–962, 2020.

[25] J. A. Ghauri, S. Hakimov, and R. Ewerth, "Supervised video summarization via multiple feature sets with parallel attention," in *Proc. IEEE Int. Conf. Multimedia Expo (ICME)*, 2021.

[26] M. Otani, Y. Nakashima, E. Rahtu, and J. Heikkila, "Rethinking the evaluation of video summaries," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2019, pp. 7596–7604.

[27] V. Kaushal, S. Subramanian, S. Kothawade, R. Iyer, and G. Ramakrishnan, "A framework towards domain-specific video summarization," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, Jan. 2019, pp. 666–675.

[28] P. Li, Q. Ye, L. Zhang, L. Yuan, X. Xu, and L. Shao, "Exploring global diverse attention via pairwise temporal relation for video summarization," *Pattern Recognit.*, vol. 111, p. 107677, 2021.

[29] B. Zhao, X. Li, and X. Lu, "TTH-RNN: Tensor-train hierarchical recurrent neural network for video summarization," *IEEE Trans. Ind. Electron.*, vol. 68, no. 4, pp. 3629–3637, 2020.

[30] B. Zhao, X. Li, and X. Lu, "Hierarchical recurrent neural network for video summarization," in *Proc. 25th ACM Int. Conf. Multimedia*, 2017.

[31] K. Zhang, W. L. Chao, F. Sha, and K. Grauman, "Summary transfer: Exemplar-based subset selection for video summarization," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2016, pp. 1059–1067.

[32] K. Zhang, W. L. Chao, F. Sha, and K. Grauman, "Video summarization with long short-term memory," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Amsterdam, The Netherlands, Oct. 11–14, 2016, Part VII, Springer Int. Publ., pp. 766–782.

[33] M. Fei, W. Jiang, and W. Mao, "Learning user interest with improved triplet deep ranking and web-image priors for topic-related video summarization," *Expert Syst. Appl.*, vol. 166, p. 114036, 2021.

[34] Y. Wei, X. Wang, L. Nie, X. He, R. Hong, and T. S. Chua, "MMGCN: Multi-modal graph convolution network for personalized recommendation of micro-video," in *Proc. 27th ACM Int. Conf. Multimedia*, Oct. 2019, pp. 1437–1445.

[35] S. Lee, J. Sung, Y. Yu, and G. Kim, "A memory network approach for story-based temporal summarization of 360 videos," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 1410–1419.

[36] J. Park, J. Lee, I. J. Kim, and K. Sohn, "Sumgraph: Video summarization via recursive graph modeling," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Glasgow, UK, Aug. 23–28, 2020, Part XXV, Springer Int. Publ., pp. 647–663.

[37] Y. Yuan, T. Mei, P. Cui, and W. Zhu, "Video summarization by learning deep side semantic embedding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 1, pp. 226–237, 2017.

[38] R. Panda and A. K. Roy-Chowdhury, "Collaborative summarization of topic-related videos," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2017.

[39] S. S. Zang, H. Yu, Y. Song, and R. Zeng, "Unsupervised video summarization using deep non-local video summarization networks," *Neurocomputing*, vol. 519, pp. 26–35, 2023.

[40] K. Zhang, K. Grauman, and F. Sha, "Retrospective encoders for video summarization," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, 2018.

[41] A. Sharghi, A. Borji, C. Li, T. Yang, and B. Gong, "Improving sequential determinantal point processes for supervised video summarization," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, 2018, pp. 517–533.

[42] M. Fei, W. Jiang, and W. Mao, "Creating memorable video summaries that satisfy the user's intention for taking the videos," *Neurocomputing*, vol. 275, pp. 1911–1920, 2018.

[43] J. Gao, X. Yang, Y. Zhang, and C. Xu, "Unsupervised video summarization via relation-aware assignment learning," *IEEE Trans. Multimedia*, vol. 23, pp. 3203–3214, 2020.

[44] T. Liu, Y. Yuan, G. Teng, and X. Meng, "Improved deep convolutional neural network-based method for detecting winter jujube fruit in orchards," *Eng. Lett.*, vol. 32, no. 3, 2024.

[45] Y. Fu, L. Qiu, X. Kong, and H. Xu, "Deep learning-based online surface defect detection method for door trim panel," *Eng. Lett.*, vol. 32, no. 5, 2024.

[46] M. Rochan and Y. Wang, "Video summarization by learning from unpaired data," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2019.

[47] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.

[48] N. Lu, T. Yin, and X. Jing, "Deep learning solutions for motor imagery classification: A comparison study," in *Proc. 8th Int. Winter Conf. Brain-Comput. Interface (BCI)*, 2020.

[49] Y. K. Musallam, N. I. AlFassam, G. Muhammad, S. U. Amin, M. Alsulaiman, W. Abdul, and M. Algabri, "Electroencephalography-based motor imagery classification using temporal convolutional network fusion," *Biomed. Signal Process. Control*, vol. 69, p. 102826, 2021.

[50] J. L. Ba, J. R. Kiros, and G. E. Hinton, "Layer normalization," *arXiv preprint arXiv:1607.06450*, 2016.

[51] M. Gygli, H. Grabner, H. Riemenschneider, and L. Van Gool, "Creating summaries from user videos," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Zurich, Switzerland, Sep. 6–12, 2014, Part VII, Springer Int. Publ., pp. 505–520.

[52] Y. Song, J. Vallmitjana, A. Stent, and A. Jaimes, "TVSum: Summarizing web videos using titles," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2015, pp. 5179–5187.

[53] P. Over and W. Kraaij, "Evaluation campaigns and TRECVID," in *Proc. ACM SIGMM Int. Workshop Multimedia Inf. Retrieval*, 2006.

[54] S. E. F. De Avila, A. P. B. Lopes, A. da Luz Jr., and A. de Albuquerque Araújo, "VSUMM: A mechanism designed to produce static video summaries and a novel evaluation method," *Pattern Recognit. Lett.*, vol. 32, no. 1, pp. 56–68, 2011.

[55] G. Geisler and G. Marchionini, "The open video project: Research-oriented digital video repository," in *Proc. Fifth ACM Conf. Digital Libr.*, 2000.

[56] B. Gong, W. L. Chao, K. Grauman, and F. Sha, "Diverse sequential subset selection for supervised video summarization," *Adv. Neural Inf. Process. Syst.*, vol. 27, 2014.

[57] X. Li, B. Zhao, and X. Lu, "A general framework for edited video and raw video summarization," *IEEE Trans. Image Process.*, vol. 26, no. 8, pp. 3652–3664, 2017.

[58] Z. Ji, K. Xiong, Y. Pang, and X. Li, "Video summarization with attention-based encoder–decoder networks," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 6, pp. 1709–1717, 2019.

[59] J. Lin, S.-h. Zhong, and A. Fares, "Deep hierarchical LSTM networks with attention for video summarization," *Comput. Electr. Eng.*, vol. 97, p. 107618, 2022.

A Taxonomic Study: Data Placement Strategies in Cloud Replication Environments

Fazlina Mohd Ali[1], Marizuana Mat Daud[2], Fadilla Atyka Nor Rashid[3],
Nazhatul Hafizah Kamarudin[4], Syahanim Mohd Salleh[5], Nur Arzilawati Md Yunus[6]
Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia, Selangor, Malaysia[1, 3, 4, 5]
Institute of Visual Informatics, Universiti Kebangsaan Malaysia (UKM), Bangi 43600, Selangor, Malaysia[2]
Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), Selangor, Malaysia[6]

***Abstract*—Since the past decades, the data replication trend has not subsided; it is progressing rapidly from multiple perspectives to enhance cloud replication performance. Researchers are eagerly focusing on improving the strategies in various perceptions; unfortunately, the vulnerability in every strategy is inevitable. A non-comprehensive replica strategy would have vulnerability and drawbacks. The drawbacks that usually reside in the developed strategies are not limited to high network usage, high process time, high response time, high storage consumption, and more, depending on the research areas. Many researchers are out of ideas to identify state-of-the-art issues. This exhaustive taxonomic study focused on analyzing the diversified contributions and limitations terrain of the cloud replication environment, focusing on data placement strategies. It seeks to delve deeply into its fundamental strategy, practical implementations, and the intricate challenges it poses. Concerning the imminent cloud-driven future, this structured review paper is a vital resource for researchers, policymakers, and industry professionals grappling with the complexities of this emerging paradigm. By illuminating the intricacies of data replication strategies, this study fosters a deeper appreciation for the transformative potential and the multifaceted challenges ahead of cloud data replications.**

***Keywords*—Cloud environment; data replication; placement strategies; replication taxonomy; performance metrics**

I. Introduction

An enormous amount of data is used extensively in the current era globally [1]–[3]. According to the International Data Corporation (IDC), global data will increase by 61% to 175 zettabytes by 2025, with most of that data being stored in cloud computing environments rather than data centers. This phenomenon is derived from the most interconnected Internet of Things (IoT) devices, leading to 100 billion terminals connected in 2025 [4], [5].

A. Cloud Computing

Cloud computing is well known as a data management platform that addresses the high volume of data demanded to be accessible by users anytime from anywhere [6], [7]. Cloud computing offers users a dynamic pricing model since it enables multiple services such as Software as a Service (SaaS), which provides real-time application services, Platform as a Service (PaaS), which delivers various operating systems, Consistency as a Service (CaaS), which promises data consistency in storage nodes, and Infrastructure as a Service (IaaS), which provides many hardware solutions to users as an on-demand basis [8]–[12].

Cloud computing offers users a "pay-as-you-go" basis since it enables multiple services, as shown in Fig. 1. The hardware resides as the fundamental facility in cloud computing architecture. The IaaS is the bottom layer in cloud services, which offers various large-scale infrastructure services with multi-specification of servers, CPU, memory, storage, and more. In the middle layer is PaaS, which enables numerous platforms like operating systems and software frameworks that can be tailored based on clients' required environments. The top layer is SaaS, which is directly accessible to users with multiple applications such as web services, user interface systems like enterprise systems, and many more [13]–[15]. In the IaaS layer, the foremost benefit received by cloud users is the agility of the services. Cloud providers serve their clients by off-loading the hustle of managing the data center. Therefore, clients can freely focus on evolving their business [16].

Consequently, it improves the ability to meet user demands and reduce costs as the user can provision the resource amount accordingly [17]. Cost-saving is the most significant benefit a cloud tenant gains, as the pay-as-you-go paradigm reduces expenses on the overall data center maintenance cost. This foreseen cost can be a transition to operational expenses, vividly beneficial for business goals. Additionally, the SaaS layer delivers rapid deployment of client applications around the globe with only a few clicks [11]. PaaS enables the deployment of the necessary software applications, while SaaS, as the top layer, provides users with ready-to-use applications [13], [18]. These benefits have been the core reasons that drive users to choose the cloud as their data management platform.

B. Data Management

Data management is one of the prominent services enabled in cloud platforms. As a mass platform to serve high-volume data, the cloud is a multi-device technology that enables data management in a few deployment models: private cloud, public cloud, community cloud, and hybrid cloud. However, cloud tenants must choose an appropriate cloud model because every cloud model is distinguished depending on data criticality and resources [19]–[22]. Cloud providers need technical and business knowledge to propose the best model for organizations to ensure cloud tenants obtain efficient data management services. Comprehensive data management solutions are

delivered to cloud tenants in the respective models, including data processing, security, storage, and recovery services.

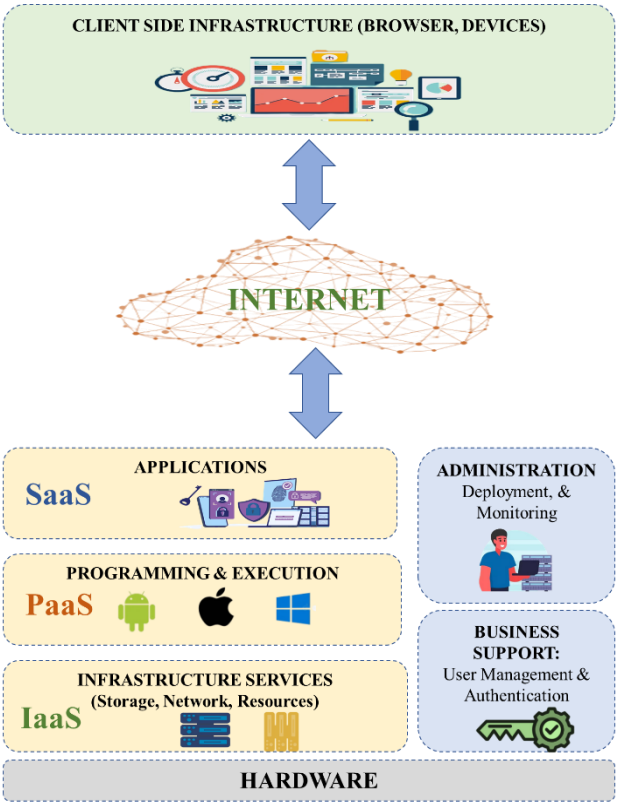


Fig. 1. Basic cloud computing architecture.

C. Data Recovery

Data Recovery must be adopted in any platform, including cloud environments [23]. The researcher in study [24] focused on data recovery in their study, whereby the researcher accentuated that the importance of data recovery is intolerable because the ambiguities of data absence are extremely anticipated in cloud platforms. Additionally, the researcher emphasizes that data recovery or failover costs are crucial before implementing cloud models. Therefore, the cloud as a data management platform has prepared data recovery mechanisms such as data backup, replication, and checkpointing [25]. The available approaches are playing different roles based on different circumstances.

D. Data Replication

Data replication is recognized as a promising cloud environment service that offers strategies to keep data in secure environments [25] safely. Data replication is defined as a heuristic multi-dimensional technique that saves one or more copies of data in multiple storage nodes in clouds [26]–[28]. According to study [29], data replication preserves the master data from catastrophic events (floods, earthquakes, etc.) and human errors, such as accidentally deleting information in the master files or deleting entire master files by users. The middleware manages replica copies in different environments known as disaster recovery centers. Therefore, copies of data are managed and kept safe in different nodes at different places. Thus, any unfortunate incidents that happen to the replicas would not affect the other replica copies. This would prevent data loss in any environment. Data replication is identified as a strategy that creates multiple copies in cloud storage in a big data environment, accelerating cloud system performance [29]–[31].

Replication strategies are commonly divided into two (2) mechanisms: static and dynamic data replications [32]–[34]. Static replication is a predetermined environment for dedicated cloud replication systems [14], [27]. The number of nodes, number of replicas, and many other architectures are fixed based on certain cloud system necessities before the replication strategy is implemented [35], [36]. The second mechanism is dynamic replication, or flexible replication strategies, where the algorithm can automatically create and delete replicas depending on the system users' access patterns [37]. However, the static replication mechanism is relatively simple and not preferable to be adapted in many cloud replication environments. The architecture is mainly foreordained, sometimes unsuitable for complex cloud replication systems [38], [39].

According to literature perceptions, a comprehensive cloud replication strategy always has a few significant phases; the first phase is usually the File Selection Strategy, which is to identify crucial data to be selected as replication candidates. The next phase is the Data Placement Technique, where the required number of replicas is identified, and the location to send the replicas is determined. Finally, the Data Center Selection Method is the stage to accomplish the replication process by identifying the best factors to select appropriate nodes to store the replicas in the cloud replication environment. Every stage complements different requirements. Researchers have the right to consolidate every phase in one research work as a complete replication process or develop every phase separately as fulfilments in respective research works. This research focuses on data placement strategies and factors in placing replicas in cloud environments.

A typical replication management architecture for a cloud environment is illustrated in Fig. 2.

Fig. 2 demonstrates a basic replication architecture in a cloud environment. Users in the architecture are also recognized as clients or tenants for cloud providers. The replication process is triggered when a user requests a data file from the cloud. A Global Replica Manager (GRM), typically the broker, manages and schedules replication tasks in the whole infrastructure. Conversely, the Local Replica Manager (LRM) manages local or inbound replication jobs for data centers. Usually, data centers are grouped in clusters, depending on the configuration of the cloud replication. The GRM and LRM must continually adhere to the rules and protocols in the algorithm specified in the replication system. The data file verification will occur when the manager receives user data requests. File information such as file names and locations are available as a comprehensive metadata table in the GRM and LRM. Then, the managers process the requested data according to the algorithm rules and identify candidate files for replication. The requested data file will be sent off to users, and new replica copies will be placed, conferring to the pre-determined placement technique in data centers.

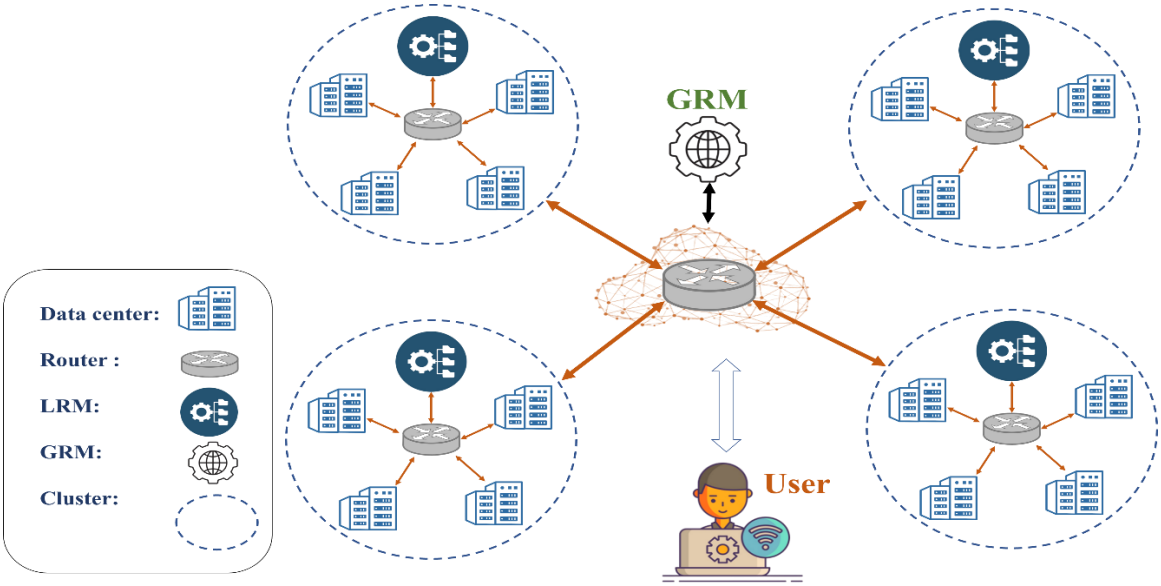


Fig. 2. Basic data replication architecture.

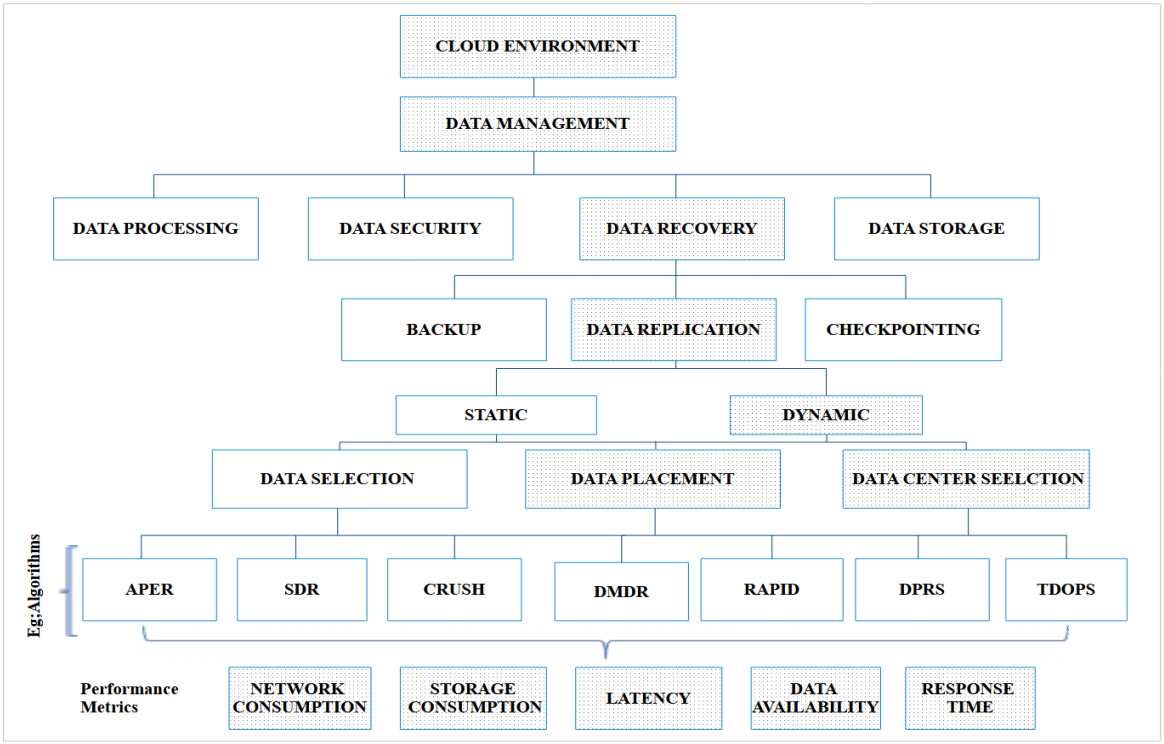


Fig. 3. Cloud replication taxonomy.

According to study [40] the taxonomy study can make the knowledge found in documents and texts clear and usable by other researchers also practitioners. Fig. 3 illustrates the data replication taxonomy in a cloud environment, which can be discovered in this study. This entire study is structured and organized as this taxonomy. The shaded boxes are the main focus of this study.

This taxonomy-based study thoroughly discusses similar studies related to this research area. The topic was explained and drilled down from top to bottom of the taxonomy, deriving the dedicated research area.

A taxonomy study on cloud computing is described, followed by the definition and overview of data management until the data replication body of knowledge.

A thorough discussion on existing research works in data replications and placements strategies with insights on contributions and achievements in numerous performance metrics enhancement.

Analysis tables and relevant analytics graphs are presented to share the essential details of related research works according to the research questions, highlighting research trends, contributions, and limitations.

II. Related Works

The advent of cloud computing has revolutionized how data is stored and managed. A critical aspect of cloud computing is data replication which involves creating and maintaining multiple copies of data across different locations to ensure high availability and reliability [41], [42].

Cloud computing empowers users with various resilient services that stand vibrantly as preferable technology for almost everyone to ensure data are efficiently managed and business continuity is guaranteed too [43]–[46]. However, cloud computing as a reliable multiple-service provider is not exceptional in facing issues in providing high data availability to users while preserving data sensitivity. Fear of losing data during node failures is one of the core issues too [2], [11], [39], [47].

Hence, to mitigate the concerns that arise in a cloud platform, data replication is recognised as a promising cloud environment strategy [4], [7], [48]–[50]. Data replication is an empirical technique to accelerate system performance by generating identical data copies across multiple storage [51], [52]. Precisely, in a cloud environment, data replication is defined as creating several physical copies for every logical data item and locating the replica copies in different sites or storage nodes [36], [53], [54]. Depending on the cloud replication objectives, there are several ways to apply the data replication function.

There are two (2) prominent traditional techniques in cloud replication. First is static replication, where data copies are pre-determined and evenly distributed across nodes to ensure fault tolerance and load balancing. However, static replication may not adapt well to dynamic workloads and changing data access patterns. Dynamic replication dynamically adapts the replication scheme based on data access patterns and system conditions. These approaches aim to improve data availability and reduce access latency by dynamically creating or removing replicas as required. Dynamic replication techniques often utilize monitoring and feedback mechanisms to make informed decisions about replica placement [55], [56].

A taxonomy study is the structured names and definitions used to organize information and knowledge. Researcher in study [57] proposed a broad taxonomy of storage efficiency, with the performance metrics focused on cost optimization. The other research work by [58] introduces a taxonomy that organizes existing solutions for maintenance operations in cloud, edge, and IoT environments. This research work does not discuss any performance metrics yet; it merely reviews existing research work according to the taxonomy structure and presents the challenges within the research field. Similarly, [59] examines the migration field's characteristics and proposes a management-centric taxonomy in cloud computing. Researchers [60] and [61] embarked on cloud replication strategies and presented relevant taxonomy related to this research area. However, their studies proposed a very high-level taxonomy for this body of knowledge, which is not comprehensive enough to overview the entire structure of data replication processes in a cloud environment.

As enormous technologies are emerging extensively around the globe, many new approaches, such as artificial intelligence (AI), have been discovered as compatible techniques for replication strategies in cloud environments. Hence, researchers are continuously attempting novel replication strategies to place replica copies in cloud storage that provides multiple key services with resilient infrastructures for every cloud consumer [61], [62]. The cloud computing architectures, standards, and tools provide prospects for advancement in services, which offer various benefits to cloud clients [22], [63]–[65].

Thus, recent research works incorporated AI-based approaches in replication strategies to breed performance enhancements [66]. As such, similar studies like [67] and many state-of-the-art studies must not be overlooked and must be visible for future researchers' knowledge. In this context, there is still a lack of studies that present comprehensive surveys to produce a widespread taxonomy related to replication strategy in cloud environments. These limitations of the existing research motivated this study to produce a comprehensive taxonomy for data placement strategies in cloud replication environments. The taxonomy offers collections of replication strategies that allow cloud providers to scrutinize and implement them in real-cloud replication settings. Further, cloud providers would serve accelerated performance to users with better data availability, faster response time, low fault tolerance, reduced storage usage, and efficient network usage [28], [37], [68]–[70].

III. Method and Materials

This taxonomy study mainly explores the existing literature to investigate the coverage of multiple related topics, the research trends, and the critical review of relevant studies that have been published. The methodology implied in obtaining the source papers in this study mainly follows the guidelines suggested by [71]. According to study [40] the taxonomy study can make the knowledge found in documents and texts clear and usable by other researchers also practitioners. The guidelines for this study follow the essential steps of defining the research questions, searching for relevant papers, screening the papers, keywording the abstracts, extracting the data, and mapping. Each process step has an outcome, and the outcome of the complete process is the taxonomy mapping.

A. Research Questions (RQ)

1) Definition of research questions (Research Scope): The primary goal of a taxonomy study is to provide an overview of a research area and identify relevant research also results available within this field.

2) The Primary RQ of this study: ‘What are the Data Placement Strategies in a Cloud Replication Environment?’ This primary question was divided into four RQs. Table I lists the formulated RQs.

B. Data Sources

1) Search for primary studies (all papers): Primary research was found using keyword search terms on scientific

databases or by personally looking through pertinent journal articles or conference proceedings.

2) The primary data Sources: Scopus online databases were primary data sources for potentially related studies. Other data sources were not considered to impede the overlapping of source results.

C. Search Terms

1) Keywording of abstracts (classification scheme): Keywording is a way to reduce the time needed to develop the classification scheme and ensure that the method considers the existing studies.

2) Search the related research effectively: It is imperative to identify the pertinent search phrases. Kitchenham *et al.* [72] suggested population, intervention, comparison, and outcome (PICO) approach is fitting in this regard. Many review papers have broadly adopted these viewpoints. Here, the relevant PICO terms are listed:

- Population: Primary studies in Data Replication.
- Intervention: Placement strategies.
- Comparison: Strategies, Advantages, limitations.
- Performance metric, and future direction.
- Outcome: Placement Strategies, Advantages, and constraints in cloud replication environments.

D. Inclusion and Exclusion Criteria

1) Screening of papers for inclusion and exclusion (relevant papers): Studies that were irrelevant to addressing the study issues were eliminated using inclusion and exclusion criteria.

2) Inclusion and exclusion criteria: applied to determine and discard relevant studies from the data sources to answer the RQs in this taxonomy study.

3) Data extraction and taxonomy mapping of studies: Once the classification scheme was in place, the relevant articles were discussed according to the structure.

E. Research Questions (RQ)

1) Definition of research questions (research scope): The primary goal of a taxonomy study is to provide an overview of a research area and identify relevant research also results available within this field.

2) The Primary RQ of this study: 'What are the Data Placement Strategies in a Cloud Replication Environment?' This primary question was divided into four RQs. Table I lists the formulated RQs.

As shown in Fig. 4, a literature search was done using the keywords "(replication OR placement AND strategies AND in AND cloud), (replication AND strategies AND in AND cloud), (Data AND Replication OR placement AND strategies AND in AND cloud) identified 1,057 initial articles. A three-step screening process ensured high-quality and relevant studies. First, 399 articles were excluded for lacking peer-review or being in a language other than English. The second screening focused on article completeness, removing 399 articles lacking full text (available only as abstracts or presentations) or not directly relevant to cloud replication strategies. This left 258 articles for further evaluation. Finally, a rigorous selection process focusing on data placement strategies within cloud replication resulted in a final set of 25 anchor references for in-depth analysis. These principles were employed in all the studies retrieved during the different phases of the study selection procedure (see Table II)

TABLE I. RESEARCH QUESTIONS

RQ	Research Question	Motivation
RQ1.	What are the publication trends for research topics related to cloud data replication environments?	To investigate publication trends in this research field throughout recent years
RQ2.	What are data placement strategies and factors employed in existing research works?	To explore cloud replication strategies in state-of-the-art
RQ3.	What are the performance metrics that contribute to the enhancement of replica placement strategies in cloud replication environments?	To discover performance enhancements addressed in individual research
RQ4.	What are the common limitations across existing research on data placement strategies in cloud replication environments?	To gain the gaps in existing research that can guide future research explorations and improvements

TABLE II. INCLUSION AND EXCLUSION CRITERIA

Inclusion criteria	
IC1	Articles that are peer-reviewed
IC2	Articles providing research in Cloud Replication Strategies
IC3	Articles published from 2017 to 2024
Exclusion criteria	
EC1	Articles that do not meet the inclusion criteria
EC2	Articles without full text (only abstract or presentation)
EC3	Studies in languages other than English
EC4	Articles with unclear results or findings

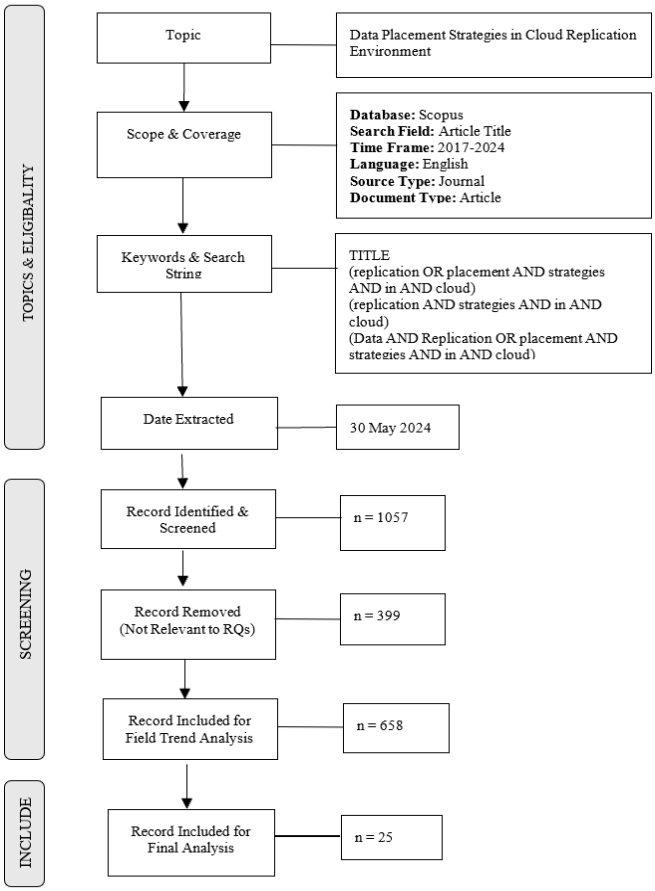


Fig. 4. Search strategy flow diagram.

IV. Findings and Discussions

A. RQ1: What are the Publication Trends for Cloud Data Replication Environments Research Topics?

Fig. 5 presents the publication trends in data placement strategies in cloud replication environments across six prominent journals and conferences from 2017 to May 2024. The data indicate significant growth in this research area, reflecting its increasing importance in cloud computing. The publication venues examined include Lecture Notes in Computer Science (LNCS), IEEE Access, Cluster Computing, Journal of Supercomputing, Future Generation Computer Systems (FGCS), and IEEE Transactions on Cloud Computing (TCC).

The total number of publications on data placement strategies in the Scopus online database from 2017 to May 2024 across all publication outlets is 658. The distribution of these publications among the six venues reveals distinct trends.

- Lecture Notes in Computer Science (LNCS) publications have increased from six papers in 2017 to 32 papers by May 2024. This represents a total of 175 publications, accounting for approximately 26.60% of the total publications.
- IEEE Access shows a significant rise from two papers in 2017 to 29 papers by May 2024, resulting in a total of 136 publications, which is about 20.67% of the total.
- Cluster Computing publications in *Cluster Computing* grew from 0 in 2017 to 26 by May 2024, with a total of 93 publications, making up around 14.14% of the total.
- Journal of Supercomputing starting from no publications in 2017 to 24 by May 2024, the *Journal of Supercomputing* accumulated a total of 110 publications, about 16.72% of the total.
- Future Generation Computer Systems (FGCS) publications increased from 3 in 2017 to 19 by May 2024, totaling 79 publications, approximately 12.01% of the total.
- IEEE Transactions on Cloud Computing (TCC) grew from no publications in 2017 to 19 by May 2024, amounting to a total of 65 publications, which is about 9.88% of the total.

The analysis of publication trends from 2017 to May 2024 illustrates a significant and growing interest in data placement strategies within cloud replication environments. This proves the evolving landscape in data placement strategies research, providing a foundation for future studies and developments in this pivotal area.

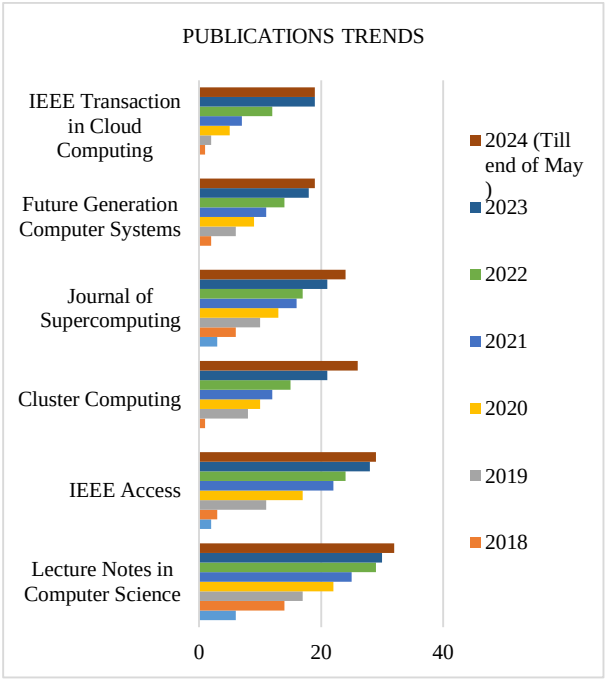


Fig. 5. Publication trends.

B. RQ2: What Data Placement Strategies and Factors are Employed in Existing Research Works?

1) Data placement strategies: Abundant studies cohesively developed numerous strategies to place replicas in the replication storage. At this point, scholars usually innovate a novel strategy to decide how to replicate the desired data, how many replicas are needed, and where to place the replicas [73]. the data placement method usually emphasizes the goal of accomplishing a cost-effective method with minimal storage

consumption, high data availability, optimal replica copies, faster replication time, etc.

a) Low response time: A heuristic data replication and placements introduced by the authors [74] evaluated big data analytics queries in a distributed cloud. The researchers placed the source data of queries at multiple geo-distributed data centers. This technique ensured that the respective queries were locked with certain trial counts until they reached the specified threshold. The query will be passed to the next replica for a response. Another focus of this study is to place a sample of source data at appropriate data centers to meet users' rigorous query response time. The aim here is to minimise the evaluation cost while the response time is accelerated.

b) Low response time, low cost and low resource: Another group of researchers [75] developed a data replication strategy that mainly fulfils cloud tenants without neglecting cloud provider profits; the strategy was named Achieving Query Performance in the Cloud via a Cost-effective Data Replication (APER). The study proposed a cost-effective replica placement strategy that improves database queries with specific estimations to attain better response time. To achieve the desired response time, this study pre-determined that a particular replication time must be less than one particular service level objective (SLO) response time threshold. Later, replicas were placed using heuristic techniques that reduced both resource usage and monetary cost. The APER places new replicas by discarding previous copies from the cloud only if the threshold of access history is reached. As claimed by the researcher, the response time was successfully reduced in this study.

c) Low response time and low storage: The redundancy rate is another issue that can be rectified with comprehensive data replication. A group of researchers was dedicated and solved this problem by proposing a Time Series-based Deduplication and Optimal Data Placement Strategy (TDOPS) in their study [76]. Deduplication techniques were deployed, and data placement was determined based on capacity constraints, cloud data center load balance, and data transportation costs. The researchers in this study achieve improvements in space reduction, efficient retrieval, data transportation costs, and data transmission time.

d) High data availability: The Controlled Replication Under Scalable Hashing (CRUSH) algorithm has been improvised by the researcher [77] to resolve the bottleneck issues of the previous CRUSH. In the last CRUSH algorithm, replicas were inconsistently segregated in available storage nodes. The older version of CRUSH persistently sent generated replicas to the same active servers, consequently degrading the performance in the replication system due to a long queue to retrieve replicas, thus concurrently contributing to network congestion. The enhanced CRUSH algorithm [77] is recognised as a data placement technique capable of dynamically obtaining data at the next available replica place when the first requested replica is pending in response. In CRUSH, the proposed replication architecture to place data is the RING topology, where the direction to entertain user requests on data is more structured and bidirectional. As claimed in this research, the improved CRUSH method outstrips the previous studies in better data availability.

e) High data availability and low cost: Improving Clustering Based Critical Parent (CbCP) with a Replication (ICR) algorithm was proposed to address performance enhancement on replica placement scheduling [78]. The ICR consists of three sub-algorithms: scheduling algorithm, starting replication tasks, and task replication algorithm is used to identify any available resource until replica placement. The key aim of this study is to identify the possible and earliest time to start every replication task using the available resources without adding extra cost. Data reliability increased in this research, and execution costs were reduced significantly.

f) High data availability and low latency: A study by [79] offers an Artificial Bee Colony technique for data replication optimization in cloud environments. Another researcher suggests a multi-objective optimization data placement model based on numerous data replicas in a hybrid fog-cloud environment [80]. The articles suggest that AI can help minimize latency and improve data location.

g) Low cost and low latency: The researcher [81] proposed cost-effective, dynamic data placement, consisting of greedy and dynamic algorithms used to find the most reasonable cloud data placement solution. The greedy approach can find the optimum number of appropriate data centers to replicate the user's most accessed data. This study aims to deliver dynamic and optimised data placement with tolerable latency while incurring minimal service costs in social networks like Facebook. The proposed data placement strategy will determine the necessity of replica creation and choose the best data centers to place new replicas in the nearest data center for every user with minimal latency. The researcher aimed to reduce storage and latency, while the monetary problem was also addressed.

h) Low cost and low storage: Researcher in study [82] focused on financial cost reduction with good data consistency is the research objective attained by the researcher. The researcher proposed a Dynamic Replica Placement Strategy to satisfy the user experience while reducing the storage overheads, eventually contributing to cost reduction. The researcher implied a node renting concept to fulfill the capacity of the edge cloud to address the overload problem. Rented nodes are used whenever users in edge computing suffer low performance and release a rented node from the cloud during the users' stable performance. Therefore, this strategy evidenced that total financial costs were saved, and user experience was sustained during the replica placement phase.

i) Low cost, low storage usage, and efficient network: A dynamic data replication management technique was combined with a novel data placement strategy in the research work of [83]. The main goal was to reduce the network usage and costs associated with data transfers between data centers. Similarly, researchers [86] proposed Initialization Scheme-Based GA (ISGA) with a primary focus on reducing storage and network utilization costs. The study adopted an interval pricing technique to choose the best location for data in a multi-cloud environment.

j) Low storage: A Dynamic Redundant replica strategy based on the Security Level (SL-DRM) was proposed [84]. It flexibly adjusts the number of replicas and places the replica via constructing the data cache strategy using the Location Correlation of Cache (LC-Cache) to improve data read speed. The most crucial video footage was re-duplicated and saved in the storage. Therefore, as better security is required, the proposed technique dynamically changed the influence factors and instructed the algorithm to place new copies of video footage for a particular area. Thus, the data cache strategy focuses on the cameras' locations and time correlations of the video files by predicting the users' playback behaviors. This strategy achieved low storage consumption with a limited number of video copies.

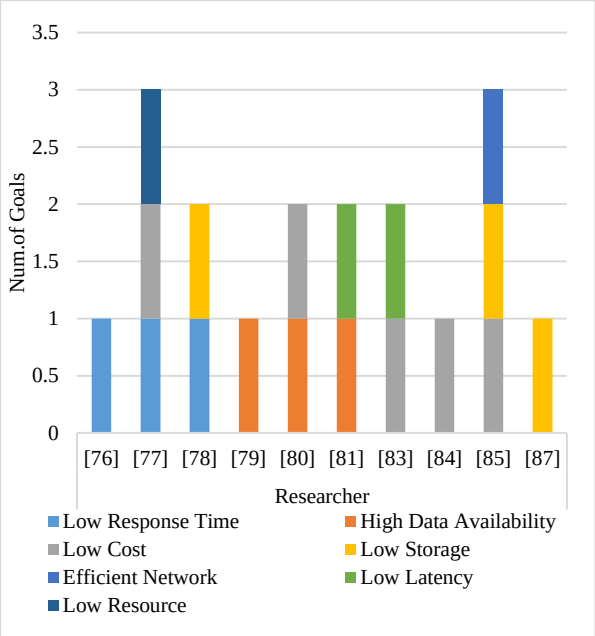


Fig. 6. Various goals achieved.

Fig. 6 is the bar chart that summarizes the key features and goals achieved by the various data placement strategies as discussed in this subsection. Each bar represents the number of goals achieved by a specific strategy. The strategies are listed along the x-axis, and the number of goals achieved is represented on the y-axis. The different colors indicate which specific goals are achieved by each strategy. This visual representation helps to quickly understand the focus and effectiveness of each strategy in achieving key performance and efficiency metrics.

2) Data placement strategies with data center selection factors: Data center selection is another significant method to place replicas in the cloud replication system process. This method is frequently integrated with the data placement process in almost every replication strategy. However, it is a considerable critical portion of accomplishing the replication process, whereby essential factors are determined to select the appropriate data center and storage to store replica copies. Therefore, researchers developed numerous methods to ensure a suitable location was identified. Usually, researchers determine a few factors to ensure the best data center has been determined to place the replica copies. The proposed factors or parameters directly affect various performance enhancements, in cloud replication environments [73]. Subsequent discussions will be categorized based on the number of factors employed in the respective research works.

a) Six factors: The Fuzzy Self-Defence Algorithm (FSDA) was proposed by study [85], which focused on a novel data center selection method. The FSDA determines the optimal number of replicas without degrading performance by implying a prey-predator model based on a fuzzy system to reproduce communication between prey and predator populations. The input parameters included in the fuzzy inference are system availability, service time, load, energy consumption, latency, and centrality. The researcher introduced several formulations to obtain merit values evaluated to determine the best nodes to place replica copies. The study claimed to improve hit ratio, energy consumption, and availability.

b) Five factors: A similar objective was achieved by [48] via producing a comprehensive algorithm named Cost Function based on an Analytic Hierarchy Process for data replication strategy (CF-AHP). CF-AHP is a multi-criteria optimization model that addresses cost-effective replica placement strategies that reduce energy consumption in data centers in cloud replication environments. The cost function is deployed to determine the best data center candidates to place newly generated replicas. The data center selection criterion consists of mean service time, access rate, latency, load variance, and storage usage. In the computation, weights are deployed to facilitate the user's task of determining system needs in respective parameters. The study achieved its goal of saving energy usage in its architecture.

In the same year, the author discovered an enhanced idea by proposing two (2) different Multiple-Criteria Decision Analysis (MCDA) approaches to determine the best data center to store replicas [86]. The first approach is to choose the best candidate site, and a cost function is computed using the weightage relationship concept in multi-criteria optimization known as AHP (Analytic Hierarchy Process). The second approach is ELECTRE-I, which consists of three (3) crucial stages; introduction of weight of criteria and calculation of concordance indices, calculation of the discordance indices, and over-ranking correlations. The criteria are further calculated using a weightage sum to obtain the values used to distinguish among available data centers. This study's data center selection criterion induces cost function calculation using AHP to acquire data center merits. The criterion consists of mean service time, access rate, latency, load variance, and storage usage, as adapted from another study by [87]. The respective criteria are computed using dedicated mathematical formulations. Results in this study evidenced that the cost function is sufficient to identify a candidate data center to place the replicas. The data center with the lowest cost value function is chosen to store the replica copies. Furthermore, when the system has insufficient space in storage nodes, replacement strategies are anticipated in this research work. This data center selection criteria method has

attained efficient bandwidth usage and minimized data movement.

Another researcher developed a novel intelligent approach for dynamic data replication in a cloud environment [88]. The proposed algorithm in this research is bio-based. The first is the Multi-Objective Particle Swarm Optimization (MO-PSO), which selects a replica depending on the most requested. Second is the Ant Colony Optimization (MO-ACO) to retrieve the best replica placement decision. A data center selection criterion was used in this study using MO-ACO through comparing individual data centers based on the shortest distance, data centers with high access, storage capacity, and output, and data centers with a high number of hosts and VMs. All factors were compared, and the best data center with the highest data availability was selected to store replica copies. The study achieved betterments in replication cost by accelerating the response time and replication time and succeeded in enhancing network usage efficiency.

c) Four factors: In the same year, [67] proposed a CSO-based approach for Secure Data Replication (SDR) that uses fuzzy inferences to select the best data center to place replica copies. The data center selection criterion trained in the fuzzy inference is fewer than FSDA and centrality, energy, storage usage, and load. The best data center is selected via a fuzzy approach, and the data is chucked into a few segments to place in a few different storage nodes based on data center capacity. The parallel downloads can reduce download time and security because data files segregated in a few chunks in diverse data centers will not be meaningful if attackers compromise either one of the servers or data centers in cloud replication.

Another researcher focused on addressing optimization problems in a cloud replication environment [50]. The researcher enhanced the ant lion optimizer (ALO) algorithm and a fuzzy system by introducing a heuristic ALO (HH-ALO-Tabu). The proposed algorithm works dynamically in selecting the primary population based on chaotic maps (CMs), opposition-based learning (OBL), and random walk strategies depending on the differential evolution (DE) algorithm. The placement of replicas is based on four key parameters: service time, system availability, load variance, and providers' expenditures. With the key parameters, the selection of the best data center is determined, and replicas are placed accordingly. The study effectively guaranteed the cloud providers' economic revenue hands increased the users' satisfaction in upgrading the performance in cloud replication environments.

d) Three factors: Dynamic Popularity-aware Replication Strategy (DPRS) [89] constitutes a data center selection method to determine the best data center. The data center selection method is the final contribution to the research work, and it was implemented in every cluster with consideration of several significant factors. The factors are the number of file requests, storage availability, and data center distance. Each factor is computed to obtain average values in this phase, called data center merit. In this study, the weightage concept was adapted in the data center merit computation, whereby system administrator intervention was required to identify the necessary weights according to the system goals. Once the best data centers are determined, the candidate file is chunked to certain data block sizes and sent to a predetermined number of distributed storage nodes. DPRS attained efficient network usage with a parallel download concept and reduced replication frequency with the proposed data center selection method.

e) Two factors: Researchers proposed a replication placement and replacement technique with fuzzy-based deletion (HRS) for heterogeneous cloud data centers [90]. The study goal was to preserve storage space and enhance network efficiency. Thus, HRS ascertains the data center merit approach by considering a few significant parameters, such as the number of accesses and centrality with weightage for each parameter before the replica in storage nodes. The researcher selected a data center based on the temporal locality concept. Therefore, the data center with the highest access is considered in this study as closeness centrality. Subsequently, this researcher introduced the factors and computation to identify the lowest total cost provider. Additionally, HRS introduced fuzzy inference in the replacement strategy, which has insufficient space to store new replicas during storage. Therefore, the developed fuzzy algorithm will clarify existing files in other nodes and the last access history of a specific replica and predict future access to the replica. The researcher proved this by conducting beneficial experiments to address storage imbalance, insufficient response time, and high network usage.

Researchers [8] proposed Data Mining-based Data Replication (DMDR) in their research, which used data center selection criteria to select the best data center in the cloud replication environment. This study improvises storage utilization by introducing two (2) criteria; most central and the number of accesses. An accumulation using closeness formulation by [91] was adopted in DMDR. The weightage is used in the formulation, ensuring the system administrator has the authority to fulfill the system objective accordingly. Finally, if the data center does not have adequate storage space, the replacement strategy will be applied to delete unnecessary replicas based on predetermined factors. The researcher intended to minimise network usage during file retrieval by introducing this data center criterion.

Reducing the financial burden associated with excessive duplication presented by [54] with an approach to distribute Online Social Network (OSN) data across different Cloud Service Providers (CSPs). Their study presented an algorithm that uses metrics like access and interaction rates to determine which data objects are the most popular and in what order. The algorithm then calculates the minimum number of replica copies needed and places them in the best storage class. The storage of data is classified as Reduced Redundancy Storage (RRS), Standard Storage (SS), or Infrequent Access Storage (IAS), and distinct data are mapped to be placed in the most appropriate storage. Furthermore, when data becomes less often accessed over time, the system automatically switches to the Reduced Redundancy Storage (RRS) class by modifying the storage class dynamically based on access patterns. The study obtained low storage consumption with a minimum number of replica copies.

f) One factor: Research by [92] embarked on a dynamic replication approach that addresses massive data movement among data centers in the cloud. The author proposed an inter-

data center data replication system with a Bandwidth Dynamic Separation algorithm called BDS+. The algorithm aims to speed up data transfer via adapting dynamic bandwidth separation, ensuring bandwidth is allocated for online traffic through estimating traffic demand and rescheduling bulk-data transfers for offline data services. It uses application-level multicast on the network with centralised architecture, which appoints the central controller to manage intermediate server data transmission. The researcher effectively improved bandwidth in this study.

The researcher proposed a cost-effective Hybrid PSO TS (HPSOTS) algorithm [93], which places restricted data copies in predetermined storage nodes to reduce energy consumption as the primary goal. The researcher used PSO's ability and TS's sturdy local search capability to obtain results on the appropriate data center to place replicas. Metaheuristic approaches were deployed to address the energy optimization issue via integrating Particle Swarm Optimization (PSO) and Tabu Search (TS) algorithms in their study. HPSOTS can determine the number of replicas before replication activities are triggered in a cloud environment. The integration of TS and PSO collaboratively exchanges inputs and eventually places the particles among six (6) fixed cloud data centers in encoded orders. The researchers succeeded in decreasing energy consumption and cost.

Conversely, [69] proposed the Replica Placement Based on Load Balance (RPBLB) technique to select the best data center to place replicas. The study aims to reduce remote users' access time. As replicas must always have fast retrieval rates, replicas must be placed in the closest nodes to users. Therefore, RPBLB most frequently duplicates access data in new storage nodes based on user demand for particular files. Research goals were achieved with response time reduced during user file download because data are kept in the closest data center.

An integrated algorithm between the Location-Aware Storage Technique (LAST) and the open-source Hadoop Distributed File System (HDFS) called LAST-HDFS was proposed by [94]. The study addressed the reliability of cloud providers and data integrity issues when users store their data in unknown storage locations. Unlike other research work, the LAST-HDFS did not use many parameters to determine the best data center to store data. On the other hand, the proposed algorithm allocated replicas to the data center by considering user-specified privacy policies. Users who store data in the same region place Every piece of data based on similar privacy preferences. The proposed algorithm proactively performs data placement balancing within the clusters and finally protects illegal data transfers through monitoring socket communications during migration or the replication process in the cloud environment. The study achieved high security by storing data according to privacy needs.

Table III summarizes the different strategies and number of factors considered for data placement in cloud replication environments. Fig. 7 depicts the factors employed in the data placement formulation to store the replica copies. No obvious trends suggest the number of factors considered has changed over time. Instead, to address some challenges, researchers have used these factors selectively, depending on their own research goals.

Holistically, every study shares similar research goals to improve performance in cloud replication environments, yet some ignored parallel drawbacks in their research. Existing studies contributed novel placement strategies for placing the replica copies in appropriate storage nodes. Table IV. includes a summary of existing research on data placement strategies, which comprises the contributions of every work.

TABLE III. SUMMARY OF DATA PLACEMENT STRATEGIES IN CLOUD REPLICATION

Strategy	Researcher Id	Number of Factors
FSDA	[85]	6
CF-AHP	[48]	5
MCDA	[86]	5
MO-ACO	[88]	5
HH-ALO-Tabu	[50]	4
SDR	[67]	4
DPRS	[89]	3
DMDR	[8]	2
HRS	[90]	2
OSN	[54]	2
LAST-HDFS	[94]	1
BDS+	[92]	1
HPSOTS	[93]	1
RPBLB	[69]	1

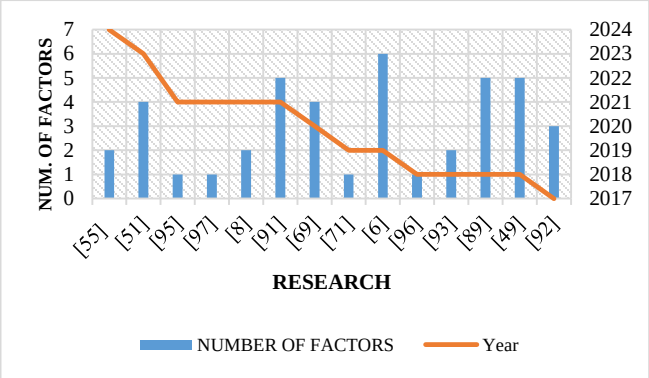


Fig. 7. Data placement factors.

C. RQ3: What are the Performance Metrics that Contribute to the Enhancement of Replica Placement Strategies in Cloud Replication Environments?

The existing research on data placement strategies in cloud replication environments has addressed various performance metrics advancement. As in Fig. 8, Efficient Network Usage (26%), Low Storage Usage (19%), and Low Response Time (18%) are the most significant advantages, collectively accounting for 63% of the total achievements. These metrics ensure efficient resource utilization, minimize storage costs, and provide timely data access in cloud replication environments.

TABLE IV. CONTRIBUTION DATA PLACEMENT STRATEGIES IN CLOUD REPLICATION

Ref.	Contribution Algorithm
[77]	Controlled Replication Under Scalable Hashing (CRUSH)
[74]	Heuristic Data Placement
[89]	Dynamic Popularity aware Replication Strategy (DPRS)
[84]	Security Level (SL-DRM)
[93]	Hybrid PSO TS (HPSOTS)
[90]	Hybrid data Replication Strategy (HRS)
[48]	Cost Function based on Analytic Hierarchy Process (CF-AHP)
[86]	Multiple-Criteria Decision Analysis (MCDA)
[69]	Replica Placement Based on Load Balance (RPBLB)
[8]	Data Mining-based Data Replication (DMDR)
[85]	Fuzzy Self-Defence Algorithm (FSDA)
[67]	Secure Data Replication (SDR)
[81]	Cost-Effective Dynamic Data Placement
[82]	Dynamic Replica Placement Strategy
[78]	Improving Clustering Based Critical Parent (CbCP)
[75]	Achieving Query Performance in the Cloud via Cost-effective Data Replication (APER)
[92]	Bandwidth Dynamic Separation (BDS+)
[94]	Location-Aware Storage Technique (LAST) and Hadoop Distributed File System (HDFS) called LAST-HDFS
[88]	Multi-Objective Particle Swarm Optimization (MO-PSO) and Ant Colony Optimization (MO-ACO)
[80]	Multi-objective optimization data placement model
[76]	Time Series-based Deduplication and Optimal Data Placement Strategy (TDOPS)
[50]	ALO (HH-ALO-Tabu)
[83]	Dynamic data replication and placement strategy
[95]	Initialization Scheme-Based GA (ISGA)
[54]	Distribute Online Social Network (OSN)

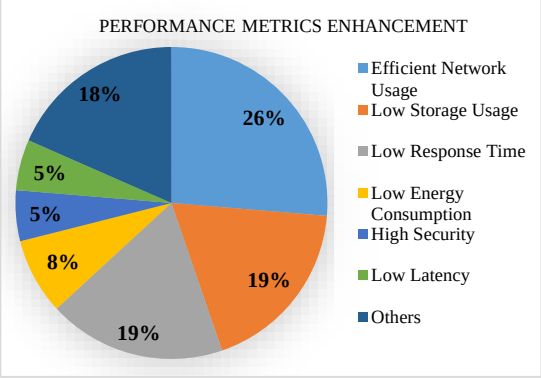


Fig. 8. Performance metrics.

Low Energy Consumption (8%), Low Latency, and High Security (5%) are also notable achievements. Other advantages of various performance metrics, such as low cost, high data availability, increased revenue, high user satisfaction, high load balance, and high hit ratio, are contributing to another 18% advancement. This stastical chart shows researchers' aims and successfully addresses various aspects of performance in cloud replication environments.

D. RQ4: What are the Common Limitations Across Existing Research on Data Placement Strategies in Cloud Replication Environments?

Here are the limitation in respective research works as discussed in RQ2:

- Researchers in [74] proposed a replica placement strategy that minimizes the evaluation cost. However, the disadvantage of this research is high bandwidth usage when queries are locked, and much hopping involved till the replicas are retrievable.
- The enhanced CRUSH algorithm [77] can dynamically place data and obtain data, which outstrips the previous study, yet data reliability issues are undeniable. The possibility of data loss is very high during data placement because when a dataset is sent to a particular server, any inevitable matters can happen at the server's level, such as server crashes or network breakdowns.
- SL-DRM achieved low storage consumption with a limited number of replica copies for videos [84]. Conversely, the major concern in this study was that the data availability was uncertain as crucial files were copied to unknown locations.

- The researcher [81] proposed cost-effective dynamic data placement using greedy algorithms. The solution was complex in formulation and caused extensive bandwidth usage while collecting numerous data, and prior decisions were made for replica creation and placement. Thus, computation overheads are a major drawback in this study.
- Researcher in study [82] proposed a Dynamic Replica Placement that focuses on financial cost reduction with good data consistency. As saving cost, storage space and consistency were the primary aims of this research, the data availability was neglected as it was not measured in this study.
- The ICR aims to identify the earliest available resource and time slots to proceed with replica replication until replica placement [78]. The trade-off in this study is high network usage due to the algorithm imposing an increased number of tasks to be executed whenever resources are available, and replica placement will occur endlessly. Furthermore, high energy consumption is another disadvantage in this study because resources are continuously used without idle time.
- Researchers in [75] developed the APER, a data replication strategy that allows a file to be replicated many times as long as it is profitable for both the tenant and cloud provider based on revenue and expenditures. The drawback is the high replication time affected by the overdue process of verifying every task to comply with the profitable criterion before the replication process and placement.
- In a hybrid Fog-Cloud environment, researcher Salah suggests a multi-objective optimization data placement model based on numerous data replicas [80]. Overall, the articles point to the possibility that while focusing on AI to minimize latency and improve data location the risks of data leakage concerning data privacy and the high requirement for specialist hardware and software are issues unattended in this study.
- The TDOPS with deduplication technique introduced in another study [76], overlooked the high replication time due to deduplication imposing a longer time for processing.
- Dynamic data replication management techniques notably focus on the costs related to storage and network use, ignoring the possibility of optimization through storage use [83].
- Researchers in study [95] adopted the ISGA, an interval pricing technique in multi-cloud environments, which has a primary disadvantage in the contributions of neglected cost-cutting strategies like resource optimization.
- The Dynamic Popularity-aware Replication Strategy (DPRS) [89] constitutes a data center selection method to determine the best location for replica placement. The researcher disregarded fault tolerance due to a heavy traffic load. Then the system will suffer from data loss and high response delay too.
- The HPSOTS algorithm was proposed by the researcher [93]. The data availability is relatively low due to the static number of replicas fixed in the strategy. Thus, any decisive data might not have sufficient copies, affecting poor availability and high wait time for file downloads.
- The researcher in study [90] proved the proposed HRS was beneficial to address storage imbalance, low response time, and high network usage. However, the system performance might suffer from execution overheads caused by extended verification time using the fuzzy technique.
- CF-AHP is a multi-criteria optimization model to save energy usage in their architecture [48]. The research disregarded the impact on the central database, which suffers a high update rate during replication.
- The Criteria Decision Analysis (MCDA) approach to determine the best data center to store replicas [86]. High energy usage and high replication time were neglected in this study.
- Researchers in study [71] propose the RPBLB strategy that requires additional storage to place replicas at the nearest data center. The algorithm demands extra time to verify the appropriate data center to store the replicas, thus affecting high process time.
- The additional computation time is identified in DMDR proposed by the researcher [8]. It has insufficient storage, and a high replication process while computing several factors during replica replacement activities that eventually delay the replication process.
- The researcher [85] and [67], introduced Fuzzy inferences in their placement strategies. Both researchers overlooked the fuzzy inference, causing a high process that derives a high response time. Concurrently, the proposed algorithm causes high storage consumption in [85].
- Research by [92] proposed an inter-data center data replication system that effectively improved bandwidth usage but overlooked high replication time. The algorithm requires more time to sort the traffic schedule than only triggering the replication process until the replica placement is complete.
- An integrated algorithm called LAST-HDFS was proposed by [94] achieved high security by storing data according to privacy classifications. However, the algorithm is cost-expensive due to the sophisticated security features. Another drawback in the research is high network usage caused by location monitoring and detection requiring data collection in real-time.
- Researchers [91] proposed a bio-based algorithm that overlooked the trade-off of computations overheads and high replication frequencies.

- Drawbacks in the heuristic ALO (HH-ALO-Tabu) strategy introduced by [50] is computational overheads.
- To decrease the financial liability associated with excessive duplication, [54] presented a strategy to distribute Online Social Network (OSN) data copies across a few Cloud Service Providers (CSPs). The study overlooked the impact of high costs and varying levels of data availability, which could present additional challenges when utilizing different services from various cloud service providers (CSPs).

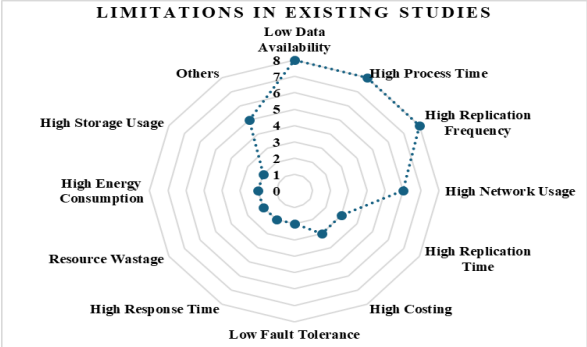


Fig. 9. Limitations in existing studies.

Fig. 9 and Table V present detailed analyses of common limitations in existing data placement strategies within cloud replication environments revealing several recurrent issues. The most frequently identified limitations include low data availability, high process time, and high replication frequency among 8 respective research studies (32%). These metrics indicate that many current strategies struggle to maintain consistent data access, handle data efficiently, and manage replication activities without excessive resource consumption. High network usage is down the road, with 6 research works contributing 24% of similar limitations. High-cost drawbacks (12%) are also significant concerns, highlighting inefficiencies in data transfer mechanisms and economic viability. These issues' occurrence emphasizes room for improvement and hinders performance degradation in replication activities.

TABLE V. RESEARCH WITH COMMON LIMITATIONS

Performance Metric	Authors
Low Data Availability	[77] [89] [93] [67] [82] [78] [54]
High Process Time	[90] [86] [85] [75] [92] [88] [80] [76] [50]
High Replication Frequency	[89] [84] [93] [8] [85] [92] [94] [88]
High Network Usage	[74] [85] [67] [81] [78] [94]
High Replication Time	[86] [75] [76]
High Costing	[69] [94] [80]
Low Fault Tolerance	[77] [89]
High Response Time	[48] [75]
Resource Wastage	[50] [83]
High Energy Consumption	[85] [78]
High Storage Usage	[89] [78]
Others	[89] [48] [75] [88] [80]

Numerous existing research works revealed that cloud computing has been the most prevalent platform for many other researchers' works [96]–[99]. Similarly, addressing these cloud replication limitations is critical for enhancing cloud computing environments' overall performance and reliability [100], [101]. Future research should prioritize the betterment of strategies that mitigate these common issues. By tackling these challenges, researchers can contribute to more robust and efficient data placement strategies, ultimately leading to more cost-effective and high-performing cloud services. Ensuring these improvements will be essential for meeting the increasing demands of cloud computing and providing reliable and accessible data management services.

V. CONCLUSION AND FUTURE DIRECTIONS

This paper presented a thorough taxonomic analysis of data placement strategies in cloud replication systems and has uncovered several important insights into this crucial area of cloud computing. This study has identified and categorized several techniques through this systematic review according to their primary goals, selection criteria for data placement, and performance metrics. The results suggest that placement strategies provide dynamic approaches that exhibit exceptional flexibility in response to shifting goal requirements. The study explicitly underscores how placement strategies have emerged as viable approaches to optimizing replica distribution in intricate cloud environments.

This study delivers a theoretical contribution that provides insights into existing research works by crafting a novel taxonomy for data placement strategies in cloud replication environments. The comprehensive analysis and discussion stipulate trends in replication performance enhancement. Further, gaps in existing studies are highlighted, forecasting new ideas for future researchers to develop a novel replication strategy to address the most prominent issues in cloud replication environments.

As for practical implications, this taxonomy study offers collections of replication strategies that allow cloud providers to scrutinize and adapt them in real-cloud replication settings. Hence, cloud providers can serve accelerated performance to users with better data availability, faster response time, low fault tolerance, reduced storage usage, and efficient network usage. This may offload pressure from cloud users' demands for quick data access, high data availability, fast replication process, low storage consumption, and affordable data maintenance.

Cloud technologies are evolving so quickly; thus, the taxonomy in this study may not fully encompass all new or specialized data placement techniques. Forthcoming tactics might differ greatly from those examined in this research. Future research can advance the field by addressing these gaps with more thorough literature discovery and provide practical solutions for efficient and dynamic data placement in cloud environments. Additionally, as the multi-cloud and hybrid cloud deployments grow more prevalent, data placement solutions that optimize across many cloud providers and on-premises infrastructure should be the focus of future studies. This is crafting strategies that can easily handle data placement in various distributed and heterogeneous situations. Besides, future researchers, policymakers, and professionals are suggested to

explore more effective and dependable data placement, which could be ensured by utilizing artificial intelligence approaches to anticipate and adjust to changing circumstances. Real-world adaption may entail expanding and placing these ideas into practice by collaborating with businesses that use multi-cloud configurations.

ACKNOWLEDGMENT

This study is supported by the National University of Malaysia (UKM) (GGPM-2023-072). Sincerely grateful for the facilities and funding provided, which were essential for completing this research.

REFERENCES

[1] R. Kaur, I. Chana, and J. Bhattacharya, "Data deduplication techniques for efficient cloud storage management: a systematic review," J. Supercomput., vol. 74, no. 5, pp. 2035–2085, 2018, doi: 10.1007/s11227-017-2210-8.

[2] S. Nannai John and T. T. Mirnalinee, "A novel dynamic data replication strategy to improve access efficiency of cloud storage," Inf. Syst. E-bus. Manag., vol. 18, no. 3, pp. 405–426, 2020, doi: 10.1007/s10257-019-00422-x.

[3] M. Wang, Y. Qin, J. Liu, and W. Li, "Identifying personal physiological data risks to the Internet of Everything: the case of facial data breach risks," Humanit. Soc. Sci. Commun., vol. 10, no. 1, pp. 1–15, 2023, doi: 10.1057/s41599-023-01673-3.

[4] Y. Shao, C. Li, Z. Fu, L. Jia, and Y. Luo, "Cost-effective replication management and scheduling in edge computing," J. Netw. Comput. Appl., vol. 129, no. May 2018, pp. 46–61, 2019, doi: 10.1016/j.jnca.2019.01.001.

[5] K. Rajalakshmi, M. Sambath, L. Joseph, K. Ramesh, and R. Surendiran, "An Effective Approach for Improving Data Access Time using Intelligent Node Selection Model (INSM) in Cloud Computing Environment," SSRG Int. J. Electr. Electron. Eng., vol. 10, no. 5, pp. 174–184, 2023, doi: 10.14445/23488379/IJEEE-V10I5P116.

[6] D. Mrozek, "A review of Cloud computing technologies for comprehensive microRNA analyses," Comput. Biol. Chem., vol. 88, no. July, p. 107365, 2020, doi: 10.1016/j.compbiolchem.2020.107365.

[7] A. Shakarami, M. G. Ali, S. Mohammad, and M. Hamid, "Data Replication Schemes in Cloud Computing : A Survey," Cluster Comput., vol. 7, 2021, doi: 10.1007/s10586-021-03283-7.

[8] N. Mansouri, M. M. Javidi, and B. Mohammad Hasani Zade, "Using data mining techniques to improve replica management in cloud environment," Soft Comput., vol. 0123456789, 2019, doi: 10.1007/s00500-019-04357-w.

[9] C. Li, Y. Wang, H. Tang, and Y. Luo, "Dynamic multi-objective optimized replica placement and migration strategies for SaaS applications in edge cloud," Futur. Gener. Comput. Syst., vol. 100, pp. 921–938, 2019, doi: 10.1016/j.future.2019.05.003.

[10] M. Vikhe and J. Malhotra, "A Review on Backup-up Practices using Deduplication," vol. 4, no. 9, pp. 338–344, 2015.

[11] S. Logesswari, S. Jayanthi, D. Kalaiselvi, S. Muthusundari, and V. Aswin, "Materials Today : Proceedings A study on cloud computing challenges and its mitigations," Mater. Today Proc., no. xxxx, 2020, doi: 10.1016/j.matpr.2020.10.655.

[12] U. Khalil, Mueen-Uddin, O. A. Malik, and S. Hussain, "A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art Advancements, Challenges and Future Research Directions," IEEE Access, vol. 10, no. June, pp. 76805–76823, 2022, doi: 10.1109/ACCESS.2022.3189998.

[13] A. Tripathi and A. Mishra, "Cloud computing security considerations," 2011 IEEE Int. Conf. Signal Process. Commun. Comput. ICSPCC 2011, 2011, doi: 10.1109/ICSPCC.2011.6061557.

[14] N. Mansouri, R. Ghafari, and B. M. H. Zade, "Cloud computing simulators: A comprehensive review," Simul. Model. Pract. Theory, vol. 104, no. July, 2020, doi: 10.1016/j.simpat.2020.102144.

[15] A. Arivuselvi, T. Amudha, P. Deepan Babu, and M. P. Scholar, "An Effective Ant Colony Optimization Methodology For Virtual Machine Placement In Cloud Data Centre," turcomat.org, vol. 12, no. 10, pp. 3460–3467, 2021, Accessed: Aug. 07, 2023. [Online]. Available: https://www.turcomat.org/index.php/turkbilmat/article/view/5024

[16] F. A. M. Ibrahim and E. E. Hemayed, "Trusted Cloud Computing Architectures for infrastructure as a service: Survey and systematic literature review," Comput. Secur., vol. 82, pp. 196–226, 2019, doi: 10.1016/j.cose.2018.12.014.

[17] T. Lynn, P. Rosati, A. Lejeune, and V. Emeakaroha, "A Preliminary Review of Enterprise Serverless Cloud Computing (Function-as-a-Service) Platforms," Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, vol. 2017-Decem, pp. 162–169, 2017, doi: 10.1109/CloudCom.2017.15.

[18] V. C. Pezoulas, T. P. Exarchos, and D. I. Fotiadis, Cloud infrastructures for data sharing, no. iii. 2020. doi: 10.1016/b978-0-12-816507-2.00006-2.

[19] F. Lui et al., "NIST Cloud Computing Reference Architecture: Recommendations of NIST," 2011.

[20] C. Ji, Y. Li, W. Qiu, U. Awada, and K. Li, "Big data processing in cloud computing environments," Proc. 2012 Int. Symp. Pervasive Syst. Algorithms, Networks, I-SPAN 2012, pp. 17–23, 2012, doi: 10.1109/I-SPAN.2012.9.

[21] K. Grolinger, W. A. Higashino, A. Tiwari, and M. A. M. Capretz, "Data management in cloud environments: NoSQL and NewSQL data stores," J. Cloud Comput., vol. 2, no. 1, 2013, doi: 10.1186/2192-113X-2-22.

[22] M. Yang, "Inverted Ant Colony Optimization Algorithm for Data Replication in Cloud Computing," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 7, pp. 1029–1038, 2023, doi: 10.14569/IJACSA.2023.01407111.

[23] V. Chang, "Towards a Big Data system disaster recovery in a Private Cloud," Ad Hoc Networks, vol. 35, pp. 65–82, 2015, doi: 10.1016/j.adhoc.2015.07.012.

[24] M. M. Alshammari, A. A. Alwan, A. Nordin, and A. Z. Abualkishik, "Disaster Recovery with Minimum Replica Plan for Reliability Checking in Multi-Cloud," Procedia Comput. Sci., vol. 130, pp. 247–254, 2018, doi: 10.1016/j.procs.2018.04.036.

[25] Y. Jun and Y. Lihong, "The Cloud Technology Double Live Data Center Information System Research and Design Based on Disaster Recovery Platform," Procedia Eng., vol. 174, pp. 1356–1370, 2017, doi: 10.1016/j.proeng.2017.01.289.

[26] N. Chaturvedi, "Analysis of Replication and Replication Algorithms in Distributed System," vol. 2, no. 5, pp. 261–266, 2012.

[27] S. George and E. B. Edwin, "A Review on Data Replication Strategy in Cloud Computing," 2017 IEEE Int. Conf. Comput. Intell. Comput. Res. ICCIC 2017, pp. 1–4, 2018, doi: 10.1109/ICCIC.2017.8524269.

[28] M. Zheng, X. Du, Z. Lu, and Q. Duan, "A balanced and reliable data replica placement scheme based on reinforcement learning in edge–cloud environments," Futur. Gener. Comput. Syst., vol. 155, no. November 2023, pp. 132–145, 2024, doi: 10.1016/j.future.2024.02.004.

[29] M. Shorfuzzaman and M. Masud, "Leveraging a multi-objective approach to data replication in cloud computing environment to support big data applications," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 3, pp. 418–429, 2019, doi: 10.14569/IJACSA.2019.0100354.

[30] S. S. Saleh, I. Alansari, M. K. Hamiaz, W. Ead, R. A. Tarabishi, and H. Khater, "iFogRep: An intelligent consistent approach for replication and placement of IoT based on fog computing," Egypt. Informatics J., vol. 24, no. 2, pp. 327–339, 2023, doi: 10.1016/j.eij.2023.05.003.

[31] N. N. M.-R. O. B. D. R. in C. C. Vishnoi-I, V. Singh, S. Sharma, and P. Kumar, "Enhanced Naked Mole-Rat Optimization Based Data Replication in Cloud Computing," Int. J. Intell. Syst. Appl. Eng., vol. 12, no. 3s, pp. 355 – 362, 2024, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85179340068&partnerID=40&md5=924d44ff456f26dcb0fef55fdfbb7d55

[32] R. Mokadem and A. Hameurlain, "A data replication strategy with tenant performance and provider economic profit guarantees in Cloud data centers," J. Syst. Softw., vol. 159, p. 110447, 2020, doi: 10.1016/j.jss.2019.110447.

[33] M. Seguela, R. Mokadem, and J.-M. Pierson, "Comparing energy-aware vs. cost-aware data replication strategy," Int. Green Sustain. Comput. Conf., pp. 1–8, 2020, doi: 10.1109/igsc48788.2019.8957206.

[34] B. Arasteh, S. S. Sefati, S. Halunga, O. Fratu, and T. Allahviranloo, "A Hybrid Heuristic Algorithm Using Artificial Agents for Data Replication Problem in Distributed Systems," Symmetry (Basel)., vol. 15, no. 2, 2023, doi: 10.3390/sym15020487.

[35] N. K. Gill and S. Singh, "A dynamic, cost-aware, optimized data replication strategy for heterogeneous cloud data centers," Futur. Gener. Comput. Syst., vol. 65, pp. 10–32, 2016, doi: 10.1016/j.future.2016.05.016.

[36] B. Alami Milani and N. Jafari Navimipour, "A comprehensive review of the data replication techniques in the cloud environments: Major trends and future directions," J. Netw. Comput. Appl., vol. 64, pp. 229–238, 2016, doi: 10.1016/j.jnca.2016.02.005.

[37] B. Alami Milani and N. Jafari Navimipour, "A Systematic Literature Review of the Data Replication Techniques in the Cloud Environments," Big Data Res., vol. 10, no. C, pp. 1–7, 2017, doi: 10.1016/j.bdr.2017.06.003.

[38] C. Li, Y. Wang, H. Tang, Y. Zhang, Y. Xin, and Y. Luo, "Flexible replica placement for enhancing the availability in edge computing environment," Comput. Commun., 2019, doi: 10.1016/j.comcom.2019.07.013.

[39] K. Sabaghian, K. Khamforoosh, and A. Ghaderzadeh, "Data Replication and Placement Strategies in Distributed Systems: A State of the Art Survey," Wireless Personal Communications, vol. 129, no. 4. Springer, pp. 2419–2453, Apr. 01, 2023. doi: 10.1007/s11277-023-10240-7.

[40] S. Yazdani, A. Shirvani, and P. Heidarpoor, "A Model for the Taxonomy of Research Studies: A Practical Guide to Knowledge Production and Knowledge Management," Archives of Pediatric Infectious Diseases, vol. 9, no. 4. 2021. doi: 10.5812/pedinfect.112456.

[41] P. Elango, K. Kuppusamy, and N. Prabhu, "Data Replication Using Data Mining Techniques," Asian J. Comput. Sci. Technol., vol. 8, no. S1, pp. 107–109, 2021, doi: 10.51983/ajcst-2019.8.s1.1939.

[42] I. Kuraj, A. Solar-Lezama, and N. Polikarpova, "POSTER: Optimizing Consistency for Partially Replicated Data Stores," Proc. ACM SIGPLAN Symp. Princ. Pract. Parallel Program. PPOPP, pp. 457–458, 2022, doi: 10.1145/3503221.3508438.

[43] C. B. Tan, M. H. A. Hijazi, Y. Lim, and A. Gani, "A survey on Proof of Retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends," J. Netw. Comput. Appl., vol. 110, no. August 2017, pp. 75–86, 2018, doi: 10.1016/j.jnca.2018.03.017.

[44] N. K. Nivetha and D. Vijayakumar, "Modeling fuzzy based replication strategy to improve data availabiity in cloud datacenter," in 2016 International Conference on Computing Technologies and Intelligent Data Engineering, ICCTIDE 2016, IEEE, 2016, pp. 1–6. doi: 10.1109/ICCTIDE.2016.7725322.

[45] Q. Liu, G. Wang, and J. Wu, "Consistency as a service: Auditing cloud consistency," IEEE Trans. Netw. Serv. Manag., vol. 11, no. 1, pp. 25–35, 2014, doi: 10.1109/TNSM.2013.122613.130411.

[46] R. D and G. A, "Optimization assisted frequent pattern mining for data replication in cloud: Combining sealion and grey wolf algorithm," Adv. Eng. Softw., vol. 176, no. January, p. 103401, 2023, doi: 10.1016/j.advengsoft.2022.103401.

[47] J. Wang, H. Wu, and R. Wang, "A new reliability model in replication-based big data storage systems," J. Parallel Distrib. Comput., vol. 108, pp. 14–27, 2017, doi: 10.1016/j.jpdc.2017.02.001.

[48] M. R. Djebbara and H. Belbachir, "Cost Function Based On Analytic Hierarchy Process for Data Replication Strategy in Cloud Environment," J. Theor. Appl. Inf. Technol., vol. 96, pp. 2638–2648, 2018.

[49] F. Xie, J. Yan, and J. Shen, "Towards Cost Reduction in Cloud-Based Workflow Management through Data Replication," 2017 Fifth Int. Conf. Adv. Cloud Big Data, pp. 94–99, 2017, doi: 10.1109/CBD.2017.24.

[50] B. Mohammad Hasani Zade, N. Mansouri, and M. M. Javidi, A new hyper-heuristic based on ant lion optimizer and Tabu search algorithm for replica management in cloud environment, vol. 56, no. 9. Springer Netherlands, 2023. doi: 10.1007/s10462-022-10309-y.

[51] B. Spinnewyn, J. F. Botero, and S. Latre, "Cost-effective replica management in fault-tolerant cloud environments," in 2017 13th International Conference on Network and Service Management, CNSM 2017, 2018, pp. 1–9. doi: 10.23919/CNSM.2017.8256019.

[52] N. Mansouri, M. M. Javidi, and B. M. H. Zade, "Hierarchical data replication strategy to improve performance in cloud computing," Front. Comput. Sci., vol. 15, no. 2, 2021, doi: 10.1007/s11704-019-9099-8.

[53] A. Khelifa, T. Hamrouni, R. Mokadem, and F. Ben Charrada, "SLA-aware task scheduling and data replication for enhancing provider profit in clouds," Procedia Comput. Sci., vol. 176, pp. 3143–3152, 2020, doi: 10.1016/j.procs.2020.09.174.

[54] A. Y. Aldailamy, A. Muhammed, R. Latip, N. A. W. A. Hamid, and W. Ismail, "Online dynamic replication and placement algorithms for cost optimization of online social networks in two-tier multi-cloud," J. Netw. Comput. Appl., vol. 224, p. 103827, 2024, doi: 10.1016/j.jnca.2024.103827.

[55] M. A. Fazlina, R. Latip, M. A. Alrshah, and S. Member, "Vigorous Replication Strategy with Balanced Quorum for Optimizing The Storage and Response Time in Cloud Environments," pp. 1–13, 2021.

[56] P. Zhao, X. Sun, J. Shang, J. Lin, M. Dong, and B. Li, "A Dynamic Convergent Replica Selection Strategy Based on Cloud Storage," Proc. - 2019 Int. Conf. Artif. Intell. Adv. Manuf. AIAM 2019, pp. 473–478, 2019, doi: 10.1109/AIAM48774.2019.00100.

[57] M. Liu, L. Pan, and S. Liu, "Cost Optimization for Cloud Storage from User Perspectives: Recent Advances, Taxonomy, and Survey," ACM Comput. Surv., vol. 55, no. 13s, Jul. 2023, doi: 10.1145/3582883.

[58] P. Souza, T. Ferreto, and R. Calheiros, "Maintenance Operations on Cloud, Edge, and IoT Environments: Taxonomy, Survey, and Research Challenges," ACM Comput. Surv., vol. 56, no. 10, Jun. 2024, doi: 10.1145/3659097.

[59] T. He and R. Buyya, "A Taxonomy of Live Migration Management in Cloud Computing," ACM Comput. Surv., vol. 56, no. 3, Oct. 2023, doi: 10.1145/3615353.

[60] Q. Waseem, W. I. S. Wan Din, S. S. Alshamrani, A. Alharbi, and A. Nazir, "Quantitative analysis and performance evaluation of target-oriented replication strategies in cloud computing," Electron., vol. 10, no. 6, pp. 1–49, 2021, doi: 10.3390/electronics10060672.

[61] S. Slimani, T. Hamrouni, and F. Ben Charrada, "Service-oriented replication strategies for improving quality-of-service in cloud computing: a survey," Cluster Comput., vol. 24, no. 1, pp. 361–392, 2021, doi: 10.1007/s10586-020-03108-z.

[62] J. Ma, G. Wang, and X. Liu, "DedupeSwift: Object-oriented storage system based on data deduplication," in IEEE Trustcom/BigDataSE/ISPA, IEEE, 2016, pp. 1069–1076. doi: 10.1109/TrustCom.2016.0177.

[63] L. Rajabion, A. A. Shaltooki, M. Taghikhah, A. Ghasemi, and A. Badfar, "Healthcare big data processing mechanisms: The role of cloud computing," Int. J. Inf. Manage., vol. 49, no. June 2017, pp. 271–289, 2019, doi: 10.1016/j.ijinfomgt.2019.05.017.

[64] D. L. J. C.Venish Raja, "A Cost Effective Scalable Scheme for Dynamic Data Service in Heterogeneous Cloud Environment," Int. J. Adv. Sci. Technol., vol. Vol. 28, N, no. January, 2020.

[65] B. Prasad Babu, P. Peddi, and S. Pappala, "Optimization for Dynamic Replication in Cloud Center," Int. J. Adv. Res. Arts, Sci. Eng. Manag., vol. 10, no. 5, pp. 2641–2646, 2023.

[66] M. A. Ahmed, M. H. Khafagy, M. E. Shaheen, and M. R. Kaseb, "Dynamic Replication Policy on HDFS Based on Machine Learning Clustering," IEEE Access, vol. 11, no. January, pp. 18551–18559, 2023, doi: 10.1109/ACCESS.2023.3247190.

[67] N. Mansouri, M. M. Javidi, and B. A. Mohammad Hasani Zade, "A CSO-based approach for secure data replication in cloud," J. Supercomput., vol. 77, no. 6, pp. 5882–5933, 2020, doi: 10.1007/s11227-020-03497-3.

[68] S. U. R. Malik et al., "Performance analysis of data intensive cloud systems based on data management and replication: a survey," Distrib. Parallel Databases, vol. 34, no. 2, pp. 179–215, 2016, doi: 10.1007/s10619-015-7173-2.

[69] X. Fu, J. Li, W. Liu, S. Deng, and J. Wang, "Data Replica Placement Policy Based on Load Balance in Cloud Storage System," 2019 IEEE 3rd

Inf. Technol. Networking, Electron. Autom. Control Conf., no. Itnec, pp. 682–685, 2019, doi: 10.1109/ITNEC.2019.8728995.

[70] K. Liu, J. Peng, J. Wang, W. Liu, Z. Huang, and J. Pan, "Scalable and adaptive data replica placement for geo-distributed cloud storages," IEEE Trans. Parallel Distrib. Syst., vol. 31, no. 7, pp. 1575–1587, 2020, doi: 10.1109/TPDS.2020.2968321.

[71] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," 12th Int. Conf. Eval. Assess. Softw. Eng. EASE 2008, no. June, 2008, doi: 10.14236/ewic/ease2008.8.

[72] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," Information and Software Technology, vol. 51, no. 1. Elsevier B.V., pp. 7–15, 2009. doi: 10.1016/j.infsof.2008.09.009.

[73] S. Mazumdar, D. Seybold, K. Kritikos, and Y. Verginadis, A survey on data storage and placement methodologies for Cloud-Big Data ecosystem, vol. 6, no. 1. Springer International Publishing, 2019. doi: 10.1186/s40537-019-0178-3.

[74] Q. Xia, W. Liang, and Z. Xu, "QoS-aware data replications and placements for query evaluation of big data analytics," IEEE Int. Conf. Commun., vol. 2017 IEEE, no. 2017, pp. 1–7, 2017, doi: 10.1109/ICC.2017.7997238.

[75] U. Tos, R. Mokadem, A. Hameurlain, and T. Ayav, "Achieving query performance in the cloud via a cost-effective data replication strategy," Soft Comput., vol. 25, no. 7, pp. 5437–5454, 2021, doi: 10.1007/s00500-020-05544-w.

[76] S. U. Muthunagai and R. Anitha, "TDOPS: Time series based deduplication and optimal data placement strategy for IIoT in cloud environment," J. Intell. Fuzzy Syst., vol. 43, no. 1, pp. 1583–1597, 2022, doi: 10.3233/JIFS-212568.

[77] P. Carns, K. Harms, J. Jenkins, M. Mubarak, R. Ross, and C. Carothers, "Impact of data placement on resilience in large-scale object storage systems," IEEE Symp. Mass Storage Syst. Technol., 2017, doi: 10.1109/MSST.2016.7897091.

[78] S. S. Mousavi Nik, M. Naghibzadeh, and Y. Sedaghat, "Task replication to improve the reliability of running workflows on the cloud," Cluster Comput., vol. 24, no. 1, pp. 343–359, 2021, doi: 10.1007/s10586-020-03109-y.

[79] R. Salem, M. A. Salam, H. Abdelkader, and A. Awad Mohamed, "An Artificial Bee Colony Algorithm for Data Replication Optimization in Cloud Environments," IEEE Access, vol. 8, pp. 51841–51852, 2020, doi: 10.1109/ACCESS.2019.2957436.

[80] N. Ben Salah and N. Bellamine Ben Saoud, An IoT-oriented Multiple Data Replicas Placement Strategy in Hybrid Fog-Cloud Environment, vol. 1, no. 1. Association for Computing Machinery, 2021. doi: 10.1145/3437959.3459251.

[81] H. Khalajzadeh, D. Yuan, B. B. Zhou, J. Grundy, and Y. Yang, "Cost effective dynamic data placement for efficient access of social networks," J. Parallel Distrib. Comput., vol. 141, pp. 82–98, 2020, doi: 10.1016/j.jpdc.2020.03.013.

[82] C. Li, J. Bai, Y. Chen, and Y. Luo, "Resource and replica management strategy for optimizing financial cost and user experience in edge cloud computing system," Inf. Sci. (Ny)., vol. 516, pp. 33–55, 2020, doi: 10.1016/j.ins.2019.12.049.

[83] L. Bouhouch, M. Zbakh, and C. Tadonki, "Dynamic data replication and placement strategy in geographically distributed data centers," in Concurrency and Computation: Practice and Experience, 2023. doi: 10.1002/cpe.6858.

[84] R. Li, J. Zhang, and W. Shen, "Replicas Strategy and Cache Optimization of Video Surveillance Systems Based on Cloud Storage," Futur. Internet, vol. 10, no. 4, p. 34, 2018, doi: 10.3390/fi10040034.

[85] N. Mansouri, B. Mohammad Hasani Zade, and M. M. Javidi, "A multi-objective optimized replication using fuzzy based self-defense algorithm for cloud computing," J. Netw. Comput. Appl., vol. 171, no. October 2019, p. 102811, 2020, doi: 10.1016/j.jnca.2020.102811.

[86] M. R. Djebbara and H. Belbachir, "Cloud data replication strategy using multiple-criteria decision analysis methods," Multiagent Grid Syst., vol. 14, no. 2, pp. 203–218, 2018, doi: 10.3233/mgs-180288.

[87] M. Radi, "Replica Placement Strategy Based on Analytic Hierarchy Process in Heterogeneous Cloud Data Storage," Int. Arab Conf. Inf. Technol. (ACIT ' 2016), no. December 2016, 2017.

[88] A. Awad, R. Salem, H. Abdelkader, and M. A. Salam, "A Novel Intelligent Approach for Dynamic Data Replication in Cloud Environment," IEEE Access, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3064917.

[89] N. Mansouri, M. K. Rafsanjani, and M. M. Javidi, "DPRS: A dynamic popularity aware replication strategy with parallel download scheme in cloud environments," Simul. Model. Pract. Theory, vol. 77, pp. 177–196, 2017, doi: 10.1016/j.simpat.2017.06.001.

[90] N. Mansouri and M. M. Javidi, "A hybrid data replication strategy with fuzzy-based deletion for heterogeneous cloud data centers," J. Supercomput., vol. 74, no. 10, pp. 5349–5372, 2018, doi: 10.1007/s11227-018-2427-1.

[91] M. E. J. Newman, "Networks of networks - An introduction," (2010, Oxford Univ. Press. Artif. life., vol. 80, pp. 1–6, 2009, doi: 10.1016/j.chaos.2015.03.016.

[92] Y. Zhang et al., "BDS+: An Inter-Datacenter Data Replication System With Dynamic Bandwidth Separation," IEEE/ACM Trans. Netw., vol. 29, no. 2, pp. 918–934, 2021, doi: 10.1109/TNET.2021.3054924.

[93] Y. Ebadi and N. Jafari Navimipour, "An energy-aware method for data replication in the cloud environments using a Tabu search and particle swarm optimization algorithm," Concurr. Comput. Pract. Exp., no. July 2017, p. e4757, 2018, doi: 10.1002/cpe.4757.

[94] A. Bowers, C. Liao, D. Steiert, D. Lin, A. Squicciarini, and A. Hurson, "Detecting Suspicious File Migration or Replication in the Cloud," IEEE Trans. Dependable Secur. Comput., vol. Vol. 18, N, no. 1, pp. 296–309, 2021.

[95] P. Wang, Z. Chen, M. C. Zhou, Z. Zhang, A. Abusorrah, and A. C. Ammari, "Cost-Effective and Latency-Minimized Data Placement Strategy for Spatial Crowdsourcing in Multi-Cloud Environment," IEEE Trans. Cloud Comput., vol. 11, no. 1, pp. 868–878, 2023, doi: 10.1109/TCC.2021.3119862.

[96] H. M. F. Noman et al., "Machine Learning Empowered Emerging Wireless Networks in 6G: Recent Advancements, Challenges and Future Trends," IEEE Access, vol. 11, no. July, pp. 83017–83051, 2023, doi: 10.1109/ACCESS.2023.3302250.

[97] N. K. Naseri, E. Sundararajan, and M. Ayob, "Smart Root Search (SRS) in Solving Service Time–Cost Optimization in Cloud Computing Service Composition (STCOCCSC) Problems," Symmetry (Basel)., vol. 15, no. 2, Feb. 2023, doi: 10.3390/sym15020272.

[98] F. Mohd Ali, N. A. Md Yunus, N. N. Mohamed, M. Mat Daud, and E. A. Sundararajan, "A Systematic Mapping: Exploring Internet of Everything Technologies and Innovations," Symmetry, vol. 15, no. 11. p. 1964, 2023. doi: 10.3390/sym15111964.

[99] L. S. Xue, N. A. A. Majid, and E. A. Sundararajan, "A principal component analysis and clustering based load balancing strategy for cloud computing," TEM J., vol. 9, no. 1, pp. 93–100, 2020, doi: 10.18421/TEM91-14.

[100] S. S. Alnuaimi, E. A. Sundararajan, and A. H. A. Rahman, "Data Distribution Optimization Over Multi Cloud Storage," J. Theor. Appl. Inf. Technol., vol. 100, no. 5, pp. 1378–1389, 2022.

[101] H. Sallehudin, R. Che Razak, M. Ismail, A. F. Md Fadzil, and R. Baker, "Cloud Computing Implementation in The Public Sector: Factors and Impact," Asia-Pacific J. Inf. Technol. Multimed., vol. 07, no. 02(02), pp. 27–42, 2018, doi: 10.17576/apjitm-2018-0702(02)-03.

Optimizing House Renovation Projects Using Industrial Engineering-Based Approaches

Lim Rou Yan[1], Siti Noor Asyikin Mohd Razali[2], Muhammad Ammar Shafi[3], Norazman Arbin[4]
Department of Mathematics and Statistics-Faculty of Applied Sciences and Technology,
Universiti Tun Hussein Onn Malaysia, Hab Pendidikan Tinggi Pagoh, KM[1],
Jalan Panchor, 84600 Pagoh, Muar, Johor, Malaysia[1, 2]
Department of Technology and Management-Faculty of Technology Management and Business,
Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Batu Pahat, Johor, Malaysia[3]
Department of Mathematics-Faculty of Sciences and Mathematics,
Universiti Pendidikan Sultan Idris, 35900 Tanjong Malim, Perak, Malaysia[4]

***Abstract*—The persistent challenge of project delays poses significant issues with the escalating demand for house renovations. The company in Kedah, Malaysia, faces frequent project delays due to ineffective project management, leading to substantial liquidated damages. This study aims to minimise project delays and ensure timely completion within budget constraints, focusing on both the entire house renovation project and the kitchen renovation project. This study employed the Program Evaluation and Review Technique to illustrate the project network and utilised the Critical Path Method to identify the critical path while implementing project crashing with linear programming to optimise activity duration reduction and minimise costs. The PERT method results in an illustrative network diagram that aids subsequent analysis. The completion time for the entire house renovation project is determined to be 58 days using CPM, with a 96.8% probability of completion within 60 days. In contrast, for the kitchen renovation project, the completion time is identified as 38 days, with a 0% probability of meeting the 30-day deadline. Therefore, linear programming was successfully applied, shortening the kitchen project to 30 days at a total cost of RM 18,517.50, further reduced to 20 days with a cost of RM 20,980. Both scenarios remained below the total penalty cost of RM 21,780. The finding enables the company to make informed decisions on resource allocation to accelerate project duration and avoid delays. Future research should delve into realistic models, considering labour allocation and indirect costs, for a more comprehensive evaluation of project crashing strategies and their financial impacts.**

Keywords*—House renovation; Program Evaluation and Review Technique (PERT); Critical Path Method (CPM); project crashing techniques; construction project management; linear programming optimisation

I. Introduction

In any generation, houses serve as essential shelter, playing an important role in people's lives. House renovation has become a common phenomenon in recent years as the quality of life improves and people focus more on creating a comfortable and safer home environment. Simultaneously, the growing trend of renovating kitchens underscores this space's unique role as the hub and heart of the home. Homeowners are increasingly investing in both entire house and kitchen renovation projects, driven by a desire to enhance functionality, increase property value, and create inviting spaces for family gatherings and social events. These renovations, offering customisation within budget constraints, also pose challenges with project deadlines. Delays often arise from factors such as ineffective planning, material and labour shortages, adverse weather, and equipment failures [1]. In addition, as project complexity increases, improper management can lead to cost overruns and schedule delays. To mitigate these challenges, this study aims to minimise project delays and ensure timely completion within budget by employing effective project management tools and techniques. This study was conducted on two cases, an entire house and a kitchen renovation, by a renovation company in Kedah, Malaysia.

According to a study [2], the construction industry historically faces challenges like delays, exceeding budgeted costs, and substandard quality. Similar causes of delays, such as inadequate planning and scheduling and insufficient site management, have been emphasised in studies by [1], [3], [4], and [5]. Besides that, the ever-changing nature of project development poses challenges for construction companies lacking adequate project management skills [6]. Therefore, as [7] emphasises, efficient project management has several advantages, including cost, time, and quality assurance. According to study [8], project management is characterised by using knowledge, skills, tools, and techniques to manage project activities and meet specific requirements effectively. Similarly, [9] proposes that utilising project management tools can alleviate challenges in planning, organising, and managing diverse sets of resources. [10] and [11] emphasise that effective project planning and scheduling are essential for successful construction projects, ensuring timely completion within budget and meeting quality standards. However, project planning and scheduling represent one of the most difficult tasks faced by managers, requiring a deep understanding of the planned work [12], especially for complex construction projects where careful consideration of project scheduling and cost planning is essential [13].

The Critical Path Method (CPM) and Program Evaluation and Review Technique (PERT) are proven approaches that aid in planning, scheduling, and controlling construction projects [14]. Studies by [15], [16], and [17] highlight the effectiveness of CPM and PERT in identifying the critical path, allowing for better control and acceleration of activities to ensure timely

project completion. Project crashing is a strategy for utilising additional resources to expedite critical activities and meet deadlines [18] and [19]. [20] assert that delays can be mitigated by implementing project crashing strategies while considering the cost factor simultaneously. Additionally, [21] and [22] apply linear programming, which results in a cost increase but significantly shortens the project duration. However, the study in [23] stated that combining linear programming with project crashing can minimise project overruns. These methods have proven helpful in project management, allowing for proper planning and scheduling of projects and effective control of costs.

In this study, two crucial components of project management, PERT and CPM, will be utilised to illustrate the project network, identify critical paths, and estimate the probability of completion time for both the entire house and kitchen renovation projects. Subsequently, linear programming will be applied for project crashing in the kitchen renovation project. Finally, the performance of the project crash results will be compared with the current project cost and completion time for the kitchen renovation project. This study will help various renovation companies understand the importance of applying project management principles to their projects.

II. Materials and Methods

A. Data Description

The data obtained from a private renovation company in Kedah, Malaysia, consists of two case studies: the entire house and the kitchen renovation projects. This deliberate selection aims to evaluate the applicability of various project management tools to datasets of different sizes. The entire house renovation dataset, representing a large-scale project with a 60-day deadline, includes the duration of each activity and the corresponding total renovation cost for each project scope. In contrast, the kitchen renovation dataset reflects a smaller-scale project with a 30-day deadline. This dataset provides comprehensive information on the duration and cost associated with each renovation step within the kitchen. This dual-dataset approach enables a comprehensive assessment of project management tools across varying project complexities. A one-week delay resulted in a penalty of approximately RM4,000 for these projects.

B. PERT

The PERT methodology facilitates a comprehensive analysis of project completion time by incorporating a three-point time estimate, addressing uncertainties in activity duration. It employs three different time estimates: optimistic (a), most likely (m), and pessimistic (b) to account for variability [24]. The optimistic estimate signifies the minimum activity duration; the most likely estimate reflects the duration expected to occur most frequently; and the pessimistic estimate represents the maximum expected duration. To calculate the expected time (Te) and variance (V) of each activity duration, specific formulas are utilised. Eq. (1) estimates the average duration, while Eq. (2) quantifies the level of uncertainty associated with each activity [25].

$$\mathrm{Te} = \frac{(a + 4m + b)}{6} \tag{1}$$

$$\mathrm{V} = \left[\frac{b - a}{6}\right]^2 \tag{2}$$

C. CPM

Using a network-based approach, the CPM identifies time-sensitive activities crucial for project success, considering parameters such as earliest start (ES), earliest finish (EF), latest start (LS), latest finish (LF), and slack time (S) [26]. Eq. (3) and (4) determine the earliest start and finish times, while Eq. (5) and (6) establish late start and finish times [27]. These calculations indirectly yield slack time, defined as the maximum allowable delay for an activity without affecting project completion. The critical path, characterised by zero slack, represents the path with the longest duration in the network [28], with the formula for slack time outlined in Eq. (7). Determining the critical path is vital for guiding completion time, coordinating activities, developing schedules, and monitoring project planning [29].

$$ES(j) = maximum\,\{EF(i)\}, j = 1,2,3,\dots,n \tag{3}$$

$$ES(j) = ES(j) + Duration \tag{4}$$

$$LF(i) = minimum\,\{LS(j)\}, i + n - 1, n - 2, \dots, 0 \tag{5}$$

$$LS(i) = LF(i) - Duration \tag{6}$$

$$S = LS - ES = LF - EF \tag{7}$$

Furthermore, the variations in activities along the critical path can significantly impact the overall project completion. Assessing the variances of critical path activities contributes to a more comprehensive understanding of project uncertainty. The standard normal (Z) can be obtained from Eq. (8), thus referring to the normal distribution table to find the probability. A higher calculated probability, approaching 100%, signifies a greater likelihood of meeting the project deadline, whereas a lower probability, nearing 0%, suggests a reduced likelihood of achieving the project duration [30].

$$\mathrm{Z} = \frac{\text{Due date} - \sum \text{Expected date of completion}}{\sum \sqrt{\text{All the variance of critical activities}}} \tag{8}$$

D. Project Crashing

Project crashing involves minimising a project's remaining duration by reducing the time required for critical activities, resulting in additional costs, known as crash costs, due to the increased allocation of resources to ensure timely completion [31]. The methodology includes identifying the normal critical path and its critical activities. Following this, the crash cost per period for various activities is computed using Eq. (9). Next, the critical path activity with the lowest crash cost per period is identified and accelerated to the maximum extent possible or until the desired deadline. The process is iteratively checked to ensure the critical path remains unchanged. This iterative approach continues until the optimal solution is attained and the project reaches its desired completion date [32].

$$\text{Crash cost per time period} = \frac{\text{Crash cost} - \text{Normal cost}}{\text{Normal time} - \text{Crash time}} \tag{9}$$

E. Linear Programming

Linear programming serves as an alternative approach to optimising project crashing schedules, involving three key components: decision variables, an objective function, and constraints. The objective is to minimise the cost of crashing the

entire project. Therefore, the objective function can be defined based on Eq. (10) [32]. The objective function is subject to several constraints, such as the maximum reduction constraint, the start time constraint, the project duration constraint, and non-negativity constraints [14]. The maximum reduction constraint ensures each activity does not crash more than the maximum crashing time. In a project, activities are interconnected, and the beginning of certain activities relies on the completion of others. To ensure a smooth flow of work, the sequence of activities needs to be established by setting start time constraints. The project duration constraint is determined at the last activity before the project deadline.

Minimise crash cost, $z = \sum_{i=1}^{n} C_i Y_i, i = 1, 2, 3, \dots, n$ (10)

Subject to:

- Maximum reduction constraint, $y_i \leq$ Allowable crashing time for activity i measured in terms of days
- Start time constraint, $X_i \geq X_{\text{Predecessor}} + (t - Y_i)$
- Project duration constraint, $X_{\text{Finish}} \leq$ The completion project time at the last activity
- Non – negativity constraint, $x_i, y_i \geq 0$

Where X_i represents the time when the event i will occur, measured since the beginning of the project; Y_i represents the number of time activity will be crashed, where $i = (1, 2, 3, \dots, n)$; X_{Start} represents the start time for the project (usually 0); X_{Finish} represents the earliest finish time of the project; C_i represents the crash cost per unit of time for activity i.

III. Result and Discussion

This section explores two case studies: the entire house renovation project and the kitchen renovation project.

A. Case Study 1: Entire House Renovation Project

Illustrating the project network, identifying the critical path and activities, and estimating the probability of completing the overall project are the key objectives for this case study.

1) Project network for case study 1: For the entire house renovation project, there are a total of 31 activities.

Fig. 1 displays the PERT network diagram, which starts with activity A and ends with activity AF. Notably, activities E and F have the highest number of predecessors, with three dependents each, originating from activities B, C, and D. Following this, the second-highest number of predecessors is found in activities G, M, P, W, X, Y, and AE, each having two dependents.

2) Critical path and activities for case study 1: Fig. 2 clearly shows the duration, earliest start (ES) time, earliest finish (EF) time, latest start (LS) time, latest finish (LF) time, and slack time for each activity in the entire house renovation project.

The yellow path in Fig. 2 represents the critical path, which is characterised by zero slack and represents the critical activities in case study 1. Notably, there are two critical paths in the project, totalling 58 days.

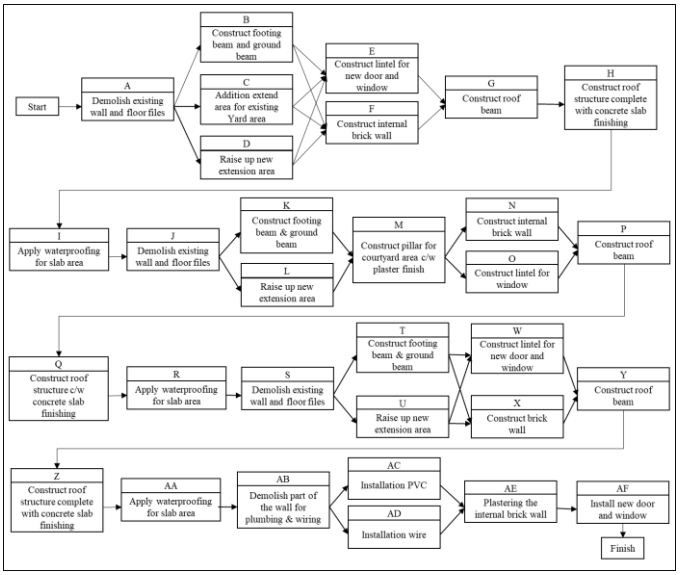


Fig. 1. PERT network diagram for case study 1.

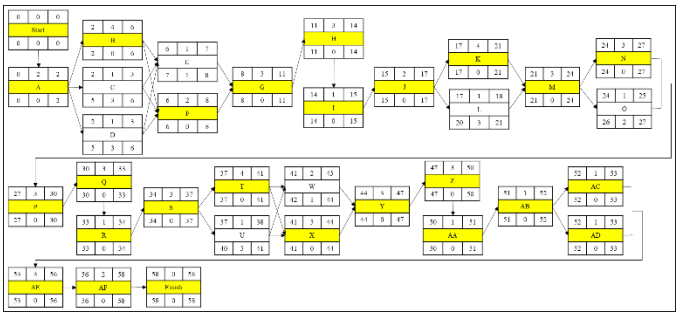


Fig. 2. CPM network diagram for case study 1.

3) Probability of completion time for case study 1: The PERT method employs three-time estimates, which are optimistic time (a), most likely time (m), and pessimistic time (b). Using Eq. (1) and Eq. (2), the PERT method calculates the expected time and variances. The results are presented in Table I.

The deadline for this project is 60 days, and the expected date of completion is 58 days. So, the z value can be obtained using Eq. (8):

$$Z = \frac{60 - 58}{\sqrt{1.167}} = 1.8514$$

Then, this z value can be seen in the standard normal distribution table. The z-value of 1.8514 obtained from the standard normal distribution table corresponds to a probability of 0.9679, which is expressed as a percentage of approximately 96.8%. This high probability suggests a strong likelihood that the project will be completed on schedule in less than or equal to 60 days. Given this higher probability and the absence of a risk of penalties for project delay, the application of linear programming for project crashing was deemed unnecessary. Implementing project crashing would typically involve additional costs to expedite critical activities, and in this context, the substantial likelihood of on-time completion rendered the incurring of extra expenses unnecessary.

TABLE I. PROJECT VARIANCE FOR EACH ACTIVITY IN CASE STUDY 1

Activity Code	Estimation Time (day)			Expected time, Te	Variance, V
	a	*m*	*b*		
A	1.5	2	3	2.083	0.063
B	3	4	5	4.000	0.111
C	0.5	1	1	0.917	0.007
D	0.5	0.5	1	0.583	0.007
E	0.5	1	2	1.083	0.063
F	2	2.5	3	2.500	0.028
G	2	3	3	2.833	0.028
H	2	3	4	3.000	0.111
I	0.5	0.5	1	0.583	0.007
J	1.5	2	3	2.083	0.063
K	3	4	5	4.000	0.111
L	0.5	0.5	1	0.583	0.007
M	2	3	3	2.833	0.028
N	2	2.5	3	2.500	0.028
O	0.5	0.5	1	0.583	0.007
P	2	3	3	2.833	0.028
Q	2	3	4	3.000	0.111
R	0.5	0.5	1	0.583	0.007
S	1.5	2	3	2.083	0.063
T	3	4	5	4.000	0.111
U	0.5	0.5	1	0.583	0.007
W	0.5	1	2	1.083	0.063
X	2	2.5	3	2.500	0.028
Y	2	3	3	2.833	0.028
Z	2	3	4	3.000	0.111
AA	0.5	0.5	1	0.583	0.007
AB	1	1	2	1.167	0.028
AC	0.5	1	1	0.917	0.007
AD	0.5	1	1	0.917	0.007
AE	2	3	3	2.833	0.028
AF	1	1.5	2	1.500	0.028

B. Case Study 2: Kitchen Renovation Project

The process for case study 2 involves illustrating the project network, identifying the critical path and activities, estimating the probability of completion time, utilising linear programming for resource allocation to accelerate the schedule, and finally, comparing the project crash results with the current cost and completion time of the kitchen renovation project.

1) Project network for case study 2: For the kitchen renovation project, there are a total of 18 activities.

Fig. 3 illustrates the PERT network diagram, starting with activities A and B. It is worth noting that both activities L and M have the highest number of predecessors, with each having four dependent activities from activities H, I, J, and K, respectively. Then, activities C, N, and Q each have two dependent activities.

2) Critical path and activities for case study 2: Fig. 4 clearly shows the duration, earliest start (ES) time, earliest finish (EF) time, latest start (LS) time, latest finish (LF) time, and slack time for each activity in the kitchen renovation project.

In Fig. 4, the yellow path represents the critical path with zero slack, indicating the critical activities in case study 2. It is evident that in the kitchen renovation project, there are eight critical paths, amounting to 38 days in total.

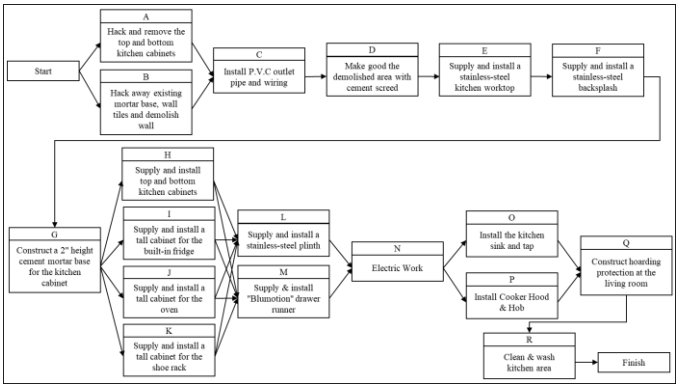


Fig. 3. PERT network diagram for case study 2.

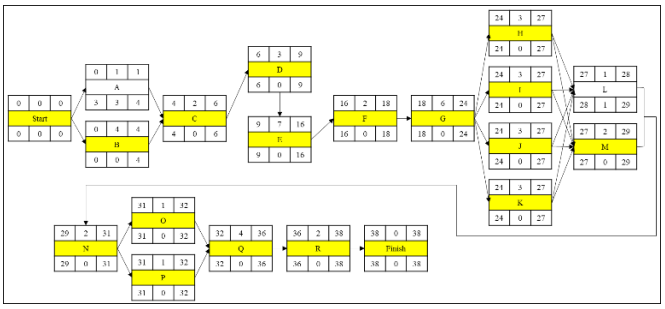


Fig. 4. CPM network diagram for case study 2.

3) Probability of completion time for case study 2: The expected time and variance of the PERT method were calculated by applying Eq. (1) and Eq. (2), as detailed in Table II.

TABLE II. PROJECT VARIANCE FOR EACH ACTIVITY IN CASE STUDY 2

Activity Code	Estimation Time (day)			Expected time, Te	Variance, V
	a	*m*	*b*		
A	0.5	1	1	0.917	0.007
B	3	3.5	4	3.500	0.028
C	1	1.5	2	1.500	0.028
D	2	3	4	3.000	0.111
E	6	7	8	7.000	0.111
F	1	1.5	2	1.500	0.028
G	4	6	7	5.833	0.250
H	2.5	3	4	3.083	0.063
I	2	2.5	3	2.500	0.028
J	2	2.5	3	2.500	0.028
K	2	2.5	3	2.500	0.028
L	0.5	1	1	0.917	0.007
M	1	1.5	2	1.500	0.028
N	1	1.5	2	1.500	0.028
O	0.5	1	1	0.917	0.007
P	0.5	1	1	0.917	0.007
Q	2	4	5	3.833	0.250
R	1	1.5	2	1.500	0.028

The deadline for this project is 30 days, and the expected date of completion is 38 days. So the z value obtained is:

$$Z = \frac{30 - 38}{\sqrt{1.049}} = -7.8109$$

Next, the z value of -7.8109 corresponds to a probability value of 0. When expressed as a percentage, this indicates a 0% probability of completing the project in 30 days or less, signifying that completing the duration is unlikely. Faced with this challenge, the implementation of the project crashing became critical. By accelerating critical activities through project crashing, the likelihood of completing the project within the 30-day deadline significantly increased.

4) Apply linear programming method for project crashing in case study 2: The linear programming method for project crashing is being applied to achieve the shortest possible duration at the least cost. Table III shows the cost-time slope of the kitchen renovation project, including the additional costs incurred resulting from the time reduction, with the crash cost per time calculated using Eq. (9).

TABLE III. COST-TIME SLOPE OF CASE STUDY 2

	Activity description	Normal Time (Days)	Crash Time (Days)	Normal Cost (RM)	Crash Cost (RM)	Crash cost per time
A	Hack and remove the top and bottom kitchen cabinets	1	0.5	350	450	200
B	Hack away existing mortar base, wall tiles and demolish wall	4	2	1000	1450	225
C	Install P.V.C outlet pipe and wiring for kitchen & washing machine	2	0.5	450	600	100
D	Make good the demolished area with cement screed	3	2	1000	1150	150
E	Supply and install a stainless-steel kitchen worktop	7	4	2200	3000	266.67
F	Supply and install a stainless-steel backsplash	2	0.5	800	900	66.67
G	Construct a 2" height cement mortar base for the	6	4	450	770	160

	kitchen cabinet					
H	Supply and install top and bottom kitchen cabinets	3	2	3380	3560	180
I	Supply and install a tall cabinet for the built-in fridge	3	2	780	880	100
J	Supply and install a tall cabinet for the oven	3	2	780	880	100
K	Supply and install a tall cabinet for the shoe rack	3	2	780	880	100
L	Supply and install a stainless-steel plinth.	1	1	3370	3370	0.00
M	Supply & install "Blumotion" drawer runner	2	1	480	580	100
N	Electric Work	2	0.5	800	900	66.67
O	Install the kitchen sink and tap	1	0.5	80	180	200
P	Install Cooker Hood & Hob	1	0.5	100	200	200
Q	Construct hoarding protection at the living room	4	2	700	950	125
R	Clean & wash kitchen area	2	1	280	380	100
Total		50	28	17780	21080	2440

After formulating the objective function and constraints, the linear programming model is applied using Excel Solver. The results of the model solution reduced to 30 days are presented in Table IV.

TABLE IV. SOLUTION OF THE LP PROBLEM USING EXCEL SOLVER FOR 30 DAYS

Objective Value	Final Value
Min Z	RM 737.50
$X_A, X_B, X_D, X_E, X_G, X_H, X_I, X_J, X_K, X_L, X_O, X_P$	0
X_C, X_F, X_N, X_Q	1.5
X_M, X_R	1

In order to meet the desired project completion time of 30 days, specific activities required acceleration. Critical activities identified for crashing were C, F, N, and Q, each requiring a reduction of 1.5 days. Additionally, activities M and R were expedited by 1 day each to align with the targeted project timeline. Initially, the linear programming method was utilised to ensure the completion of the kitchen renovation project within the 30-day deadline by allocating additional resources to accelerate specific tasks. The total cost incurred for crashing these activities amounts to RM737.50.

Subsequently, considering a further reduction in the project duration to 20 days, a detailed analysis was conducted. The application of linear programming successfully achieved the goal of shortening the project duration. The results of the model solution for the 20-day timeline are presented in Table V.

TABLE V. SOLUTION OF THE LP PROBLEM USING EXCEL SOLVER FOR 20 DAYS

Objective Value	Final Value
Min Z	RM 3200
X_A, X_L	0
X_B, X_G, X_Q	2
X_C, X_F, X_N	1.5
$X_D, X_H, X_I, X_J, X_K, X_M, X_R$	1
X_E	3
X_O, X_P	0.5

To meet the project completion time of 20 days, specific adjustments were made to various activities. Activities B, G, and Q were reduced by two days, while activities C, F, and N were accelerated by 1.5 days. Additionally, activities D, H, I, J, K, M, and R were shortened by 1 day each. Further improvements included a 3-day acceleration for activity E and a 0.5-day acceleration for activities O and P. The total cost of crashing these activities into 20 days is RM3,200. Thus, the final project cost, determined through the linear programming method, is RM20,980.

5) Compare the performance of project crashing result with the current project cost and completion time for case study 2: Table VI shows the results of project crashing for the kitchen renovation project in comparison to the current project cost and completion time.

TABLE VI. COMPARISON TABLE IN PROJECT COST AND COMPLETION TIME

	Time	Cost	Penalty	Total Cost
Normal	38 days	RM 17,780	RM4,000	RM 21,780.00
Crash	30 days	RM 737.50	-	**RM 18517.50**
Crash	20 days	RM3200.00	-	**RM 20980.00**

Table VI displays the total direct cost for completing the project within the normal 38-day duration, amounting to RM 17,780, with a penalty of RM 4,000 for a one-week delay. The cost, including the penalty, for completing the project without activity crashing is RM 21,780. Additionally, crashing for 30 days is RM 18,517.50, and for 20 days, it is RM 20,980. Despite the increased cost for shorter durations due to additional resources, both remain below the total cost without crashing. Therefore, the company can decide to add additional resources for crashing the activities to accelerate the project duration. This analysis affirms that the project crashing strategy is cost-effective, helping meet deadlines and avoid penalties.

IV. CONCLUSION

In conclusion, the application of Program Evaluation and Review Techniques and the Critical Path Method has successfully managed and evaluated two distinct renovation projects: an entire house renovation and a kitchen renovation. This study achieved its first and second objectives by illustrating project networks, estimating completion probabilities, and identifying critical paths and activities for both cases.

For the entire house renovation, the PERT method was employed to construct network diagrams and determine expected times and variances. Critical activities were identified using the Critical Path Method, resulting in a high likelihood of project completion within the 60-day deadline.

In contrast, the kitchen renovation presented challenges with a 30-day deadline and a calculated 38-day completion time using CPM, indicating potential delays. The application of linear programming for project crashing successfully reduced the duration to 30 days, incurring an additional cost of RM737.50. A further reduction to 20 days was achieved, incurring an additional cost of RM3,200. The comparison with the original cost structure confirmed the feasibility of completing the project within the specified time and at a lower cost.

This study contributes significantly to house renovation project management by addressing two projects and providing valuable insights for future research. It effectively tackles persistent project delays through the strategic use of tools like CPM, PERT, and linear programming. The findings emphasise the crucial role of acquiring skills for efficient tool application. The practical implications extend to the industry, aiding renovation companies in improving project management practices for timely and cost-effective outcomes. In summary, this research advances academic understanding and offers actionable strategies for enhancing efficiency and cost-effectiveness in house renovation projects.

However, limitations include challenges in linear programming for projects with complex dependencies and a lack of detailed information on worker allocation and indirect costs. Future research should explore real-world models, consider resource availability, and analyse the impact of worker allocation on project costs and completion time. Additionally, including detailed information on indirect costs would provide a more comprehensive evaluation of project crashing financial impacts. Furthermore, to mitigate delays caused by a lack of project management expertise, it is recommended that companies hire professional project managers. This can enhance planning, scheduling, and overall project efficiency, reducing the likelihood of delays in future house renovation projects.

REFERENCES

[1] M. Sambasivan, and Y. W. Soon, "Causes and effects of delays in Malaysian construction industry," International Journal of project management, vol. 25, no. 5, pp. 517-526, July. 2007, doi:10.1016/j.ijproman.2006.11.007.

[2] J. K. Larsen, G. Q. Shen, S. M. Lindhard, and T. D. Brunoe, "Factors affecting schedule delay, cost overrun, and quality level in public construction projects," Journal of management in engineering, vol. 32, no. 1, pp. 04015032, Jan. 2016, doi: 10.1061/(asce)me.1943-5479.0000391.

[3] M. Haseeb, Xinhai-Lu, A. Bibi, Maloof-ud-Dyian, and W. Rabbani, "Problems of projects and effects of delays in the construction industry of Pakistan," Australian Journal of Business and Management Research, vol. 1, no. 5, pp. 41–50, Sep. 2011.

[4] H. Doloi, A. Sawhney, K. C. Iyer, and S. Rentala, "Analysing factors affecting delays in Indian construction projects," International journal of project management, vol. 30, no. 4, pp. 479-489, May. 2012, doi: 10.1016/j.ijproman.2011.10.004.

[5] J. B. H. Yap, P. L. Goay, Y. B. Woon, and M. Skitmore, "Revisiting critical delay factors for construction: Analysing projects in Malaysia," Alexandria Engineering Journal, vol. 60, no. 1, pp. 1717-1729, Feb. 2021, https://doi.org/10.1016/j.aej.2020.11.021.

[6] A. Serpell, and H. Rubio, "Evaluating project management (PM) readiness in construction companies: cases from Chile," Procedia Computer Science, vol. 219, pp. 1642-1649, 2023, doi: 10.1016/j.procs.2023.01.457.

[7] Q. Shi, "Rethinking the implementation of project management: A Value Adding Path Map approach," International Journal of Project Management, vol. 29, no. 3, pp. 295–302, Apr. 2011, doi:10.1016/j.ijproman.2010.03.007.

[8] Project Management Institute, "A guide to the Project Management Body of Knowledge (PMBOK guide) (6th ed.)," Project Management Institute, 2017.

[9] M. Clemente, and L. Domingues, "Analysis of Project Management Tools to support Knowledge Management," Procedia Computer Science, vol. 219, pp. 1769–1776, 2023, doi: 10.1016/j.procs.2023.01.472.

[10] C. Chowdeswari, D. S. Chandra, and S. Asadi, "Optimal planning and scheduling of high rise buildings," Int. J. Civ. Eng. Technol, vol. 8, pp. 312-324, Jan. 2017.

[11] S. Gaur, "Understanding the importance of project planning and scheduling in Indian construction projects," Journal of Positive School Psychology, vol. 6, no. 3, pp. 3535-3544, 2022.

[12] Z. K. Nemaa, and G. K. Aswed, "Forecasting construction time for road projects and infrastructure using the fuzzy PERT method," IOP Conference Series: Materials Science and Engineering, vol. 1076, no. 1, pp. 012123, 2021, doi:10.1088/1757-899X/1076/1/012123.

[13] F. Habibi, O. T. Birgani, H. Koppelaar, and S. Radenović, "Using fuzzy logic to improve the project time and cost estimation based on Project Evaluation and Review Technique (PERT)," Journal of Project Management, vol. 3, no. 4, pp. 183–196, 2018, doi: 10.5267/j.jpm.2018.4.002.

[14] W. Agyei, "Project planning and scheduling using PERT and CPM techniques with linear programming: case study," International journal of scientific & technology research, vol. 4, no. 8, pp. 222-227, Aug. 2015.

[15] M. Kholil, B. N. Alfa, and M. Hariadi, "Scheduling of house development projects with CPM and PERT method for time efficiency (Case study: House type 36)," IOP Conference Series: Earth and Environmental Science, vol. 140, no. 1, pp. 012010, 2018, doi: 10.1088/1755-1315/140/1/012010.

[16] N. Nahendra, I. N. Daulay, and A. Paramitha, "The optimization of Gebe Airport project using PERT and CPM method," Operations Management and Information System Studies, vol. 2, no. 4, pp. 208-218, 2022, https://doi.org/10.24036/omiss.v2i4.

[17] M. Simion, G. Vasile, C. Dinu and R. E. Scutariu, "CPM and PERT techniques for small-scale R&D projects," National Research and Development Institute for Industrial Ecology, INCD-ECOIND, pp. 166-174, Sep. 2019, DOI:10.21698/simi.2019.fp22.

[18] M. R. Feylizadeh, A. Mahmoudi, M. Bagherpour and D. -F. Li, "Project crashing using a fuzzy multi-objective model considering time, cost, quality and risk under fast tracking technique: A case study," Journal of Intelligent & Fuzzy Systems, vol. 35, no. 3, pp. 3615-3631, 2018, doi: 10.3233/jifs-18171.

[19] Y. Li, Z. Cui, H. Shen, and L. Zhang, "Target-based project crashing problem by adaptive distributionally robust optimization.," Computers & Industrial Engineering, vol. 157, pp. 107160, 2021, doi:10.1016/j.cie.2021.107160.

[20] Andiyan, R. M. Putra, G. D. Rembulan, and H. Tannady, "Construction project evaluation using CPM-Crashing, CPM-PERT and CCPM for minimize project delays," Journal of Physics: Conference Series, vol. 1933, no. 1, pp. 012096, 2021, doi:10.1088/1742-6596/1933/1/012096.

[21] C. L. Karmaker, and P. Halder, "Scheduling project crashing time using linear programming approach: Case study," International Journal of Research in Industrial Engineering, vol. 6, no. 4, pp. 283-292, 2017, DOI: 10.22105/riej.2017.96572.1010.

[22] S. Sharma, N. Bedi, and V. K. Sukhwani, "Optimization of Time and Cost for a Research Project by Project Crashing Method," IOP Conference Series: Materials Science and Engineering, vol. 998, no. 1, pp. 012057, 2020, doi: 10.1088/1757-899x/998/1/012057.

[23] R. J. Gade, "A proposed solution to the problem of construction industry overruns: lean construction techniques and linear programming," Indian Journal of Science and Technology, vol. 9, no. 25, pp. 1-12, Jul. 2016, doi: 10.17485/ijst/2016/v9i25/91929.

[24] Q.-T. Huynh, and N.-T. Nguyen, "Probabilistic Method for Managing Common Risks in Software Project Scheduling Based on Program Evaluation Review Technique," International Journal of Information Technology Project Management, vol. 11, no. 3, pp. 77–94, 2020, doi: 10.4018/ijitpm.2020070105.

[25] O. U. Cynthia, "Implementation of Project Evaluation and Review Technique (PERT) and Critical Path Method (CPM): A Comparative Study," International Journal of Industrial and Operations Research, vol. 3, no. 004, Mar. 2020, doi: 10.35840/2633-8947/6504.

[26] I. A. Kusumadarma, D. Pratami, I. P. Yasa, and W. Tripiawan, "Developing project schedule in telecommunication projects using critical path method (CPM)," International Journal of Integrated Engineering, vol. 12, no. 3, pp. 60–67, 2020.

[27] S. Zareei, "Project scheduling for constructing biogas plant using critical path method," Renewable and Sustainable Energy Reviews, vol. 81, pp. 756-759, Jan. 2018, https://doi.org/10.1016/j.rser.2017.08.025.

[28] P. Tamrakar, "Analysis and improvement by the application of network analysis (Pert/Cpm)," The International Journal of Engineering and Science, vol. 2, no. 1, pp. 154-159, Jan. 2013.

[29] Y. Takakura, T. Yajima, Y. Kawajiri, and S. Hashizume, "Application of critical path method to stochastic processes with historical operation data," Chemical Engineering Research and Design, vol. 149, pp. 195-208, Sep. 2019, https://doi.org/10.1016/j.cherd.2019.06.027.

[30] Y. Farida, and L. P. Anenda, "Network Planning Analysis on Road Construction Projects by CV. X Using Evaluation Review Technique (PERT)-Critical Path Method (CPM) and Crashing Method," International Journal of Integrated Engineering, vol. 14, no. 4, pp. 377-390, 2022.

[31] Y. E. P. R. Waliulu, and T. J. W. Adi, "A system dynamic thinking for modeling infrastructure project duration acceleration," Procedia Computer Science, vol. 197, pp. 420-427, 2022, https://doi.org/10.1016/j.procs.2021.12.181.

[32] M. N. Islam, M. B. Rana, S. Rafique and T. Aziza, "Crashing project time with least cost: A linear programming approach," Journal of Business Research, vol. 6, 2004, doi: 10.2139/ssrn.1012525.

FSFYOLO: A Lightweight Model for Forest Smoke and Fire Detection

Yinglai HUANG, Jing LIU, Liusong YANG*
College of Computer and Control Engineering, Northeast Forestry University, Harbin, Heilongjiang 150040, China

***Abstract*—The detection and identification of forest smoke and fire are critical for forest fire prevention efforts. However, current forest smoke and fire target detection algorithms confront obstacles such as high memory usage, computational costs, and deployment difficulty. Regarding these key issues, this paper presents FSFYOLO, a lightweight forest smoke and fire detection model based on the YOLOv8s model. To efficiently extract key features from forest smoke and fire images while reducing computational redundancy, the lightweight network EfficientViT is used as the backbone network. A lightweight detection head, Partial Convolutional Head (PCHead), is designed using the shared parameters idea to greatly minimize the amount of parameters and computations by leveraging shared convolutional layers and branched processing, thus achieving the lightweight design of the model. In the neck network, a lightweight feature extraction module, C2f-FL, is built to more fully extract local features and surrounding contextual information to widen the receptive field. Additionally, a Coordinate Attention (CA) mechanism is integrated into both the backbone and neck networks to capture cross-channel information, directional awareness, as well as position-sensitive information, improving the model's capacity to precisely pinpoint fire and smoke in forests. The experimental outcomes results on our self-constructed forest smoke and fire dataset demonstrate that FSFYOLO reduces the number of parameters and computation by 47.6% and 60.9%, respectively, compared to the original model, while improving precision, recall, and mAP50 by 1.3%, 1.0%, and 1.0%, respectively. This demonstrates that FSFYOLO strikes a good compromise between model lightweighting and detection accuracy.**

***Keywords*—Forest smoke and fire; target detection; lightweight; YOLOv8; EfficientViT**

I. Introduction

Forests are one of Earth's most valuable natural resources. They not only provide essential materials and minerals for production, but also play a critical role in maintaining ecological balance, preventing and mitigating drought, and conserving water resources [1], [2], [3]. However, forest fires often go undetected until they have spread across vast areas, making them difficult or even impossible to control and extinguish [4]. Such fires can cause irreversible and devastating damage to the environment, including contributing to global warming, soil erosion, the extinction of rare species of flora and fauna, and impairing the forest's ability to self-regulate [5], [6]. Moreover, these fires pose significant risks to human life, infrastructure, and property [7]. Thus, quickly detecting forest fires and accurately identifying smoke areas is crucial for enabling firefighting personnel to take timely action, controlling the spread of the fire, which helps reduce the damage to ecosystems, infrastructure, and loss of life caused by forest fires [8].

The detection methods for forest fires are divided into smoke detection and flame detection [9]. Smoke, as an early indicator of fire, appears sooner, covers a larger volume, spreads faster, and is more easily detected by the naked eye [10], making it a critical clue for early fire detection. Flames, on the other hand, are essential for accurately pinpointing the fire's location [11], with color and varying shapes serving as key visual features that provide valuable information for firefighting efforts [12]. Therefore, integrating both smoke and fire detection significantly enhances the accuracy of forest fire monitoring, helping to protect forest resources and mitigate damage [13].

As a result of the quick development of computer vision technology, digital image processing techniques have been extensively used to identify forest fires. For the purpose of detection, early digital image processing techniques mainly extract the color, shape, and texture properties of smoke and flames. Unfortunately, manual feature extraction is heavily depended upon by these methods, and susceptibility to subjective human factors, as well as environmental complexities such as weather and lighting conditions, often leads to unsatisfactory detection performance [14]. Recently, the advances in deep learning have opened up new approaches to identifying forest fires. Deep learning models greatly improve the accuracy and robustness of fire detection models by providing benefits in terms of accuracy, detection speed, deployment flexibility, and adaptability to various fire characteristics [15], [16].

Despite promising progress in forest smoke and fire detection, several challenges remain unresolved. A key issue is how to achieve high detection accuracy, particularly in forest fire scenarios where the background is complex, interference is high, and the morphology of smoke and flames is highly variable. Furthermore, designing lightweight models for resource-constrained devices, such as edge and mobile devices, remains a critical research challenge. Thus, with the goal of addressing these concerns, this study proposes a lightweight forest smoke and fire detection model (FSFYOLO) built on YOLOv8s, which aims to reduce the computational load and parameter count through a lightweight design, enhancing detection accuracy. This makes it more feasible to deploy on resource-constrained devices, such as edge and mobile devices, allowing for rapid and accurate detection of smoke and fire in the early stages of a forest fire. This facilitates the issuance of timely warnings, reduces the time for rescue operations, and

minimizes the severe harm and losses caused by the spread of fires.

The main contributions of this paper are as follows: First, EfficientViT, a lightweight network, is employed as the backbone for YOLOv8s. Second, a new lightweight detection head, PCHead, is designed using the concept of shared parameters. Third, to fully extract local features and contextual information, the neck network is using the lightweight feature extraction module C2f-FL. Finally, a coordinate attention mechanism is introduced to capture direction-aware and position-sensitive information from forest smoke and fire images.

The remaining significant sections of this document are listed below: Section II provides a review of related research. Section III describes the improved model in this study. Section IV summarizes the dataset, experimental setup, parameters, and assessment measures that were employed during the studies. Section V performs pertinent experiments and discusses the findings. Finally, Section VI summarizes the entire effort of this study.

II. Related Works

With its strong feature extraction and pattern recognition capabilities, deep learning can automatically extract important information about forest fires from vast amounts of photos and videos. Therefore, deep learning-based recognition techniques have been used extensively in forest smoke and fire detection missions due to their notable benefits in forest smoke and fire recognition in recent years.

This research in [17] aimed to detect early forest fire smoke by improving the deformable DETR model. This approach improves detection capabilities for little or unobtrusive smoke by incorporating modules like Dense Pyramid Pooling. An iterative bounding box combination technique is described for producing more exact bounding boxes. In addition, a forest fire smoke dataset was created to validate the capability of the improved network. However, the improved model still has a larger number of parameters.

In the study [18], based on SqueezeNet, an efficient lightweight forest fire detection network was proposed. The model integrates Attention Gate (AG) units into the skip connections to enhance key features and suppress irrelevant information. Standard convolutions are replaced with depthwise convolutions, and a channel shuffle operation is introduced to optimize feature transmission. Although the model achieves good segmentation accuracy for forest fires, it may have limitations in broader fire detection tasks.

This paper in [19] described a methodology for detecting forest fires automatically that combines the Atom Search Optimizer (ASO) and deep transfer learning. The ResNet50 model is utilized to generate feature vectors, and the ASO is used to optimize the ResNet model's hyperparameters. A quasi-recurrent neural network model is used for fire categorization, with promising recognition and detection results.

The authors in [20] improved the YOLOv5 model to classify and detect forest fires. By incorporating the Weighted Bi-directional Feature Pyramid Network (BiFPN) and the Convolutional Block Attention Module (CBAM), the model enhances its ability to recognize various types of fires in complex backgrounds. The bounding box loss function adopts SIoU loss and introduces directionality to accelerate model convergence, effectively detecting different types of forest fires.

The research in [21] introduced a multi-task learning model for forest fire detection, which includes detection, classification, and segmentation tasks. The model includes a diagonal random origin swapping data augmentation approach that significantly enhances detection performance for small fire targets. When compared to single-task models, the upgraded model reduces missed and incorrect detections and has better feature extraction capabilities.

This paper in [22] improved the YOLOv8 model by adding a large-object detection head and introducing an Efficient Multi-Scale Attention (EMA) mechanism to reduce background noise and improve the identification of smoke targets and large-scale fires. The proposed path aggregation network bag structure further improves accuracy in detecting fires and smoke with uneven feature distributions and variable shapes. The improved model achieves higher detection accuracy.

III. Improved Methodology

A. The Forest Smoke and Fire YOLO Model

YOLOv8 is a high-performance object detection algorithm, available in five versions: n, s, m, l, and x, ranging from small to large. These versions have the same network structure, with differences only in network depth and width. YOLOv8s offers notable advantages, including strong feature extraction capabilities, high accuracy, compact size, and ease of deployment. Therefore, this study uses YOLOv8s as the baseline network and proposes a lightweight forest smoke and fire detection model, named FSFYOLO (Forest Smoke and Fire YOLO). Fig. 1 shows the FSFYOLO network structure.

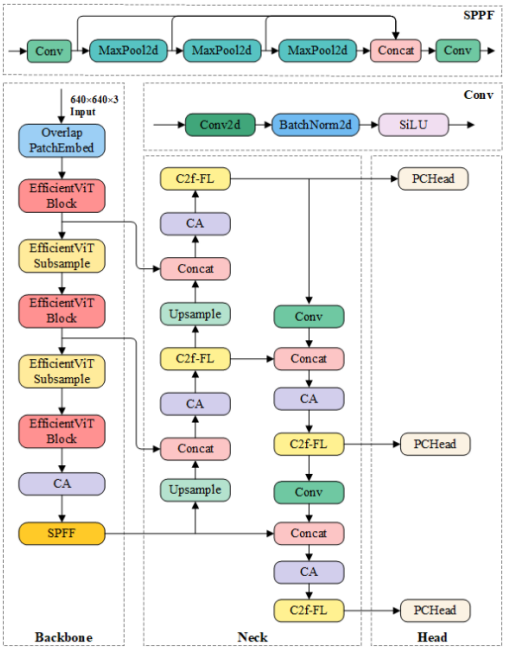


Fig. 1. Architecture of FSFYOLO.

The FSFYOLO network enhances the ability to accurately capture smoke and fire features in images while reducing computational redundancy by using the lightweight EfficientViT as the backbone network. Partial convolution is introduced, and a lightweight detection head, PCHead, is designed by sharing convolutional layers and branching processing, which productively minimizes the count of parameters and computational cost. In the neck network, to fully extract local features of smoke and fire as well as the surrounding contextual information, the LCFE block is proposed. This block is combined with the FasterNet Block and then integrated into the C2f module to form the lightweight feature extraction module C2f-FL, which expands the receptive field and lowers computational complexity. The coordinate attention, which extracts location sensitivity, directional awareness, and cross-channel information from fire and smoke images, is included into the backbone and neck networks. This mechanism filters out superfluous features in forest smoke and fire images, suppressing the impact of unrelated background information.

B. *EfficientViT*

The YOLOv8 backbone network, composed of multiple convolutional and pooling layers, results in high computational and storage costs. Furthermore, it struggles to accurately capture both local and global features of smoke and fire when processing cross-scale information. To address these issues, this study adopts EfficientViT as the backbone network of YOLOv8s. EfficientViT [23] is a high-speed vision transformer model that strikes a balance between speed and accuracy by optimizing memory efficiency and reducing attention computation redundancy. The EfficientViT network consists of overlapping patch embedding layers, EfficientViT blocks, and EfficientViT subsample layers, as shown in Fig. 2.

The input feature map first passes through the overlapping patch embedding layer, which divides the input into 16×16 patches and transforms them into vector tokens of a specified dimension, enabling better learning of the underlying features of the feature map.

The EfficientViT block is the core module of the EfficientViT network, with each block consisting of a sandwich layout formed by 2N FeedForward Network (FFN) layers, a token interaction layer, and Cascaded Group Attention (CGA). The token interaction layer, built with depthwise convolution (DWConv), is placed before the FFN layers to better capture local features in the image, thereby enhancing the model's overall performance. Unlike the conventional Multi-head Self-Attention Mechanism (MHSA), the CGA mechanism first divides the heads before generating Q, K, and V, and adds each head's output to the following head's input, thus providing each head with different features, improving the diversity of the attention maps. The outputs of all heads are spliced together and then passed through a linear layer to get the final output. Additionally, comparable to group convolution, this method lowers computational complexity and parameter count by lowering the Q, K, and V layers' input and output channels by a factor of 1/G, where G is the number of groups.

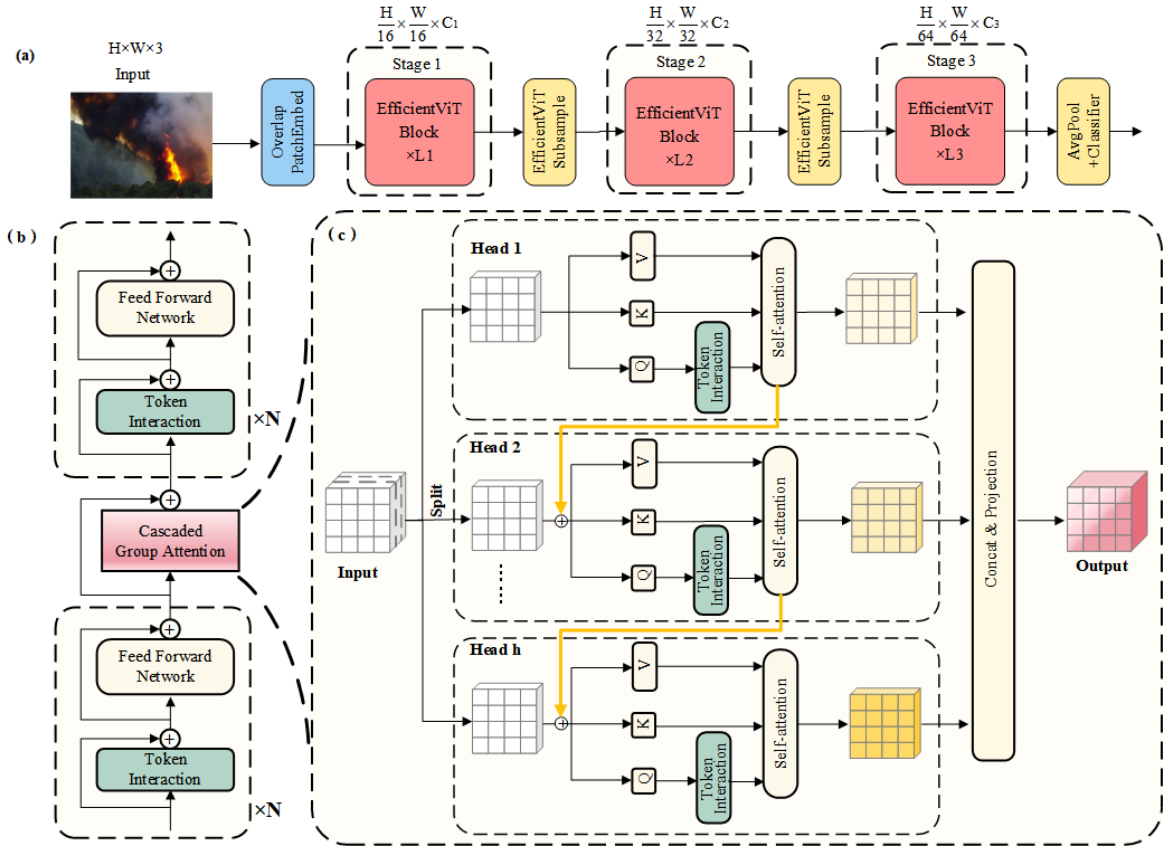


Fig. 2. (a) Architecture of EfficientViT; (b) Structure of sandwich layout block; (c) Structure of cascaded group attention.

CGA is expressed by the formula:

$$\tilde{X}_{ij} = Attn(X_{ij}W_{ij}^{Q}, X_{ij}W_{ij}^{K}, X_{ij}W_{ij}^{V}) \quad (1)$$

$$\tilde{X}_{i+1} = Concat[\tilde{X}_{ij}]_{j=1:h}W_{i}^{P} \quad (2)$$

$$X_{ij}^{'} = X_{ij} + \tilde{X}_{i(j-1)}, 1 < j \le h \quad (3)$$

In Eq. (1) and Eq. (2), $\tilde{X}_{ij}$ represents the output of X_{ij} after being processed by the self-attention mechanism in the j-th head. X_{ij} refers to the j-th slice of the input feature map X_i, i.e. $X_i=[X_{i1},X_{i2},...,X_{ih}]$, , where $1<j\le h$ and h represent the total number of attention heads. $W_{ij}^{Q},W_{ij}^{K},W_{ij}^{V}$ denotes the weight matrix, and W_i^P represents the linear layer.

In Eq. (3), $X_{ij}^{'}$ represents the sum of X_{ij}, the j-th slice of X_i and the output $\tilde{X}_{i(j-1)}$ from the (j-1)-th head, as obtained through Eq. (1) and Eq. (2). At this point, $X_{ij}^{'}$ replaces X_{ij} as the j-th head's original input feature map.

The EfficientViT subsampling layer downscales the feature map. Unlike traditional Transformer models, EfficientViT uses an inverted residual block in the subsample block instead of a self-attention layer, reducing potential information loss during downsampling.

C. The Lightweight Design of the Detection Head

Both branches of the YOLOv8 detecting head start with two 3×3 convolution modules, then a Conv2d module. Finally, they calculate the Cls and Bbox losses individually. Fig. 3 shows the specific structure of the YOLOv8 detection head.

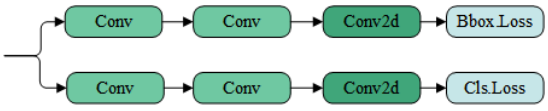


Fig. 3. YOLOv8 detection head structure.

To detect smoke and fire targets at different scales, the YOLOv8 detection head requires more convolution operations to process multi-scale feature maps, which increases the depth and number of parameters in the network. We adopt Partial Convolution (PConv) from the FasterNet Block [24] to modify the lightweight design of the YOLOv8s detection head to address these issues. Fig. 4 displays the FasterNet Block and PConv network structure diagram.

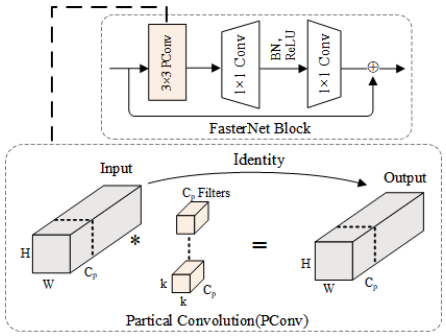


Fig. 4. Network structure of FasterBlock and PConv.

Comprising three layers, the FasterNet Block is composed of PConv layer, 1×1 convolutional layer, and 1×1 2D convolutional layer. PConv selectively applies regular convolution to specific input channels to extract spatial features; the remaining input channels remain unaltered and are directly translated to the output channels, resulting in significant computational redundancy reduction.

The new detection head first shares a PConv layer and a 1×1 convolutional layer, and then branches into two paths. Each path computes the Bbox loss and Cls loss, respectively, after passing through a Conv2d module. This new detection head is called PCHead (Partial Convolutional Head), and its structure is shown in Fig. 5.

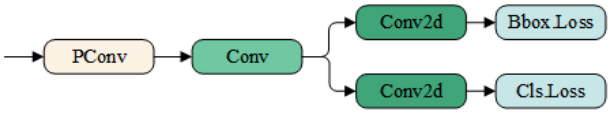


Fig. 5. PCHead structure.

D. C2f-FL Lightweight Feature Extraction Module

1) Local and Contextual Feature Extraction (LCFE) block: Traditional convolution operations confront issues such as information loss and a limited receptive field when capturing the diverse features of forest smoke and fires in various conditions. This hinders the model's ability to effectively extract local forest smoke and fire features and the corresponding surrounding contextual information, which in turn affects the extraction of fire-related features and restricts the expansion of the receptive field. In order to overcome this limitation, we propose a Local and Contextual Feature Extraction (LCFE) block, as illustrated in Fig. 6. The LCFE block is designed to efficiently capture local forest smoke and fire features while also extracting related contextual information, broadening the model's receptive field, and improving the network's capacity to identify fire features.

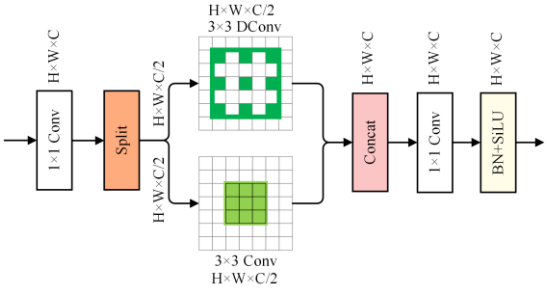


Fig. 6. LCFE block structure.

The LCFE block integrates information from several channels of the input feature map using a 1×1 convolution, thus enabling information interaction within the receptive field. The feature map is then partitioned evenly along the channel dimension into two sub-feature maps with an equal number of channels. One sub-feature map uses 3×3 conventional convolution to extract local features from eight neighboring vectors, while the other uses 3×3 dilated convolution to capture contextual information as well as widen the receptive field. Subsequently, concatenation of the extracted characteristics

occurs along the channel dimension; the local features and contextual information are combined using a 1×1 convolution. The fused features are then normalized and nonlinearized using batch normalization (BN) and the SiLU activation function, yielding the final output. Through this design method, the LCFE block is able to fully capture the intricate characteristics of smoke and fires, improving the model's recognition capabilities.

$$f_1, f_2 = Split(F_n(X)) \tag{4}$$

$$f = W(F_n(Concat(F_n(f_1), F_m^d(f_2)))) \tag{5}$$

In this context, X represents the input feature map, F_n denotes an n × n convolution operation, and F_m^d refers to a dilated convolution with a dilation rate d and a kernel size of m × m. f_1 and f_2 are the output feature maps, uniformly divided along the channel dimension. $W(\cdot)$ denotes the Batch Normalization (BN) and SiLU activation procedures; $Concat(\cdot)$ denotes concatenation along the channel dimension; $Split(\cdot)$ denotes the operation of splitting the feature map along the channel dimension. Ultimately, after being processed by the LCFE block, the output feature map f is obtained.

2) C2f-FL module: In YOLOv8, the C2f module makes use of a bottleneck structure made up of many convolutional layers, which requires repetitive dimensionality reduction and channel expansion of the input feature map. This approach can cause information loss while also increasing the model's computational complexity and parameter count. To tackle these issues, this study introduces the FasterNet Block, which reduces the model's parameter load and computational complexity while achieving efficient spatial feature extraction. Additionally, the LCFE block is incorporated into the forward propagation of the FasterNet Block, forming the FL block. This FL block serves as the bottleneck module within the C2f module of the neck network, resulting in the new lightweight feature extraction module, C2f-FL. This improvement reduces the parameters and computation required for smoke and flame feature extraction, effectively enhancing both target feature extraction and overall model efficiency. The structure of the FL block and C2f-FL is shown in Fig. 7.

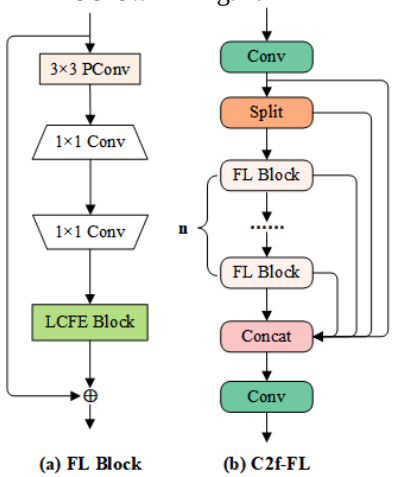


Fig. 7. Structure of FL block and C2f-FL module.

E. Coordinate Attention (CA)

Given the complexity of background textures and the abundance of irrelevant information in forest smoke and fire images, existing attention mechanisms often focus only on channel dependencies, neglecting the importance of spatial information. This results in significant redundancy in the spatial dimension of the extracted feature maps. To address this issue, a coordinate attention (CA) [25] mechanism is integrated into the network: before the backbone network's SPPF module and after the neck network's feature fusion module. This approach enhances the extraction of both channel and spatial information, effectively filtering out redundant features in forest smoke and fire images. Fig. 8 depicts the structure of the coordinate attention mechanism.

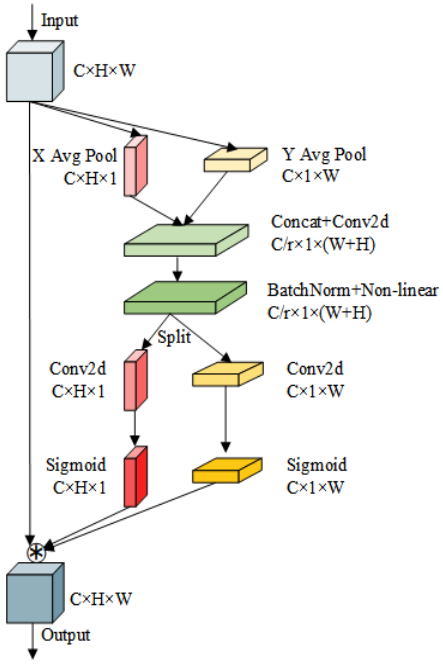


Fig. 8. Structure of the coordinate attention mechanism.

Two-dimensional global pooling is broken down by CA into two one-dimensional global poolings in separate directions. The input feature map is aggregated separately along the vertical and horizontal directions, resulting in two independent feature maps that are direction-aware and position-sensitive. This approach enables the capture of long-range dependencies along different spatial dimensions while avoiding the loss of spatial details, thus accurately preserving positional information from the original image. Subsequently, these direction-specific feature maps undergo operations such as stacking and normalization to encode attention maps. Finally, these attention maps are applied to the input feature maps in a complementary manner through elemental multiplication.

IV. Dataset and Experimental Setup

A. Dataset

One of the challenges in this study is the absence of a publicly available, unified forest fire dataset. To address this, a custom dataset containing instances of smoke and fire was created. The images in the dataset come from two sources: the

first involves collecting forest smoke and fire images and videos from the Internet, extracting one frame every 5 frames of the videos to create still images; the second source includes partial images from the FLAME dataset [26] published by Northern Arizona University. The dataset contains a total of 3,895 images, all manually labeled using LabelImg. It is separated into two sets: training and validation, in a 4:1 ratio, with 3,116 images for training and 779 for validation. Fig. 9 depicts sample photos from the collection.

Fig. 9. Partial experimental data.

B. Experimental Environment

The system used for the experiments in this study runs on Windows 11 with 16GB of RAM. The hardware includes a 13th Gen Intel(R) Core(TM) i7-13700H CPU and an NVIDIA GeForce RTX 4060 Laptop GPU. Pycharm was used as the software environment, and the PyTorch deep learning framework, based on Python, was utilized. The Python version used was 3.10.

C. Hyperparameter Settings

In this work, all models' hyperparameters are kept consistent during training and validation. The experimental parameters utilized for network training are listed in Table I:

TABLE I. EXPERIMENTAL HYPERPARAMETERS

Parameter name	Configuration
Size of the input image	640×640
Optimizer	SGD
Batchsize	16
Epochs	150
Momentum	0.937
Lr0	0.01
Weight decay	0.0005

D. Evaluation Criterion

Precision (P), Recall (R), Mean Average Precision (mAP), Giga Floating Point Operations per Second (GFLOPs), number of parameters (Params), and model weight file size (in MB) were used as assessment measures to analyze the network performance in this study.

Precision refers to the fraction of true positive samples among those predicted as positive by the model. It is calculated using the following formula:

$$P = \frac{TP}{TP + FP} \tag{6}$$

Recall evaluates the proportion of true positive samples that are correctly predicted among all actual positive samples. Its calculation is as follows:

$$R = \frac{TP}{TP + FN} \tag{7}$$

where TP, FP and FN denote the number of true, false positive and false negative cases, respectively.

AP represents the average precision for a single target category. It is calculated using the following formula:

$$AP = \int_0^1 P(R)\ dR \tag{8}$$

mAP is the average of AP values across all categories. It is calculated using the following formula:

$$mAP = \frac{1}{n}\sum_{i=1}^{n} AP_i \tag{9}$$

The Intersection over Union (IoU) represents the ratio of the intersection area to the union area between the predicted bounding box and the ground truth bounding box. By setting different IoU thresholds, corresponding mAP values can be obtained. In this study, mAP at IoU = 0.5 (mAP50) is adopted as the evaluation metric to assess the model's localization and classification capabilities for detected objects, providing a comprehensive evaluation of its overall detection performance.

GFLOPs is an indication for determining a model's computational complexity; a lower GFLOPs value indicates reduced computational cost. The parameter count measures the size of the model, and fewer parameters help accelerate the training process. The number of bytes in the file created during training is referred to as the weight file size for the model, with smaller weight files facilitating deployment and operation on resource-constrained devices.

V. RESULTS AND DISCUSSION

A. Ablation Experiments

To verify the effectiveness of the proposed detection model FSFYOLO in smoke and fire detection tasks, four groups of ablation experiments were conducted. Throughout these tests, the same dataset and hyperparameters were used to train each model, with only the modules under evaluation being changed. Table II presents the experimental results obtained.

The ablation experiment outcomes show that incorporating EfficientViT as the backbone network for YOLOv8s leads to reductions of 24.6% in the number of parameters, 28.2% in GFLOPs, and 22.0% in the size of the weight file compared to the original network. This proves that EfficientViT effectively reduces the model's complexity and computational burden. Additionally, by using the PCHead as the detection head, which shares convolutional layers and employs branch-based processing, the parameters and computational load are further reduced on the YOLOv8s-EfficientViT foundation, greatly decreasing model complexity. In addition, the network is further lightweighted by using the lightweight feature

extraction module C2f-FL, resulting in reductions of 16.9% in parameters, 17.9% in GFLOPs, and 15.3% in weight file size compared to YOLOv8s-EfficientViT-PCHead. The recall and mAP50 of the model compare favorably to the original network in terms of performance, suggesting that adding the C2f-FL module can recognize target items more thoroughly and lower the miss detection rate. Lastly, by adding the CA mechanism, the model's precision increases by 1%, reducing false positives in smoke and fire detection, as it better captures directional and positional information from the images. Importantly, the inclusion of CA does not significantly increase the parameter count or computation load, demonstrating that performance improvements are achieved without a notable increase in model size. The experimental results confirm that the FSFYOLO model proposed achieves superior performance in forest smoke and fire image recognition tasks.

TABLE II. THE RESULTS OF ABLATION EXPERIMENTS

YOLOv8s	EfficientViT	PCHead	C2f-FL	CA	P	R	mAP50	Params/10^6	GFLOPs	Weight File Size/MB
+					0.904	0.873	0.923	11.13	28.4	21.4
+	+				0.896	0.872	0.922	8.39	20.4	16.7
+	+	+			0.906	0.868	0.926	6.86	13.4	13.7
+	+	+	+		0.907	0.886	0.931	5.70	11.0	11.6
+	+	+	+	+	0.917	0.883	0.933	5.83	11.1	11.8

B. Comparative Experiments

To further validate the effectiveness of the improved network in detecting forest smoke and fire, a comparative analysis was conducted under the same experimental settings, dataset, and training strategies, using other mainstream object detection models. These models include SSD [27], YOLOX [28], YOLOv5, YOLOv6 [29], YOLOv7 [30], RT-DETR [31], the improved YOLOv5s model by Yang et al. [32], and the improved YOLOv8s model by Kong et al. [33]. Performance indicators such as precision (P), recall (R), mAP50, number of parameters, GFLOPs, and model weight file size were used as evaluation criteria. Table III presents the experimental results obtained.

The experimental results indicate that the SSD, RT-DETR, and YOLOv6s detection algorithms have relatively large parameter counts and computational costs. These factors result in larger model weight files and impose higher demands on hardware resources. In contrast, the parameter count of the FSFYOLO model is approximately one-fourth that of SSD, one-fifth that of RT-DETR, and one-third that of YOLOv6s. Therefore, SSD, RT-DETR, and YOLOv6s are deemed unsuitable for lightweight, real-time detection of forest smoke and fire. The YOLOv5s, YOLOv7, and FSFYOLO models include some identical feature extraction modules, such as the Conv module, and share similar network architectures. As a result, they exhibit only minor differences in parameter count, computational complexity, and model weight size. However, FSFYOLO achieves significant advantages by optimizing the C2f feature extraction module and introducing the CA mechanism to enhance feature extraction. Consequently, FSFYOLO outperforms YOLOv5s and YOLOv7 in terms of accuracy, recall, and mAP50, demonstrating a clear and distinct advantage. Although YOLOXs has a computational cost close to that of FSFYOLO, its parameter count is 34.8% higher, and its weight file is 2.9 times larger, with lower precision, recall, and mAP50 compared to FSFYOLO. Yang et al. [32] proposed an improved YOLOv5s model by adding C3Ghost and Ghost modules, resulting in parameter counts and GFLOPs of 3.78×10^6 and 8.3, respectively. However, due to the Ghost module only performing standard convolution operations on half of the spatial features, the model exhibits limitations in capturing detailed features for complex forest fire smoke detection tasks. Consequently, its precision, recall, and mAP50 do not surpass FSFYOLO. Similarly, Kong et al. [33] introduced Efficient Multi-Scale Attention (EMA) and GSConv to optimize YOLOv8s, reducing its parameter count, GFLOPs, and weight file size, but all performance metrics remain lower than those of FSFYOLO. Compared to the baseline YOLOv8s, the improved network outperforms the original in all key metrics. Based on a comprehensive analysis of all evaluation metrics, FSFYOLO offers significantly enhanced detection capabilities and is better suited for forest fire detection compared to other models.

C. Visual Analysis

To better further confirm the FSFYOLO network performance in forest smoke and fire detection tasks, we conducted a visual analysis utilizing the Gradient-weighted Class Activation Mapping (Grad-CAM) [34] approach. Grad-CAM heatmaps show that deeper colors indicate more attention to the respective locations, while lighter colors suggest less attention. We chose a few typical photos from the experimental validation set to compare the detection performance of YOLOv8s with FSFYOLO under various fire conditions. Fig. 10 displays the detection results, with (a) and (b) containing both fire and smoke, (c) containing only smoke, and (d) containing only fire.

It is evident from the heatmaps that YOLOv8s and FSFYOLO are equally adept at identifying and pinpointing target locations that are characterized by smoke and fire. But the FSFYOLO model has a higher confidence level, focuses more accurately on the regions of fire and smoke in the image, and focuses on regions very close to the actual smoke and fire shapes. Specifically, YOLOv8s may be affected by complex background interference present in forest fire images, leading to a dispersed focus on target objects. In contrast, FSFYOLO, through its lightweight design and optimized feature extraction modules, not only suppresses background noise but also enhances the precise capture of target features, improving accuracy. This again demonstrates the effectiveness of FSFYOLO in the task of forest smoke and fire detection.

TABLE III. THE RESULTS OF COMPARATIVE EXPERIMENTS

Model	P	R	mAP50	Params/10^6	GFLOPs	Weight File Size/MB
SSD	0.900	0.667	0.848	23.75	136.8	91.1
YOLOXs	0.905	0.864	0.908	8.94	13.4	34.3
YOLOv5s	0.899	0.879	0.920	7.03	15.8	13.7
YOLOv6s	0.898	0.884	0.917	18.50	45.3	38.7
YOLOv7	0.904	0.870	0.916	6.02	13.2	11.7
RT-DETR	0.890	0.837	0.901	32.81	108.0	63.0
Yang et al. [32]	0.898	0.874	0.917	3.78	8.3	7.7
Kong et al. [33]	0.897	0.879	0.922	8.56	20.9	16.6
YOLOv8s	0.904	0.873	0.923	11.13	28.4	21.4
FSFYOLO	0.917	0.883	0.933	5.83	11.1	11.8

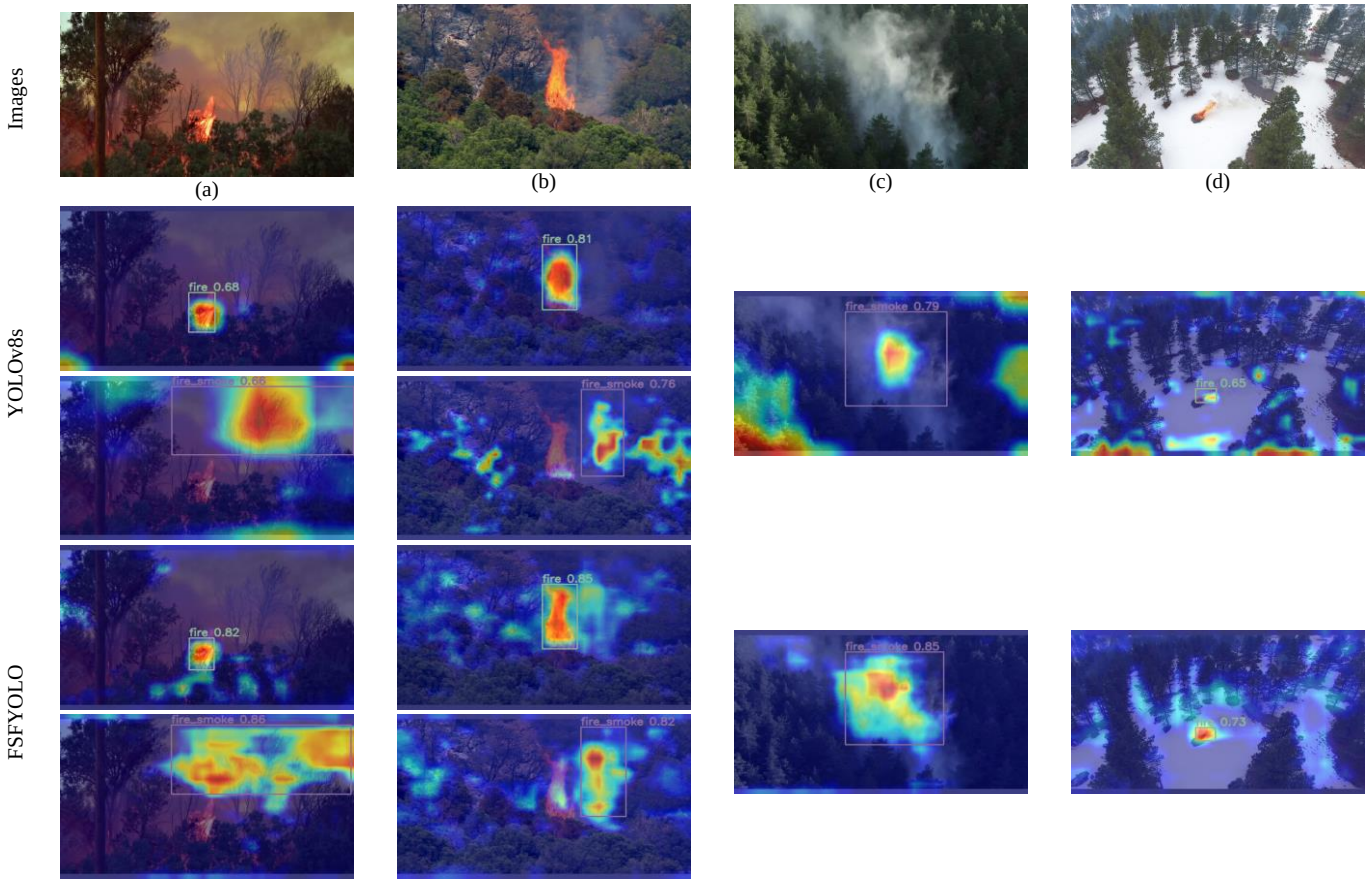


Fig. 10. Schematic visualization of YOLOv8s and FSFYOLO detection results.

D. Generalization Verification

In this experiment, the proposed FSFYOLO model was evaluated for generalization performance using the open FM-VOC Dataset18644 [35], which contains instances of smoke and fire. The dataset contains 16,844 photos depicting fires in a variety of contexts, including building fires, grassland fires, indoor fires, forest fires, and road fires. Experiments were conducted to compare the YOLOv8s and FSFYOLO models on the FM-VOC Dataset18644. The experimental conditions, parameter settings, and evaluation metrics were consistent with those used in other experiments in this study. The results are shown in Table IV.

As Table IV illustrates, compared to the baseline YOLOv8s model, the FSFYOLO model achieved improvements of 1.3%, 2.3%, and 1.3% in precision, recall, and mAP50, respectively, on the FM-VOC Dataset18644. Additionally, the FSFYOLO model demonstrated reductions of 47.6%, 60.9%, and 44.9% in parameter count, GFLOPs, and model weight size, respectively. The experimental results confirm that the FSFYOLO model achieves a good balance between detection performance and lightweight design, effectively detecting and recognizing fires

across different scenarios. Therefore, the FSFYOLO model exhibits excellent generalization performance, which will broaden the application of target detection in forest fire scenarios.

TABLE IV. COMPARISON OF EXPERIMENTAL RESULTS ON THE FM-VOC DATASET18644

Evaluation Metrics	YOLOv8s	FSFYOLO
P	0.917	0.930
R	0.872	0.895
mAP50	0.939	0.952
Params/10^6	11.13	5.83
GFLOPs	28.4	11.1
Weight File Size/MB	21.4	11.8

VI. CONCLUSION

To accomplish precise and timely forest fire detection, we present FSFYOLO, a lightweight forest smoke and fire detection network based on YOLOv8s. To begin, EfficientViT, a lightweight transformer network, serves as the backbone network to improve network feature extraction capability. Second, a lightweight detection head, PCHead, is designed using the shared parameters idea, which decreases the model's complexity while preserving detection performance. Third, the lightweight feature extraction module C2f-FL is introduced to effectively capture local features of forest smoke and fire, as well as relevant surrounding contextual information, which achieves the dual enhancement of model computation efficiency and feature extraction capability. Finally, a coordinate attention mechanism is integrated to extract both channel and spatial location information, filtering out superfluous features in forest fire images. Experimental validation shows that the FSFYOLO network achieves higher accuracy than other networks, with significantly reduced parameter count and computational cost, satisfying real-time needs for forest smoke and fire detection. Additionally, the FSFYOLO network is easily deployable on resource-constrained devices, providing an effective method for forest fire detection. However, this study still has some limitations. For example, the forest fire dataset used in the experiments is relatively small, and the range of scene coverage is insufficient. Moreover, although the FSFYOLO network decreases the number of parameters and computing costs while increasing accuracy, there is still room for optimization in the model structure and performance. In future work, we will focus on expanding the forest fire dataset to cover more complex scenarios and exploring more efficient, parameter-reduced methods to further enhance the performance and precision of forest fire detection models.

REFERENCES

[1] A. Khan, B. Hassan, S. Khan, R. Ahmed and A. Abuassba, "DeepFire: A novel dataset and deep transfer learning benchmark for forest fire detection," Mob Inf Syst, vol. 2022, no.1, p. 5358359, 2022.

[2] S.D. Wang, L.L. Miao and G.X. Peng, "An improved algorithm for forest fire detection using HJ data," Procedia Environ Sci, vol. 13, pp. 140-150, 2012.

[3] M.S. Anggreainy, B. Kurniawan and F.I. Kurniadi, "Reduced false alarm for forest fires detection and monitoring using fuzzy logic algorithm," International Journal of Advanced Computer Science and Applications(IJACSA), vol. 13, no. 7, pp. 535-541 2022.

[4] A.A. Alkhatib, "A review on forest fire detection techniques," Int J Distrib Sens Netw, vol. 10, no. 3, p. 597368, 2014.

[5] S.T. Seydi, V. Saeidi, B. Kalantar, N. Ueda and A.A. Halin, "Fire - Net: A Deep Learning Framework for Active Forest Fire Detection," J Sensors, vol. 2022, no. 1, p. 8044390, 2022.

[6] M. Yandouzi, M. Grari, I. Idrissi, M. Boukabous, O. Mous-saoui, M. Azizi, K. Ghoumid and A.K. Elmiad, "Forest fires detection using deep transfer learning," International Journal of Advanced Computer Science and Applications(IJACSA), vol. 13, no. 8, pp. 268-275, 2022.

[7] Q. Jiao, M. Fan, J. Tao, W. Wang, D. Liu and P. Wang, "Forest fire patterns and lightning-caused forest fire detection in Heilongjiang Province of China using satellite data," Fire, vol. 6, no. 4, p. 166, 2023.

[8] Y. Peng and Y. Wang, "Real-time forest smoke detection using hand-designed features and deep learning," Comput Electron Agric, vol. 167, p. 105029, 2019.

[9] J. Zhan, Y. Hu, G. Zhou, Y. Wang, W. Cai and L. Li, "A high-precision forest fire smoke detection approach based on ARGNet," Comput Electron Agric, vol, 196, p. 106874, 2022.

[10] X. Zheng, F. Chen, L. Lou, P. Cheng and Y. Huang, "Real-time detection of full-scale forest fire smoke based on deep convolution neural network," Remote Sensing, vol. 14, no. 3, p. 536, 2022.

[11] P.E.N.G. Bo, "Research on classification of forest fire risk based on GIS technology in Xichang City, Sichuan Province," Journal of Sichuan Forestry Science and Technology, vol. 42, no. 5, pp. 53-57, 2021.

[12] C. Emmy Prema, S.S. Vinsley and S. Suresh, "Efficient flame detection based on static and dynamic texture analysis in forest fire detection," Fire technology, vol. 54, pp. 255-288, 2018.

[13] A. Gaur, A. Singh, A. Kumar, A. Kumar and K. Kapoor, "Video flame and smoke based fire detection algorithms: A literature review," Fire technology, vol. 56, pp. 1943-1980, 2020.

[14] J. Lin, H. Lin and F. Wang, "A semi-supervised method for real-time forest fire detection algorithm based on adaptively spatial feature fusion," Forests, vol. 14, no. 2, p. 361, 2023.

[15] J. Lin, H. Lin and F. Wang, "STPM_SAHI: A Small-Target forest fire detection model based on Swin Transformer and Slicing Aided Hyper inference," Forests, vol. 13, no.10, p. 1603, 2022.

[16] Z. Guan, X. Miao, Y. Mu, Q. Sun, Q. Ye and D. Gao, "Forest fire segmentation from Aerial Imagery data Using an improved instance segmentation model," Remote Sensing, vol. 14, no. 13, p. 3159, 2022.

[17] J. Huang, J. Zhou, H. Yang, Y. Liu and H. Liu, "A small-target forest fire smoke detection model based on deformable transformer for end-to-end object detection," Forests, vol. 14, no. 1, p. 162, 2023.

[18] J. Zhang, H. Zhu, P. Wang and X. Ling, "ATT squeeze U-Net: A lightweight network for forest fire detection and recognition," IEEE Access, vol. 9, pp. 10858-10870, 2021.

[19] K. Alice, A. Thillaivanan, G.R.K. Rao, S. Rajalakshmi, K. Singh and R. Rastogi, "Automated forest fire detection using atom search optimizer with deep transfer learning model," ICAAIC, pp. 222-227, IEEE, 2023.

[20] Q. Xue, H. Lin and F. Wang, "Fcdm: an improved forest fire classification and detection model based on yolov5," Forests, vol. 13, no. 12, p. 2129, 2022.

[21] K. Lu,, J. Huang, J. Li, J. Zhou, X. Chen and Y. Liu, "MTL-FFDET: A multi-task learning-based model for forest fire detection," Forests, vol. 13, no. 9, p. 1448, 2022.

[22] T. Zhang, F. Wang, W. Wang, Q. Zhao, W. Ning and H. Wu, "Research on fire smoke detection algorithm based on improved YOLOv8," IEEE Access, vol. 14, pp. 117354-117362, 2024.

[23] X. Liu, H. Peng, N. Zheng, Y. Yang, H. Hu and Y. Yuan, "Efficientvit: Memory efficient vision transformer with cascaded group attention," in Proceedings of the IEEE/ CVF conference on computer vision and pattern recognition, pp. 14420-14430, 2023.

[24] J. Chen, S.H. Kao, H. He, W. Zhuo, S. Wen, C.H. Lee and S.H.G. Chan, "Run, don't walk: chasing higher FLOPS for faster neural networks," in

Proceedings of the IEEE/ CVF conference on computer vision and pattern recognition, pp. 12021-12031, 2023.

[25] Q. Hou, D. Zhou and J. Feng, "Coordinate attention for efficient mobile network design," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 13713-13722, 2021.

[26] A. Shamsoshoara, F. Afghah, A. Razi, L. Zheng, P.Z. Fulé and E. Blasch, "Aerial imagery pile burn detection using deep learning: The FLAME dataset," Computer Networks, vol. 193, p. 108001, 2021.

[27] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C.Y. Fu and A.C. Berg, "Ssd: Single shot multibox detector," in Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11–14, 2016, Proceedings, Part I 14, pp. 21-37, Springer International Publishing, 2016.

[28] G. Zheng, L. Songtao, W. Feng, L. Zeming and S. Jian, "YOLOX: Exceeding YOLO series in 2021," arXiv preprint arXiv: 2107.08430, 2021.

[29] C. Li, L. Li, H. Jiang, K. Weng, Y. Geng, L. Li, Z. Ke, Q. Li, M. Cheng, W. Nie and Y. Li, "YOLOv6: A single-stage object detection framework for industrial applications," arXiv preprint arXiv: 2209.02976, 2022.

[30] C.Y. Wang, A. Bochkovskiy and H.Y.M. Liao, "YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 7464-7475, 2023.

[31] Y. Zhao, W. Lv, S. Xu, J. Wei, G. Wang, Q. Dang, Y. Liu and J. Chen, "Detrs beat yolos on real-time object detection," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 16965-16974, 2024.

[32] J. Yang, W. Zhu, T. Sun, X. Ren and F. Liu, "Lightweight forest smoke and fire detection algorithm based on improved YOLOv5," PLoS one, vol. 18, no. 9, p. e0291359, 2023.

[33] D. Kong, Y. Li and M. Duan, "Fire and smoke real-time detection algorithm for coal mines based on improved YOLOv8s," Plos one, vol. 19, no. 4, p. e0300502, 2024.

[34] R.R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh and D. Batra, "Grad-cam: Visual explanations from deep networks via gradient-based localization," in Proceedings of the IEEE international conference on computer vision, pp. 618-626, 2017.

[35] X. Geng, Y. Su, X. Cao, H. Li and L. Liu, "YOLOFM: an improved fire and smoke object detection algorithm based on YOLOv5n," Scientific Reports, vol. 14, no. 1, p. 4543, 2024.

Identification of Chili Plant Diseases Based on Leaves Using Hyperparameter Optimization Architecture Convolutional Neural Network

Murinto, Sri Winiarti, Ardi Pujiyanta
Department of Informatics, Universitas Ahmad Dahlan Yogyakarta, Indonesia

***Abstract*—This paper proposes a method to detect chili plant diseases based on leaves. Studies in recent years have shown that chili production in Indonesia has decreased. This is because there are several influencing factors. One common factor is the presence of diseases in chili plants that cause less than optimal harvest production. Fungi or pests on chili leaves usually cause diseases that often appear in chili plants. Chili leaf diseases have a negative impact on chili harvest yields. Chili leaf diseases can result in significant decreases in both the quantity and quality of chili harvests. Accurate disease diagnosis will help increase farmer profits. This study identified four major leaf diseases, namely leaf curl, leaf spot, yellowish, and white spot. In this research images were taken using a digital camera. These diseases were classified into five classes (healthy, leaf curl, leaf spot, yellowish, and white spot) using two different pre-trained deep learning networks, namely MobileNetV2 and VGG16, using chili leaf data through deep learning transfer. The experimental results showed the model with the best performance was the VGG16 model. This model achieved a validation accuracy of 94% on public and own data sets. Meanwhile, the next best-performing model is MobileNetV2, which achieved an accuracy of 90%, followed by the Traditional CNN Model, which achieved a validation accuracy of 88%. In future developments, we intend to deploy it on mobile devices to automatically monitor and identify various types of chili plant disease information based on leaves.**

***Keywords*—Chili leaf; deep learning; MobileNetV2; transfer learning; VGG16**

I. INTRODUCTION

In several agricultural countries, the country's main income is agricultural products. The condition of the soil environment and land requirements are important influences on the harvest produced. However, farmers need help with several problems, such as water shortages, natural disasters, plant diseases, etc. However, some of these problems can be reduced by providing technical facilities for farmers. An automatic plant disease identification and prevention system is one solution that can help farmers. This type of system can overcome the problem of lack of knowledge about plant diseases because there are very few experts in this field [1],[2],[3]. The automatic system will also save time and help increase farmers' profits [4]. In agriculture, detecting and classifying leaf diseases is important because farmers often have to decide whether the cultivated plants are thriving.

Generally, examination through observation of leaves, roots, stems, flowers and fruits can identify the type of food crop that is suffering. This manual approach does not guarantee accuracy in identifying the plant disease. In addition, not all plant diseases in plants can be identified manually. Likewise, manual identification of plant diseases takes a long time. The research that is currently being done is to identify and classify plant diseases automatically using the help of artificial intelligence. Automation in monitoring types of food crops will greatly assist farmers in monitoring their plants. If the plant disease can be detected early, the possibility of producing a good harvest will be achieved [5].

Automatic detection of plant diseases based on images is one of the jobs in Computer Vision. One of the techniques used in Computer Vision is Machine Learning Techniques. In the field of agriculture, machine learning techniques can produce very significant improvements when applied. Detection and classification of plant diseases using deep learning is one example used to help farmers detect types of plant diseases. Research on the identification, detection and classification of plant diseases using deep learning techniques has become a subject of much research in recent years. Conventional computer vision algorithms, support vector machine (SVM) [6], K-nearest neighbors (KNN) [7], and K-means clustering methods [8] of machine learning algorithms have been used for early detection in various fields.

The process of grouping an object based on certain parts is called classification. Classification is one part of the work in machine learning. While machine learning itself is part of Artificial Intelligence (AI). In general, AI is a branch of computer science that focuses on development that has human intelligence capabilities. One part of Machine Learning is Deep Learning [9]. In Deep Learning, several algorithms are already known and often used, including the algorithm is Recurrent Neural Networks (RNN) [10], Convolutional Neural Networks (CNN) [11], [12], [13], and Deep Generative Model (DG) [14]. Convolution Neural Network is a model in deep learning that is usually widely used in classification work. One of the known classifications is how chili plant diseases are classified into several types based on their leaves.

A large number of parameters need to be trained in CNN and its variants, while training these CNN architectures also requires several labelled samples and substantial resources from scratch to assess their performance of the technique. Collecting a large labelled dataset is a challenging task. Despite its limitations, previous investigations have successfully demonstrated the potential of deep learning algorithms. In particular, deep transfer learning alleviates the problems classical deep learning methods

face. The solution consists of using a pre-trained network where only the parameters of the final classification level need to be inferred from scratch. Some existing deep learning transfers include the following: Alexnet [15], VGG16 [16], MobileNetV2 [16], GoogleNet [17], Resnet [18]. However, not all deep learning transfers suit all problems. Transfer learning has been widely used in several recent studies, including MobileNetV2 and VGG16, which have been applied in various fields.

This study aims to apply the latest transfer learning deep learning technique for chili plant disease recognition based on visible leaf images. Traditional Convolutional Neural Network (CNN) is used to perform the classification, which is then compared with existing transfer learning models, namely MobileNetV2 and VGG16. This study recognizes diseased plants based on symptoms to achieve recognition without the influence of several disease symptoms that appear on one leaf.

II. Materials and Method

A. Materials

A dataset of images containing symptom images of four chili plant diseases, namely yellowish, leaf spot, leaf curl, and white spot, was created. Based on this dataset, CNN, MobileNetV2, and VGG16 models were trained to recognize chili plant diseases.

1) Dataset chili plant diseases: The trained dataset contains several diseases that attack chili plants. Using a mobile phone camera, images are collected under several conditions depending on the time (e.g., lighting), season (e.g., temperature, humidity), and location of the image capture. For this reason, we have visited several chili plantations in the Semarang and Klaten Regencies. Other data was obtained from Kaggle.com, which is public data. The data we use consists of 250 images of chili plant leaves. The images are divided into 5 categories: a healthy image class and four classes of diseased images representing four diseases: whitefly, curl leaf, gray mold, and yellowing. The four types of chili plant diseases are:

a) Yellowish. Symptoms of this disease are leaves that appear wilted, starting from the bottom, then turning yellow up towards the young branches. The body parts of the chili plant infected with this disease will be covered in white hyphae like cotton. If the chili plant is attacked while it is still growing, fruit can still be produced. However, if the disease has spread to the stem area, the young chilies will fall off. Fig. 1 shows several examples of chili plant diseases based on leaves called yellowish.

b) White fly. Yellow virus is also commonly called bule or bulai disease, the yellow virus causes chili plants to appear yellow. This disease caused by the gemini virus can be carried from seeds or seeds and transmitted by lice. Because it is caused by a virus, chemical poisons will not work to overcome it. Therefore, control must be carried out from the beginning, namely by selecting superior seeds that are resistant to virus attacks. In addition, of course, eradicating vector pests, such as lice. Fig. 2 shows several examples of chili plant diseases based on leaves called white fly.

Fig. 1. The example of yellowish disease.

Fig. 2. The example of white fly disease.

c) Leaf spot. Symptoms of chili plants affected by leaf spots are the appearance of round brown spots on the leaves. These spots are usually about 1 inch in size with a pale to white center with darker colored edges. Caused by the fungus Cercospora capsici, this disease can be carried by wind, rainwater, vector pests, and agricultural tools. Among the supporting factors for leaf spots are environmental conditions that are always rainy. To prevent it, you can choose healthy seeds that are free of pathogens. In addition, improving drainage and choosing the right planting time also need to be done to minimize the possibility of attacks. Fig. 3 shows several examples of chili plant diseases based on leaves called leaf spot.

Fig. 3. The example of leaf spot.

d) Curl leaf. Finally, leaf curl or mosaic is a disease caused by Cucumber Mosaic Virus (CMV). Insects can transmit diseases from one tree to another. If the chili plant is attacked by leaf curl, its growth becomes stunted and the size of the leaves is smaller. The possibility of spreading disease can be reduced,the destruction of chili plants that have been attacked needs to be done. Fig. 4 shows several examples of chili plant diseases based on leaves called curl leaf.

Fig. 4. The example of curl leaf disease.

B. Research Method

Fig. 5 shows a detailed overview of the detection and classification of chili plant diseases based on leaves proposed using deep transfer learning techniques with the first stage of collecting chili plant disease images based on leaves, the second is image pre-processing and image augmentation, the third part is the process of forming a mode where this stage includes the training, validation and testing processes, while the fourth process is the results and evaluation process. In the third process, the transfer learning models used are VGG16 and MobileNetV2.

C. Convolutional Neural Network

The convolutional neural network architecture model has four main components, namely: convolution layer, pooling layer, activation function and fully-connected layer. One of the known activation functions is the non-linear activation function Rectified Linear Unit (ReLU). The CNN Architecture model is shown in Fig. 6. The convolutional neural network architecture model consists of an input image measuring 28x28x1. When using a color image, the input image size is 28x28x3. RGB color images have three channels, namely Red (R), Green (G) and Blue (B). Furthermore, the input image is fed into the convolution layer using a valid padding kernel measuring 5x5. This process produces n1 channels with an image size of 24x24x1. The next process is max pooling 2x2 which produces an image measuring 12x12x1. Stride 2 is used to reduce the convolution layer in the next layer. This process is then repeated by running the convolution process and then max pooling again. After the max pooling process is complete. Furthermore, the process is carried out through a Fully-Connected Neural Network using the ReLU activation function. The result of this process is the classification of objects into several previously determined classes. In this study, the Softmax activation function was used in the last layer because the object of chili plant disease based on leaves has more than two classes.

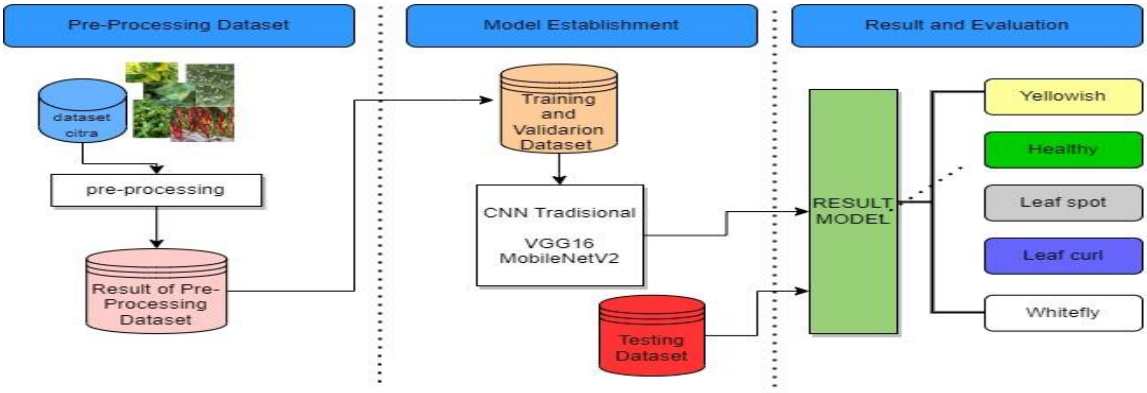


Fig. 5. Methodology of the detection and classification of chili plant diseases based on leaves.

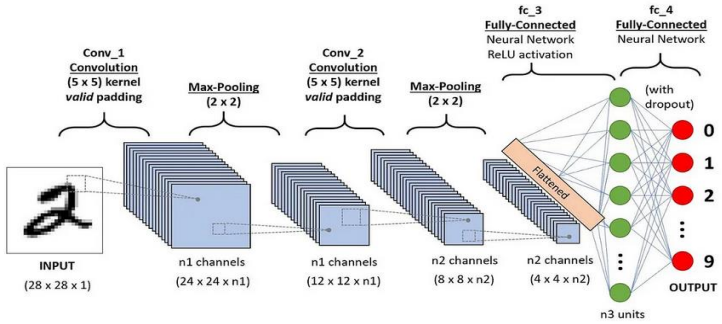


Fig. 6. The architecture of the CNN model.

D. VGG16 Model

The VGG model developed by A. Zisserman and K. Simonyan from the University of Oxford (2014) [19] is a CNN architecture with about 138 million parameters. The feature of this architecture is that it always has the same convolutional layers using 3x3 filters with a stride of 1 and the same padding and max pooling layers using 2x2 filters with a stride of 2. The VGG16 architecture follows this arrangement of convolutional and pooling layers consistently across the architecture. Finally, there are 3 FC layers, the first with ReLU and the last with SoftMax activation function. This architecture contains 16 layers, and the input layer takes an image of 224x224 pixels in size. VGG-16 A convolutional neural network model called the VGG model, or VGGNet, which supports 16 layers, is also known as VGG16. This model significantly outperforms Alexnet by replacing some 3x3 kernel-sized filters with large kernel-sized filters. VGGNet-16 has 16 layers and can classify photos into 1000 different object categories. This model also accepts images with a 224 x 224 x 7 resolution. The VGG16 Architecture model is shown in Fig. 7.

E. MobileNetV2 Model

The MobileNetV2 CNN model was introduced by Sandler et al. (2019). This model is based on the MobileNetV1 architecture by Howard et al. (2017). MobileNetV2 is a lightweight CNN model with 53 deeper layers, fewer parameters, and an input size of 224 × 224. The MobileNetV1 architecture uses the concept of depth wise separable convolutions that apply one filter to each input channel, and pointwise convolutions (1 × 11 × 1) aim to combine the outputs of depth wise convolutions. The MobileNetV2 model is a CNN architecture that attempts to perform well on mobile devices. This architecture is based on an inverse residual structure where residual connections are between the bottleneck layers. The intermediate expansion layer applies lightweight depthwise convolutions to filter features, introducing non-linearity. Overall, the MobileNetV2 architecture contains an initial complete convolution layer with 32 filters, followed by 19 residual bottleneck layers. The MobileNetV2 Architecture model is shown in Fig. 8.

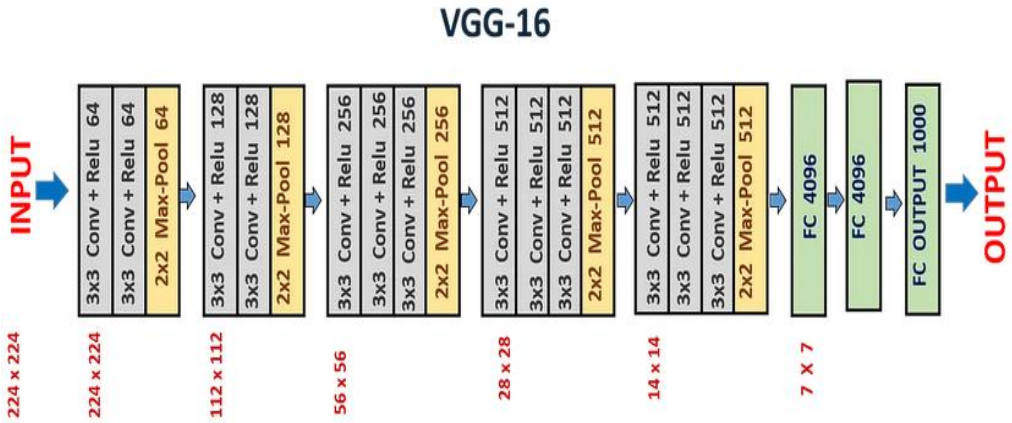


Fig. 7. The architecture of the VGG16 model.

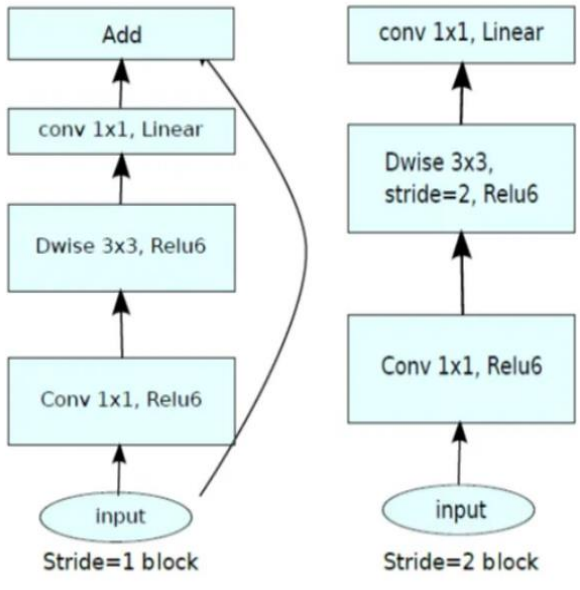


Fig. 8. The architecture of the MobileNetV2 model.

III. Result and Discussion

The model described in Section II was trained and tested using the parameters as shown in Table I. Training and testing were implemented using Python on Google Collab. The batch size of the training model was taken as eight, and a stochastic gradient optimizer was used. Image preprocessing algorithms, data augmentation, and deep learning algorithms were implemented using Python 3.7. The complete software and hardware specification for training on various images of chili plant leaves is Confusion Matrix. Considering the values in the confusion matrix obtained in the classification, the given metrics are calculated using indices such as True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). Here, TP is the number of disease images correctly classified in each category, while TN, on the other hand, represents the number of images correctly classified in all other categories except for the relevant category. FN gives the number of images incorrectly classified from the relevant category. FP gives the number of images incorrectly classified in all other categories except for the relevant category. In Eq. (1), (2), (3), and (4), each states precision, recall, accuracy, and F1-Score [20].

$$\text{precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (1)$$

$$recall = \frac{TP}{TP+FN} \quad (2)$$

$$Accuracy = \frac{\text{TP+TN}}{\text{TP+FP+TN+FN}} \quad (3)$$

$$F1\ Score = 2 * \left(\frac{Precision * Recall}{Precision + Recall}\right) \quad (4)$$

The performance of the pre-trained networks VGG16 and MobileNetV2, tested, is tested by transfer learning in this section. The features learned by VGG16 and MobileNetV2 are then transferred to the new task of chili plant disease recognition based on leaves. The training parameters used for VGG16 and MobileNetV2 are the same as mentioned before. The results of both transfer learning models are compared with the traditional CNN model. Fig. 9 to Fig. 11 show the accuracy and loss graphs of the models used in this study. Fig. 12 show result of confusion matrix in this research. Table I show the performance of Traditional CNN, MobileNetV2, and VGG16 with transfer learning. The results presented in Table I show that the VGG16 Model achieves better performance than MobileNetV2 and Traditional CNN. The accuracies of Traditional CNN, MobileNetV2, and VGG16 Model are 88.0%, 91.00%, and 94%, respectively. As expected, the VGG16 Model with transfer learning outperforms Traditional CNN and MobileNetV2 trained from scratch, which may be due to the reason that it has been trained on more than one million images. Therefore, the feature presentation is much richer than CNN trained from scratch.

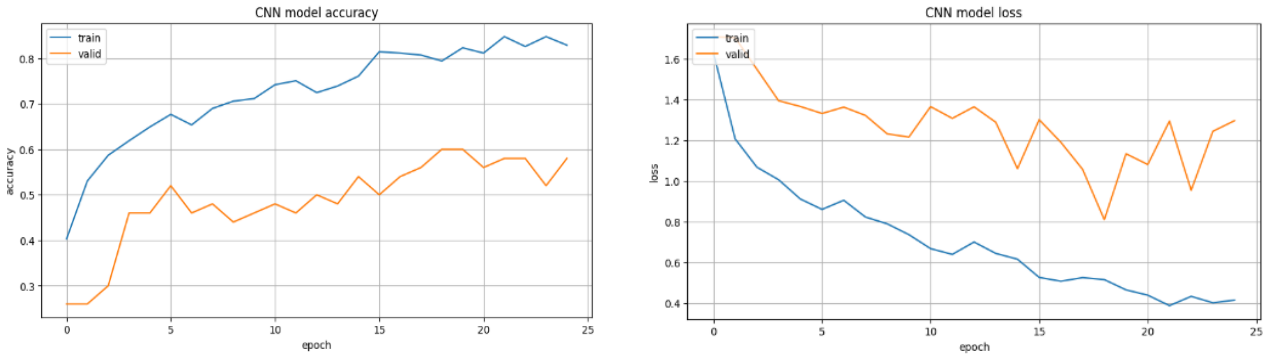


Fig. 9. The accuracy and loss CNN model.

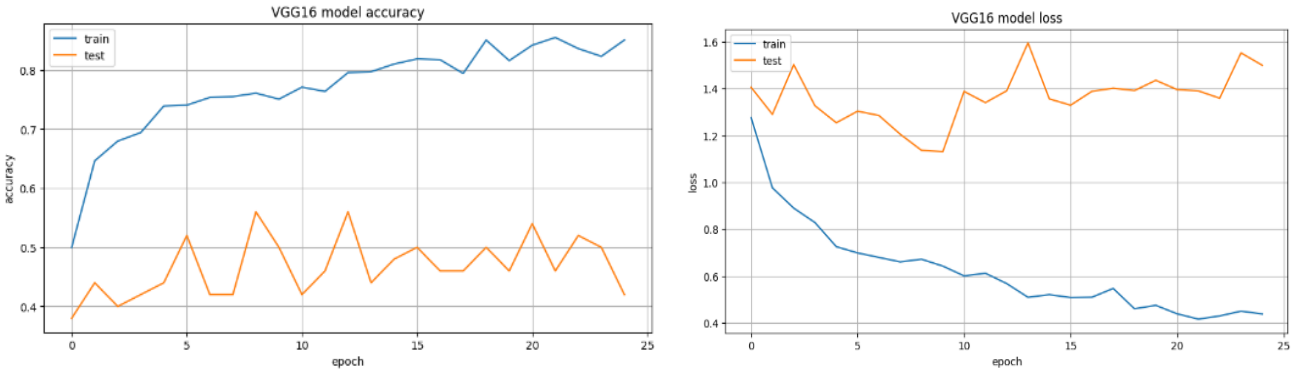


Fig. 10. The accuracy and loss VGG16 model.

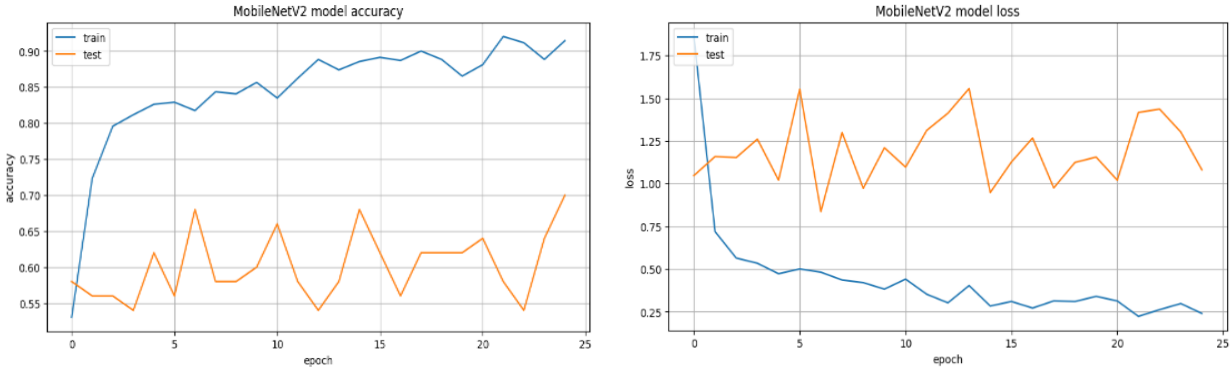


Fig. 11. The accuracy and loss MobileNetV2 model.

TABLE I. CONFUSION MATRIX OF CNN TRADITIONAL, MOBILENETV2 AND VGG16 MODEL

Chili Diseases	Precision	Recall	F1-Score	Precision	Recall	F1-Score	Precision	Recall	F1-Score
	CNN Model			VGG16 Model			MobileNetV2 Model		
Healthy	0.86	0.60	0.71	0.75	0.90	0.81	0.86	0.60	0.71
Leaf curl	0.50	0.40	0.44	0.67	0.60	0.63	0.50	0.40	0.44
Leaf spot	0.33	0.60	0.43	0.82	0.90	0.43	0.33	0.60	0.43
Whitefly	0.78	0.70	0.74	0.88	0.70	0.78	0.78	0.70	0.74
Yellowish	0.97	0.96	0.97	0.98	0.98	0.98	0.97	0.96	0.97
Accuration			**0.88**			**0.94**			0.91

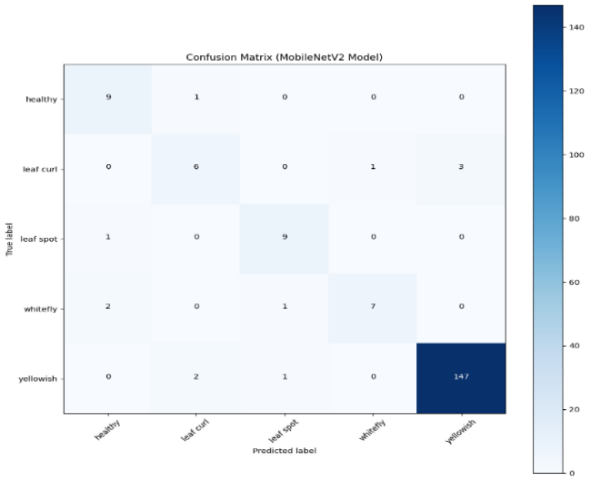


Fig. 12. The confusion matrix of MobileNetV2 Model.

Table I shows the data results on the chili leaf image dataset test. From the CNN architecture model confusion matrix, the accuracy value is 0.88 or 88% while the precision is 0.6860, ecall is 0.6520, F1-Score is 0.6580. In this study, three CNN architectures were used, namely: Traditional CNN Model, MobileNetV2 and VGG16. From the experimental results, it can be seen that the highest classification accuracy was obtained when using the VGG16 architecture model, which was 94%. These results indicate that when using the VGG16 architecture, there was a 6% increase in accuracy when compared to when using traditional CNN. An increase of 6% compared to when using traditional CNN is a positive trend. Classification accuracy is possible to be improved when using the transfer learning model. One way that can be used is through the appropriate hyperparameter setting. Through this hyperparameter setting, the CNN architecture used will be optimal. It is hoped that in the next study, hyperparameter optimization techniques can be used. One that can be used is to optimize using Particle Swarm Optimization and its Modifications, Genetic Algorithms and other optimization algorithms.

IV. CONCLUSION

This study identifies four significant diseases in chili plants based on leaves: leaf spot, yellowish, white fly, and curl leaf. The images used in this study were taken from the image dataset on Kaggle and also taken independently at the location of the chili plant, including healthy leaves labeled as healthy, so this study was divided into five classes. The chili leaf dataset is balanced, meaning that all classes have the same number of samples, namely 50 images per class and a total of 250 images with a size of 224 x 224 × 3. The experimental results show that the model with the best performance is the VGG16 model. This model achieves a validation accuracy of 94% on public and own data sets. The next best-performing model is MobileNetV2, which achieves an accuracy of 90%, followed by the Traditional CNN Model, which achieves a validation accuracy of 88%. In future developments, we intend to deploy it on mobile devices to automatically monitor and identify various types of chili plant disease information based on leaves. This study has limitations in terms of the dataset collected. Further research is expected to use a complete dataset so that training accuracy can be further improved.

ACKNOWLEDGMENT

The author expresses his deepest gratitude to Ristekdikti Kemdikbud Indonesia who has provided research funds in 2024 so that this research can be carried out through the Fundamental Research Research (PRF) scheme.

REFERENCES

[1] J. Ma, K. Du, F. Zheng, L. Zhang, Z. Gong, and Z. Sun, “Original papers A recognition method for cucumber diseases using leaf symptom images based on deep convolutional neural network,” Comput. Electron. Agric., vol. 154, no. June, pp. 18–24, 2018.

[2] Ü. Atila, M. Uçar, K. Akyol, and E. Uçar, “Jo ur na l P re of,” Ecol. Inform., p. 101182, 2020.

[3] A. Abbas, S. Jain, M. Gour, and S. Vankudothu, “Tomato plant disease detection using transfer learning with C-GAN synthetic images,” Comput. Electron. Agric., vol. 187, no. April, p. 106279, 2021, doi: 10.1016/j.c

[4] M. Karuna, B. S. Varsha, S. R. M, G. K. Meghana, and B. Student, “Early Detection of Chili Plant Leaf Diseases using Machine Learning,” Int. J. Eng. Sci. Comput., vol. 9, no. 5, pp. 22328–22335, 2019, [Online]. Available: http://ijesc.org/

[5] K. R. Aravind and P. Maheswari, “Crop disease classification using deep learning approach : an overview and a case study,” 2020, doi: 10.1016/B978-0-12-819764-6.00010-7.

[6] Y. Tarabalka, M. Fauvel, J. Chanussot, and J. A. Benediktsson, “SVM- and MRF-based method for accurate classification of hyperspectral images,” IEEE Geosci. Remote Sens. Lett., vol. 7, no. 4, pp. 736–740, 2010, doi: 10.1109/LGRS.2010.2047711.

[7] N. M. T. Nguyen and N. S. Liou, “Ripeness Evaluation of Achacha Fruit Using Hyperspectral Image Data,” Agric., vol. 12, no. 12, 2022, doi: 10.3390/agriculture12122145.

[8] K. Rajesh Babu, L. S. P. Sairam Nadipalli, C. Sai Tejaswini, G. Bharath Kumar, and P. Vasantha, “CNN Fusion Based Brain Tumor Detection from MRI images using Active Contour Segmentation Techniques,” J. Phys. Conf. Ser., vol. 1804, no. 1, 2021, doi: 10.1088/1742-6596/1804/1/012176.

[9] M. Kayed, A. Anter, and H. Mohamed, "Classification of Garments from Fashion MNIST Dataset Using CNN LeNet-5 Architecture," Proc. 2020 Int. Conf. Innov. Trends Commun. Comput. Eng. ITCE 2020, no. June, pp. 238–243, 2020, doi: 10.1109/ITCE48509.2020.9047776.

[10] H. A. Saputri and D. D. Santika, "Flood Prediction Based on Weather and Water Level Historical Data Using Recurrent Neural Networks : A Case Study of Jakarta Flood Incidents," vol. 10, no. 4, pp. 195–200, 2022.

[11] A. D. M. Africa, "Ripe Fruit Detection and Classification using Machine Learning," Int. J. Emerg. Trends Eng. Res., vol. 8, no. 5, pp. 1845–1849, 2020, doi: 10.30534/ijeter/2020/60852020.

[12] B. Benmouna, G. García-Mateos, S. Sabzi, R. Fernandez-Beltran, D. Parras-Burgos, and J. M. Molina-Martínez, "Convolutional Neural Networks for Estimating the Ripening State of Fuji Apples Using Visible and Near-Infrared Spectroscopy," Food Bioprocess Technol., vol. 15, no. 10, pp. 2226–2236, 2022, doi: 10.1007/s11947-022-02880-7.

[13] N. Nurkhasanah and M. Murinto, "Klasifikasi Penyakit Kulit Wajah Menggunakan Metode Convolutional Neural Network," Sainteks, vol. 18, no. 2, p. 183, 2022, doi: 10.30595/sainteks.v18i2.13188.

[14] S. Mo, "話題の Deep Learning とは ？ 山下 隆義 Deep Learning について," Nature, vol. 26, no. January, pp. 1102–1109, 2020.

[15] D. Han, Q. Liu, and W. Fan, "A new image classification method using CNN transfer learning and web data augmentation," Expert Syst. Appl., vol. 95, pp. 43–56, 2018, doi: 10.1016/j.eswa.2017.11.028.

[16] D. Zhang, F. Ren, Y. Li, L. Na, and Y. Ma, "Pneumonia detection from chest x-ray images based on convolutional neural network," Electron., vol. 10, no. 13, 2021, doi: 10.3390/electronics10131512.

[17] J. Praveen Gujjar, H. R. Prasanna Kumar, and N. N. Chiplunkar, "Image classification and prediction using transfer learning in colab notebook," Glob. Transitions Proc., vol. 2, no. 2, pp. 382–385, 2021, doi: 10.1016/j.gltp.2021.08.068.

[18] Z. Su et al., "Application of Hyperspectral Imaging for Maturity and Soluble Solids Content Determination of Strawberry With Deep Learning Approaches," Front. Plant Sci., vol. 12, no. September, pp. 1–13, 2021, doi: 10.3389/fpls.2021.736334.

[19] I. M. Wismadi, D. C. Khrisne, and I. M. A. Suyadnya, "Detecting the Ripeness of Harvest-Ready Dragon Fruit using Smaller VGGNet-Like Network," J. Electr. Electron. Informatics, vol. 3, no. 2, p. 35, 2020, doi: 10.24843/jeei.2019.v03.i02.p01.

[20] "Confusion Matrix," SpringerReference. 2012. doi: 10.1007/springerreference_178869.

The Application of K-MEANS Algorithm-Based Data Mining in Optimizing Marketing Strategies of Tobacco Companies

Mingqian Ma
School of Economics and Management, Jiangsu Vocational College of Finance Economics, Huaian, 223003, China

***Abstract*—With the continuous development of data mining technology, more and more industries are applying data mining techniques to optimize their marketing strategies. In response to the persistent decline in tobacco sales and the gradual erosion of customer base in a particular enterprise in recent years, this study employs data mining technology to enhance the current tobacco marketing strategy. Firstly, in response to the current shortcomings of the company, a marketing optimization design scheme was proposed and a customer classification evaluation index system was constructed. Subsequently, homomorphic encryption technology and enhanced peak density thinking were employed to enhance the conventional K-means algorithm. The enhanced algorithm was then utilized in the customer clustering and partitioning scheme, with the objective of investigating the underlying information present in customer consumption data. The performance of the algorithm was tested, and the results showed that the mean square error of the improved K-means algorithm was about 0.1, with an average absolute error of about 0.05. The highest detection rate in the validation set was 0.95, and the lowest false alarm rate was 0.07. Both experts and customers were highly satisfied with the marketing strategy under the enhanced K-means algorithm. In summary, the clustering analysis method used in this study can effectively uncover the hidden value behind various types of customer data, thereby helping companies to make better marketing strategies.**

***Keywords*—Data mining; homomorphic encryption; k-means; tobacco; marketing strategy; indicator system**

I. Introduction

In today's fiercely competitive market environment, tobacco companies are facing unprecedented challenges and opportunities. In light of evolving consumer preferences and heightened awareness of health concerns, traditional marketing strategies are proving inadequate in meeting market demand. In particular, tobacco companies must contend with not only stringent regulatory constraints but also the necessity of devising bespoke marketing strategies for disparate consumer segments. As a result, accurate customer segmentation and efficient marketing strategies are key to improving sales performance. Currently, many tobacco companies have recognized the importance of data mining (DM) and customer segmentation [1]. By analyzing customer buying patterns and preferences, companies can better understand market demand and develop more accurate marketing plans. However, traditional customer classification methods are often limited by privacy concerns, especially when sensitive information is involved. It has become an urgent problem to solve how to effectively analyze while protecting customer privacy. In addition, although clustering analysis and other techniques have been applied in customer segmentation, existing algorithms still have certain limitations in handling high-dimensional data and ensuring result stability. With the continuous development of DM technology, DM technology using K-means algorithm (KMA) has been extensively applied to the optimization of tobacco companies' marketing strategies [2-3]. In the optimization of marketing strategies for tobacco companies, KMA can help tobacco companies to analyze data such as consumers' consumption habits, taste preferences, and purchasing behavior to develop more scientific and reasonable marketing strategies [4]. In response to this background, this study will use KMA to cluster customer data and identify relevant factors that affect tobacco sales quotas for optimization.

II. Related Work

The KMA is a clustering algorithm in view of distance calculation, which can classify data points with similar features into different clustering centers, thus achieving data analysis and mining. Currently, many scholars have conducted a series of studies on this algorithm [5-6]. Huang B et al. combined the KMA in clustering analysis with moving windows to propose a more effective method for static friction testing. The research results indicated that the method improves the detection accuracy by 15.3% compared to existing static friction detection methods. Applying this technology to practical industrial production could provide effective estimates of static resistance bands, as well as detect severe valve static resistance and unexpected valve closure situations [7]. In response to the severe faults that solar energy may face during use, Et Taleby et al. designed a solar panel detection system using wireless communication technology combined with KMA. The system diagnosed the failure of photovoltaic panels by detecting their thermal images. The outcomes indicated that the detection accuracy of the method used in solar energy fault detection was as high as 96.54%, which had good performance and could diagnose faults in a timely manner to effectively avoid accidents such as fires [8]. Zhang et al. proposed a new encrypted K-means clustering analysis algorithm in a collaborative manner to address the issue of KMA being unable to ensure data privacy during data clustering. In this algorithm, Zhang et al. used secure multi-party computation and differential privacy technology to train the K-means clustering model, aiming to protect data privacy and ensure that data can be output normally for analysis. The outcomes indicated that the adopted method possessed excellent clustering performance,

not only ensuring that data was not leaked during processing, but also updating the cluster center faster to ensure better clustering results [9]. In response to the issue of unequal resource allocation in the current multi-level sales operation network, Sin et al. rebuilt a resource allocation model and achieved the goal of multi-level task automatic allocation through this model. The experiment showed that the sales resource allocation model constructed could automatically allocate personnel and various resources, thereby achieving maximum resource utilization [10]. Currently the construction industry is facing problems such as waste management. It has been the concern of many scholars to find out how to effectively manage waste while maximizing economic benefits. Queheille E et al. proposed a multi-objective optimization algorithm and used the algorithm in waste management in the construction industry, aiming to design a suitable solution through the algorithm, which can maximize the use of human and material resources. The results of the study showed that the multi-objective optimization algorithm used was able to effectively calculate the number of workers required, the type of waste disposal and the optimal management plan, which had a certain value of utilization [11]. In light of the evolving landscape of social media and consumer behavior, the development of effective marketing strategies has emerged as a pivotal concern for major merchants. Gao M et al. used methods such as literature analysis and survey analysis to investigate the sales effect under different operating modes. In addition, multi-objective optimization and backward induction were used to optimize the current product pricing strategy. Finally, the results of the effects of different sales strategies under different network structures were verified through numerical simulation experiments. The experimental results showed that enterprises formulate appropriate marketing strategies could greatly promote the sales of commodities, so as to achieve the purpose of maximizing profitability [12].

In summary, current research on KMA has spread across various fields. In the past, scholars often used KMA to solve problems such as fault diagnosis, data analysis, and resource allocation. At present, no scholars have applied KMA to optimize the marketing strategies of tobacco companies. In response to the current situation of poor tobacco sales performance and frequent customer feedback problems in a certain tobacco company, this study applies KMA to optimize the marketing strategy of the tobacco company. This is aimed at further mining customer information through the KMA to optimize the company's current marketing situation.

III. Research on Marketing Strategies of Tobacco Companies Based on Homomorphic Encryption KMA

For optimizing the current marketing strategy of a tobacco company and improve its sales performance, this study takes a listed tobacco company as an example, first analyzes its current sales problems, proposes a series of improvement measures, and constructs a customer classification evaluation index system. Then it uses the improved peak density KMA under homomorphic encryption technology to evaluate the customer classification evaluation index system, and designs the final customer clustering division scheme. This is to further analyze customer consumption data to optimize marketing strategies.

A. Optimization Design of Marketing Strategy for Tobacco Companies

Homomorphic encryption is an encryption technique that allows the computation of ciphertext without decrypting the data, and ensures that the computed results are consistent with the original plaintext after decryption. Peak density is a concept commonly used to analyze signal or data set features. It describes the density of peak values in a signal or data set and is typically used to measure the distribution of a feature in the data. Tobacco marketing refers to the use of marketing strategies by tobacco companies to increase product sales and market share. In the tobacco company's marketing strategy, its composition includes the research on the target market, customer needs and competitors, as well as the development of personalized Marketing plan [13]. The goal of tobacco marketing is to increase brand awareness, customer satisfaction, and sales revenue to meet customer needs. This study takes a listed tobacco company as an example. In response to its current poor tobacco sales strategy and low sales revenue, a series of improvement and optimization measures are first proposed. Then, clustering analysis algorithm is used to mine data on its tobacco consumer types, to further improve the current tobacco strategy and increase the company's tobacco sales in view of different customer consumption situations. Fig. 1 shows the marketing strategy optimization path of a tobacco company.

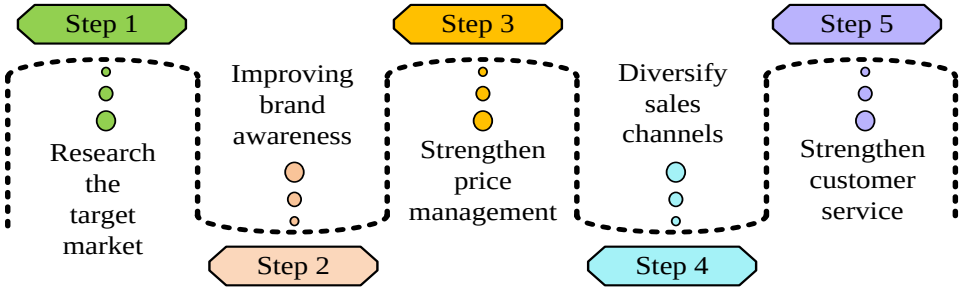


Fig. 1. Optimization path of Tobacco Company's marketing strategy.

Fig. 1 shows the optimization path of the tobacco company's marketing strategy. The entire optimization path consists of five parts, namely, researching the target market, improving brand awareness, strengthening price management, diversifying distribution channels, and strengthening customer service. The purpose of studying the target market is to determine consumer needs so that the company's overall tobacco marketing goals are in line with consumer needs. Improving brand awareness means creating a brand effect. Strengthening price management means that management should formulate reasonable pricing policies to ensure the stability of brand value. With the development of the Internet, traditional offline sales are no longer the only way for people to consume. Diversified sales channels require merchants to combine various online and offline channels for marketing to meet the needs of different consumers. Strengthening customer service requires improving customer satisfaction with their purchases, thereby enhancing their purchasing opinions. Among the above optimization measures, the long-term stable tobacco purchasing behavior of customers is an important guarantee for tobacco sales profitability.

For better understanding customer needs and develop appropriate tobacco sales plans, it is necessary to use DM technology to further mine the current customer information, discover the hidden value behind the data, and effectively improve the current sales model. Customer segmentation theory is a theory that categorizes customers according to certain criteria, to better understand their characteristics, needs, and preferences, and distinguish different categories of customers. Customer segmentation theory can help companies better understand customer needs and behaviors, thereby developing more personalized and effective marketing strategies and improving customer satisfaction and loyalty. In customer segmentation theory, key indicators such as customer purchase frequency, purchase amount, preference level, etc. are usually used to evaluate customer demand for a company's products and services. This study first utilized customer segmentation theory to construct a customer classification index system. Next, it uses the indicator system as an evaluation standard and uses clustering analysis algorithms to study the relationship between various types of customer behavior characteristics and their underlying purchasing behavior. Table I shows the customer classification evaluation index system.

Table I shows the customer classification evaluation index system. Table I shows that the entire customer classification evaluation index system consists of three primary indicators and 13 secondary indicators. According to the customer segmentation theory, customers are classified into three primary indicators: customer value, customer characteristics, and customer behavior. Customer value is further divided into three secondary indicators: total sales quota, total business quota, and average sales price. Customer characteristics are subdivided into five secondary indicators: business location, business market, business form, business nature, and business scale. Customer behavior is divided into five secondary indicators in view of customers' preferences for purchasing tobacco: first class tobacco proportion, second class tobacco proportion, third class tobacco proportion, fourth class tobacco proportion, and fifth class tobacco proportion. The proportion of cigarettes in one category refers to the proportion of customers who purchase tobacco for a single amount between 80 and 100 yuan. The proportion of second-class cigarettes refers to the proportion of customers who buy tobacco for a single amount of 60-80 yuan. The proportion of three kinds of cigarettes refers to the proportion of customers who buy tobacco for a single amount of 40-60 yuan. The proportion of four kinds of cigarettes refers to the proportion of customers who buy tobacco for a single amount of 20-40 yuan. The proportion of five kinds of cigarettes refers to the proportion of customers who buy tobacco for a single amount of less than 20 yuan.

TABLE I. CUSTOMER CLASSIFICATION EVALUATION INDEX SYSTEM

Evaluation Indicator System	First-level indicators	Second-level indicators	Code
Customer classification evaluation index system	Customer Value	Total sales limit	Y1
		Total business limit	Y2
		Average sales price	Y3
	Customer Characteristics	Business location	Y4
		Operating the market	Y5
		Business form	Y6
		Business nature	Y7
		Business scale	Y8
	Customer Behavior	Buy Class I cigarettes	Y9
		Buy Class II cigarettes	Y10
		Buy Class III cigarettes	Y11
		Buy Class IV cigarettes	Y12
		Buy Class V cigarettes	Y13

B. Construction of Tobacco Consumer Segmentation Model Based on Homomorphic Encryption KMA

Homomorphic encryption technology is a cryptographic technology, which enables encrypted objects to be calculated without revealing any useful information [14-15]. In addition, homomorphic encryption can convert encrypted data into the same form as ordinary data, and then perform calculations, so that users can get the expected calculation results even if they do not know the contents of encrypted data. This research applies the homomorphic encryption technology to the KMA, aiming to ensure that the algorithm can obtain information encryption in the running process, so as to prevent data information leakage. The homomorphic encryption process is shown in Fig. 2.

Fig. 2 shows the homomorphic encryption process. Firstly, it is necessary to generate a key suitable for encryption. Keys can be generated using non-public algorithms, such as secret sharing or common algorithms used to solve mathematical Hard problem of consciousness. Next, it uses the key to encrypt the data. This step can be done using a technology called homomorphic encryption, which converts encrypted data into the same form as ordinary data and then encrypts it. In the case of homomorphic encryption, anyone can compute the encrypted data without knowing the key. The ciphertext operation can be achieved by using machine learning algorithms.. Finally, the user needs to receive the decrypted plaintext and provide feedback on the encryption result to determine whether the desired result has been obtained. The encryption process of ciphertext is shown in Eq. (1) to Eq. (3) [16].

$$C = \left(c_1, c_2, \cdots c_n\right) \tag{1}$$

In Eq. (1), C represents the ciphertext data set. c_1, c_2 and c_n represent the ciphertext in the ciphertext dataset, respectively [17-18].

$$M = \left(m_1, m_2, \cdots m_n\right) \tag{2}$$

In Eq. (2), M represents the set of plaintext data. m_1, m_2 and m_n represent the plaintext in the plaintext dataset, respectively. The plaintext encryption process obtained by combining Eq. (1) and Eq. (2) is shown in Eq. (3).

$$\begin{cases} c_1 = Enc\left(m_1\right) \\ c_2 = Enc\left(m_2\right) \end{cases} \tag{3}$$

In Eq. (3), $Enc(\cdot)$ represents the encryption algorithm. Clear text m_1 and m_2 can obtain corresponding ciphertext through encryption algorithms, denoted as c_1 and c_2.

$$c_1 \odot c_2 = Enc(m_1) \odot Enc(m_2) = Enc(m_1 \odot m_2) \tag{4}$$

In Eq. (4), $\odot$represents an effective algorithm. If Eq. (4) satisfies the pre - and post equality relationship under the operation of an effective algorithm, then $Enc(\cdot)$ is said to have homomorphism.

$$Enc\left(m_1\right) \oplus Enc\left(m_2\right) = Enc\left(m_1 + m_2\right) \tag{5}$$

Eq. (5) is the calculation formula of addition homomorphic encryption. $\oplus$ represents an addition operation, and if Eq. (5) is satisfied, it indicates that the encryption algorithm used has additive homomorphism.

$$Enc\left(m_1\right) \otimes Enc\left(m_2\right) = Enc\left(m_1 \otimes m_2\right) \tag{6}$$

Eq. (6) is the calculation formula of multiplicative homomorphic encryption. $\otimes$ represents multiplication operation. Moreover, if Eq. (6) is satisfied, it indicates that the encryption algorithm used has multiplicative homomorphism [19-20].

$$Enc\left(m_1\right) \otimes m_2 = Enc\left(m_1 \times m_2\right) \tag{7}$$

Eq. (7) is the calculation formula of mixed multiplication homomorphic encryption. If equation (7) is satisfied, it indicates that the encryption algorithm used has mixed multiplicative homomorphism.

The KMA is a common clustering algorithm that can assign data objects to the clusters they belong to, so that each object has the same category throughout the entire dataset [21]. The traditional KMA is generally divided into several steps: initializing parameters, clustering, adjusting clustering, and repeating clustering. The clustering process is shown in Fig. 3.

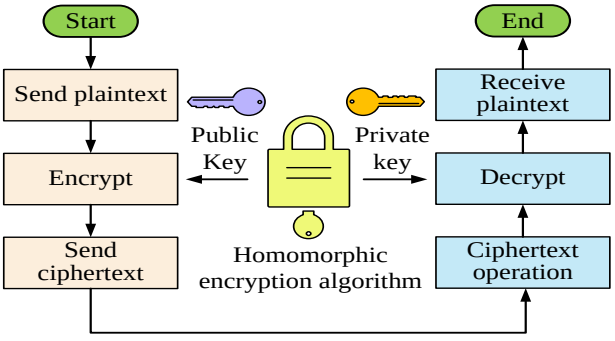


Fig. 2. Homomorphic encryption process.

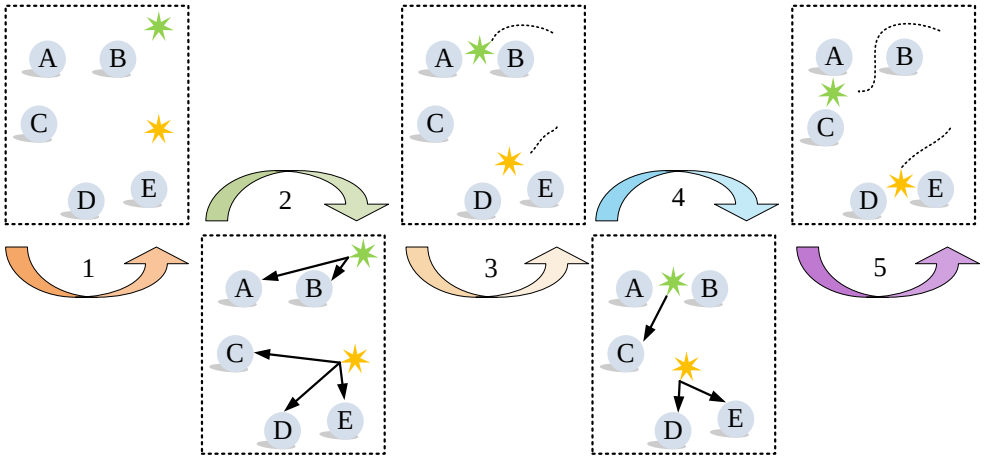


Fig. 3. KMA clustering process.

Fig. 3 shows the clustering process of the KMA. Fig. 3 shows that in the K-means clustering, the initial clustering needs to be selected first. The KMA uses a random selection method to determine the position of each data object in the dataset, and then clusters the data objects and assigns them to the corresponding clusters [22-23]. Over time, the size of the cluster is continuously adjusted to ensure that each object has the same category throughout the entire dataset. It continuously repeats the KMA for generating the best clustering [24-25]. The KMA generally utilizes Euclidean distance for measuring the similarity between two samples, and its mathematical expression is shown in Eq. (8).

$$D(X,Y)=\sqrt{\sum_{t=1}^{m}(x_i-y_i)^2} \tag{8}$$

In Eq. (8), assuming that the dataset has n samples of the m dimension, the distance expression between any two samples X and Y is denoted as $D(X,Y)$. Among them, $i \in 1,2,\mathrm{L},m$.

$$u_i=\frac{1}{|C_i|}\sum_{j=1}^{|C_i|}X_j=\frac{1}{|C_i|}\left(X_1+X_2+\mathrm{L}+X_{|C_i|}\right) \tag{9}$$

Eq. (9) is the iterative calculation formula for the centroid u_i in the KMA. C_i represents the i-th partition cluster. $|C_i|$ represents the quantity of samples contained in the i-th partition cluster.

$$SSE=\sum_{i=1}^{k}\sum_{j=1}^{|C_i|}\left(d\left(X_{i,j},u_i\right)\right)^2 \tag{10}$$

Eq. (10) is the mathematical expression for the standard function SSE of the sum of squared errors. The value of the error squared sum standard function can determine whether the algorithm iteration has ended. When the sum of squares of errors is less than the set error, the algorithm is terminated. k represents dividing the sample into Class k. $X_{i,j}$ represents the j-th sample in the i-th cluster. $d\left(X_{i,j},u_i\right)$ represents the distance from the sample to the center of mass.

$$CPD=\frac{1}{k}\sum_{i=1}^{k}d\left(u_i,u_i'\right) \tag{11}$$

Eq. (11) is the formula for calculating the difference in centroid changes. In addition to using SSE for judgment, this formula can also be used to determine whether the algorithm has ended. u_i' represents the position of the centroid of the previous generation in the i-th cluster. u_i represents the position of the current centroid. $d\left(u_i,u_i'\right)$ represents the Euclidean distance between two centroids. If the difference in centroid changes meets the requirements, the algorithm will be terminated.

Although the K-means clustering analysis algorithm has the characteristics of simple operation, high stability, and good analysis results, it still has certain limitations when used in different scenarios. For example, it has a strong dependence on the k-value of the divided sample category, and the algorithm is greatly affected by the center point. The algorithm has high randomness, making it difficult to converge to the optimal solution state. In response to the above issues, this study attempts to enhance the sample density in the algorithm dataset and uses the principle of maximum density to select the center point. Finally, it proposes a KMA with improved peak density to improve the stability of the traditional KMA and accelerate its Rate of convergence.

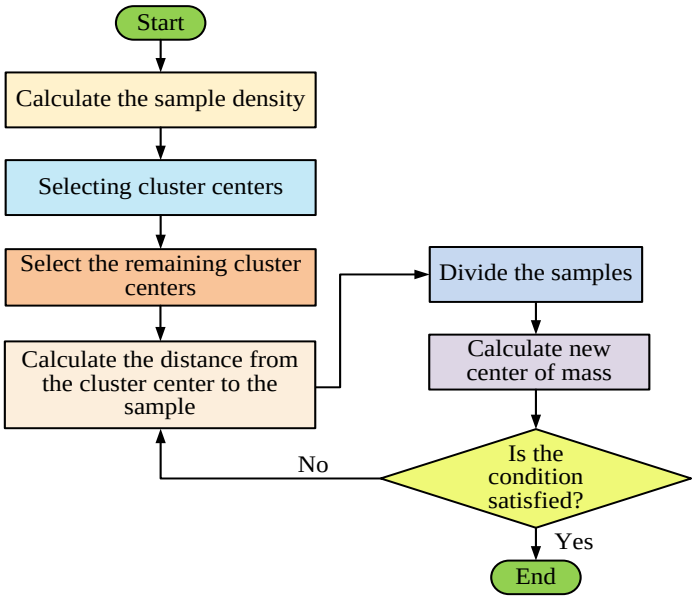


Fig. 4. Flow chart of KMA for improving peak density.

Fig. 4 shows the flowchart of the KMA for improving peak density. The input of the whole algorithm includes the original dataset D, the half price parameter q, the number of clusters k and the error parameter e. The output result is the divided clustering result. Firstly, it sets r and calculates the sample density, recording the sample with the highest density as x_i and the corresponding density value of the sample as $p(x_i)$. It places x_i into set x and removes other sample values within its radius range from the dataset, performing this operation on all samples in the dataset until the initial cluster center set x is obtained. It selects the sample with the highest density as the first clustering center, and then selects the second sample with the farthest distance as the second clustering center, using this method to select the remaining initial centers. Next, it uses the distance formula mentioned above to calculate the distance between the sample and the center, and divides the samples according to the principle of minimum distance. Then it calculates the new centroid for each classification cluster in the partitioned dataset using Eq. (9). Finally, it determines whether the output result is less than the error parameter e in view of the convergence judgment formula. If it is true, the algorithm is terminated. The improved peak density KMA is clustered using homomorphic encryption technology, and the customer segmentation scheme is shown in Fig. 5.

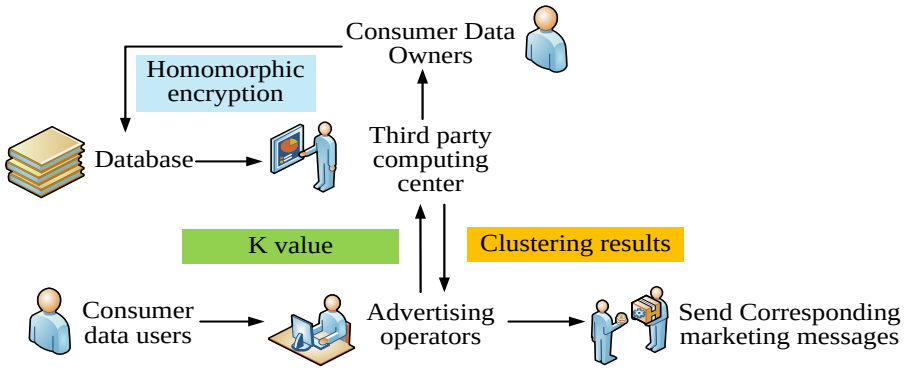


Fig. 5. Design diagram of customer clustering and division scheme.

Fig. 5 shows the design diagram of the customer clustering division scheme. To ensure the maximum utilization of consumption data, it is first necessary for data users to provide consumption data of their stores to advertising operators. However, to ensure the privacy of data information, the system will introduce homomorphic encryption technology to encrypt information during the entire data transmission process. Then it shares the data information with the third-party computing center, so as to use the KMA to analyze the customer consumption data, and then generate the corresponding marketing messages.

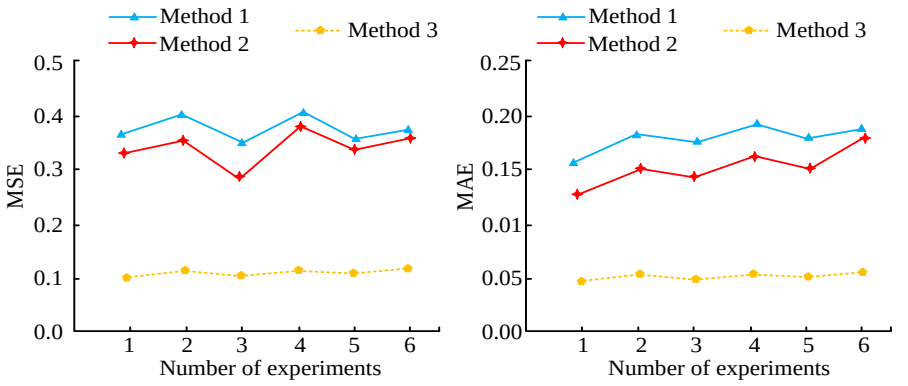
IV. Analysis of Tobacco Company Marketing Strategy Optimization Effect Based on Homomorphic Encryption KMA

For testing the effectiveness of the methods used in the research, the results analysis part first tested the performance of the improved peak density KMA under homomorphic encryption. Moreover, it proves that the improved peak density

KMA performs better than other comparative algorithms in four indicators: detection rate, false alarm rate, accuracy, and clustering running time. Subsequently, this study applied the improved peak density KMA to analyze customer consumption data, validated the customer classification evaluation index system, and obtained the application effect of tobacco company marketing strategy optimization.

A. *Performance Test of Improved Peak Density KMA Under Homomorphic Encryption*

It selected the tobacco sales data of a listed tobacco company in the past three years as the dataset for this experiment. After simple preprocessing of the dataset, the remaining data is divided into a training set and a validation set in a 9:1 ratio to test the performance of different clustering algorithms. The mean squared error (MSE) and mean absolute error (MAE) of the traditional KMA (subsequently recorded as method 1), the Mean shift algorithm (subsequently recorded as method 2), and the improved peak density KMA (subsequently recorded as method 3) in the same tobacco dataset are shown in Fig. 6.

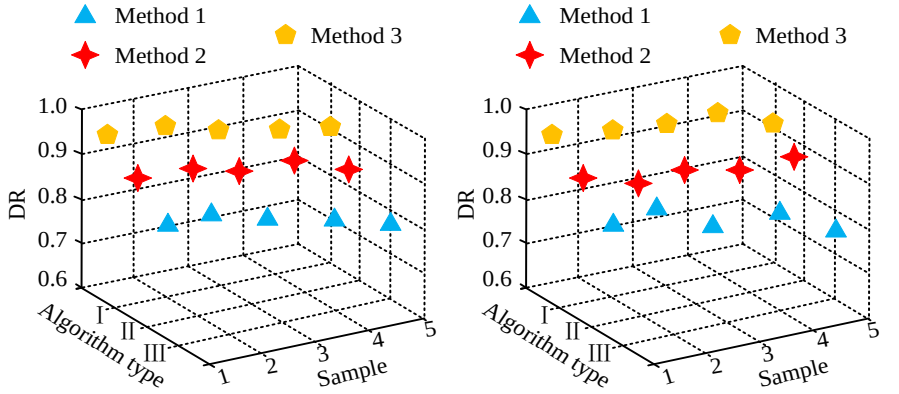


(a) MSE of each algorithm model under different experimental times

(b) MAE of each algorithm model under different experimental times

Fig. 6. MSE and MAE changes of three clustering methods.

Fig. 6 (a) shows the MSE changes of the three methods under different experimental times. As the number of experiments increases, the MSE of Method 1 and Method 2 fluctuates up and down, with a large fluctuation range, while the MSE of Method 3 is stable at around 0.1. Fig. 6 (b) shows the MAE changes of the three methods under different experimental times. The MAE values of Method 1 and Method 2 have significant changes, while the MAE values of Method 3 are stable at around 0.05.

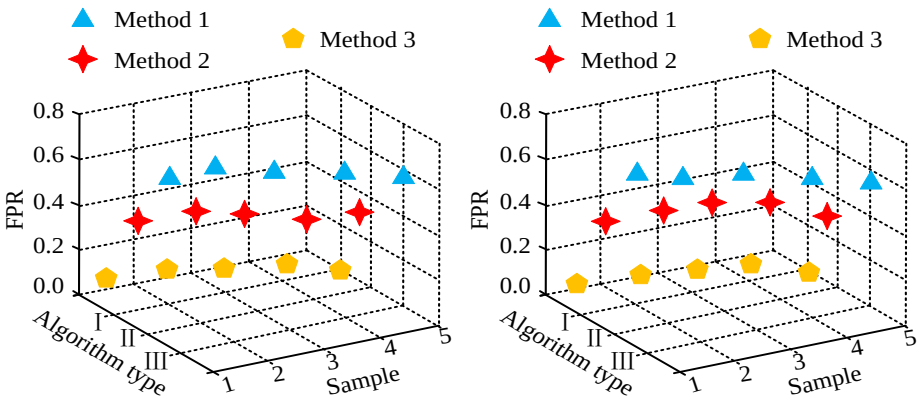


(a) Detection rate of different types of algorithms in training sets

(b) Detection rate of different types of algorithms in the test set

Fig. 7. DR changes of three clustering methods.

Fig. 7 (a) and 7 (b) show the changes in detection rates of the three clustering methods in the training and validation sets, respectively. Fig. 7 (a) shows that the highest detection rates of Method 1, Method 2, and Method 3 in the training set are 0.76, 0.85, and 0.97, respectively. Fig. 7 (b) shows that the highest detection rates of Method 1, Method 2, and Method 3 in the validation set are 0.77, 0.88, and 0.95, respectively. In summary, method three has the best data detection effect.

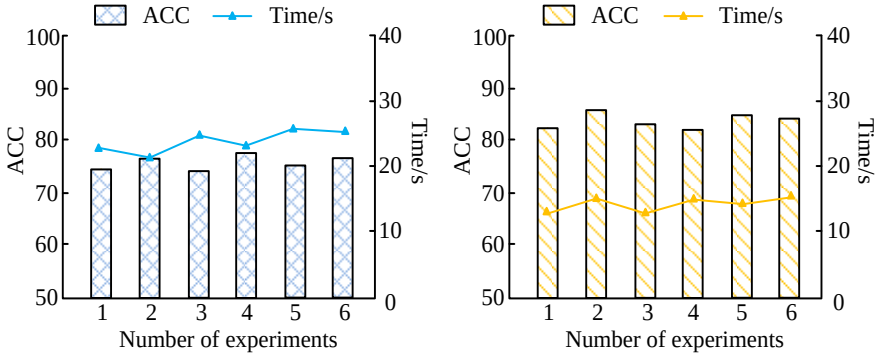


(a) False Positive Rate of different types of algorithms in training sets

(b) False Positive Rate of different types of algorithms in the test set

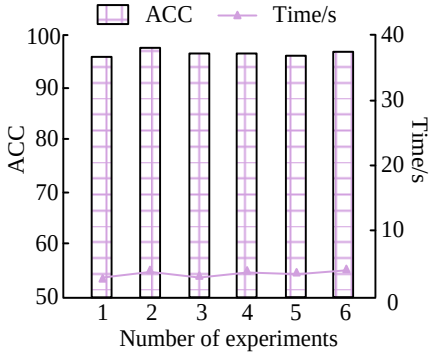
Fig. 8. FPR variation of three clustering methods.

Fig. 8 (a) and Fig. 8 (b) show the changes in false positive rates of the three clustering methods in the training and validation sets, respectively. Fig. 8 (a) shows that the highest false positive rates of Method 1, Method 2, and Method 3 in the training set are 0.56, 0.38, and 0.09, respectively. Fig. 8 (b) shows that the highest false alarm rates for Method 1, Method 2, and Method 3 in the validation set are 0.52, 0.39, and 0.07, respectively. In summary, method three has the best false alarm rate performance.



(a) The clustering accuracy and runtime of the method 1

(b) The clustering accuracy and runtime of the method 2



(c) The clustering accuracy and runtime of the method 3

Fig. 9. ACC and time variation of three clustering methods.

Fig. 9 (a), 9 (b), and 9 (c) respectively show the clustering accuracy and runtime changes of the three clustering methods under multiple experiments. Figure 9 (a) shows that the average clustering accuracy of Method 1 in six experiments is 73.26. As the number of experiments changes, its running time always fluctuates between 20 and 30 seconds, with significant fluctuations. Fig. 9 (b) shows that the average clustering accuracy of Method 2 in six experiments is 84.12. As the number of experiments increases, its running time always fluctuates between 10-20 seconds, with a smaller fluctuation compared to Method 1. Fig. 9 (c) shows that the average clustering accuracy of Method 3 in six experiments is 96.08, and its running time remains around 4 seconds as the number of experiments increases.

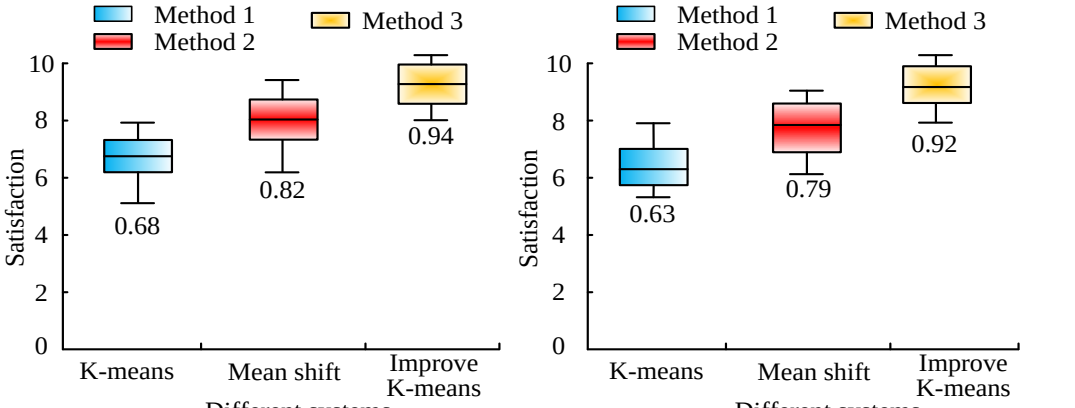
B. Analysis of the Optimization Effect of Tobacco Company's Marketing Strategy

After testing the performance of the improved peak density KMA under homomorphic encryption, the research applied it to the customer classification evaluation index system, input various customer data into the model, and obtained the final output results as shown in Table II. By examining the results of various outputs, it is possible to assist staff in the implementation of corresponding marketing plans, thereby achieving the goal of optimizing marketing plans and increasing sales.

TABLE II. OUTPUT RESULTS OF CUSTOMER CLASSIFICATION EVALUATION INDICATORS

Evaluation indicator system	First-level indicators	Second-level indicators	Code	Output value
Customer classification evaluation index system	Customer value	Total sales limit	Y1	8.7
		Total business limit	Y2	8.8
		Average sales price	Y3	9.3
	Customer Characteristics	Business location	Y4	9.2
		Operating the market	Y5	8.5
		Business form	Y6	8.6
		Business nature	Y7	9.0
		Business scale	Y8	8.3
	Customer behavior	Buy Class I cigarettes	Y9	7.7
		Buy Class II cigarettes	Y10	8.1
		Buy Class III cigarettes	Y11	8.8
		Buy Class IV cigarettes	Y12	8.7
		Buy Class V cigarettes	Y13	7.6

Table II shows the output results of customer classification evaluation indicators. Table II shows that out of the 13 secondary indicators, a total of 3 secondary indicators have output values above 9 points, namely average sales price, business location, and business nature. In addition, 8 secondary indicators have an initial value of more than 8 points. Given the above scoring results, tobacco company executives should optimize the drivers with higher scores to increase the company's tobacco revenues.



（a）User satisfaction with marketing strategies for various systems （b）Expert satisfaction with marketing strategies for various systems

Fig. 10. Satisfaction of users and experts with different marketing schemes.

Fig. 10 shows the satisfaction of users and experts with different marketing plans. Fig. 10 (a) shows the satisfaction of users with marketing solutions under different clustering methods. Fig. 10 (a) shows that users' satisfaction with marketing solutions under the three clustering methods of K-means, Mean shift, and Improve K-means is 0.68, 0.82, and 0.94, respectively. Fig. 10 (b) shows the satisfaction of experts with marketing solutions under different clustering methods. Fig. 10 (b) shows that experts' satisfaction with marketing solutions under the three clustering methods of K-means, Mean shift, and Improve K-means is 0.63, 0.79, and 0.92, respectively.

V. DISCUSSION

The research focused on optimizing the marketing strategies of tobacco companies, and achieved efficient customer classification and privacy protection through the improved peak

density KMA with homomorphic encryption. In practice, the marketing challenges faced by tobacco companies were mainly due to the intensification of market competition and the diversification of consumer demand. Traditional marketing methods were difficult to accurately reach target customers, resulting in persistently low sales. Therefore, using modern DM techniques for customer segmentation could not only help companies identify the characteristics of different customer groups, but also develop more personalized marketing strategies based on these characteristics. The experimental results showed that the improved KMA outperformed the traditional methods in clustering performance. In the experiment, the detection rate of the improved algorithm reached 97%, while the detection rates of the traditional KMA and the mean shift algorithm were 76% and 85%, respectively. This gap indicated the effectiveness of the improved algorithms in handling complex data sets, especially in capturing subtle differences in customer behavior. In addition, the false positive rate of the enhanced algorithm was only 9%, which was significantly lower than the 56% and 38% of the traditional algorithms. This improved accuracy was due to the optimization of the algorithm in the initial cluster center selection, which reduced the problem of inaccurate clustering caused by improper center selection. The introduction of homomorphic encryption technology effectively solved the privacy problem and ensured the security of customer information during the analysis process, which was particularly important for the tobacco industry. Due to increasingly stringent industry regulations, protecting customer privacy become a key factor in the sustainable development of companies. For example, data breaches could result in significant fines and loss of brand reputation. Therefore, the adoption of homomorphic encryption technology to ensure the privacy of customer data during the analysis process was a necessary choice in line with industry trends. In conclusion, the improved peak density KMA based on homomorphic encryption provided an effective solution for optimizing the marketing strategies of tobacco companies. On this basis, future research could further explore other data processing techniques and algorithms to cope with increasingly complex market environments and customer demands.

VI. Conclusion

In response to the problems of a certain tobacco company's current sales quota not being ideal and a large number of users losing, this study used the KMA in cluster analysis to analyze its customer data and optimize its current marketing strategy. The research results indicated that the improved KMA used had good clustering performance, with MSE and MAE values fluctuating around 0.1 and 0.05, respectively, which was much smaller than the traditional KMA and Mean shift algorithm. The maximum detection rate of improved K-means in the validation set was 0.95, the minimum false alarm rate was 0.07, and the average clustering accuracy under six experiments was 96.08. The clustering time was maintained at around four seconds, and its performance was superior to the other two comparative algorithms. In addition, the improved KMA had high output values for average sales price, business location, and business nature. Therefore, targeted optimization was needed for these three secondary indicators. In the end, both experts and users had a satisfaction level of over 0.9 with the optimized marketing plan. In summary, the improved K-means method adopted in this study could better develop appropriate marketing plans in view of consumer data characteristics, thereby obtaining the satisfaction of users and experts, and helping the company achieve maximum profitability. However, due to only analyzing customer impact indicators, there was still some error. Future research directions could explore more influencing factors, not limited to the customer. In addition to customer impact indicators, future research may wish to consider the inclusion of multidimensional variables such as market environment, competitor behavior, and economic factors in order to provide a more comprehensive evaluation of their impact on sales. Furthermore, a hybrid approach combining deep learning techniques with traditional clustering algorithms may be employed to enhance the accuracy and adaptability of the model.

References

[1] Jeong W, Almubarak M S, Tsingas C. Quality control for the geophone reorientation of ocean bottom seismic data using k-means clustering. Geophysical Prospecting, 2021, 69(7):1487-1502.

[2] Fan Y, Liu Y, Qi H, Liu F, Ji X J. Anti-Interference Technology of Surface Acoustic Wave Sensor Based on K-Means Clustering Algorithm. IEEE Sensors Journal, 2021, 21(7):8998-9007.

[3] Pan S, Yan K, Yang H, Jiang C, Qin Z. A sparse spike deconvolution method based on Recurrent Neural Network like improved Iterative Shrinkage Thresholding Algorithm. Geophysical Prospecting for Petroleum, 2022, 58(4):533-540.

[4] Gao S, Gao S, Pan W, Wang M. Design of Improved PID Controller Based on PSO-GA Hybrid Optimization Algorithm in Vehicle Lateral Control. Studies in informatics and control, 2021, 30(4):55-65.

[5] Liu S, Sun L, Zhu S, Li J, Chen X, Zhong W. Operation strategy optimization of desulfurization system based on data mining. Applied Mathematical Modelling, 2020, 81(5):144-158.

[6] Niu X, Wang J. A combined model based on data preprocessing strategy and multi-objective optimization algorithm for short-term wind speed forecasting. Applied Energy, 2019, 241(5):519-539.

[7] Huang B, Zheng D, Sun X, Amalraj J, Shah A, Damarla S K. Valve Stiction Detection and Quantification Using a K-Means Clustering Based Moving Window Approach. Industrial & Engineering Chemistry Research, 2021, 60(6):2563-2577.

[8] Et-Taleby A, Chaibi Y, Boussetta M, Allouhi A, Benslimane M. A novel fault detection technique for PV systems based on the K-means algorithm, coded wireless Orthogonal Frequency Division Multiplexing and thermal image processing techniques. Solar Energy, 2022, 237(5):365-376.

[9] Zhang E, Li H, Huang Y, Hong S, Zhao L, Ji C. Practical Multi-party Private Collaborative k-means Clustering. Neurocomputing, 2022, 467(1):256-265.

[10] Sin H H, Parlar M. Modeling and optimization of multilevel marketing operations. Naval Research Logistics (NRL), 2022, 69(4):581-598.

[11] Queheille E, Taillandier F, Saiyouri N. Optimization of strategy planning for building deconstruction. Automation in Construction, 2019, 98(2):236-247.

[12] Gao M, Zhao M, Qin J. Marketing strategy selection of referral reward under social network: RRWS, RRMS, or dual strategy? International Transactions in Operational Research, 2022, 29(3):1970-2001.

[13] Hall J, Cho H D, Guo Y, Mildred M, Thompson L A, Shenkman E, Salloum R.Association of Rates of Smoking During Pregnancy With Corporate Tobacco Sales Policies. Jama Pediatrics, 2019, 173(3):284-286.

[14] Guo Y, Mustafaoglu Z, Koundal D. Spam Detection Using Bidirectional Transformers and Machine Learning Classifier Algorithms. Journal of Computational and Cognitive Engineering, 2022, 2(1):5-9.

[15] Zhao X, Nie F, Wang R, Li X. Improving projected fuzzy K-means clustering via robust learning. Neurocomputing, 2022, 491(6):34-43.

[16] Bingqian Z, Xingsheng G. Multi-block statistics local kernel principal component analysis algorithm and its application in nonlinear process fault detection. Neurocomputing, 2020, 376(2):222-231.

[17] Ghaffari R, Golpardaz M, Helfroush M S, Danyali H. A fast, weighted CRF algorithm based on a two-step superpixel generation for SAR image segmentation. International Journal of Remote Sensing, 2020, 41(9):3535-3557.

[18] Mano A, Anand S. Method of multi-region tumour segmentation in brain MRI images using grid-based segmentation and weighted bee swarm optimisation. IET Image Processing, 2020, 14(12):2901-2910.

[19] Dickinson T A, Richman M B, Furtado J C. Subseasonal to Seasonal Extreme Precipitation Events in the Contiguous United States: Generation of a Database and Climatology. Journal of Climate, 2021, 34(18):7571-7586.

[20] Lee E H, Kim K, Kho S Y, Kim D K, Cho S H. Estimating Express Train Preference of Urban Railway Passengers Based on Extreme Gradient Boosting (XGBoost) using Smart Card Data.Transportation Research Record, 2021, 2675(11):64-76.

[21] Tao T, Liu Y, Qiao Y, Gao L , Lu J, Zhang C, Wang Y. Wind turbine blade icing diagnosis using hybrid features and Stacked-XGBoost algorithm. Renewable Energy, 2021, 180(12):1004-1013.

[22] Sagi O, Rokach L. Approximating XGBoost with an interpretable decision tree. Information Sciences, 2021, 572(2):522-542.

[23] Zhao X, Nie F, Wang R, Li X. Improving projected fuzzy K-means clustering via robust learning. Neurocomputing, 2022, 491(6):34-43.

[24] Changhua L, Yanxia Z, Chenzhou C. Identification of BASS DR3 sources as stars, galaxies, and quasars by XGBoost. Monthly Notices of the Royal Astronomical Society, 2021, 506(2):1651-1664.

[25] Raichura M, Chothani N, Patel D. Efficient CNN-XGBoost technique for classification of power transformer internal faults against various abnormal conditions. IET Generation, Transmission & Distribution, 2021, 15(5):972-985.

Application of Machine Learning Algorithms for Predicting Energy Consumption of Servers

Meryeme EL YADARI[1*], Saloua EL MOTAKI[2], Ali YAHYAOUY[3],
Khalid EL FAZAZY[4], Hamid GUALOUS[5], Stéphane LE MASSON[6]
Computer Science, Sidi Mohamed Ben Abdellah University, Fes, Morocco[1, 3, 4]
Electrical Engineering, Caen Normandy University, Saint-lô, France[1, 5]
Computer Science, Chouaib Doukkali University, El Jadida, Morocco[2]
LaMSN - The House of Digital Sciences, USPN, Paris, France[3]
Orange Lab's, Lannion, France[6]

***Abstract*—Energy management in data centers is currently a major challenge and arouses considerable interest. Many data center operators are seeking solutions to reduce energy consumption. In this work, the problem of resource overutilization-defined as the excessive usage of critical server resources such as CPU, RAM and storage surpassing their optimal capacity-in data centers is addressed, with a particular focus on servers. Estimating the energy consumption of servers in data centers allows its managers to allocate the necessary resources to ensure adequate quality of service. The research involved generating workloads performance on various servers, each connected to a wattmeter for energy consumption measurement. Data on resource utilization rates and server energy consumption were stored and analyzed. Machine learning models were then used to forecast server energy consumption. Parametric, non-parametric, and ensemble methods were employed and validated using accuracy measurements, non-parametric tests, and model complexity to assess the quality of energy consumption prediction models. The results demonstrated that certain models could provide predictions with a low margin of error and minimal complexity like polynomial regression, while other models showed lower performance. A comparative analysis is conducted to evaluate the performance and limitations of each approach.**

***Keywords*—Data center; server; machine learning; energy consumption; parametric methods; ensemble methods**

I. INTRODUCTION

Data centers are centralized collections where networked computers provide computational resources for various applications such as web hosting, e-commerce, grid computing, cloud computing, and social networks [1]. The computing equipment also enables the processing, storage, and analysis of data within the data center. A data center is used in the form of a cloud computing infrastructure that offers enough storage capacity and computing for Internet of Things (IoT) services and managing real time massive IoT data generated by numerous IoT devices. However, to ensure optimal performance and high reliability, it is common for the data center network to be oversized, resulting in relatively low utilization of links in real life scenarios based on empirical observations [2]. Cooling or power interruptions can have significant repercussions on the environment of a data center. Since system failures can be extremely costly, it is crucial to implement reliability and redundancy measures. Redundancy in cooling systems helps minimize the risk of failure and improves performance by reducing downtime for maintenance and repairs. The primary advantage of redundancy is to increase system reliability [3]. Energy management is an important process that requires a systemic approach by addressing both the energy consumption of idle resources and the supporting infrastructure. However, truly sustainable operation should not only focus on energy management but also include investments in research and development of green energies, the utilization of renewable energy sources, and active measures to preserve the environment [4].

The data center infrastructure can be divided into three areas: the computer room, the support zone, and accessory spaces. The computer room is a space with controlled environmental conditions designed to accommodate equipment as well as cables directly linked to computer and telecommunications systems that generate a significant amount of heat. Additionally, Information Technology (IT) equipment is extremely susceptible to changes in humidity and temperature, so a data center must maintain constrained conditions to ensure the reliability and proper functioning of the equipment it contains. The support zones are where a variety of systems such as Uninterruptible Power Supplies (UPS), cooling control systems, and communication panels are situated. Finally, the accessory sections primarily consist of offices, a lobby, and restrooms [5].

The massive energy consumed by servers in data centers poses a major problem that requires strategic research to address such as high energy costs, environmental impact, and resource overutilization. Estimating server energy consumption is essential for efficient energy management, providing the necessary power to IT infrastructure, managing data center resources, and minimizing costs. The goal is to estimate servers' energy consumption using ML algorithms and build models with a low margin of error and weak complexity, which refers to the time required for model creation. Three methods, namely parametric, non-parametric, and ensemble methods, are employed for this purpose. Parametric methods rely on assumptions regarding the data's underlying distribution and use a fixed number of parameters to describe it. Non-parametric techniques do not presume any specific distribution about the distribution of data. They are flexible and can handle complex relationships without specifying a fixed number of parameters. Ensemble methods integrate several models to enhance

predictive quality. They aggregate the predictions of several base models to produce a more accurate and robust prediction. Different models from each method were employed to assess the performance of each model and conduct a comparative study among them. We mention that the selection of parametric, non-parametric, and ensemble methods was based on their encompassment of techniques commonly utilized in regression problems. This study involves the creation of workloads that consume server resources and used multiple ML models to predict energy consumption using a collected database. A comparative study among different models was conducted to demonstrate the effectiveness of each model, using accuracy metrics, models complexities, and non-parametric tests.

The primary contributions of this research are detailed below:

- Creation of workloads that vary the resource utilization rates of servers in terms of CPU, RAM, and hard drive.
- Application of parametric, non-parametric, and ensemble methods on three heterogeneous servers, to verify the capability of ML models to predict the energy consumption of different servers.
- Validation of the ML models through precision measurements, non- parametric tests, and complexity.

The structure of this article is organized as follows: Section II presents the related work. Section III discusses the data center equipment and system architecture. Section IV reviews parametric, non-parametric, and ensemble methods. Section V details the data extraction processes, including the data extracted for each server, the designed algorithms, a comparison of the methods used to create workloads, and a description of the experiment. Section VI focuses on the prediction phase, applying parametric, non-parametric, and ensemble methods. Sections VII and VIII respectively present the results and discussion, including a comparison of the three types of methods across the three servers. Finally, Section IX is dedicated to the conclusion.

II. Related Work

In the literature, several authors have worked on energy management and consumption in data centers, as well as virtual machine (VM) placement on physical machines (PMs). In study [7], the authors propose two VM placement algorithms on PMs, considering CPU, RAM, memory utilization, and correlation values. These algorithms have shown performance in terms of energy consumption and service quality improvement compared to other methods [8]. The second approach involves optimal VM placement on servers using heuristics while considering hardware vulnerabilities, server energy consumption, and interference collocation among VMs [9]. This method selects an optimal approach from options such as dot product, norm2, first fit, ω-greedy, ρ-greedy, and η-greedy. Other authors in [10] studied the correlation between server resource utilization and energy consumption. They applied different workloads on two different servers and measured their energy consumption using two methods: resources utilization rate obtained from performance counters, and from external energy meter device. The results showed a strong correlation between CPU utilization and energy consumption, and a weaker correlation with RAM and disk utilization. This study can help data centers operate more energy-efficiently by optimizing resource consumption and lowering energy expenditure.

A power consumption prediction model for servers called PCP-2LSTM was proposed in study [11], this model applies a moving average smoothing technique to remove noise from the power consumption time series data and utilizes two stacked Long Short Term Memory (LSTM) networks to predict the power consumption for the next 30 seconds. A power consumption monitoring system is created to collect data and analyze power consumption, while ensuring the stationarity of the power series. CPU intensive workloads are used to collect power consumption data, and Collectd is used as a measurement tool to collect data such as CPU usage, frequency, memory usage, etc. The results show that PCP-2LSTM outperforms other models such as 2LSTM, LSTM, GBR, RAE, and ARIMA, with a normalized Root Mean Squared Error (nRMSE) of 0.417. However, it is important to note that the implementation of this model is simplified compared to a real data center, where there are various types of user requests beyond just CPU utilization. Another study proposes a VM selection policy called Maximum Correlation of sum of Squares of Deviation (MCSSD) [12]. This policy is implemented using the CloudSim tool with a heterogeneous server environment consisting of 800 servers. Workload traces from the CoMon project [13] are used, and the experiment is repeated with each server calculating resource utilization every minute. The results demonstrate that the proposed policy consumes less energy and minimizes the number of VM migrations compared to other policies such as Maximum Correlation, Minimum Utilization, and Minimum Migration Time.

Authors in study [14] developed a stochastic model to estimate the power consumption based on archived data. They consider workload and power as random variables and establish a correlation relationship between these two entities using a non-parametric approach. This makes the task complex as it requires estimating the complete distribution from the data. AI techniques were used to classify VMs based on their RAM and CPU usage [15], as well as to group user tasks based on their size and details extracted from the log file. Multiple tasks can share the same resources of a VM. The objective is to allow more dynamic resource allocation and enhance QoS standards by ensuring better resource allocation, raising user satisfaction, and lowering the number of rejected tasks. In [16], the authors present methods for evaluating and modeling the energy consumption of these resources and describe techniques that operate at the distributed system level, aiming to better manage resource scheduling, distribution, and network traffic management. Their research aims to make network and computing resources more efficient. A system proposed by [17] identifies frequently used data from application traces. Replication management and data placement are used to allocate frequently used files to "hot" disks and other files to "cold" disks. This system adds disk management to the cloud environment, which has proven effective in saving 39% of energy with an 18.26% reduction in execution time. The article also proposes an energy efficient storage system for a disk, combining energy efficient placement with a smart scheduling algorithm. The

system assigns data to a disk based on its data usage model. Data replication used in the algorithm ensures fast and easy data availability. The system maximizes energy savings by associating requests to the most available disks, thereby reducing query execution time. It also considers the minimum wait time and maximum remaining idle time when research disks are active or inactive, respectively. This approach applies data replication with the appropriate number of replicas across a hybrid system, ensuring the QoS for cloud applications.

On the subject of triggering queries, researchers in study [18] noticed that the frequency of triggering the same query to access data is quite high. Therefore, forecasting and preloading often accessed queries can elevate performance levels by reducing execution time and increasing cache hit rates. Hence, they develop a prediction model that first generates memory traces to assess data usage patterns related to query frequency. Future query requests were predicted and organized using an ensemble strategy, resulting in an accuracy of 87.5%. In study [19], the authors define Random Allocation as a policy that randomly assigns arrived tasks to a queue without considering how many tasks are waiting in the queue. This can lead to overflow in one queue while others remain empty or partially filled, increasing the probability of task loss. Short tasks may wait for a long duration in front of large tasks, which the random scheduler does not detect. However, implementing this policy is easy and does not require knowledge about the system. The Shortest Queue is defined as a strategy that overcomes the problem of balanced load across queues. Upon task arrival, the policy directs them to the queues with the shortest waiting time. This ensures that full queues do not appear while others still have available capacity, reducing the probability of task loss. However, short tasks may be delayed in front of long duration tasks. This strategy only considers waiting time and not service demands. The policy requires knowledge of the queue states. A notion of Task Assignment based on Guessing Size (TAGS) is introduced, aiming to allocate tasks when the service demands are not known before execution. In this case, a task is sent to a server's queue, and the server executes the task in the queue until it is completed or the execution time elapses. In the latter case, the task is sent to another server, and the same operations are repeated, increasing the waiting time as it moves from one server to another. Compared to the shortest queue strategy and random allocation, TAGS solves the problem of short tasks waiting behind long tasks. However, performance may be affected due to repetitive service. If the waiting time is very short, multiple tasks will require repetitive services, and if it is longer, the duration will delay completion. In study [20], the authors define reliability, energy consumption, and execution time as the principal scheduling parameters for real time embedded systems. In their work, while considering three constraints: the partial order of task modules, time limitations, and reliability, based on a Directed Acyclic Graphs (DAG) and Quantum behaved Particle Swarm Optimization (QPSO). When compared to alternative algorithms, the findings demonstrate that the two proposed algorithms provide effective optimization. These two algorithms are DAG_QPSO_I and DAG_QPSO_II. The first one demonstrates efficiency in terms of energy consumption, while the second one best meets the requirements of time and reliability. In this work, workloads have been created and launched to consume resources from heterogeneous servers and ML methods belonging to different parametric, non-parametric, and ensemble methods were implemented. A comparative study was conducted between these methods for each server. Estimating server energy consumption will enable better management of energy consumption in a data center. On the other hand, data center managers can adjust resources based on server demand, which helps reduce costs. Another objective is to optimize energy efficiency by identifying energy consuming areas and implementing. In contrast to many other studies that use limited or simulated workload data, this work involves the construction and deployment of real workloads which make use of resources from diverse servers. This method provides a more accurate assessment of the energy and servers performance. Moreover, comprehensive comparisons and the selection of the optimal models for diverse circumstances are made possible by the utilization of diverse ML methods. A comparative analysis was done for each server independently to make sure the results are accurate and applicable to different servers' configurations. This degree of specificity offers useful management insights for data centers.

III. Data Center Equipment and System Architecture

The power distribution systems of the data center are intended to provide electricity to the system loads or IT and mechanical equipment, ensuring proper levels of power quality and supply security. Since the public grid may experience voltage drops or prolonged outages that can result in malfunction or even a complete shutdown of the data center, it is crucial to ensure proper power supply. In a standard data center, there is a backup diesel generator or generator set to provide power in case of major grid failures. The UPS is capable of using different storage solutions like batteries, it is typically designed to keep power supply under appropriate conditions during the startup of the diesel generator. Power supply units (PSUs) and Power distribution units (PDUs) are in charge of distributing and regulating power for servers [5]. Fig. 1. illustrate the main elements of the data center responsible for power supply. It is important to note that generators or batteries provide backup power during a power outage. Racked servers and critical datacenter infrastructure can smoothly switch to this backup power for uninterrupted service. They can support primary power during periods of high demand or grid instability. They can help to balance the load on the power infrastructure of the data center and ensure a stable and reliable supply of power to the rack servers. During peak power usage periods, when energy demand is high, generators or batteries can supplement the power supply to avoid overloading the grid. This helps manage peak demand and avoid potential blackouts. They can also provide voltage regulation to ensure that the power supplied to rack servers remains within acceptable voltage ranges. This helps maintain the stability and longevity of server hardware. Rack servers, networking equipment, storage devices and other critical infrastructure within the data center rely on stable and reliable power to function optimally. Generators and batteries provide the necessary backup power to support these loads during emergencies or planned maintenance activities. In total, effective use of generators or batteries in a data center ensures reliable power to rack servers, improves energy efficiency, and

contributes to the resiliency and sustainability of the data center infrastructure.

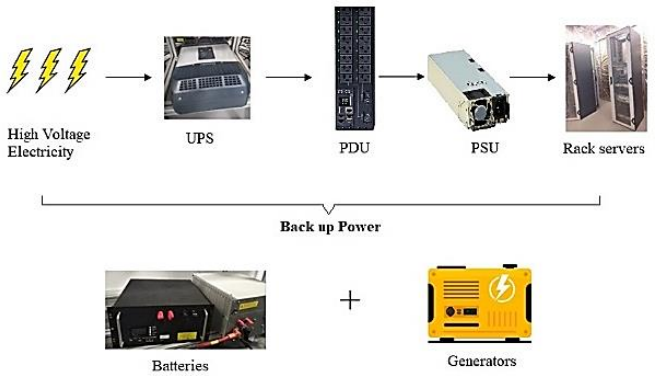


Fig. 1. Data center elements responsible for the power supply.

Most traditional data centers, including small and medium sized ones, have a power consumption breakdown as illustrated in Fig. 2 [6]. It can be observed that IT equipment accounts for 50% of the total data center power, followed by cooling systems, which represent 25% of the total power. Air handling equipment utilizes 12%, UPS units consume 10%, while lighting and other equipment consume 3% of the power. It is important to emphasize that servers, as part of the IT equipment, consume a significant fraction of the total power within data centers. This observation highlights the need to develop Machine Learning (ML) models to predict server energy consumption, enabling data center managers to better allocate their resources based on users' needs. The amount of energy consumed by servers compared to other components in a data center will vary based on factors such as workload type, server efficiency, cooling systems, and the data center design. In a conventional data center environment, as shown in Fig. 2, servers typically account for approximately 50% of total energy consumption. For this reason, and due to the limitations in accessing a real data center environment, this study focused primarily on servers, other elements such as networking equipment and cooling systems are not considered.

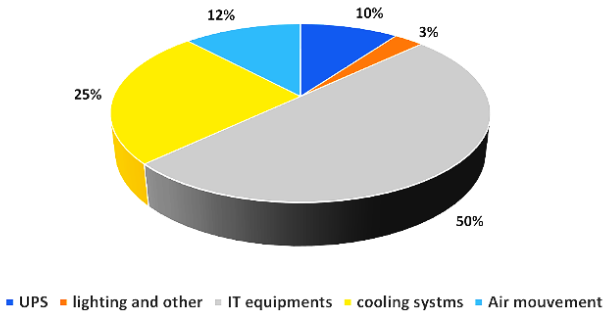


Fig. 2. Distribution of power consumption in a traditional data center [6].

Fig. 3 showcases the architecture of the system developed in this work, starting with the creation of workloads and their deployment on three servers, and ends with the generation of the proposed models.

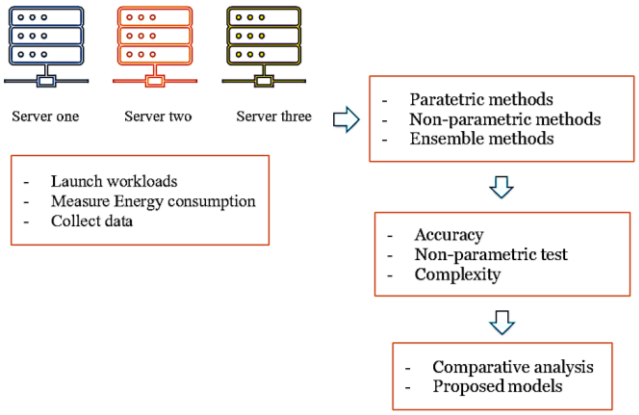


Fig. 3. System architecture.

IV. BACKGROUND

A. Parametric Methods

Parametric regression techniques are statistical tools employed to examine the relationship between a dependent variable and multiple independent variables [21]. This relationship is expressed through a mathematical equation that contains a set of parameters. The objective is to estimate the values of these parameters based on the data. Common examples of parametric regression models include polynomial regression, which is a statistical study that models the variation of a dependent variable using a polynomial function of an explanatory variable. The mathematical representation of the polynomial regression is provided in Eq. (1). Where x is the independent variable, y is the dependent variable, a_i; $i=1,\ldots, k$ is the coefficient or the parameter. Lasso regression (L1 regularization) is another method of statistical regression that combines linear regression with regularization, aiming to eliminate features that do not contribute to the training. Eq. (2) illustrates the formula utilized in Lasso regression, where k is the number of observations. y_i is the observed value of the observation i. x_{ij} is the value of the predictor j for the observation i. α_j is the coefficient to be estimated and strictly between zero and one. m is the number of predictor variables, and γ is the regularized parameter that controls the strength of the penalty term. Determining the ideal value of γ, or the value that strikes a balance between the model's fidelity and other factors is crucial [22]. Elastic Network (L1+L2) is a linear combination of L1 and L2 resulting in a regularizer that combines the advantages of both L1 (Lasso) and L2 (Ridge) regularization techniques, similar to Lasso regression, uses regularization to control the complexity of the model by selecting the most relevant variables. Many studies have utilized the Elastic Network, including the work presented by authors in [23], which introduces a novel algorithm for clustering analysis based on elastic networks and leveraging weighted properties. Also, in study [24] authors propose a novel approach called the Elastic Network Algorithm for Clustering based on Cluster Center Shift, which combines Mean-Shift with the Elastic Network algorithm to optimize both cluster stability and effectiveness in the cluster analysis. Lastly, Neural Networks (NN) are a type of ML that consists of interconnected neurons organized in layers and capable of learning from data by adjusting connection weights between neurons. For NN with

multiple layers, the output of each layer *l* can be calculated using the output of the previous layer. Eq. (3) outlines the structural formulation of NN, where $a^{(l)}$ is the output of the layer *l*, σ is the activation function, $w^{(l)}$ is the weight matrix of layer *l*, $a^{(l-1)}$ is the input to the layer *l*, and $b^{(l)}$ is the bias for layer *l*. Lasso regression minimizes the sum of squared errors between the actual and predicted values. It works by iteratively reducing the coefficients of less important variables towards zero. It utilizes a regularization parameter, alpha, which controls the strength of the L1 penalty. A larger value of alpha leads to coefficients closer to zero. The formulation for Elastic Network can be found in Eq. (4), where *N* is the number of observations, y_i is the observed value for the observation *i*. β_k, *k=0,..*, *p* is the coefficient to be estimated. *p* is the number of predictor variables. λ_1 and λ_2 are the regularization parameters for L1 and L2 penalties. x_i is the value of the predictor variable *j* for the observation *i*. For each server, 80% of data was used for training the model, and the obtained error values were recorded. It should be noted that for each server, the models were trained using non-normalized data.

$$y = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_k x^k \quad (1)$$

$$\mathrm{L} = \sum_{i=1}^{k} \left(y_i - \sum_{j=1}^{m} x_{ij} . \alpha_j \right)^2 + \gamma \sum_{j=1}^{m} |\alpha_j| \quad (2)$$

$$a^{(l)} = \sigma(w^{(l)} a^{(l-1)} + b^{(l)}) \quad (3)$$

$$min_{\beta_0,\beta} \left(\sum_{i=1}^{N} (y_i - \beta_0 - x_i^T \beta)^2 + \lambda_1 \sum_{j=1}^{p} |\beta_j| + \lambda_2 \sum_{j=1}^{p} \beta_j^2 \right) \quad (4)$$

B. Non-parametric Methods

Non-parametric methods apply statistical analysis to investigate the connection between a dependent variable and multiple independent variables without making specific assumptions about the functional form or equation that describes the relationship [25]. These methods estimate the relationship based on the data itself. Common examples of non-parametric regression models include Support Vector Regression (SVR), which is a supervised learning method based on support vectors that model the data and find a hyperplane that separates the data by minimizing the squared error. It is useful for complex regression problems where the data has nonlinear relationships. The formula for SVR is presented in Eq. (5). Where ω is the weight vector or coefficients associated with the input features *x*. This vector determines the importance of each feature in the prediction. *x* is the input feature, and *b* is the bias term. Decision trees are ML algorithms used for classification and regression problems. They model the relationships between input variables and output variables using a graphical representation with connected nodes. The algorithm selects the most informative variable to split the data into categories, and the process is repeated until a stopping condition is met. Random forests are an ensemble of decision trees constructed randomly based on the training data. The prediction for an observation is based on the average or majority value of the individual predictions from the trees. Gaussian Process Regression (GPR) is a probabilistic approach based on the concept of a Gaussian process, which is a collection of random variables that have a joint Gaussian distribution for any finite number of variables. This model can capture complex and nonlinear relationships between variables without assuming a specific functional form of the relationship.

$$y = f(x) = \langle \omega, x \rangle + b;\ \omega, x \in \mathbb{R}^M, b \in \mathbb{R} \quad (5)$$

C. Ensemble Methods

Ensemble methods refer to a class of ML models that blend several models to increase the system's predictive effectiveness [26]. These models can be of the same type (homogeneous) or different types (heterogeneous). The idea behind ensemble methods is to reduce the variance and bias of individual models by combining their outputs. This is achieved through different strategies, such as bagging, which is based on an ensemble estimator using base regressors trained on random subsets of the dataset and merges their predictions, either via voting or averaging, to generate the final output. Bagging involves creating multiple versions of the same model on different subsets of the data and combining their outputs by averaging or voting. Eq. (6) illustrates the formula utilized in Bagging. Where $f_{bagging}(x)$ is the aggregated prediction for the input *x*. *N* is the total number of base learners, and $f_i(x)$ is the prediction of the base learner *i*. Boosting is a ML method that involves creating a series of models aimed at reducing errors in predictive data analysis. Each subsequent model learns from the errors of the previous one. Boosting addresses the problem of biased models when using new data by successively training multiple models to improve the overall system accuracy. Data scientists often use boosting with decision tree algorithms [27]. Boosting combines multiple models sequentially and assigns weights to the outputs of individual models, giving higher weight and input to the next model for incorrect predictions from the previous model. Stacking is an ensemble method that reduces the error rate of one or multiple estimators during prediction. It works by stacking the outputs of each individual estimator and using a regressor to compute the final prediction. This method allows leveraging the strengths of each estimator by using their outputs as input to a final estimator. It is important to mention that the base estimators are fitted on the dataset, while the final estimator is trained using the cross-validation predictions of the base estimators. Stacking incorporates boosting and aggregation, which combines the outputs of models and achieves high accuracy and low variance. The formula of Stacking can be found in Eq. (7). Where $f_{stacking}(x)$ is the final prediction of the stacking ensemble for input *x*, and $f_k(x)$, *k=1,…, N* is the predictions of base learners. *Meta_learner* is the meta learner that combines the predictions. Typically, the number of estimators used in this method ranges from three to five. In this work, parametric and non-parametric models were used and developed earlier while keeping the same chosen configurations.

$$\hat{f}_{bagging}(x) = \frac{1}{N} \sum_{i=1}^{N} \hat{f}_i(x) \quad (6)$$

$$\hat{f}_{stacking}(x) = Meta\_learner(\hat{f}_1(x), \hat{f}_2(x), \ldots, \hat{f}_N(x)) \quad (7)$$

V. Data Extraction

In this experiment, workloads that consume CPU, RAM, and hard disk resources of three servers were created and executed, each one is connected to a wattmeter that accurately measures the server's energy consumption with a precision of one mwh. The number of data points used for server one, server two and server three is 897, 945, and 951, respectively. Each data element represents the median value of resources utilization for the server over a period of one hour. In other words, workloads

that varied the usage of CPU, RAM, and/or hard disk were executed for one hour and recorded the server's state during that execution. If the resource utilization varies frequently, the configuration is discarded; otherwise, it is kept. For the three servers, each data point (vector representing a workload) includes CPU values ranging from 10% to 100%, RAM values ranging from 10% to 90%, and disk usage ranging from zero GB to the maximum storage capacity of each server. The servers used in this study are documented in Fig. 4, which illustrates the work conducted at the LUSAC laboratory of the University of Caen Normandy in France.

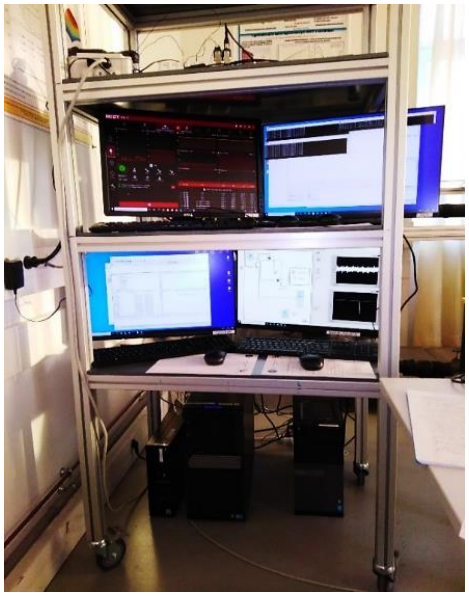


Fig. 4. Servers used in the experimentation conducted at LUSAC laboratory.

In the following, the algorithms used to generate workloads that consume CPU, RAM, and disk resources of the servers are presented. For the implementation of those algorithms, the Python programming language was utilized, and every algorithm was launched in every server. After creating and executing the workloads, the energy consumption of the servers is measured. Then, on a computer, models belonging to different categories: parametric, non-parametric and ensemble, were built with the aim of predicting the energy consumption of the servers. It is mentioned that the results obtained come from a computer and not from a simulator. Also, the duration is the same in the three algorithms. For the first algorithm, OCCT was utilized to generate workloads that would stress the CPU of the server. In the second algorithm, programs such as Google Chrome were launched continuously to consume the RAM of the server, the memory usage is measured after executing those programs. In the third algorithm, files were created and duplicated on the hard drive to write data on it. After each execution, the files created to run the algorithm with different parameters were deleted (number of bytes to write). It is noted that various input data values are employed for writing operations on the hard drive. This approach aimed to create workloads that would write on the server's hard drive with continuous writing operations. Initially, the process was initiated by writing at a rate of 100 bytes per second for a duration of one hour. Subsequently, the byte values were incrementally increased in the following simulations.

Algorithm1: Workload_CPU
Input: nbr_process, duration
Output: cpu_rate, ram_rate, hard_drive_rate, energy_consumption
Start
  For var p in [1: nbr_process]:
    Create_process()
    Launch_process()
  End for
  While time < duration:
    Save (cpu_rate, ram_rate, hard_drive_rate, energy_consumption)
    If time == duration:
      For var p in [1: nbr_process]
        destroy_process ()
      End for
    End if
  End while
End

Algorithm2 Workload_RAM
Input: nbr_process, duration
Output: cpu_rate, ram_rate, hard_drive_rate, energy_consumption
Start
  For var p in [1: nbr_process]:
    Launch_program()
  End for
  While time < duration:
    Save (cpu_rate, ram_rate, hard_drive_rate, energy_consumption)
    If time == duration:
      For var p in [1: nbr_process]
        Destroy_process ()
      End For
      Break
    End If
  End While
End

Algorithm3: Workload_hard_drive
Input: nbr_bytes, duration
Output: cpu_rate, ram_rate, hard_drive_rate, energy_consumption
Start
  While time < duration:
    write_bytes()
    Save (cpu_rate, ram_rate, hard_drive_rate, energy_consumption)
    If time == duration:
      Break
    End if
  End while
End

The characteristics of each server are presented in Table I. It should be noted that the selection of servers is based on their availability in the research laboratory where this study is conducted.

TABLE I. SERVERS CHARACTERISTICS

Server one	Server two	Server three
processor Intel(R) Xeon(R) CPU W3565 @ 3.20 GHz, RAM 16 Go, Disk SATA SSD 256Go, NVIDIA Quadro 400, os Windows 10	Intel(R) Core (TM) i5-10500 CPU @ 3.10GHz, RAM 8GB, Disk 512GB, and OS windows server 2022 Standard version os.	Processor Intel (R) core (TM) i3 CPU 540 @ 3.07 GHz, RAM 4 Go, disk 120 Go SSD, Intel(R) HD Graphics, os Windows 10.

VI. PREDICTION PHASE

A. Application of Parametric, Non-parametric, and Ensemble Methods on Servers

We applied parametric methods to analyze the behavior of three servers. Starting with server one, according to Fig. 5, Fig. 6 and Fig. 7 which show the error rate, the p-value, and the models' complexity respectively, It is observed that some models, such as NN, have high complexity, followed by Bagging_GPR. In terms of MSE, Lasso regression, elastic network, GPR, and other models exhibit high values around six wh. Table II presents the error rates, the p-values of non-parametric tests Wilcoxon rank sum and the complexity of each method. The results show that the polynomial regression of degree two performs the best with a low MSE of 0.71 wh. Followed by NN, which consists of two layers with 64 neurons each, using the Adam optimizer and trained with 2600 epochs. It achieves a high R^2 of one and low errors, indicating that this model can accurately predict the server's energy consumption. Lasso regression and Elastic Network have similar R^2 values, with a coefficient alpha of 0.69 for Lasso regression, an alpha and L1 coefficients of 0.34 and 0.9, respectively, for Elastic Network. The MSE of both methods exceeds five wh, indicating that these two models struggle to explain the variation in the data. The p-value of the models is relatively similar for all three models, suggesting no significant difference in their performance. For each model used, different parameters were tested, and those that yielded the best results were selected. It is interesting to note that the polynomial regression, Lasso regression, and Elastic Network models have negligible predictions and construction times. However, NN stands out with a construction time of 283 seconds, primarily due to the high number of epochs used and the complexity of its structure.

Concerning the second server, as shown in Table III, the polynomial regression of degree two had the least bias, with a MSE rate of 0.04 wh and a p-value of 0.98. Followed by NN model, configured with 2600 epochs, a sigmoid activation function for the first and the second layers, 128 neurons, and the Root Mean Squared Propagation (rmsprop) optimizer. The best result for Elastic Network was achieved with an alpha of 0.01 and an L1 of 0.01, resulting in a MSE rate of 0.07 wh. As for the Lasso regression model, it is observed that the error rate increases with the increase in the alpha coefficient. The best performance was obtained with an alpha of 0.01, resulting in a MSE of 0.08 wh. Overall, the results indicate that the parametric methods generally perform well in predicting the energy consumption for this server. Indicating a high probability that the real and predicted vectors are significantly similar. It is observed that polynomial regression, Lasso regression, and Elastic Network stand out for their reduced model construction time and negligible prediction time. On the other hand, NN model requires a longer construction time, reaching up to 110.9 s. However, it achieves a fast prediction rate of 0.1 s.

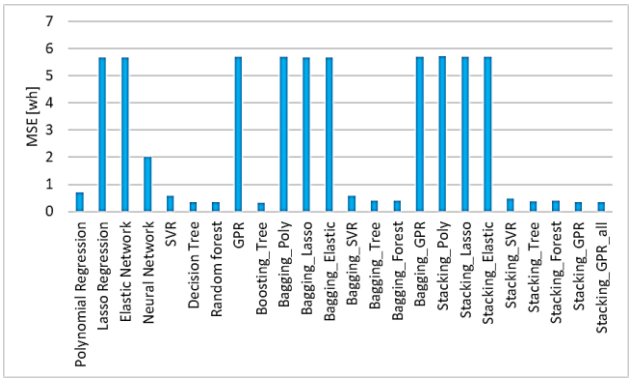


Fig. 5. MSE of server one's models.

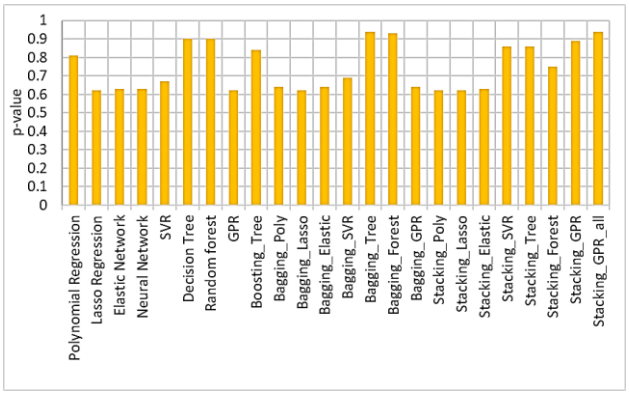


Fig. 6. P-value of server one's models.

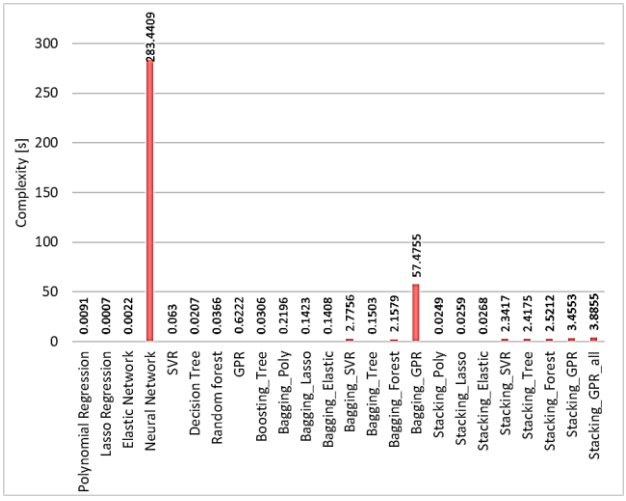


Fig. 7. Complexity of server one's models.

TABLE II. ACCURACY MEASUREMENTS, NON-PARAMETRIC TESTS AND COMPLEXITY OF PARAMETRIC METHODS OF SERVER ONE

	R^2	MSE [wh]	MAE [wh]	RMSE [wh]	MAPE [%]	Wilcoxon rank-sum test	Model construction time [s]	Prediction time [s]
Polynomial Regression	**1.0**	**0.71**	**0.57**	**0.84**	**0.45**	**0.812**	**0.0091**	**0.0**
Lasso Regression	0.99	5.69	1.81	2.39	1.39	0.62	0.0007	0.0
Elastic Network	0.99	5.69	1.82	2.39	1.41	0.63	0.0022	0.0010
Neural Network	1.0	2.02	0.62	1.42	0.50	0.63	283.4409	0.1547

TABLE III. ACCURACY MEASUREMENTS, NON-PARAMETRIC TESTS AND COMPLEXITY OF PARAMETRIC METHODS OF SERVER TWO

	R^2	MSE [wh]	MAE [wh]	RMSE [wh]	MAPE [%]	Wilcoxon rank-sum test	Model construction time [s]	Prediction time [s]
Polynomial Regression	**0.99**	**0.04**	**0.16**	**0.2**	**0.87**	**0.98**	**0.0019**	**0.0**
Lasso Regression	0.98	0.08	0.21	0.28	1.14	0.42	0.0019	0.0005
Elastic Network	0.98	0.07	0.21	0.26	1.12	0.49	0.0020	0.0
Neural Network	0.99	0.05	0.12	0.22	0.66	0.48	110.9219	0.1096

On server three, the polynomial regression model of degree two was employed, Lasso regression with an alpha of 0.01, Elastic Network with an alpha of 0.01 and an L1 of 0.01. The NN is configured with a number of epochs of 2600, two layers of 128 neurons each, using the hyperbolic tangent activation function 'tanh'. We used the Stochastic Gradient Descent optimizer 'sgd' for the NN. Table IV indicates that NN turned out to be the least biased model, with a MSE of 0.07 wh, followed by polynomial regression with a MSE of 0.09 wh. Lasso regression and Elastic Network produced similar prediction values, with a MSE of 1.24 wh and 1.23 wh, respectively. Like servers one and two, all the parametric models are characterized by their low complexity in terms of model construction and prediction. Except NN model that requires 108.34 s for model construction.

Proceeding with non-parametric methods, models were used to evaluate the performance of the servers. For the first one, the results show that decision trees, random forests, and SVR models achieve the best performance with a MSE below 0.58 wh. On the other hand, the GPR model exhibits a significantly higher MSE of 5.71 wh, indicating lower performance compared to the other models. For the SVR model, the Radial Basis Function (RBF) kernel was used with an epsilon value of 0.1 and a regularization parameter C of 19.6. The depth of the decision tree and random forests are 9 and 10, respectively, with 20 estimators for random forests. Lastly, for the GPR model, the DotProduct kernel and WhiteKernel were utilized. As observed in Table V the SVR model, decision trees, and random forests have minimal construction and prediction times, making them computationally advantageous. However, the GPR model stands out from the others in terms of construction and prediction time, being higher.

Similarly for server one, server two results, as cited in Table VI show that decision trees, random forests, and SVR are the best models for predicting server energy consumption, with a MSE rate of 0.02 wh. Although GPR model follows the other three models in terms of precision, it is also performant. We note that SVR model is configured with an epsilon and a C parameter of 0.1 and 3.0 respectively. The optimal depth for decision trees and random forests is five. The kernel used in the GPR model is based on DotProduct and WhiteKernel. Also, all selected non-parametric methods stand out for their low complexity in terms of model construction and prediction time. Likewise to the first and second servers, random forests, decision trees, and SVR are the best models for predicting the energy consumption of server three. The SVR model was trained with an epsilon of 0.06 and a C value of 16.1, while the decision trees and random forests have a maximum depth of six. On the other hand, the GPR model has a high MSE of 1.23 wh. It was trained with a DotProduct and WhiteKernel. Based on the results obtained in Table VII, it can be observed that all the proposed non-parametric models can provide energy consumption predictions with an error rate below 1.23 wh and relatively low complexity.

TABLE IV. ACCURACY MEASUREMENTS, NON-PARAMETRIC TESTS AND COMPLEXITY OF PARAMETRIC METHODS OF SERVER THREE

	R^2	MSE [wh]	MAE [wh]	RMSE [wh]	MAPE [%]	Wilcoxon rank-sum test	Model construction time [s]	Prediction time [s]
Polynomial Regression	**1.0**	**0.09**	**0.21**	**0.3**	**0.41**	**0.64**	**0.0029**	**0.0**
Lasso Regression	0.98	1.24	0.88	1.11	1.81	0.35	0.0009	0.0009
Elastic Network	0.98	1.23	0.88	1.11	1.81	0.35	0.0009	0.0010
Neural Network	1.0	0.07	0.19	0.26	0.37	0.29	108.3468	0.1140

TABLE V. ACCURACY MEASUREMENTS, NON-PARAMETRIC TESTS AND COMPLEXITY OF NON-PARAMETRIC METHODS OF SERVER ONE

	R^2	MSE [wh]	MAE [wh]	RMSE [wh]	MAPE [%]	Wilcoxon rank-sum test	Model construction time [s]	Prediction time [s]
SVR	1.0	0.57	0.47	0.75	0.37	0.67	0.0630	0.0079
Decision Tree	**1.0**	**0.34**	**0.36**	**0.58**	**0.3**	**0.9**	**0.0207**	**0.0**
Random forest	1.0	0.35	0.35	0.59	0.29	0.9	0.0366	0.0
GPR	0.99	5.71	1.84	2.39	1.42	0.62	0.6222	0.0315

TABLE VI. ACCURACY MEASUREMENTS, NON-PARAMETRIC TESTS AND COMPLEXITY OF NON-PARAMETRIC METHODS OF SERVER TWO

	R^2	MSE [wh]	MAE [wh]	RMSE [wh]	MAPE [%]	Wilcoxon rank-sum test	Model construction time [s]	Prediction time [s]
SVR	0.99	0.02	0.1	0.14	0.53	0.9	0.0189	0.0039
Decision Tree	**1.0**	**0.02**	**0.04**	**0.14**	**0.19**	**0.9**	**0.0010**	**0.0**
Random forest	1.0	0.02	0.04	0.14	0.22	0.89	0.0927	0.0069
GPR	0.97	0.11	0.26	0.33	1.46	0.8	0.0867	0.0029

TABLE VII. ACCURACY MEASUREMENTS, NON-PARAMETRIC TESTS AND COMPLEXITY OF NON-PARAMETRIC METHODS OF SERVER THREE

	R^2	MSE [wh]	MAE [wh]	RMSE [wh]	MAPE [%]	Wilcoxon rank-sum test	Model construction time [s]	Prediction time [s]
SVR	**1.0**	**0.06**	**0.16**	**0.24**	**0.3**	**0.86**	**0.0486**	**0.0161**
Decision Tree	1.0	0.03	0.1	0.17	0.2	0.63	0.0038	0.0
Random forest	1.0	0.02	0.09	0.14	0.19	0.48	0.1523	0.0081
GPR	0.98	1.23	0.88	1.11	1.81	0.36	0.9312	0.0081

Different ensemble methods were used, namely boosting, bagging, and stacking. The boosting model was configured with a learning rate of 0.41 and 50 estimators, using a decision tree with a depth of nine as the base estimator. The bagging model was evaluated using various regression methods as base estimators, including polynomial regression, Lasso regression, Elastic Network, SVR, decision trees, random forests, and the GPR model, denoted in Table VIII as Bagging_Poly, Bagging_Lasso, Bagging_Elastic, Bagging_SVR, Bagging_Tree, Bagging_Forest, and Bagging_GPR, respectively. The parameters for these models were defined as mentioned previously, with an optimal number of estimators set to 100. Regarding the first server, the results showed that the boosting model had the least bias, followed by the stacking model configured with GPR and the decision tree as base estimator. Next, the bagging model trained with decision trees achieved good results, as well as the stacking model configured with random forests and SVR model, along with the bagging model trained with the SVR estimator. The MSE of these models ranged from 0.32 wh to 0.59 wh, with a p-value above 0.69. However, except for the bagging model with the GPR estimator, the bagging and stacking methods trained with polynomial regression, Lasso regression, and Elastic Network as base estimators yielded less accurate prediction results compared to the aforementioned models. These models exhibited a higher MSE above five wh. It is observed that certain models had both high error rates and low model construction time, such as bagging and stacking trained with parametric methods. The bagging using the GPR model is distinguished with high error rates and significant model construction time. On the other hand, other models such as boosting and bagging using non-parametric methods other than GPR, as well as stacking using non-parametric models or a combination of the two methods, were characterized by low error rates and model construction times below 3.8 s.

Moving to the second server, the MSE of the boosting model is 0.02 wh and the R^2 reaches one, indicating that the model is capable of predicting energy consumption with negligeable error. As shown in Table IX, the p-value of the Wilcoxon tests is indicating that this method provides predicted values similar to the real values. By applying bagging and stacking models with different estimators. The best results were obtained using decision trees, random forests, and polynomial regression as base estimators for both methods. The average MSE in these models is below 0.07 wh, with a high value of R^2. The stacking model trained with the GPR estimator is the least biased in terms of precision measurement among all the proposed ensemble methods, with a MSE of 0.01 wh. The Bagging_Lasso, Bagging_Elastic, Bagging_GPR, Stacking_Lasso, and Stacking_Elastic models follow the previously mentioned models in terms of prediction quality. Among the ensemble methods, it is noteworthy that all models are characterized by their low complexity, with a model construction time of 9.18 s for the bagging model trained with the base estimator GPR.

TABLE VIII. ACCURACY MEASUREMENTS, NON-PARAMETRIC TESTS AND COMPLEXITY OF ENSEMBLE METHODS OF SERVER ONE

	R^2	MSE [wh]	MAE [wh]	RMSE [wh]	MAPE [%]	Wilcoxon rank-sum test	Model construction time [s]	Prediction time [s]
Boosting_Tree	**1.0**	**0.32**	**0.36**	**0.57**	**0.29**	**0.84**	**0.0306**	**0.0**
Bagging_Poly	0.99	5.7	1.83	2.39	1.42	0.64	0.2196	0.0159
Bagging_Lasso	0.99	5.69	1.81	2.39	1.39	0.62	0.1423	0.0059
Bagging_Elastic	0.99	5.69	1.82	2.39	1.40	0.64	0.1408	0.0049
Bagging_SVR	1.0	0.59	0.48	0.77	0.37	0.69	2.7756	0.8097
Bagging_Tree	1.0	0.4	0.36	0.63	0.29	0.94	0.1503	0.0069
Bagging_Forest	1.0	0.41	0.37	0.64	0.3	0.93	2.1579	0.1466
Bagging_GPR	0.99	5.7	1.84	2.39	1.42	0.64	57.4755	0.0947
Stacking_Poly	0.99	5.74	1.84	2.4	1.43	0.62	0.0249	0.0009
Stacking_Lasso	0.99	5.7	1.83	2.39	1.41	0.62	0.0259	0.0009
Stacking_Elastic	0.99	5.7	1.83	2.39	1.42	0.63	0.0268	0.0009
Stacking_SVR	1.0	0.47	0.4	0.69	0.31	0.86	2.3417	0.0269
Stacking_Tree	1.0	0.37	0.37	0.61	0.3	0.86	2.4175	0.0119
Stacking_Forest	1.0	0.41	0.4	0.64	0.32	0.75	2.5212	0.0139
Stacking_GPR	1.0	0.34	0.36	0.58	0.29	0.89	3.4553	0.0119
Stacking_GPR_all	1.0	0.35	0.36	0.59	0.29	0.94	3.8855	0.0209

TABLE IX. ACCURACY MEASUREMENTS, NON-PARAMETRIC TESTS AND COMPLEXITY OF ENSEMBLE METHODS OF SERVER TWO

	R^2	MSE [wh]	MAE [wh]	RMSE [wh]	MAPE [%]	Wilcoxon rank-sum test	Model constr-uction time [s]	Prediction time [s]
Boosting_Tree	1.0	0.02	0.04	0.14	0.24	0.82	0.4188	0.0
Bagging_Poly	0.98	0.07	0.21	0.26	1.13	0.45	0.1134	0.0059
Bagging_Lasso	0.97	0.11	0.27	0.33	1.48	0.6	0.1276	0.0049
Bagging_Elastic	0.97	0.11	0.26	0.33	1.46	0.59	0.1386	0.0069
Bagging_SVR	0.99	0.02	0.09	0.14	0.49	0.92	0.6927	0.3383
Bagging_Tree	**1.0**	**0.02**	**0.04**	**0.14**	**0.19**	**0.87**	**0.1269**	**0.0069**
Bagging_Forest	1.0	0.02	0.01	0.14	0.2	0.87	2.2184	0.1476
Bagging_GPR	0.97	0.11	0.26	0.33	1.46	0.82	9.1893	0.2563
Stacking_Poly	0.98	0.07	0.21	0.26	1.13	0.46	0.0469	0.0
Stacking_Lasso	0.96	0.16	0.35	0.4	1.92	0.36	0.0399	0.0
Stacking_Elastic	0.98	0.1	0.25	0.32	1.41	0.31	0.0411	0.0
Stacking_SVR	1.0	0.02	0.07	0.14	0.37	0.46	0.8902	0.0089
Stacking_Tree	0.99	0.03	0.04	0.17	0.24	0.87	0.9402	0.0079
Stacking_Forest	1.0	0.02	0.04	0.14	0.22	0.79	0.9835	0.0099
Stacking_GPR	1.0	0.01	0.05	0.1	0.26	0.49	1.8894	0.0109
Stacking_GPR_all	1.0	0.02	0.05	0.14	0.25	0.88	1.9824	0.0134

Lastly, as for the third server, it can be observed that the boosting method trained with decision trees of depth six as base estimators provides predicted values with a MSE of 0.03 wh. Similarly, the bagging and stacking methods trained with the SVR model, decision trees, and random forests as base estimators have a MSE ranging from 0.02 wh to 0.06 wh. Therefore, the stacking model trained with GPR has an MSE of 0.03 wh. On the other hand, the other models such as Bagging_Poly, Bagging_Lasso, Bagging_Elastic, Bagging_GPR, Stacking_Poly, Stacking_Lasso, and Stacking_Elastic provide prediction values with an MSE of 1.23 wh and 1.24 wh. It can be observed that all ensemble methods are capable of predicting energy consumption with an error rate below 1.24 wh in terms of MSE, MAE, and MAPE, and p-values ranging from 0.35 to 0.89, as indicated in Table X. The values of the MAPE are already multiplied by 100. Therefore, a MAPE of 0.45 represents 0.45% and not 45%. Different complexity characteristics are observed among the boosting and bagging models using parametric models as base estimators. They have relatively low complexity, making them efficient in terms of model construction time. Next, bagging using decision trees, random forests, and SVR as base estimators, which also exhibit moderate but slightly higher complexity. On the other hand, the bagging model using GPR as the base estimator stands out for its higher model construction time, reaching 93.19 s. As for stacking, the results show that the methods using parametric models have a model construction time of 1.1 s, indicating relatively low complexity. On the other hand, stacking using non-parametric models has model construction times ranging from 5.3 s to 8.08 s, which remains reasonable considering the more complex nature of these models.

TABLE X. ACCURACY MEASUREMENTS, NON-PARAMETRIC TESTS AND COMPLEXITY OF ENSEMBLE METHODS OF SERVER THREE

	R^2	MSE [wh]	MAE [wh]	RMSE [wh]	MAPE [%]	Wilcoxon rank-sum test	Model construction time [s]	Prediction time [s]
Boosting_Tree	**1.0**	**0.03**	**0.1**	**0.17**	**0.21**	**0.89**	**0.0637**	**0.2169**
Bagging_Poly	0.98	1.24	0.88	1.11	1.81	0.37	0.1585	0.0100
Bagging_Lasso	0.98	1.24	0.88	1.11	1.81	0.36	0.1902	0.0080
Bagging_Elastic	0.98	1.24	0.88	1.11	1.81	0.37	0.1912	0.0080
Bagging_SVR	1.0	0.06	0.16	0.24	0.31	0.9	6.2082	0.9499
Bagging_Tree	1.0	0.02	0.09	0.14	0.19	0.48	1.3107	0.0080
Bagging_Forest	1.0	0.03	0.1	0.17	0.2	0.45	3.8057	0.1723
Bagging_GPR	0.98	1.24	0.88	1.11	1.81	0.38	93.1952	0.3245
Stacking_Poly	0.98	1.24	0.88	1.11	1.8	0.38	1.1771	0.0
Stacking_Lasso	0.98	1.23	0.88	1.11	1.81	0.35	1.1857	0.0020
Stacking_Elastic	0.98	1.23	0.88	1.11	1.81	0.35	1.1792	0.0
Stacking_SVR	1.0	0.03	0.1	0.17	0.2	0.38	5.8112	0.0201
Stacking_Tree	1.0	0.02	0.09	0.14	0.19	0.67	5.3006	0.0182
Stacking_Forest	1.0	0.05	0.1	0.22	0.22	0.53	5.6406	0.2202
Stacking_GPR	1.0	0.03	0.11	0.17	0.21	0.68	7.6102	0.0302
Stacking_GPR_all	1.0	0.03	0.11	0.17	0.23	0.65	8.0803	0.0202

VII. RESULTS

This section provides an overview of the results obtained. For the first server, observations indicate that certain parametric methods, specifically polynomial regression, perform well in terms of prediction with low error rates and reduced complexity. However, other methods like Lasso regression and Elastic Network show high error rates exceeding five wh in terms of MSE for energy consumption prediction, while maintaining relatively low complexity. Among the non-parametric methods, SVR, decision trees, and random forests have low complexity and error rates for energy consumption prediction. However, GPR model provides prediction results with a high error rate and higher complexity compared to other methods. When it comes to ensemble methods, the boosting method trained with decision trees provides results very close to the actual values with low complexity. It is to highlight that models trained with parametric models have high MSE error rates but low complexity. Conversely, models trained with non-parametric methods like SVR, decision trees, and random forests as base estimators are considered the best models with construction complexity ranging from 0.15 s to 2.77 s. However, using the GPR base estimator in the bagging method significantly increases the MSE error rate up to 5.7 wh, and the model construction complexity reaches 57.47 s.

When using the stacking method, all models trained with parametric methods provide poor prediction results. On the other hand, models trained with non-parametric methods show optimal error rates. In conclusion, the recommended model for predicting the energy consumption of this server is the stacking model, using non-parametric or both parametric + non-parametric methods as estimators and trained with GPR as final estimator. The advantage of this method is that it combines multiple ML models and selects the optimal model to provide the best results. Furthermore, the complexity of this method is low. For example, although the GPR model provides poor prediction results when used alone, it can be used as the final estimator in the stacking model to improve the model's error rate and obtain optimal results.

For server two, it is remarkable that all models have a MSE lower than 0.17 wh. Among the parametric methods, polynomial regression and NN are characterized by their high performance. However, it should be noted that NN has considerable complexity due to their architecture and computational operations involved. Next, Lasso regression and Elastic Network, which exhibit average error rates and lower complexity. For non-parametric methods, the SVR model, decision trees, and random forests achieve a MSE of 0.02 wh, indicating good prediction performance. However, the GPR model has a higher error rate, suggesting poorer performance compared to other models. In terms of complexity, all methods are characterized by low complexity, making them efficient in terms of model construction and prediction time. The boosting method offers optimal prediction results with low complexity, as behave the bagging methods trained with non-parametric models such as SVR, decision trees, and random forests, as well as the stacking methods trained with non-parametric models. The recommended model for predicting energy consumption while maintaining a trade-off between complexity and error rate is the stacking model trained with non-parametric or mixed models. Regarding complexity, all proposed methods have low complexity, except the bagging model using the base estimator GPR, which has a model construction complexity of 9.18 s.

It is observed for the third server that high performing parametric methods with low error rates are polynomial regression and NN. However, the other two parametric methods reach a MSE of 1.23 wh, with a p-value of 0.35. It is important to note that for all three servers, NN are considered complex due to their architecture. Therefore, if new data is added to retrain the model, it may not be the optimal choice in terms of complexity, even though its performance may surpass some other models. As with server one and server two, non-parametric methods other than GPR provide optimal prediction, and the complexity of all methods is low. For ensemble methods, bagging_SVR, bagging_Tree, bagging_Forest, stacking_SVR, stacking_Tree, stacking_Forest, and stacking_GPR are considered optimal in terms of MSE, MAE, and MAPE. However, some models have low error rates while others have higher error rates, notably the stacking method using non-parametric methods as estimators, resulting in complexity reaching 7.61 s. Similar to server one and server two, bagging using GPR as base estimator stands out with a higher error rate and higher complexity of 93.19 s. Other models such as bagging and stacking trained with parametric models have a MSE error rate of 1.24 wh and low complexity. The best model for predicting energy consumption of this server while maintaining a balance between complexity and error rate is the Gradient Boosting model. The stacking method is characterized by a low error rate. However, the model construction complexity is higher compared to the Gradient Boosting model, reaching up to eight seconds. These observations allow us to better understand the relationship between different models and their respective complexity. They also highlight the importance of considering this complexity when choosing and evaluating models to find the right balance between performance and computational efficiency.

VIII. DISCUSSION

The variation in servers' energy consumption with workload execution is illustrated in Fig. 8, when CPU_workloads are executed on the first server, the CPU utilization rate reaches 94.5%, resulting in an increase in server energy consumption from 98.52 wh in idle state to 177.92 wh under load. On the other hand, when RAM_workloads are executed, energy consumption reaches 130.93 wh, while CPU utilization varies between 11.2% and 24.9%. Finally, when disk-based workloads are executed and write up to 11 290.35 MB on the disk, energy consumption reaches 125.84 wh, with RAM utilization varying between 24.33% and 71.17%, and CPU utilization varying between 12.5% and 24.2%. For server two, energy consumption ranges from 16 wh to 22.73 wh when CPU-intensive workloads are executed, with CPU utilization varying between 8.1% and 92.4%. When RAM-intensive workloads are executed, energy consumption reaches 20.32 wh, with RAM utilization varying from 26.38% to 78.29%. For disk-intensive workloads, energy consumption ranges from 16.99 wh to 18.75 wh, with CPU and RAM utilization rates ranging from 10.7% to 16.6% and 51.1% to 78.29% respectively, and data written to the disk reaching up to 18 064.42 MB. Regarding server three, energy consumption varies from 41.66 wh to 62.4 wh when executing workloads that

consume between 25.6% and 100% of the CPU. For workloads that vary RAM utilization between 40.12% and 68.21% and CPU utilization between 22.2% and 23.1%, energy consumption ranges from 40.77 wh to 42.25 wh. Launching workloads that consume the hard disk results in energy consumption ranging from 35.72 wh to 44.91 wh, with CPU utilization varying between 24.6% and 33.9%, and RAM utilization ranging from 42.74% to 49.56%, with data written to the disk reaching up to 4 393.99 MB.

Note that for all three servers, each parameter was carefully selected through experimentation. Experiments were conducted extensive testing on a range of values, choosing those that yielded the best results in terms of accuracy, complexity, and non-parametric test performance. Additionally, the same workloads were launched on the three servers, but each server handled them according to its architecture and capacity. For example, when a workload is launched on server *i*, it may complete successfully within the expected duration, while on another server, it may crash due to insufficient capacity to process and execute that workload. This explains why the number of data varies from one server to another.

The MSE, complexity, and p-value performance of the three servers are shown in Fig. 9. For the three servers, it was identified that the best models were polynomial regression, decision tree, boosting_Tree, and bagging_Tree. The outcomes demonstrate that the three servers' MSEs are all less than 0.7 wh, their complexities are all under 1.31 seconds, and their p-values range from 0.48 to 0.98. These findings show those models are useful for low computational complexity and high accuracy server energy consumption prediction. Because the models' predictions are statistically similar to the actual values, as confirmed by the high p-values, they can be effectively implemented to improve energy management and efficiency.

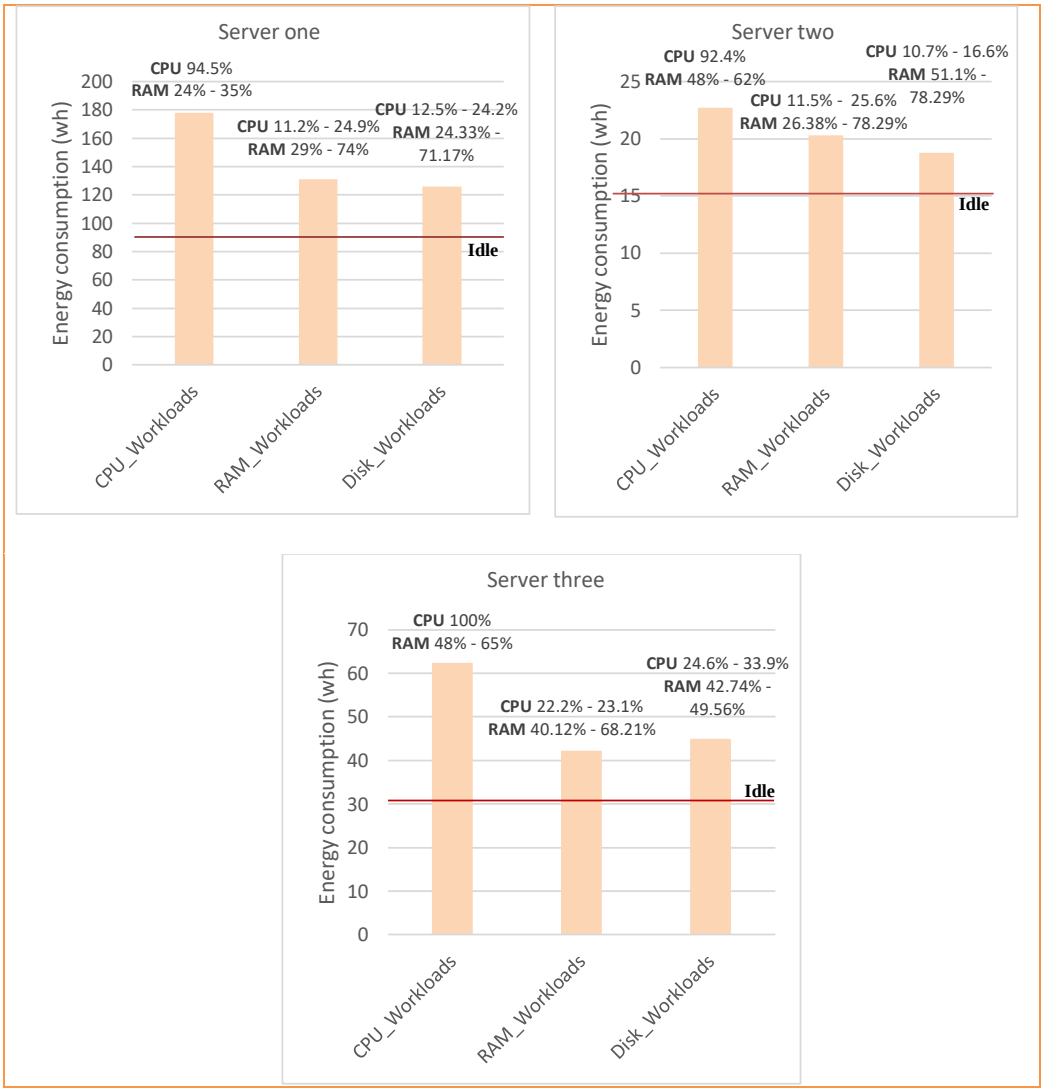


Fig. 8. Variation in servers energy consumption with workload execution.

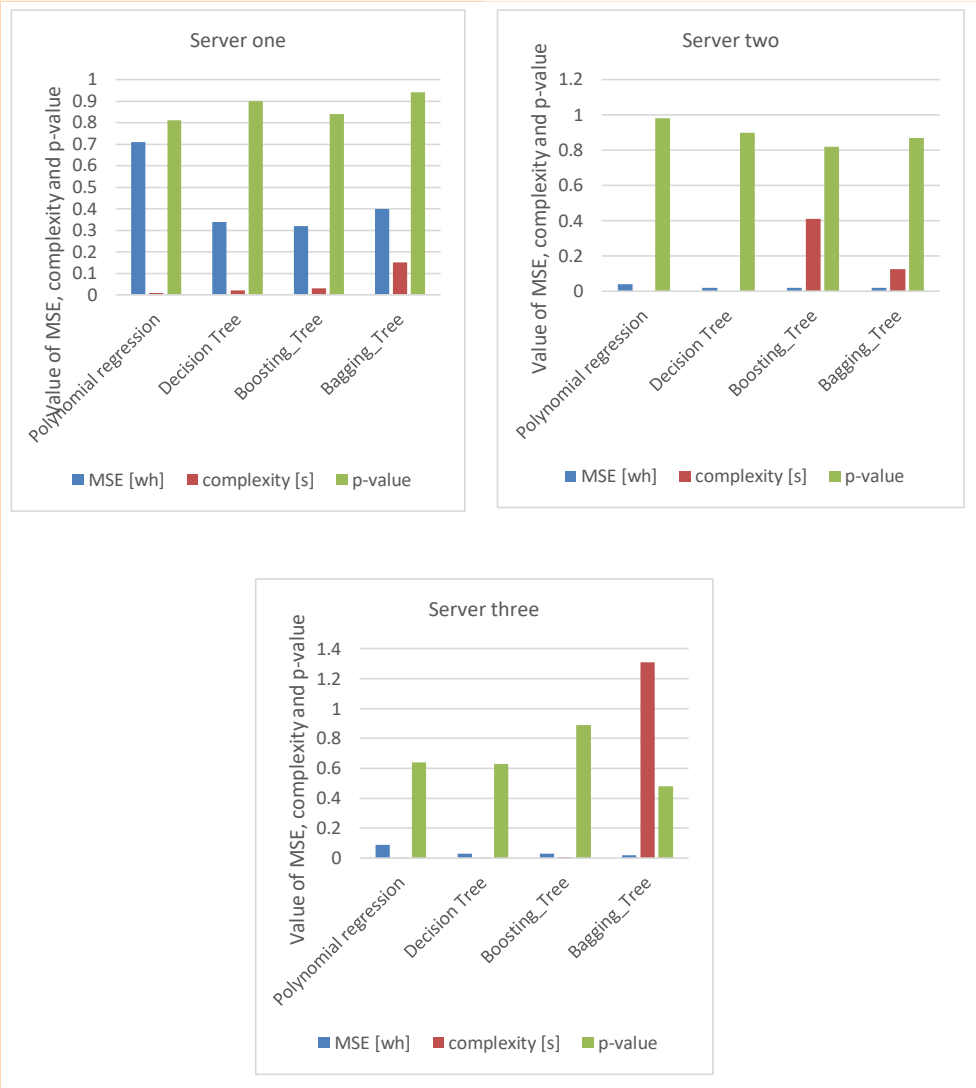


Fig. 9. Performance of the top models for the three servers.

Observation shows that for the three servers, certain methods are distinguished by low error rates and low complexity. These methods include polynomial regression belonging to parametric methods, as well as SVR, decision trees, and random forests belonging to non-parametric methods. Similarly, Boosting and Stacking with parametric models show good performance in terms of error rates. Other methods, such as Lasso regression, Elastic Network, GPR, and bagging using parametric models, have high error rates but low complexity. On the other hand, bagging methods using SVR, decision trees, and random forests, as well as Stacking with non-parametric models, are characterized by low error rates and moderate complexity. The worst results in terms of high error rates and high complexity are obtained with NN and bagging using GPR as the base estimator. Comparing the three servers, it is observed that each has a different energy consumption pattern. Server one consumes 2.85 times more energy than server three and 7.82 times more than server two. Server three, on the other hand, consumes 2.74 times more energy than server two. In this study, the complexity of the model was included as a critical factor for several reasons. For instance, after selecting a model that meets the requirements, it becomes crucial to assess its complexity. If the data center providers intend to retrain the model with additional data, understanding its complexity becomes paramount. If the complexity is high, retraining the model might not be advisable. However, if the complexity is manageable, this process can enhance the model's capability to accommodate new workloads, thereby improving its estimation accuracy. It should be highlighted that, to apply the elaborated algorithms to a real data center, it is highly recommended to use the data directly from the servers within that data center. In fact, the variability in workload characteristics influences the creation of ML models designed to predict server energy consumption. In this work, three types of servers were used to demonstrate the performance of ML models, as the type of servers may vary from one data center to another. This study aims to pinpoint the most effective models for estimating server energy usage, offering tailored recommendations for different server environments.

Predicting the future workload of servers in a data center is considered a challenging task because it is difficult to control or fully anticipate the clients' needs, as they are free to use or

consume resources according to the SLA. However, by analyzing historical server activity, patterns can be identified using various ML methods to estimate server workloads. In this study, the focus is placed on resources such as the CPU, RAM, and hard disk. Although users may request other types of resources, this study is limited to the resources. If the data center workloads shift in an irregular way and atypical manner, predictions can still be made by the proposed ML models. Besides, in this situation, it will be advised to use continuous learning, which will enable ML models to automatically update with current data and adjust over time to shifting workload patterns. Additionally, retraining the ML models on current data on a regular basis will keep them more accurate and relevant. Additionally, online learning has also the potential to be effective and enable the models to rapidly adapt to transient variations in workload.

IX. Conclusion

The choice of the appropriate method depends on the desired objectives. If the focus is on prediction quality in terms of error rates, the Stacking model, which uses the GPR model alongside other parametric and non-parametric models as internal estimators, is a good choice for predicting server energy consumption. However, if the objective is to regularly retrain the model by increasing the amount of data, it is preferable to choose a model that has both low error rates and reduced complexity. In this case, the polynomial regression model may be a good choice due to its architecture and computational requirements. It can be observed that for all three servers, the CPU consumes the most energy compared to the other resources, and the energy consumption when applying workloads that consume RAM and hard disk differs from one server to another. In this study, only CPU, RAM, and hard drive workloads are used as data to construct ML models to predict energy consumed by servers, while other types of workloads can also be handled within the data center. Also, in real data center, servers are placed in racks and installed in rooms equipped with other elements such as cooling system. However, the integration of cooling units and heat management are not elaborated in this work. Our future research will focus on exploring and refining anomaly detection in data centers as a critical frontier for ensuring the robustness and reliability of server systems by enabling the identification and mitigation of irregularities or unexpected patterns in energy consumption. Ultimately, the efforts in anomaly detection promise not only to improve system reliability, but also to facilitate more sustainable and resource-efficient operation of server networks.

Ethical Approval

As this research does not involve human participants or animals, ethical approval was not required for this study.

Competing interests

The research conducted in this article is primarily intended for academic and educational purposes.

Authors' contributions

Meryeme EL YADARI created the database, performed data analysis, conducted the experiments, and wrote the article.

Saloua EL MOTAKI contributed to this work by proposing ideas, reviewing the article, enhancing its content, and correcting the report.

Ali YAHYAOUY, and Khalid EL FAZAZY collaborated in this work by organizing meetings, where we discussed the work, provided valuable feedback, and made suggestions for content improvement.

Hamid GUALOUS provided the servers and all necessary materials for conducting the experiments, participated in the meetings, validating the work, and offering valuable remarks.

Stéphane LE MASSON actively engaged in discussions with the authors, providing insightful feedback to enhance the content of the work.

Funding

All the materials used in the experiment were provided by the University laboratory of applied sciences of Cherbourg (LUSAC).

Availability of Data and Materials

The database utilized in this work is internally developed and considered confidential; thus, there is no external link available for accessing it. The materials utilized in the experiment consist of three servers responsible for executing the tasks, one computer dedicated to data manipulation, and three wattmeters for measuring energy consumption.

References

[1] Robertazzi, Thomas. 2012. Data Centers. In Basics of Computer Networking, ed. Thomas Robertazzi, 69–72. SpringerBriefs in Electrical and Computer Engineering. New York, NY: Springer.

[2] Wang, Ting, Yu Xia, Jogesh Muppala, and Mounir Hamdi. 2018. Achieving Energy Efficiency in Data Centers Using an Artificial Intelligence Abstraction Model. IEEE Transactions on Cloud Computing 6: 612–624.

[3] Hasan, Zuhair. 2009. Redundancy for data centers. ASHRAE Journal 51. American Society of Heating, Refrigerating, and Air-Conditioning Engineers, Inc. (ASHRAE): 52–55.

[4] Lakshmi, Ganesh. 2012. Data center energy management. Faculty of the Graduate School of Cornell University: Cornell.

[5] Oró, Eduard, Victor Depoorter, Albert Garcia, and Jaume Salom. 2015. Energy efficiency and renewable energy integration in data centres. Strategies and modelling review. Renewable and Sustainable Energy Reviews 42: 429–445.

[6] Li, Munan, and Alan Porter. 2019. Can nanogenerators contribute to the global greening data centres? Nano Energy 60. https://doi.org/10.1016/j.nanoen.2019.03.046.

[7] El Yadari, Meryeme, Ali Yahyaouy, Khalid El Fazazy, Stéphane Le Masson, and Hamid Gualous. 2022. Placement methods of Virtual Machines in servers. In 2022 International Conference on Intelligent Systems and Computer Vision (ISCV), 1–7. Fez, Morocco. https://doi.org/10.1109/ISCV54655.2022.9806069.

[8] Baskaran, Nithiya, and Eswari R. 2021. Efficient VM Selection Strategies in Cloud Datacenter Using Fuzzy Soft Set. Journal of Organizational and End User Computing (JOEUC) 33. IGI Global: 153–179.

[9] Caviglione, Luca, Mauro Gaggero, Massimo Paolucci, and Roberto Ronco. 2021. Deep reinforcement learning for multi-objective placement of virtual machines in cloud datacenters. Soft Computing 25: 12569–12588.

[10] El Yadari Meryeme, Ali Yahyaouy, Stéphane Le Masson, Khalid El Fazazy, and Hamid Gualous. 2022. Study of the correlation between

server resources utilization and energy consumption. In , 6. Marseille, France: IEEE. https://doi.org/10.1109/ICSC57768.2022.9993950.

[11] Shen, Ziyu, Xusheng Zhang, Binghui Liu, Bin Xia, Zheng Liu, Yun Li, and Saiqin Long. 2019. PCP-2LSTM: Two Stacked LSTM-Based Prediction Model for Power Consumption in Data Centers. In 2019 Seventh International Conference on Advanced Cloud and Big Data (CBD), 13–18. Suzhou, China: IEEE.

[12] Reddi, Kamal Sandeeep, and Syam Kumar Pasupuleti. 2019. Optimal Energy aware Dynamic Virtual Machine consolidation in Cloud Data Centers. In 2019 IEEE 16th India Council International Conference (INDICON), 1–4. Rajkot, India: IEEE.

[13] Park, KyoungSoo, and Vivek S. Pai. 2006. CoMon: a mostly-scalable monitoring system for PlanetLab. ACM SIGOPS Operating Systems Review 40: 65–74.

[14] El Motaki Saloua, Ali Yahyaouy, and Hamid Gualous. 2022. Modeling the correlation between the workload and the power consumed by a server using stochastic and non-parametric approaches, June 13, John Wiley&Sons, Ltd edition.

[15] Elrotub, Mousa, and Abdelouahed Gherbi. 2018. Virtual Machine Classification-based Approach to Enhanced Workload Balancing for Cloud Computing Applications. Procedia Computer Science 130: 683–688.

[16] Orgerie, Anne-Cecile, Marcos Dias de Assuncao, and Laurent Lefevre. 2014. A survey on techniques for improving the energy efficiency of large-scale distributed systems. ACM Computing Surveys 46: 1–31.

[17] Arora, Sumedha, and Anju Bala. 2021. An intelligent energy efficient storage system for cloud based big data applications. Simulation Modelling Practice and Theory 108: 102260.

[18] Arora, Sumedha, and Anju Bala. 2021. An ensembled data frequency prediction based framework for fast processing using hybrid cache optimization. Journal of Ambient Intelligence and Humanized Computing 12: 285–301. https://doi.org/10.1007/s12652-020-01973-5.

[19] Alssaiari, Ali, and Nigel Thomas. 2020. Energy Consumption by Servers under Unknown Service Demand. Electronic Notes in Theoretical Computer Science 353: 21–38.

[20] Xiong, Wei, Bing Guo, and Shen Yan. 2022. Energy consumption optimization of processor scheduling for real-time embedded systems under the constraints of sequential relationship and reliability. Alexandria Engineering Journal 61: 73–80.

[21] Yavuz, Esra, and Mustafa Şahin. 2022. Investigation of Parametric, Non-Parametric and Semiparametric Methods in Regression Analysis. Sakarya University Journal of Science.

[22] Lakshmi, Mayur V., and Joab R. Winkler. 2024. Numerical properties of solutions of LASSO regression. Applied Numerical Mathematics. https://doi.org/10.1016/j.apnum.2024.03.010.

[23] Liu, Jingang, Xiaofeng Cao, Yilong Lei, and Jiayuan Zhang. 2023. The Application of Elastic Network Algorithm Based on Weighted Property in Clustering Analysis. IEEE Access 11: 136077–136090. https://doi.org/10.1109/ACCESS.2023.3335139.

[24] Junyan, Yi, and Du Xiaopeng. 2020. Elastic Network Algorithm for Clustering Based on Cluster Center Shift. In 2020 Chinese Control And Decision Conference (CCDC), 1971–1976. https://doi.org/10.1109/CCDC49329.2020.9164435.

[25] CFI, Team. 2020. Nonparametric Method. Corporate Finance Institute. June 30.

[26] Lutins, Evan. 2017. Ensemble Methods in Machine Learning: What are They and Why Use Them?

[27] AWS. 2023. Qu'est-ce que le boosting ? – Le boosting dans le cadre du machine learning expliqué – AWS. Amazon Web Services.

CQRS and Blockchain with Zero-Knowledge Proofs for Secure Multi-Agent Decision-Making

Ayman NAIT CHERIF[1]*, Mohamed YOUSSFI[2], Zakariae EN-NAIMANI[3],
Ahmed TADLAOUI[4], Maha SOULAMI[5], Omar BOUATTANE[6]
2IACS Laboratory, ENSET, Hassan II University, Casablanca, Morocco[1, 2, 4, 5]
EESS Laboratory, ENSET, Hassan II University, Casablanca, Morocco[3, 6]

***Abstract*—Autonomous decision-making in decentralized multi-agent systems (MAS) poses significant challenges related to security, scalability, and privacy. This paper introduces an innovative architecture that integrates Decentralized Identifiers (DIDs), Zero-Knowledge Proofs (ZKPs), Hyperledger Fabric blockchain, OAuth 2.0 authorization, and the Command Query Responsibility Segregation (CQRS) pattern to establish a secure, scalable, and privacy-focused framework for MAS. The use of DIDs and ZKPs ensures secure, self-sovereign identities and enables privacy-preserving interactions among autonomous agents. Hyperledger Fabric provides an immutable ledger, ensuring data integrity and facilitating transparent transaction processing through smart contracts. The CQRS pattern, combined with event sourcing, optimizes the system's ability to handle high volumes of read and write operations, enhancing performance and scalability. Practical applications are showcased in Smart Grids, Healthcare Data Management, Secure Internet of Things (IoT) Networks, and Supply Chain Management, highlighting the architecture's ability to address industry-specific challenges. This integration offers a robust solution for ensuring trust, verifiability, and scalability in distributed systems while preserving the confidentiality of agents.**

Keywords*—Decentralized multi-agent systems; decentralized identifiers; zero-knowledge proofs; hyperledger fabric; OAuth 2.0; CQRS; smart grids; healthcare data management; IoT; supply chain management

I. Introduction

In recent years, the rise of data-driven and compute-intensive applications has significantly increased the demand for scalable and decentralized systems capable of processing vast amounts of data in real-time. Multi-Agent Systems (MAS) have emerged as a robust solution for managing such complex environments. Comprising autonomous agents that collaborate to achieve common goals, MAS are integral to domains such as smart grids, supply chain management, and distributed computing, where they enable efficient, distributed decision-making [1]. However, these systems also introduce challenges related to security, scalability, and privacy [2]. Despite their potential, MAS face significant challenges in ensuring secure and private interactions among agents. Traditional security mechanisms, such as Public Key Infrastructure (PKI), are often inadequate for decentralized environments, leaving MAS vulnerable to attacks such as man-in-the-middle (MitM) and data breaches [3][4]. Additionally, the increasing need for privacy in distributed systems complicates interactions, particularly when sensitive data might be exposed during agent communication and transaction processing. These challenges lead to critical research questions: how can secure communication be ensured in MAS to prevent MitM attacks and maintain data integrity? What mechanisms can provide privacy-preserving capabilities in decentralized systems while maintaining scalability? How can blockchain and Zero-Knowledge Proofs (ZKP) be effectively integrated to address these challenges in MAS? To address these questions, the objectives of this research are to develop a secure and privacy-preserving framework for MAS to safeguard agent interactions, leverage blockchain technology for data integrity and decentralized processing, employ ZKP to enhance privacy while maintaining system scalability and security, and optimize real-time decision-making through the adoption of Command Query Responsibility Segregation (CQRS) principles in MAS.

Blockchain technology offers a promising solution to these challenges by providing decentralized, tamper-proof ledgers that enhance data integrity [5]. This approach is valuable in sectors like finance and logistics, where accountability and transparency are critical. The immutability of blockchain transactions ensures that once data is recorded, it cannot be altered, providing a verifiable record of actions. However, blockchain's transparency can also reveal sensitive information, creating further privacy challenges [6]. To address both security and privacy, this paper proposes a novel framework integrating CQRS, blockchain, and ZKP. CQRS, introduced by Greg Young, separates commands (write operations) from queries (read operations), optimizing system scalability, especially in high-volume environments like MAS that require real-time processing. While blockchain addresses data integrity, it does not inherently protect agent identities. Zero-Knowledge Proofs offer a solution by enabling agents to verify transaction authenticity without revealing the underlying data. Integrating ZKP with blockchain ensures that only authorized agents can execute transactions while maintaining anonymity [7]. Recent advancements in ZKP, including zk-SNARKs, have bolstered blockchain privacy, enabling privacy-preserving solutions for sectors such as healthcare, IoT, and decentralized finance [8][9].

This paper presents a comprehensive framework that integrates CQRS, blockchain, and ZKP to address critical challenges in MAS, including security, scalability, and privacy. It offers a theoretical analysis of the proposed architecture's features and demonstrates its real-world applicability in areas such as Smart Grids, Healthcare Data Management, Secure IoT Networks, and Supply Chain Management. Additionally, the framework's effectiveness is validated through comparisons with existing state-of-the-art solutions, highlighting its

contributions to the field. The remainder of the paper is organized as follows. Section II and Section III provide a detailed overview of the background and related work, highlighting the limitations of existing solutions. This is followed by a presentation of the proposed framework, describing its architecture and components in Section IV. Section V and Section VI analyze the framework's security, privacy, and scalability features, demonstrate its application in real-world scenarios, and discuss its performance. The paper concludes in Section VII with an outline of potential future work.

II. Related Work

The decentralized nature of Multi-Agent Systems (MAS) has led to their extensive use in distributed environments such as IoT networks, smart grids, and autonomous systems. MAS enable collaborative, autonomous decision-making but face critical challenges concerning security, scalability, and privacy. Numerous research efforts have been made to address these concerns, with a focus on authentication, data protection, and performance optimization through read/write operations.

A. Authentication and Authorization in MAS

Authentication is a cornerstone of MAS security, ensuring that agents are who they claim to be and that communications are protected. Traditionally, centralized methods like PKI have been used for authentication, but these introduce single points of failure and scalability issues [10]. Blockchain-based authentication mechanisms offer an alternative by leveraging decentralized smart contracts to eliminate trust intermediaries and prevent unauthorized access [11]. This decentralized approach is especially useful in environments where trust between agents cannot be guaranteed [12].

Despite these advancements, blockchain's high computational overhead for processing smart contracts poses challenges for real-time decision-making environments like IoT or smart grids. Moreover, these systems often lack fine-grained authorization mechanisms, which are crucial for handling multi-level access in dynamic, distributed environments. A solution to this problem, as proposed by He et al., involves a blockchain-based authentication scheme designed for mobile cloud computing, which introduces dynamic access control but struggles with resource efficiency [13].

B. Data Integrity and Privacy in Distributed MAS

In MAS, protecting data from tampering or loss is crucial. Blockchain's immutability and tamper-proof properties have been proposed as solutions to ensure data integrity [14]. Off-chain storage solutions, such as IPFS, have also been introduced to reduce on-chain storage costs, while still maintaining data integrity through cryptographic hashing. However, these systems face limitations, particularly when data stored off-chain is not protected by the same level of integrity as on-chain data.

Moreover, protecting data from loss due to network failures or agent disconnections is not adequately addressed in current off-chain storage models, which can lead to data tampering risks. To address these concerns, multi-copy data integrity auditing and batch auditing techniques in blockchain can help ensure that data availability and integrity are preserved, even in distributed environments [15].

Oliveira et al. [16] develop a modular MAS architecture for distributed data mining, effectively handling scalability but lacking stronger privacy mechanisms. Qasem et al. [17] also focus on MAS-integrated data mining, highlighting issues with data privacy and suggesting the need for secure communication protocols like ZKPs. Similarly, Nait Cherif et al [18] propose a blockchain-based solution for data integrity, though it requires significant computational resources, which may be alleviated by the CQRS-based system in this work. Ge et al. [19] survey advancements in distributed sampled-data cooperative control of MAS, emphasizing different sampling mechanisms to improve performance, yet these methods often lack real-time adaptability, posing a scalability bottleneck. In comparison, the CQRS pattern in this work supports high throughput by separating read and write operations, thus enhancing real-time performance under high loads.

C. Scalable Resource Management in Multi-Agent Systems

Efficient read/write operations are critical in distributed MAS, especially as the number of transactions scales. The CQRS pattern has been widely adopted to separate read and write operations, thereby optimizing system performance. This is particularly beneficial in high-volume transaction environments, where large amounts of data must be processed in real-time [20] [21].

However, while CQRS improves scalability, it does not inherently provide protection against man-in-the-middle (MitM) attacks or secure write operations, exposing the system to security threats [22]. Additionally, ensuring data consistency across distributed agents, especially in real-time applications, remains an unresolved issue, as CQRS alone does not guarantee that agents will have synchronized access to the latest data [23]

Dynamic and scalable MAS architectures benefit from integrating CQRS with blockchain technology. For example, Dashti et al. [24] introduce a MAS framework with dynamic agent capabilities but struggle with issues related to agent turnover. Our approach leverages blockchain for immutable tracking and secure data integrity, mitigating this issue. Similarly, Breugnot et al. [25] propose a distributed graph structure for load balancing in MAS but encounter challenges with data synchronization. By implementing CQRS in our framework, we enhance the synchronization process, enabling seamless data processing across distributed nodes.

Control and optimization are also central to MAS design, particularly in adversarial or resilience-focused settings. Wang [26] highlights the importance of distributed control but does not adequately address security against adversarial threats. In contrast, our approach integrates Decentralized Identifiers (DIDs) for secure agent identification and Zero-Knowledge Proofs (ZKPs) for verifiable, tamper-resistant interactions. This architecture not only improves resilience against data tampering but also maintains robust state management through CQRS, addressing challenges like those noted by Rust et al. [27] in state persistence across agents. Furthermore, Fanitabasi [28] discusses optimization in MAS under adversarial conditions, underscoring the need for resilience. By combining CQRS with

DIDs and ZKPs, our framework provides enhanced security and reduces vulnerabilities to malicious agents.

Lastly, transparency and secure communication in resource allocation are vital for MAS efficiency. Fu and Zhou [29] present a MAS solution for multi-project scheduling, although they struggle with transparency in resource allocation. Our framework addresses this by using blockchain to ensure verifiable transaction records, reducing information asymmetry. Additionally, Costa et al. [30] offer secure communication protocols that are limited in scalability under high agent loads. Leveraging CQRS, our architecture improves message throughput, enhancing secure, efficient communication across distributed systems.

D. Thesis for Improvement

Despite the progress made, several weaknesses in the current research need to be addressed:

- Scalability and Real-Time Challenges: Current blockchain-based authentication models suffer from scalability issues, as high computational costs limit their applicability in environments where real-time.
- Data Integrity for Off-Chain Storage: The reliance on off-chain storage solutions, such as IPFS, creates vulnerabilities in data tampering and data loss, as these systems lack the same level of cryptographic protection as on-chain storage.
- Privacy Concerns: While blockchain ensures data transparency, it falls short in protecting the privacy of agent interactions. Even with the use of Zero-Knowledge Proofs (ZKP), the high computational burden and the complexity of implementing ZKP protocols in large-scale systems make it difficult to achieve both privacy and performance.

This paper proposes a framework that combines CQRS, blockchain, zero-knowledge proofs (ZKP), and OAuth2 to address the limitations identified in existing solutions:

- Optimized Scalability: By enhancing ZKP protocols and integrating OAuth2 for efficient authentication, we reduce computational overhead and improve scalability, making the system suitable for high-frequency, real-time applications.
- Enhanced Data Protection: Utilizing blockchain's inherent immutability and tamper-proof properties, we ensure that all data remains secure and unaltered on-chain, eliminating the need for off-chain storage and its associated risks.
- Securing Write Operations: Through advanced cryptographic techniques and the integration of OAuth2 for secure authentication, we protect against man-in-the-middle attacks and ensure consistent data synchronization across distributed agents.

By addressing these gaps, our framework presents a more scalable, secure, and privacy-preserving solution for high-frequency, real-time multi-agent systems. This integration of advanced cryptographic methods and established design patterns offers a robust approach to the challenges facing MAS in complex, distributed environments.

III. BACKGROUND

In this section, we explore the foundational technologies and concepts that form the basis of the proposed framework: Multi-Agent Systems (MAS), Blockchain, Zero-Knowledge Proofs (ZKP), Command Query Responsibility Segregation (CQRS), Event-Driven Architecture (EDA), and OAuth 2.0. Together, these technologies address critical challenges like scalability, security, data integrity, and privacy in decentralized systems. Each concept builds upon the others to enhance the robustness and efficiency of MAS.

A. Multi-Agent Systems (MAS)

Multi-Agent Systems (MAS) consist of several autonomous agents working collaboratively or competitively to achieve objectives that are often too complex for a single agent or centralized system to handle. These agents interact with one another to solve problems in distributed environments, such as IoT networks, smart grids, and supply chain management. MAS are particularly effective in situations where decentralized decision-making is required, and the agents can operate independently to respond to changing conditions in real-time [31].

However, while MAS offer significant advantages in scalability and flexibility, they also introduce substantial challenges—most notably, ensuring secure communication and anonymity between agents. As agents in MAS frequently exchange sensitive information, protecting this data from unauthorized access or attacks becomes paramount. Traditional security measures often fall short in such decentralized environments, necessitating more advanced cryptographic techniques like Zero-Knowledge Proofs (ZKP). In this context, ZKP provides a solution that enhances both security and privacy within MAS by allowing authentication and access control without revealing underlying data, thereby ensuring secure and anonymous exchanges.

B. Event-Driven Architecture (EDA) and Event Sourcing

To enable more flexible and scalable interactions within MAS, many systems adopt an Event-Driven Architecture (EDA). Event-sourcing and event-driven architecture are two related but distinct concepts that are often used together in software systems. Event-driven architecture (EDA) is a design pattern that involves building a system in which different components communicate with each other by generating and reacting to events [32] (Fig. 1).

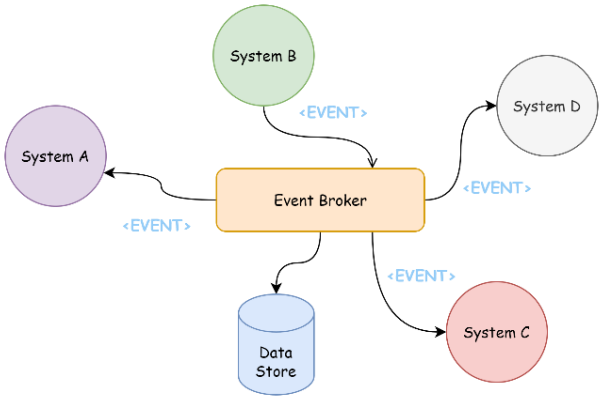


Fig. 1. Event driven architecture.

For example, when an agent in MAS detects a change in the environment or receives new data, it can trigger an event that other agents can subscribe to and react to as needed. This decoupling of event producers and consumers enables the system to scale more effectively and enhances its fault tolerance [33].

Closely related to EDA is Event Sourcing, which provides a mechanism to maintain a historical log of all state changes within the system. Rather than storing the current state of the system, event sourcing records every change as an event, allowing the system's state to be reconstructed by replaying these events in sequence. This feature is particularly useful in MAS for auditing, debugging, and recovering from failures. By integrating event sourcing with EDA, MAS can ensure that state changes are both traceable and resilient to failure [34].

The combination of EDA and Event Sourcing complements the scalability of MAS while providing a reliable mechanism to track and react to changes across distributed agents. However, while these architectures improve the system's flexibility, they do not address the security and data integrity challenges associated with state changes. This is where Blockchain plays a crucial role.

C. Command Query Responsibility Segregation (CQRS)

Building on the flexibility provided by EDA and event sourcing, Command Query Responsibility Segregation (CQRS) further enhances the scalability of MAS by separating read operations from write operations (Fig. 2).

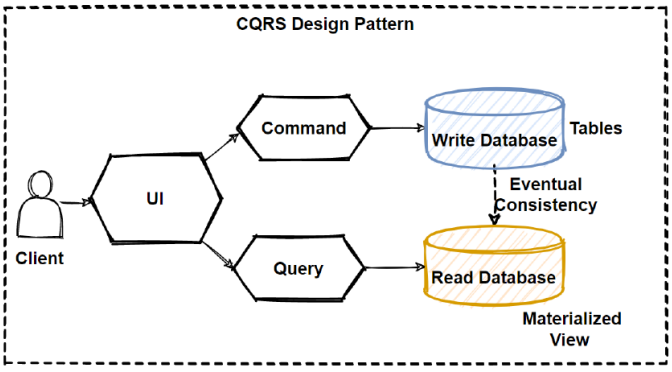


Fig. 2. CQRS design pattern.

In MAS, agents often need to perform a large number of both read (query) and write (command) operations to maintain and update the system state in real-time. By segregating these responsibilities, CQRS allows systems to scale independently for these two functions, optimizing system performance and reducing bottlenecks [35].

While CQRS improves the efficiency of MAS, particularly in high-transaction environments, it does not inherently provide security for write operations. Without adequate safeguards, the system remains vulnerable to tampering during state changes, which could lead to unauthorized alterations of critical data. At this point, Blockchain becomes essential for securing these write operations, as its tamper-proof ledger ensures that all changes to the system's state are immutably recorded and can be verified by all agents in the system [36].

The integration of CQRS with Blockchain strengthens the system's security, but it also introduces privacy concerns, particularly in public blockchains where data is visible to all participants. This necessitates the use of Zero-Knowledge Proofs (ZKP), which provide privacy-preserving mechanisms for MAS, ensuring that agents can interact securely without exposing sensitive information [37].

D. Blockchain Technology

Blockchain is a decentralized, distributed ledger that keeps a growing list of records called blocks. In a chain of blocks (hence the name "blockchain"), each block has multiple attributes including a timestamp, a link to the previous block, and its own data [38] (Fig. 3). Cryptographic techniques secure this chain of blocks, making it nearly impossible to alter its data. [38].

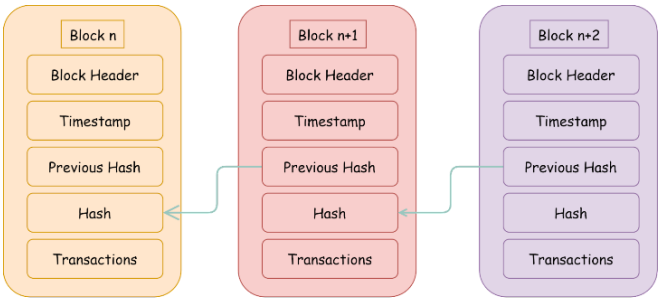


Fig. 3. Block structure.

Without the need for a centralized authority, transactions can be made using blockchain technology in a secure and transparent manner. Due to the distributed nature of blockchain data, it is virtually impossible for one entity to alter it without being detected. Because of this, blockchain technology is well suited for uses like supply chain management and financial transactions that demand a high level of transparency and trust [39]. In a typical blockchain system, transactions are initiated by users and are broadcast to the network. The integrity of these transactions is ensured by network nodes. A block is then added to the blockchain after a transaction has been verified and added to it [40].

However, while blockchain excels at maintaining data integrity and transparency, it introduces a new set of challenges regarding privacy. In a traditional blockchain system, transaction details are visible to all participants, which may not

be acceptable in scenarios where agents need to exchange sensitive data. To mitigate this issue, Zero-Knowledge Proofs (ZKP) are integrated with blockchain, allowing agents to prove that they have valid data or authorization without revealing the underlying information. This combination ensures that blockchain retains its transparency and security, while also protecting the privacy of the agents involved [41] [42].

E. Zero-Knowledge Proofs (ZKP)

Zero-Knowledge Proofs (ZKP) offer a solution to the privacy and anonymity concerns that arise in MAS when agents exchange sensitive information. It was initially brought forth in the 1980s by Shafi Goldwasser, Silvio Micali, and Charles Rackoff [43]. ZKP allows an agent to prove the validity of a claim (such as their identity or authorization) without revealing any additional details. This cryptographic technique is particularly valuable in blockchain-based MAS, where agents need to maintain both transparency and privacy during transactions.

The Zero-Knowledge Proof (ZKP) workflow, depicted in Fig. 4, illustrates the key phases of the ZKP process: setup, commitment, challenge, response, and verification. This workflow ensures that agents can authenticate their claims without revealing sensitive information, preserving both privacy and security.

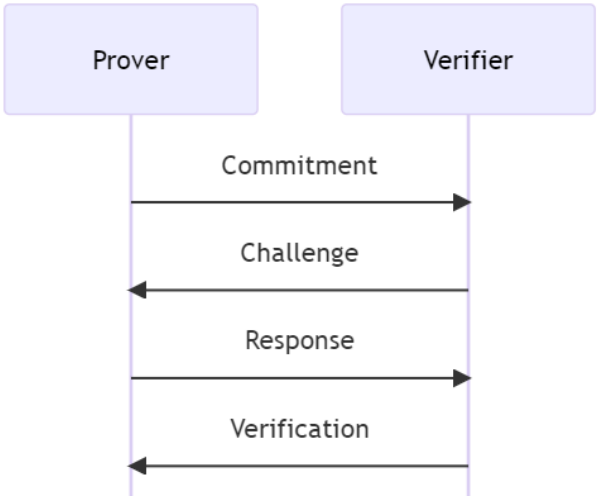


Fig. 4. ZNP workflow.

For instance, in a system where agents need to prove ownership of certain data or assets, ZKP enables them to authenticate their claims without exposing the data itself. This ensures that even as agents participate in a decentralized system like blockchain, they can retain their privacy, preventing sensitive information from being exposed to other participants [44]. However, implementing ZKP at scale presents computational challenges, as the process can be resource-intensive, making optimization a key area of research for large-scale MAS.

The benefits of ZKP in ensuring privacy and security are further enhanced when combined with OAuth 2.0, an authorization framework that allows controlled access to resources without exposing user credentials [18].

F. OAuth 2.0

OAuth 2.0 is an authorization framework widely used to secure access to resources by enabling third-party applications to interact with systems on behalf of users. In the context of MAS, OAuth 2.0 can manage access control, allowing agents to interact securely with external services without sharing their credentials directly. However, OAuth 2.0 alone does not guarantee anonymity, as it can still link access tokens to specific agents, potentially exposing their identities [45].

Fig. 5 demonstrates the OAuth 2.0 protocol flow, highlighting the interaction between agents, the authorization server, and the resource server. This process facilitates secure access token issuance and validation, ensuring controlled and authenticated access to system resources. The integration of OAuth 2.0 with ZKP in the proposed architecture further strengthens privacy by decoupling sensitive user credentials from access authorization.

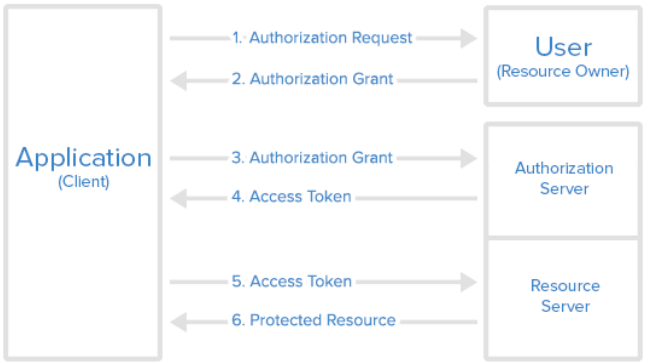


Fig. 5. OAuth 2 protocol flow.

To address this limitation, integrating ZKP with OAuth 2.0 provides a powerful solution for secure and anonymous resource access. By using ZKP to authenticate agents without revealing their identities, OAuth 2.0 can enable secure communication while preserving agent anonymity. This combination not only enhances the security of MAS but also ensures that agents can interact with external services without compromising their privacy.

The integration of OAuth 2.0 and ZKP represents a novel approach to solving the challenges of access control and privacy in MAS. This hybrid mechanism allows for secure data access while maintaining the anonymity of the agents, offering a robust solution to the security concerns present in distributed multi-agent systems [46].

IV. Proposed Architecture

The proposed architecture combines Command Query Responsibility Segregation (CQRS), blockchain, and Zero-Knowledge Proofs (ZKP) to address the core challenges of security, scalability, and privacy in Multi-Agent Systems (MAS).

Existing architectures often fall short in meeting these requirements due to their inherent limitations, such as inadequate privacy mechanisms, reliance on centralized infrastructures, and performance bottlenecks in high-volume environments.

Blockchain ensures data integrity through its immutable ledger, but its transparency can compromise sensitive information, highlighting the need for enhanced privacy measures.

To overcome this, the integration of ZKP enables secure agent authentication and transaction verification without exposing sensitive data, ensuring privacy-preserving interactions. CQRS further enhances the framework by segregating read and write operations, optimizing performance and scalability in real-time, high-demand scenarios.

Additionally, the architecture addresses vulnerabilities associated with centralized Public Key Infrastructure (PKI) by incorporating Decentralized Identifiers (DIDs), reducing single points of failure and enhancing system resilience. Unlike existing systems that struggle with consistent data synchronization and computational inefficiencies, the modular and interoperable design of the proposed framework ensures adaptability across diverse domains such as IoT, healthcare, and smart grids. This holistic integration of technologies provides a scalable, secure, and privacy-preserving solution tailored to the evolving demands of decentralized MAS.

A. Need for Enhancements in MAS Architecture

Understanding the limitations of traditional MAS architectures highlights the necessity for a paradigm shift. Addressing these challenges is crucial for developing systems that meet modern requirements.

The proposed architecture aims to:

- Eliminate Single Points of Failure: By decentralizing identity and access control mechanisms, the system enhances resilience and reduces dependency on any single component.
- Improve Scalability: Through asynchronous communication and efficient processing models like CQRS, the architecture supports the seamless addition of agents without compromising performance.
- Strengthen Security and Privacy: Using advanced cryptographic techniques, secure communication protocols, and privacy-preserving authentication methods, the system safeguards agent interactions.
- Ensure Data Integrity: Leveraging blockchain technology for immutable and verifiable data storage ensures that all agents have a consistent and trusted view of the system's state.

B. System Components and Architecture

1) Agent: Agents serve as autonomous entities within the decentralized system, representing unique participants such as users, services, or applications. Each agent is capable of performing actions, communicating with other agents, and managing its own state. The primary purpose of an agent is to interact seamlessly within the network. Functionally, agents handle identity management by generating and managing cryptographic key pairs and Decentralized Identifiers (DIDs). They utilize Zero-Knowledge Proofs (ZKP) and OAuth 2.0 tokens for authenticating and authorizing interactions. Communication between agents is secured through encrypted and signed messages transmitted via Hyperledger Fabric channels. Agents manage their state by executing commands that alter their state and recording corresponding events on the blockchain. Additionally, they can reconstruct their internal state by replaying events from the blockchain, using snapshotting techniques for efficiency. In terms of interactions, agents communicate with other agents through secure channels, interact with the Decentralized Discovery Facility (DDF) for agent discovery, and submit and retrieve events from the blockchain for state management.

2) Decentralized Identifier (DID) and DID document: DIDs provide a decentralized and self-sovereign identity framework for agents, enabling secure and verifiable interactions without relying on centralized authorities. Agents generate unique DIDs following standardized specifications, such as Hyperledger-compatible DID methods. Each DID is associated with a DID Document, which contains public keys, authentication methods, and service endpoints. These documents are published on the blockchain for public reference, facilitating secure communication and verification among agents. DIDs are shared among agents during interactions, utilized during registration with the Decentralized Discovery Facility (DDF), and play a crucial role in authentication processes.

3) Zero-Knowledge Proofs (ZKP) processing service: The ZKP Processing Service enhances privacy and security by enabling agents to prove possession of certain information, such as ownership of a DID, without revealing the information itself. This service assists agents in generating ZKPs to demonstrate control over their private keys and DIDs. It facilitates the various phases of the ZKP protocol, including setup, commitment, challenge, response, and verification. The service collaborates with agents during registration and authentication processes and interfaces with the Authorization Server during the issuance of OAuth 2.0 tokens.

4) Decentralized Discovery Facility (DDF): The DDF acts as a decentralized registry and discovery service, allowing agents to locate and interact with other agents and their services within the network. It handles the registration of agent DIDs and associated metadata after verifying ZKPs. The discovery functionality provides searchable access to registered agents and their services, enabling agents to find peers and available functionalities efficiently. The DDF receives registrations from agents along with their ZKPs and DID Documents and responds to discovery queries from agents seeking information about other participants.

5) OAuth 2.0 authorization server: The OAuth 2.0 Authorization Server is responsible for managing the issuance and validation of access tokens, thereby facilitating secure authorization for agents to access resources and communication channels within the system. It processes OAuth 2.0 authorization requests from agents, incorporating DIDs and ZKP commitments. Upon successful verification of ZKPs and issuance of authorization codes, the server generates JWT

access tokens. It also validates incoming tokens during resource access requests to ensure their authenticity and permissions. The Authorization Server interacts with agents during the token issuance process and interfaces with Resource Servers to validate access tokens presented by agents.

Fig. 6 presents the high-level interaction among components within the proposed architecture. It illustrates the communication flow between agents, the Decentralized Discovery Facility (DDF), blockchain, and resource servers. This diagram emphasizes how the architecture integrates multiple technologies to ensure seamless operation, secure agent authentication, and efficient resource management.

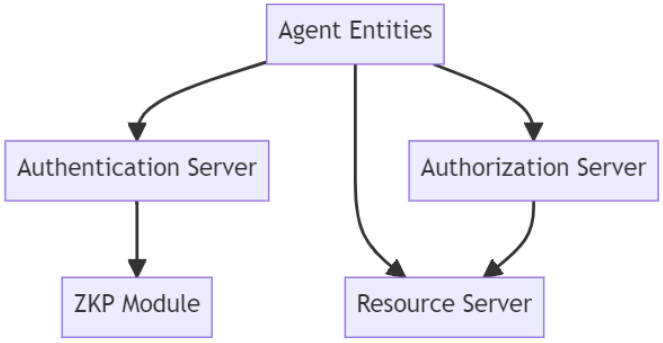


Fig. 6. Component interaction.

6) Hyperledger fabric network: The Hyperledger Fabric Network provides a permissioned blockchain infrastructure that ensures secure, immutable, and scalable communication and state management among agents. It utilizes private communication channels designated for specific groups of agents or types of interactions. The network comprises peers, which are nodes that host the ledger and execute smart contracts (chaincode), maintaining the blockchain's state, and orderers, which are nodes responsible for ordering transactions into blocks to ensure consistency and reliability across the network. Subcomponents include smart contracts that define the business logic for processing transactions, handling commands, and managing state changes, as well as the ledger, which serves as an immutable record of all transactions and events, ensuring data integrity and transparency. The Hyperledger Fabric Network facilitates message exchange between agents through its channels, records state-changing events submitted by agents to ensure immutability and verifiability and provides a reliable ledger for agents to reconstruct their state through event sourcing.

7) Resource servers: Resource Servers host protected resources such as data stores, computation services, or external APIs, and enforce access controls based on OAuth 2.0 tokens. They handle resource requests from agents seeking access to these protected resources by receiving and processing these requests. The servers validate the authenticity, validity, and permissions of JWT access tokens included in resource requests. Based on the validated tokens and associated permissions, Resource Servers grant or deny access to the requested resources. They communicate with the Authorization Server to validate access tokens and interact with agents to provide access to requested resources upon successful validation.

8) Command Query Responsibility Segregation (CQRS) components: The CQRS Components enhance system performance and scalability by separating read and write operations, allowing independent optimization of data handling. Command Handlers process state-changing commands submitted by agents, invoking smart contracts to record events on the blockchain. Query Handlers manage read operations by accessing optimized, separate data stores that provide quick and efficient data retrieval. An Event Store maintains a log of all events generated by command executions, enabling state reconstruction and auditability. These components receive commands from agents via Fabric channels, update read models based on events recorded in the blockchain, and support agents in querying the current state without interference from write operations.

9) Hardware Security Modules (HSMs): Hardware Security Modules (HSMs) are critical for securely storing cryptographic keys and performing sensitive operations, thereby protecting against unauthorized access and tampering. They safeguard private keys used by agents for signing messages and events, ensuring that these keys are never exposed in plaintext. HSMs execute cryptographic functions within a protected environment, maintaining the integrity and confidentiality of keys. Agents utilize HSMs to securely manage their cryptographic materials, and HSMs integrate with the DID generation and signing processes to ensure the security and trustworthiness of cryptographic operations within the system.

The integration of these components results in an architecture that significantly enhances the security, scalability, and privacy of Multi-Agent Systems. By addressing the limitations of traditional approaches through decentralized identity management, secure communication protocols, optimized processing models, blockchain integration, advanced cryptographic techniques like ZKP combined with OAuth, and decentralized access control mechanisms, agents can interact in a trustworthy and efficient manner. The proposed architecture lays a robust foundation for developing MAS that are resilient, scalable, and capable of meeting the complex demands of modern distributed environments.

C. Detailed Workflow from Agent Authentication to Message Exchange

1) Agent initialization and DID generation: When an agent joins the system, it begins by generating a public-private key pair. This key pair is fundamental to the agent's cryptographic identity, enabling secure communication and authentication within the network. To ensure the private key remains secure, the agent stores it in a Hardware Security Module (HSM) or a Trusted Execution Environment (TEE). These storage solutions protect the key from unauthorized access and tampering.

Next, the agent creates a Decentralized Identifier (DID) following standard specifications, such as those compatible with Hyperledger. This DID represent a unique, self-sovereign identity that operates independently of any centralized authority. By generating multiple DIDs, the agent enhances its privacy and minimizes the risk of being tracked across different interactions.

The agent then constructs a DID Document, which includes its public keys and service endpoints. This document is published on the blockchain, making the agent's identity accessible to other agents within the network. The DID Document serves as a public reference, describing the agent's DID and associated metadata to facilitate secure and verifiable interactions. This initialization process ensures that the agent maintains full control over its identity, promotes interoperability through standardized identification formats, and establishes a secure foundation for decentralized interactions.

2) Registration with Decentralized Discovery Facility (DDF) using Zero-Knowledge Proofs (ZKP): To register with the Decentralized Discovery Facility (DDF), an agent must prove ownership of its DID without revealing its private key. This is achieved using Zero-Knowledge Proofs (ZKP). The agent collaborates with a ZKP Processing Service to generate a proof that demonstrates control over its private key in a way that preserves confidentiality.

The ZKP process involves several key steps:

- Setup Phase: Public parameters are defined, including a large prime number p, a generator g, and a derived parameter h (1), where s is the agent's secret.
- Commitment: The agent selects a random nonce r and computes the commitment C (2), binding itself to the secret without revealing it.
- Challenge: The verifier issues a random challenge C to the agent.
- Response: The agent calculates z (3), proving knowledge of the secret without disclosing it.
- Verification: The verifier checks (4). If the equality holds, the verifier is convinced that the agent knows the secret without learning its value.

$$h = g^s mod\ p \quad (1)$$

$$C = g^r mod\ p \quad (2)$$

$$z = r + c.s\ mod\ (p-1) \quad (3)$$

$$g^z\ mod\ p = C.h^c\ mod\ p \quad (4)$$

After successfully generating the ZKP, the agent submits its DID Document along with the ZKP to the DDF via smart contracts. The DDF verifies the proof and records the successful registration on the blockchain. This process ensures that only legitimate agents can register, maintaining the integrity and security of the decentralized system.

3) Agent discovery: When an agent wants to discover other agents and their services, it queries the DDF for information about other agents' DIDs and available services. This querying process facilitates collaboration and the utilization of services within the network. Importantly, agents have the option to selectively disclose specific attributes or services, allowing them to control the information they share and protect sensitive data. By enabling discovery while preserving privacy, the system fosters collaboration among agents without compromising their autonomy or exposing unnecessary information.

4) Token issuance with OAuth 2.0 including DIDs: After successfully registering and authenticating, an agent can obtain an access token through the OAuth 2.0 protocol, which includes its DID. The issuance of tokens is a critical component for several reasons. Firstly, tokens provide a secure and standardized method for managing permissions and access controls within the decentralized system.

By issuing tokens that encapsulate DIDs, the system ensures that agents can be reliably identified and granted specific permissions to access various resources without the need for repeated authentication processes. This streamlines access management, reduces the overhead associated with continuous verification, and enhances overall system security by limiting the exposure of sensitive information.

The token issuance process begins with the agent preparing an OAuth 2.0 authorization request, incorporating its DID and ZKP commitment. The Authorization Server then issues a challenge C, and the agent responds with (3) , adhering to the ZKP protocol.

Upon verifying the ZKP, the server issues an authorization code, which the agent exchanges for a JWT access token containing its DID and permissions. This integration of OAuth 2.0 with ZKP ensures a secure and standardized method for managing permissions, allowing reliable agent identification without exposing sensitive information.

The integration of Zero-Knowledge Proofs (ZKP) and OAuth 2.0 is depicted in Fig. 7. This diagram shows how ZKP enhances the OAuth 2.0 authorization process by enabling agents to authenticate their interactions without revealing sensitive data. The secure issuance of access tokens, combined with privacy-preserving proof mechanisms, reinforces the system's security and ensures robust resource access control.

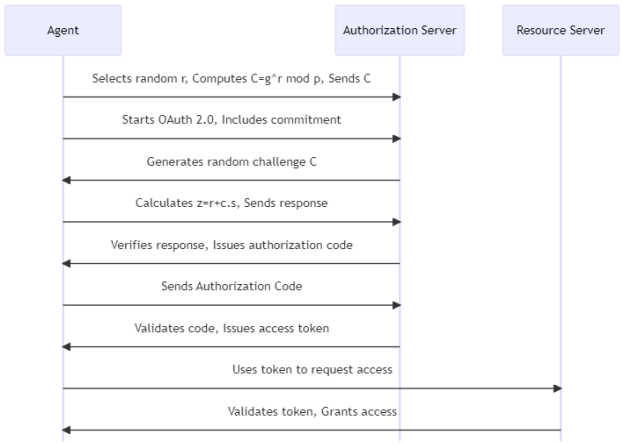


Fig. 7. ZKP and OAuth 2 flow.

5) Resource access and verification using DIDs: When an agent needs to access protected resources, it presents its JWT access token containing its DID in the resource request, typically within the Authorization header as a Bearer token. The resource server then validates the token's signature, ensures it has not expired, checks the scopes, and verifies the agent's DID. If the token is valid and the agent possesses the necessary permissions, the resource server grants access to the requested resources. This mechanism ensures that resource access is secure and controlled, leveraging DIDs for reliable identification and OAuth 2.0 for robust authorization management.

6) Agent communication, data sharing, and state management workflow: If an agent wants to send a message to other agents or read messages, it utilizes Hyperledger Fabric channels alongside the Command Query Responsibility Segregation (CQRS) pattern to ensure efficient and secure communication and state management. The agent begins by authenticating using ZKP during registration and obtaining OAuth 2.0 access tokens, which grant it permissions to interact with specific Fabric channels designated for communication.

Fig. 8 illustrates the detailed workflow for agent communication, data sharing, and state management within the architecture. By leveraging Hyperledger Fabric channels and the CQRS pattern, the diagram demonstrates how agents efficiently interact and manage their states while ensuring data integrity and consistency. This flow is critical for maintaining real-time performance and scalability in high-demand applications.

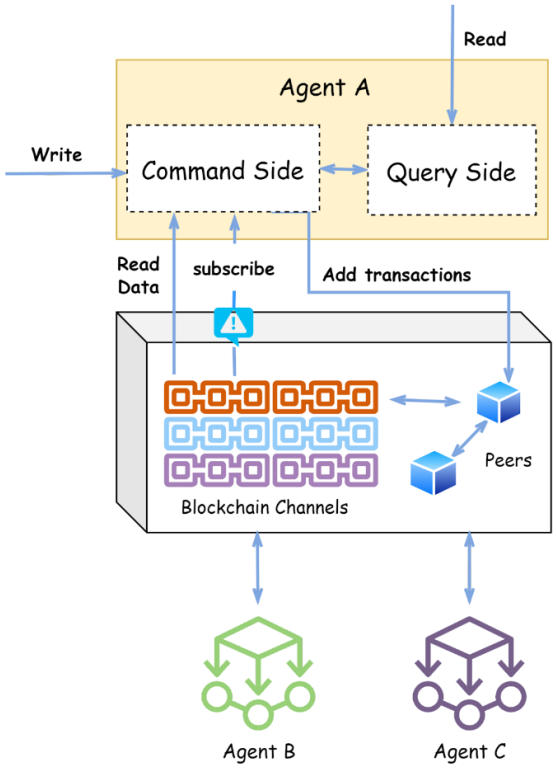


Fig. 8. Agent communication, data sharing, and state management workflow.

a) Sending a message: To send a message, the agent connects to the appropriate Fabric channel using its access token. It encrypts the message content with the recipient's public key and signs the message with its private key to ensure confidentiality and authenticity. The message, along with relevant metadata, is then published to the Fabric channel, where the blockchain handles routing based on the message's metadata and the channel's configuration.

b) Receiving a message: Receiving agents connect to the relevant Fabric channels using their access tokens, subscribe to specific channels, and asynchronously receive messages. Upon receiving a message, the agent verifies the signature using the sender's public key from the DID Document and decrypts the content using its private key. The message is then processed according to the agent's business logic.

c) Event recording and state management: When an agent executes a command that changes its state, it generates an event representing that change. The event includes details such as the event type (e.g., "OrderPlaced", "BalanceUpdated"), a timestamp recording when the event occurred, a data payload containing relevant information, and metadata like causation ID, correlation ID, or version. To ensure authenticity and prevent tampering, the agent signs the event with its private key.

The signed event is then packaged into a transaction proposal and submitted to the blockchain network. This involves creating and signing a transaction proposal that reflects the internal state changes in the form of an event. The proposal is sent to the network for validation and inclusion in the blockchain. Blockchain nodes, or peers, validate the transaction proposal by ensuring proper formatting, verifying the agent's signature, and performing authorization checks to confirm that the agent has the rights to perform the action represented by the event.

Once validated, the ordering service sequences the transactions and packages them into blocks. These blocks are then disseminated across the network and added to each node's copy of the blockchain ledger, making the event part of the immutable history of the system.

d) State reconstruction: To maintain data integrity and enable agents to recover their state independently, the system employs event sourcing and blockchain integration. When an agent needs to reconstruct its internal state, it retrieves the sequence of relevant events from the blockchain and replays them in chronological order. This process ensures that the agent's state is consistent with the system's history. For efficiency, agents may use snapshotting, creating snapshots of their state after processing a certain number of events. Future state reconstructions can begin from the latest snapshot and replay only subsequent events, ensuring consistency and integrity with the system's history.

This integrated approach ensures that communication is secure and efficient while maintaining data integrity and providing a reliable audit trail through event sourcing.

7) Conclusion: This comprehensive workflow integrates decentralized identity management, secure authentication, scalable communication, and robust data integrity mechanisms.

By leveraging Zero-Knowledge Proofs, Decentralized Identifiers, Hyperledger Fabric, OAuth 2.0, and the CQRS pattern, the system ensures that agents can interact securely, efficiently, and privately within a decentralized multi-agent environment.

Security and privacy are maintained throughout the workflow using advanced cryptographic techniques. Zero-Knowledge Proofs and OAuth 2.0 provide robust authentication and authorization without exposing sensitive information. Blockchain technology ensures data integrity by offering immutable and tamper-proof storage of events and identities, while encryption safeguards data both in transit and at rest. The CQRS pattern and event sourcing facilitate efficient state management and fault tolerance, allowing agents to recovertheir state independently by replaying blockchain-recorded events.

The system's design supports scalability and performance through asynchronous communication and the segregation of read and write operations. This allows the network to handle high transaction volumes and numerous agents efficiently. Additionally, the use of standardized protocols and identifiers promotes interoperability, enabling seamless integration with external systems. Compliance and auditability are achieved through transparent and immutable records on the blockchain, facilitating regulatory adherence and providing comprehensive audit trails for accountability and governance.

D. Additional Security Measures

To ensure the integrity, confidentiality, and availability of its components, the system incorporates robust security measures. These measures cover key management, smart contract security, and comprehensive monitoring and incident response protocols.

1) Key management and credential security: Key management protocols are designed to safeguard cryptographic keys, ensuring that only authorized entities can perform sensitive operations within the system.

a) Secure storage:

- Hardware Security Modules (HSMs) and Trusted Execution Environments (TEEs): Private keys are securely stored within HSMs, preventing unauthorized access and extraction. These modules offer physical and logical protections against theft, tampering, and malware attacks.
- Access Controls: Strict access control policies are in place, with role-based access controls (RBAC) ensuring that only authorized personnel and processes can access sensitive keys.

b) Key rotation and revocation:

- Regular Key Rotation: Keys are rotated periodically to minimize exposure risk. Upon rotation, new keys are generated, and corresponding DID Documents are promptly updated on the blockchain.
- Immediate Revocation: Protocols are established for rapid key revocation in case of a suspected compromise. All agents are ensured access to the latest DID Documents to verify key validity and prevent the use of revoked keys.

c) Access control policies:

- Least Privilege Principle: Agents and users are granted only the permissions necessary to perform their roles, reducing the attack surface.
- Segregation of Duties: Responsibilities are divided among different agents to prevent conflicts of interest and limit the impact of compromised credentials.

2) Smart contract security: Smart contracts are rigorously secured to prevent vulnerabilities that could lead to financial losses or unauthorized state changes.

a) Development best practices:

- Secure Coding Standards: Smart contracts adhere to established coding standards to prevent common vulnerabilities, with regular updates based on the latest security research.
- Use of Established Libraries: Trusted libraries and frameworks are used to minimize the risk of bugs and vulnerabilities.
- Modular Design: Smart contracts are structured into smaller, manageable modules for easier analysis, testing, and maintenance.
- Independent Security Audits: Third-party security experts conduct comprehensive reviews of smart contract code to identify vulnerabilities and verify implemented security measures.

b) Continuous testing: Automated testing pipelines with unit tests, integration tests, and fuzz testing are implemented to identify vulnerabilities early.

c) Upgradability and governance:

- Secure Upgrade Paths: Smart contracts include upgradeable patterns to allow controlled updates when necessary, with mechanisms in place to prevent unauthorized modifications.
- Governance Mechanisms: Clear governance processes are established for smart contract changes, involving relevant stakeholders to ensure transparency and collective decision-making.

3) Monitoring and incident response: Continuous monitoring and incident response protocols are established to detect and address security breaches promptly, ensuring system resilience.

a) Continuous monitoring:

- Intrusion Detection Systems (IDS): IDS monitors network traffic and system logs for signs of unauthorized access or malicious activities, using both signature-based and anomaly-based detection.
- Logging and Alerts: Comprehensive logs of system activities are maintained, with real-time alerting mechanisms to notify administrators of critical events.

b) Threat Intelligence and Updates

- Stay Informed: The system stays updated on emerging threats through security advisories and threat intelligence feeds.
- Patch Management: Security patches and updates are applied promptly based on vulnerability severity and potential system impact.

V. Security, Scalability and Performance Analysis

Ensuring that a decentralized multi-agent system operates securely, scales efficiently, and maintains high performance is paramount for its success and reliability. This analysis delves into how the system's architecture and components collectively achieve these objectives, highlighting strengths, potential challenges, and the interplay between different system aspects.

A. Security Analysis

1) Comprehensive security framework: The system employs a multi-layered security approach, integrating advanced cryptographic techniques, secure authentication and authorization protocols, and robust key management practices. By leveraging Zero-Knowledge Proofs (ZKP) and Decentralized Identifiers (DIDs), agents can authenticate and authorize interactions without exposing sensitive information, significantly reducing the risk of credential theft and unauthorized access.

2) Immutable ledger and data integrity: Hyperledger Fabric's blockchain infrastructure ensures that all transactions and state changes are immutably recorded, providing a tamper-proof audit trail. Digital signatures and secure storage mechanisms (HSMs/TEEs) further reinforce data integrity and authenticity, ensuring that only authorized agents can perform state-altering actions.

3) Smart contract security: Adhering to secure coding standards, utilizing established libraries, and implementing formal verification and independent audits fortify smart contracts against common vulnerabilities. The incorporation of modular design and secure upgrade paths allows the system to adapt and evolve without compromising security, addressing potential threats proactively.

4) Proactive threat detection and incident response: Continuous monitoring through Intrusion Detection Systems (IDS) and anomaly detection algorithms enables real-time identification of suspicious activities. A well-defined incident response plan ensures that the system can swiftly contain and mitigate threats, minimizing potential damage and maintaining operational integrity.

5) Privacy preservation: By enabling selective disclosure and employing encryption for all data exchanges, the system upholds strong privacy guarantees. Agents maintain control over their personal information, and the use of multiple DIDs prevents tracking and profiling, aligning with privacy-by-design principles and regulatory requirements.

B. Scalability Analysis

1) Command Query Responsibility Segregation (CQRS) pattern: The implementation of the CQRS pattern effectively separates read and write operations, allowing each to be optimized independently. This segregation reduces contention and enhances system throughput, enabling the system to handle a high volume of transactions and queries without performance degradation.

2) Asynchronous communication via hyperledger fabric channels: Hyperledger Fabric channels facilitate parallel and isolated communication pathways, allowing multiple groups of agents to interact concurrently without interference. This design supports horizontal scaling, as additional channels can be created to accommodate growing numbers of agents and diverse interaction requirements.

3) Event sourcing and snapshotting: Event sourcing records all state changes as discrete events, enabling efficient state reconstruction and facilitating scalability. Snapshotting further enhances performance by allowing agents to rebuild their state from recent snapshots rather than processing an extensive event history, reducing computational overhead and speeding up state initialization.

4) Distributed ledger technology: The decentralized nature of Hyperledger Fabric allows the system to scale horizontally by adding more nodes to the network. This distribution enhances fault tolerance and load balancing, ensuring that the system remains resilient and performs consistently as it grows.

5) Optimized data stores for read operations: By maintaining separate, optimized data stores for read queries, the system ensures that read-heavy operations do not impede write performance. This optimization is crucial for maintaining low latency and high availability, especially as the number of agents and interactions increases.

C. Performance Analysis

1) High throughput and low latency: The system is designed to handle a substantial number of transactions per second (TPS) with minimal latency. Hyperledger Fabric's consensus mechanisms and efficient transaction ordering services contribute to maintaining high throughput, while the use of CQRS and optimized data stores ensures rapid data retrieval and processing.

2) Efficient state management: Event sourcing, combined with snapshotting, allows for swift state reconstruction and reduces the time required for agents to initialize or recover their state. This efficiency is vital for maintaining real-time responsiveness and ensuring that agents can operate seamlessly, even under heavy load.

3) Resource optimization: The segregation of read and write operations, along with asynchronous communication channels, ensures optimal utilization of system resources. By distributing workloads effectively and minimizing bottlenecks, the system maintains consistent performance levels regardless of scaling demands.

4) Resilience and fault tolerance: The decentralized architecture and immutable ledger ensure that the system remains operational even in the face of individual node failures or attacks. Redundant data storage and distributed consensus

protocols contribute to the system's ability to recover quickly and maintain performance standards during adverse conditions.

5) Continuous improvement and adaptability: The system's architecture allows for continuous optimization and scaling without necessitating significant overhauls. The modular design of smart contracts, combined with secure upgrade paths, enables the integration of performance enhancements and new features, ensuring that the system can evolve in response to changing demands and technological advancements.

D. Trade-offs and Considerations

1) Complexity vs. security and scalability: While the system's advanced security measures and scalable architecture provide significant benefits, they also introduce additional complexity. Managing multiple DIDs, implementing ZKP, and maintaining a distributed ledger require sophisticated infrastructure and expertise, potentially increasing the initial setup and maintenance overhead.

2) Resource consumption: The use of encryption, secure storage mechanisms, and continuous monitoring can lead to increased resource consumption. Balancing security and performance with resource efficiency is essential to ensure that the system remains cost-effective and sustainable as it scales.

3) Latency in event processing: Although event sourcing and snapshotting enhance state management efficiency, there can be inherent latency in processing and recording events on the blockchain. Optimizing transaction throughput and implementing efficient event handling protocols are necessary to minimize delays and maintain real-time responsiveness.

4) Governance and upgrade management: Ensuring secure and controlled upgrades to smart contracts and system components is crucial for maintaining system integrity. Establishing robust governance mechanisms and clear procedures for implementing changes helps mitigate the risks associated with upgrades but requires ongoing coordination and management.

E. Conclusion

The system's architecture robustly addresses critical aspects of security, scalability, and performance through the integration of advanced technologies and best practices. By leveraging Hyperledger Fabric's decentralized ledger, employing the CQRS pattern for efficient state management, and implementing comprehensive security measures, the system ensures secure, scalable, and high-performing operations.

While the system presents inherent complexities and resource demands, these are outweighed by the substantial benefits of enhanced security, efficient scalability, and reliable performance. Continuous monitoring, proactive incident response, and adaptable governance frameworks further strengthen the system's resilience and capacity to evolve in response to emerging challenges and growth demands.

Overall, the system exemplifies a well-balanced approach to building a decentralized multi-agent environment that is both secure and capable of handling significant scalability and performance requirements, making it well-suited for a wide range of decentralized applications and use cases.

VI. Use Cases and Real-World Applications

In this chapter, we explore practical applications of the proposed architecture across various industries. By demonstrating how the architecture can be applied to real-world scenarios, we highlight its versatility, effectiveness, and potential impact on modern decentralized systems.

A. Smart Grids

Smart grids represent the modernization of traditional electrical grids by integrating advanced communication and control technologies. They enable efficient energy distribution, real-time monitoring, and dynamic management of energy resources. The decentralized nature of smart grids, with numerous energy producers and consumers, makes them an ideal candidate for the proposed architecture.

1) Application of the Architecture

a) Decentralized energy management:

- Autonomous Agents: Each energy producer (e.g., solar panels, wind turbines) and consumer (households, businesses) is represented by an autonomous agent.
- Decentralized Identity Management: Agents generate Decentralized Identifiers (DIDs), ensuring secure and self-sovereign identities without reliance on centralized authorities.
- Secure Communication: Agents communicate securely using mutual TLS and encrypted channels, exchanging data such as energy production, consumption, and pricing information.

b) Energy transactions and trading:

- Blockchain Integration: The blockchain serves as an immutable ledger for recording energy transactions, such as energy generation records, consumption data, and peer-to-peer energy trades.
- Smart Contracts: Automate energy trading agreements, settlement of payments, and enforcement of contractual obligations between agents.
- Event Sourcing and CQRS: Efficiently handle high volumes of transactions, separating command and query responsibilities for optimal performance.

c) Privacy-preserving data sharing:

- Zero-Knowledge Proofs (ZKP) : Allow agents to prove certain attributes (e.g., energy surplus availability) without revealing sensitive data like exact energy usage patterns.
- Data Confidentiality: Encryption ensures that only authorized agents can access specific data, protecting user privacy and complying with regulations.

2) Benefits:

- Enhanced Efficiency: Real-time data exchange and autonomous decision-making optimize energy distribution and reduce waste.

- Increased Reliability: Decentralized control reduces single points of failure, improving grid resilience.
- Cost Savings: Direct peer-to-peer energy trading lowers transaction costs and enables dynamic pricing models.
- Regulatory Compliance: Secure and privacy-preserving mechanisms align with data protection laws and industry standards.
- Challenges and considerations:
- Scalability: Managing a large number of agents and transactions requires robust scalability, addressed bythe architecture's design.
- Interoperability: Integration with existing grid infrastructure necessitates adherence to industry protocols and standards.
- Security Threats: Protecting against cyber-attacks is critical, necessitating ongoing security assessments and updates.

B. Healthcare Data Management

Managing sensitive healthcare data requires stringent security, privacy, and compliance with regulations such as HIPAA. The proposed architecture offers a secure and interoperable framework for handling electronic health records (EHRs), ensuring data integrity and patient privacy.

1) Application of the Architecture:

a) Patient records:

- Decentralized Identifiers (DIDs): Each patient is assigned a DID, and their EHRs are stored as events on the blockchain.
- Event Sourcing: Records every access and modification to patient data, providing an immutable audit trail.

b) Data access control:

- Zero-Knowledge Proofs (ZKP): Patients use ZKPs to grant healthcare providers access to specific parts of their medical records via OAuth 2.0 tokens.
- OAuth 2.0 Integration: Manages permissions, allowing patients to control who can view or update their health data. iii. Data Integrity and Audit Trails
- Immutable Logging: All access and modifications to EHRs are recorded on the blockchain, ensuring accountability and traceability.
- Smart Contracts: Enforce data access policies and automate consent management, reducing administrative overhead.

c) Efficient data retrieval:

- Command Query Responsibility Segregation (CQRS) Pattern: Enables healthcare providers to query patient data efficiently without impacting the system's write operations.
- Optimized Read Models: Ensure rapid access to necessary data, enhancing the responsiveness of healthcare services.

2) Benefits:

- Enhanced Privacy: Patients maintain control over their medical data, deciding who can access specific information.
- Data Security: Blockchain immutability and robust authentication mechanisms protect against unauthorized access and data breaches.
- Regulatory Compliance: Immutable audit trails facilitate compliance with healthcare regulations and standards.

3) Challenges and considerations:

- Data Interoperability: Ensuring compatibility with existing healthcare information systems requires adherence to industry standards.
- Scalability: Managing large volumes of healthcare data necessitates efficient storage and retrieval mechanisms.
- User Adoption: Encouraging healthcare providers and patients to adopt the new system involves overcoming resistance to change and ensuring ease of use.

C. Secure Internet of Things (IoT) Networks

IoT networks consist of numerous interconnected devices that collect and exchange data. Securing these networks is challenging due to the sheer number of devices and the potential for vulnerabilities. The proposed architecture ensures secure device authentication, data integrity, and efficient management of IoT interactions.

1) Application of the architecture:

a) Device authentication:

- Decentralized Identifiers (DIDs): Each IoT device is assigned a unique DID, ensuring secure and authenticated interactions within the network.
- Zero-Knowledge Proofs (ZKP): Devices use ZKPs to authenticate themselves without revealing sensitive credentials.

b) Data integrity:

- Blockchain Integration: Data generated by IoT devices is recorded on the blockchain, ensuring its integrity and preventing tampering.
- Immutable Logging: Critical events and data exchanges are stored immutably, providing a reliable audit trail.

c) Scalable communication:

- Asynchronous Message Queues: Manage the high volume of data exchange between devices and the blockchain, ensuring efficient processing and minimal latency.
- Secure Protocols: Ensure that all communications are encrypted and authenticated, protecting against unauthorized access and data breaches.

d) Access control:

- OAuth 2.0 Tokens: Regulate which devices can access or modify specific data streams, maintaining strict access control policies.
- Capability-Based Access Control: Use cryptographically secure tokens to manage permissions dynamically and securely.

2) Benefits:

- Secure Authentication: Decentralized authentication mechanisms prevent unauthorized devices from joining the network.
- Data Integrity: Immutable records on the blockchain ensure that IoT data remains accurate and trustworthy.
- Scalability: The system efficiently handles large-scale IoT deployments, accommodating a growing number of devices without compromising performance.

3) Challenges and considerations:

- Device Heterogeneity: Managing diverse IoT devices with varying capabilities requires adaptable and flexible security protocols.
- Resource Constraints: Ensuring that security measures are lightweight enough to operate on resource constrained IoT devices.
- Cybersecurity Threats: Protecting IoT networks from sophisticated cyber-attacks necessitates ongoing security enhancements and monitoring.

D. Supply Chain Management

Supply chains involve the movement of goods and services from suppliers to end consumers, encompassing various processes like manufacturing, logistics, and retail. The complexity and need for transparency in supply chains make them suitable for leveraging blockchain and decentralized technologies.

1) Application of the architecture:

a) Transparent tracking and traceability:

- Immutable Record Keeping: Blockchain records every event in the product lifecycle, from raw material sourcing to final delivery, ensuring data integrity.
- Event Sourcing: Each action (e.g., shipment, quality check) is recorded as an event, allowing real-time tracking and historical analysis.
- Decentralized Agents: Manufacturers, suppliers, logistics providers, and retailers operate as agents within the system, communicating securely.

b) Secure and efficient communication:

- Asynchronous Message Queues: Facilitate communication between agents, handling asynchronous updates and ensuring timely information flow.
- Secure Protocols: Mutual authentication and encrypted channels prevent unauthorized access and data breaches.

c) Confidentiality and competitive advantage:

- Zero-Knowledge Proofs (ZKP): Enable agents to verify compliance with standards or certifications without revealing proprietary information.
- Selective Disclosure: Agents can share necessary data with partners or regulators while keeping sensitive business details confidential.

2) Benefits:

- Enhanced Transparency: Consumers and stakeholders can verify the authenticity and origin of products, building trust.
- Fraud Reduction: Immutable records prevent tampering, reducing counterfeit goods and unethical practices.
- Operational Efficiency: Automation and real-time data exchange streamline processes, reducing delays and costs.
- Compliance and Reporting: Simplifies regulatory compliance by providing verifiable records and audit trails.

3) Challenges and considerations:

- Data Standardization: Ensuring consistent data formats and standards across diverse participants is essential for interoperability.
- Adoption Barriers: Convincing all supply chain participants to adopt the new system may require demonstrating clear value propositions.
- Privacy Concerns: Balancing transparency with the need to protect sensitive business information requires careful design.

E. Conclusion

By addressing real-world problems with a secure, scalable, and privacy-focused approach, the proposed architecture paves the way for innovative decentralized applications that can transform industries and enhance the way individuals and organizations interact in the digital age.

VII. Conclusion

In this paper, we have presented a comprehensive architecture designed to enhance security, scalability, data integrity, and privacy in Multi-Agent Systems (MAS). By integrating advanced technologies such as Blockchain, Zero-Knowledge Proofs (ZKP), OAuth 2.0, and Decentralized Identity Management (DID), we have addressed the critical challenges inherent in decentralized environments where autonomous agents interact and collaborate.

The architecture's contributions address key security challenges by ensuring data integrity and immutability, with blockchain technology providing an immutable ledger for all transactions, events, and identity information. Cryptographic linkages between blocks and consensus mechanisms like PBFT and DPoS prevent tampering. Privacy-preserving authentication is achieved with Zero-Knowledge Proofs, allowing agents to prove knowledge without disclosing information. Secure

authorization is reinforced by combining ZKP with OAuth 2.0, enabling fine-grained access control, while decentralized identity management leverages DIDs and DPKI to reduce reliance on centralized providers, empowering agents to manage their identities independently.

To enhance scalability and performance, the architecture uses Command Query Responsibility Segregation (CQRS) and Event Sourcing, enabling independent scaling of read and write operations. Asynchronous communication through message queues supports a high volume of non-blocking interactions, while optimized cryptographic operations using zk-STARKs, Bulletproofs, and hardware acceleration improve performance. Layer-2 solutions such as state channels and sidechains boost throughput and reduce latency by offloading transactions from the main blockchain.

Data integrity and privacy are safeguarded with an immutable event store on the blockchain, providing a tamper-proof history for auditing, compliance, and state recovery. Selective disclosure mechanisms and ZKPs empower agents to share only necessary information while preserving anonymity. The architecture aligns with global data protection regulations, such as GDPR, enhancing its compliance and adaptability.

The architecture's versatility allows it to be applied across various domains, including smart grids, supply chains and secure internet of things (IoT) networks, demonstrating its broad applicability. Its modular and interoperable design, adhering to standards like OAuth 2.0 and W3C's DIDs, promotes seamless integration with existing systems.

Despite these advancements, the architecture faces limitations. Cryptographic operations, particularly ZKPs, impose computational demands that can be challenging for devices with limited processing power. Consensus mechanism scalability may be hindered by network growth and latency, while data management requires balancing efficient storage with integrity. The complexity of implementing these advanced technologies may increase the learning curve, and decentralized system adoption may face resistance due to regulatory uncertainties.

Future research will focus on optimizing cryptographic protocols, exploring post-quantum cryptography, and enhancing scalable and energy-efficient consensus mechanisms. Improvements in identity management, integration with AI for intelligent agent behavior and real-time threat detection, and collaboration with regulatory bodies to establish supportive frameworks will further refine the architecture.

REFERENCES

[1] Applied Sciences. "Research Progress on the Application of Multi-agent Systems." MDPI (2021). MDPI

[2] P. Rajasekar, K. Kalaiselvi, R. Shanmugam, S. Tamilselvan and A. P. Pandian, "Advancing Cloud Security Frameworks Implementing Distributed Ledger Technology for Robust Data Protection and Decentralized Security Management in Cloud Computing Environments," 2024 Second International Conference on Advances in Information Technology (ICAIT), Chikkamagaluru, Karnataka, India, 2024, pp. 1-6, doi: 10.1109/ICAIT61638.2024.10690718.

[3] Aldweesh, A., Alauthman, M., & al-Qerem, A. Revolutionizing Cryptography: Blockchain as a Catalyst for Advanced Security Systems. IGI Global, 2024. IGI Global.

[4] Baptista, Frederico & Dehez Clementi, Marina & Detchart, Jonathan. (2024). DFly: A Publicly Auditable and Privacy-Preserving UAS Traffic Management System on Blockchain. Drones. 8. 10.3390/drones8080410.

[5] Kalbantner, Jan & Markantonakis, Konstantinos & Hurley-Smith, Darren & Shepherd, Carlton. (2024). ZKP Enabled Identity and Reputation Verification in P2P Marketplaces. 591-598. 10.1109/Blockchain62396.2024.00087.

[6] Ballesteros-Rodríguez, Alberto & Sánchez-Alonso, Salvador & Sicilia-Urbán, Miguel-Ángel. (2024). Enhancing Privacy and Integrity in Computing Services Provisioning Using Blockchain and Zk-SNARKs. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3447785.

[7] Xiong, S., Chen, P., Ge, S., & Ni, Q. SFOM-DT: A Secure and Fair One-to-Many Data Trading Scheme Based on Blockchain. IEEE Xplore, 2024. IEEE Xplore.

[8] Lavin, Ryan & Liu, Xuekai & Mohanty, Hardhik & Norman, Logan & Zaarour, Giovanni & Krishnamachari, Bhaskar. (2024). A Survey on the Applications of Zero-Knowledge Proofs. 10.48550/arXiv.2408.00243.

[9] Ma, Shengchen & Zhang, Xing. (2024). Integrating blockchain and ZK-ROLLUP for efficient healthcare data privacy protection system via IPFS. Scientific Reports. 14. 11746. 10.1038/s41598-024-62292-9.

[10] Harz, D., & Boman, M. (2018). The Scalability of Trustless Trust. ArXiv, abs/1801.09535. https://doi.org/10.1007/978-3-662-58820-8_19.

[11] Lad, K., Dewan, M., & Lin, F. (2020). Trust Management for Multi-Agent Systems Using Smart Contracts. 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, 414-419. https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00080.

[12] Yang, T., Liu, Y., Yang, X., & Kang, Y. (2019). A Blockchain based Smart Agent System Architecture. Proceedings of the 4th International Conference on Crowd Science and Engineering. https://doi.org/10.1145/3371238.3371244.

[13] Leng, J., Sha, W., Lin, Z., Jing, J., Liu, Q., & Chen, X. (2022). Blockchained smart contract pyramid-driven multi-agent autonomous process control for resilient individualised manufacturing towards Industry 5.0. International Journal of Production Research, 61, 4302 - 4321. https://doi.org/10.1080/00207543.2022.2089929.

[14] Wei, P., Wang, D., Zhao, Y., Tyagi, S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. Future Gener. Comput. Syst., 102, 902-911. https://doi.org/10.1016/j.future.2019.09.028.

[15] Zhang, Q., Zhang, Z., Cui, J., Zhong, H., Li, Y., Gu, C., & He, D. (2023). Efficient Blockchain-Based Data Integrity Auditing for Multi-Copy in Decentralized Storage. IEEE Transactions on Parallel and Distributed Systems, 34, 3162-3173. https://doi.org/10.1109/TPDS.2023.3323155.

[16] Oliveira, G., Silva, J., Cortes, O., & Coutinho, L. (2022). A Multi-Agent Architecture for Distributed Data Mining Systems. Anais do XVI Brazilian e-Science Workshop (BRESCI 2022). https://doi.org/10.5753/bresci.2022.222487.

[17] Qasem, M., Obeid, N., Hudaib, A., Almaiah, M., Al-Zahrani, A., & Al-Khasawneh, A. (2021). Multi-Agent System Combined With Distributed Data Mining for Mutual Collaboration Classification. IEEE Access, 9, 70531-70547. https://doi.org/10.1109/ACCESS.2021.3074125.

[18] Nait Cherif, A., Achir, Y., Youssfi, M., Elgarej, M., & Bouattane, O. (2023). Ensuring security and data integrity in Multi Micro-Agent System Middleware with Blockchain Technology. 2023 3rd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), 1-6. https://doi.org/10.1109/IRASET57153.2023.10152950.

[19] Ge, X., Han, Q., Ding, D., Zhang, X., & Ning, B. (2018). A survey on recent advances in distributed sampled-data cooperative control of multi-agent systems. Neurocomputing, 275, 1684-1701. https://doi.org/10.1016/j.neucom.2017.10.008.

[20] Long, Z. (2017). Improvement and Implementation of a High Performance CQRS Architecture. 2017 International Conference on Robots & Intelligent System (ICRIS), 170-173. https://doi.org/10.1109/ICRIS.2017.49.

[21] Debski, A., Szczepanik, B., Malawski, M., Spahr, S., & Muthig, D. (2018). A Scalable, Reactive Architecture for Cloud Applications. IEEE Software, 35, 62-71. https://doi.org/10.1109/MS.2017.265095722.

[22] Mansky, W., Appel, A., & Nogin, A. (2017). A verified messaging system. Proceedings of the ACM on Programming Languages, 1, 1 - 28. https://doi.org/10.1145/3133911.

[23] Shao, J., Yin, B., Chen, B., Wang, G., Yang, L., Yan, J., Wang, J., & Liu, W. (2016). Read Consistency in Distributed Database Based on DMVCC. 2016 IEEE 23rd International Conference on High Performance Computing (HiPC), 142-151. https://doi.org/10.1109/HiPC.2016.025.

[24] Dashti, Z., Oliva, G., Seatzu, C., Gasparri, A., & Franceschelli, M. (2022). Distributed Mode Computation in Open Multi-Agent Systems. IEEE Control Systems Letters, 6, 3481-3486. https://doi.org/10.1109/LCSYS.2022.3185419.

[25] Breugnot, P., Herrmann, B., Lang, C., & Philippe, L. (2021). A Synchronized and Dynamic Distributed Graph structure to allow the native distribution of Multi-Agent System simulations. 2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 54-61. https://doi.org/10.1109/PDP52278.2021.00017.

[26] Wang, J., & Elia, N. (2010). Control approach to distributed optimization. 2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton), 557-561. https://doi.org/10.1109/ALLERTON.2010.5706956.

[27] Rust, P., Picard, G., & Ramparany, F. (2020). Resilient Distributed Constraint Optimization in Physical Multi-Agent Systems. , 195-202. https://doi.org/10.3233/FAIA200093.

[28] Fanitabasi, F. (2018). A Review of Adversarial Behaviour in Distributed Multi-Agent Optimisation. 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), 53-58. https://doi.org/10.1109/UCC-Companion.2018.00034.

[29] Fu, F., & Zhou, H. (2021). A combined multi-agent system for distributed multi-project scheduling problems. Appl. Soft Comput., 107, 107402. https://doi.org/10.1016/J.ASOC.2021.107402.

[30] Costa, D., Garrido, D., & Silva, D. (2021). Efficient Secure Communication for Distributed Multi-Agent Systems. , 543-552. https://doi.org/10.5220/0010375605430552.

[31] Barbosa, J., Leitão, P., Ferreira, A., Queiroz, J., Geraldes, C., & Coelho, J. (2018). Implementation of a Multi-Agent System to Support ZDM Strategies in Multi-Stage Environments. 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), 822-827. https://doi.org/10.1109/INDIN.2018.8471948.

[32] Dimarogonas, D., Frazzoli, E., & Johansson, K. (2012). Distributed Event-Triggered Control for Multi-Agent Systems. IEEE Transactions on Automatic Control, 57, 1291-1297. https://doi.org/10.1109/TAC.2011.2174666.

[33] Sahingoz, O., & Sonmez, A. (2006). Fault Tolerance Mechanism of Agent-Based Distributed Event System. , 192-199. https://doi.org/10.1007/11758532_27.

[34] Cristea, V., Pop, F., Dobre, C., & Costan, A. (2011). Distributed Architectures for Event-Based Systems. , 11-45. https://doi.org/10.1007/978-3-642-19724-6_2.

[35] Long, Z. (2017). Improvement and Implementation of a High Performance CQRS Architecture. 2017 International Conference on Robots & Intelligent System (ICRIS), 170-173. https://doi.org/10.1109/ICRIS.2017.49.

[36] Navabi, S., & Nayyar, A. (2020). A Dynamic Mechanism for Security Management in Multi-Agent Networked Systems. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, 1628-1637. https://doi.org/10.1109/INFOCOM41043.2020.9155295.

[37] Lu, A., & Yang, G. (2020). Secure State Estimation for Multiagent Systems With Faulty and Malicious Agents. IEEE Transactions on Automatic Control, 65, 3471-3485. https://doi.org/10.1109/TAC.2019.2945032.

[38] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress), 557-564. https://doi.org/10.1109/BIGDATACONGRESS.2017.85.

[39] Yang, Y., Jin, K., Liang, W., Liu, Y., Li, Y., & Hosam, O. (2023). A Review of Blockchain-based Privacy Computing Research. 2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom), 241-246. https://doi.org/10.1109/CSCloud-EdgeCom58631.2023.00049.

[40] Li, W., Guo, H., Nejad, M., & Shen, C. (2020). Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach. IEEE Access, 8, 181733-181743. https://doi.org/10.1109/ACCESS.2020.3028189.

[41] Sun, X., Yu, F., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A Survey on Zero-Knowledge Proof in Blockchain. IEEE Network, 35, 198-205. https://doi.org/10.1109/MNET.011.2000473.

[42] Wang, H., & Liao, J. (2021). Blockchain Privacy Protection Algorithm Based on Pedersen Commitment and Zero-knowledge Proof. Proceedings of the 2021 4th International Conference on Blockchain Technology and Applications. https://doi.org/10.1145/3510487.3510488.

[43] Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. , 203-225. https://doi.org/10.1137/0218012.

[44] Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. Comput. Secur., 99, 102050. https://doi.org/10.1016/J.COSE.2020.102050.

[45] Fotiou, N., Siris, V., & Polyzos, G. (2021). Capability-based access control for multi-tenant systems using OAuth 2.0 and Verifiable Credentials. 2021 International Conference on Computer Communications and Networks (ICCCN), 1-9. https://doi.org/10.1109/ICCCN52240.2021.9522214.

[46] Ra, G., Kim, T., & Lee, I. (2021). VAIM: Verifiable Anonymous Identity Management for Human-Centric Security and Privacy in the Internet of Things. IEEE Access, 9, 75945-75960. https://doi.org/10.1109/ACCESS.2021.3080329.

An Efficient Privacy-Preserving Randomization-Based Approach for Classification Upon Encrypted Data in Outsourced Semi-Honest Environment

Vijayendra Sanjay Gaikwad[1], Kishor H. Walse[2], Mohammad Atique Mohammad Junaid[3]
P.G. Department of Computer Science & Engineering, Sant Gadge Baba Amravati University, Amravati, India[1, 3]
SCTR's PICT, Pune, India[1]
Sant Bhagwanbaba Kala Mahavidyalaya, Sindkhed Raja, Buldana, India[2]

***Abstract*—In cloud environment context, organizations often rely on the platform for data storage and on demand access. Data is typically encrypted either by the cloud service itself or by the data owners before outsourcing it to maintain confidentiality. However, when it comes to processing encrypted data for tasks like *k*NN classification; existing approaches either prove to be inefficient or delegate portion of the classification task to end users or do not satisfy all the privacy requirements. Also, the datasets used in many existing approaches to check the performance seem to have very less attributes and instances; but, it is observed that as dataset size increases, the efficiency and accuracy of many privacy-preserving approaches reduce significantly. In this work, we propose a set of privacy preserving protocols that collectively perform the *k*NN classification with encrypted data in outsourced semi-honest-cloud environment and also address the stated challenges. This is accomplished by building an efficient randomization-based approach called PP*k*C that leverages homomorphic cryptosystem properties. With protocol analysis we prove that the proposed approach satisfies all privacy requirements. Finally, with extensive experimentation using real-world and scaled dataset we show that the performance of proposed PP*k*C protocol is computationally efficient and also independent of the number of nearest neighbours considered.**

***Keywords*—Partial homomorphic encryption; classification using encrypted data; randomization; k- nearest neighbours**

I. INTRODUCTION

The progressive paradigm of information technology known as cloud computing provides the ability to deliver a variety of computing services including processing power, storage, and application platform, on demand. However, security has consistently posed a significant barrier to the general uptake of cloud computing technologies [1], [2]. The problem is further exacerbated by cloud computing service providers' inaccurate reporting of security flaws [3], [4], [5]. Cloud based services have raised the need to protect data privacy in outsourced databases has become a focal point of research. As discussed in study [6], [7], [8] and [9] since, a data owner (DO), contracts out the management of his or her databases to a cloud, the DO can lower database management costs by utilizing the cloud's resources as needed. Owing to the diverse range of users the dataset they offer encompasses multiple ranges of categories including personal health status details [10], back-office user database information [11], email information [12] as well as additional information about individual privacy or company trade secrets [13], [14], [15]. To safeguard the original data, access patterns as well as queries, research has been done on secure query processing over an encrypted database. Earlier approaches in [16], [17], [18], [19], [20] and [21] outsource plain texts to a cloud and alter them with their substituted data. Nonetheless, due to their vulnerability to different types of attacks, these earlier strategies are unable to fully protect both data as well as queries [22].

Consider a scenario where a hospital stores its encrypted patient database on the cloud for data mining tasks. When a doctor seeks to ascertain a patient's symptoms for diagnosis, they must submit a query containing highly personal information. To protect the patient's data privacy, cloud must be queried with only the encrypted query data. Moreover, any anomalies in cloud activity could reveal data access patterns, despite encryption. Therefore, maintaining privacy of involved data is paramount when performing classification tasks on encrypted data in an outsourced environment like the cloud.

Previously many approaches have been introduced to address this challenge, however, either the computation cost required to process the queries turned out to be inefficient or privacy requirements were not completely fulfilled. The previous methodologies predominantly relied on datasets with integer values, limiting their applicability to a narrow range of datasets; however, real-world datasets typically encompass a broader spectrum, often comprising floating-point values. Moreover, the pattern of accessing the data during k-nearest neighbours (k-NN) algorithm is also not safeguarded in [23], [24], [25] and [16]. The privacy-preserving algorithms in [26] and [27] conceal data access patterns while ensuring privacy of outsourced databases as well query. However, they have a high query processing cost as discussed in study [6].

We propose set of protocols that jointly address the privacy-preserving k-nearest neighbours outsourced classification issue with the assumption of the process of classification along with encrypted data is held in the cloud environment. The focus in this paper is only specifically on creating the privacy-preserving k-nearest neighbor technique, since k-NN is a popular and most suitable classifier for this work.

A. Problem Definition

In this paper, we assume a *'m'* dimensional database is possessed by a data holder containing total instances of size *'n'*. 0^{th} attribute serves as the record identifier (I), while the m^{th} attribute represents the class label (c). The data holder encrypts the database attribute by attribute to get $E_{pk}(t_{i,j})$ which denotes the encrypted value of a record, where *'t '*represents a tuple, *'i'* ranges from *1* to *'n'*, and *'j'* ranges from *0* to *'m'*.

E_{pk} is the encryption function of partial homomorphic encryption in [28]. After encryption, the encrypted database is sent to the cloud. After this the data holder doesn't get involved in any of the further privacy-preserving classification steps.

Authentic users can send encrypted queries $E_{pk}(Q)$= $(E_{pk}(q_1), \dots, E_{pk}(q_{m-1}))$ to the cloud to obtain resultant encrypted class label, denoted as $E_{pk}(c_q)$.

B. Our Contributions

We have proposed set of protocols that execute in a two-cloud setup to jointly address the issue of preserving privacy while classifying user's encrypted query using outsourced encrypted data. The protocols are for k-nearest neighbours classification algorithm. The proposed approach offers significantly reduced computational costs by utilizing parallel computing, so as to form more practical grounds for classification of encrypted data. Following are some requirements for privacy preserved outsourced classification:

- The user's query must stay encrypted throughout the entire classification task, ensuring it is not disclosed to the cloud.
- The original contents of the database and any intermediate computations must remain hidden from the cloud.
- The records that correspond to the k-nearest neighbours of the user's query should be kept secret from both the cloud and the user.
- Only the final class label should be disclosed to the user.

This work is inspired by the research of Samanthula, Elmehdwi, and Jiang [29], [30], focusing on enhancing the efficiency of the related sub-protocols. As indicated in [29] regarding potential enhancements to the efficiency of the $SMIN_n$ protocol, the attention in this work is directed towards enhancing execution time needed by it. Paillier cryptosystem [28] faces limitations when confronted with negative values resulting from Paillier addition. This challenge is particularly prominent if there are negative values while computing the encrypted Euclidean distance. It' s noteworthy to mention that in the proposed enhanced set of protocols accomplish all aforementioned requirements. The cloud remains oblivious to which database entries align with the nearest neighbours, and any intermediate data visible to the cloud consists solely of either encrypted or randomized values. Additionally, the resultant label remains undisclosed to both clouds.

The rest of this paper is organized as follows. We provide literature survey of state-of-the-art privacy preserving protocols in Section II. The primitives for building proposed approach are described in Section III. We describe the methodology and our proposed privacy preserving PP*k*C protocol and the sub-protocols as its building blocks along with algorithms in Section IV and in Section V, we explain the privacy analysis of these sub-protocols. In Section VI, we provide the experimental results of our proposed PP*k*C protocol using standard and scaled datasets and its comparative analysis with state-of-the-art privacy preserving protocols. We finally conclude this work in Section VII.

II. Literature Survey

In scenarios where queries for classification are executed on the cloud, the foremost and most critical requirement is to hide query details from cloud.

It is important to note that data mining operations can be conducted on encrypted data with relatively less effort using fully homomorphic encryption (FHE) introduced by Gentry et al. (2009) [31]. This cryptosystem allows arbitrary functions to be performed on encrypted data without decryption. However, FHE is computationally intensive, making it impractical for handling real-time classification requests.

Handling queries on encrypted data without the cloud decrypting it poses a significant challenge. The work by Samanthula et al. (2014) [30] outlines a collection of protocols designed to jointly solve the *k*-nearest neighbours (k-NN) query issue within an encrypted database, where both the data and the classification tasks are delegated to the cloud. As described in study [30], the objective of the secure *k*NN protocol is to find the top *k* records closest to the user's query while keeping all details hidden from the cloud. However, in this approach, the SkNN protocol in [30] results in the cloud being exposed to intermediate data, such as the calculated distance values and the subsequently determined *k* smallest distance values. In addition, the records associated with the *k* nearest neighbours of the user query are disclosed to the cloud and also exposed to the user. This again compromises the privacy of the database entries involved in the classification process.

According to Samanthula et al. (2015) in [29] ensuring privacy in *k* nearest neighbours classification is more challenging than running basic *k*NN queries on encrypted data. This complexity stems from the requirement that the k-nearest neighbours identified during the classification process must remain confidential from querying user and cloud.

Protocol presented in study [29] overlooks the issue of access patterns, which is a critical privacy concern for users. While the protocols in study [30] introduce a secure method for *k* nearest neighbours classification on encrypted data that safeguards data and user query privacy, they fail to conceal the data access patterns. Samanthula et al., in [29], expanded on their previous work from study [30] by introducing the PPkNN protocol, offering a new approach to the privacy preserved *k*-nearest neighbours classification issue.

The *k* nearest neighbours remain hidden from both the user and cloud in the PPkNN protocol [29]. Secure Minimum

protocol (SMIN) in study [30] is used to determine the nearest neighbours in a privacy preserved way. As proposed by Samanthula et al. in [29], the SMIN sub-protocol consumes nearlt 67% of the total processing time taken by the PPkNN protocol, which is significantly high and hence impractical in real-time scenario. So, the prevailing obstacle in any outsourced privacy preserving classification approach is to tackle this excess processing time which is caused due to the fact that protocols have to work upon encrypted values. A reduction in overall computational cost would bring even practical solution for the outsourced privacy preserving classification tasks.

As mentioned by Zhu et al. (2020) in [32], conventional privacy preserving approaches for kNN classification induce huge computational cost since operations are purely conducted on encrypted values. Park et al. (2020) in [33] have proposed an efficient version of the Samanthula et al.'s (2015) work in [29] by designing the PkNC protocol which executes its component protocols in parallel to find the class label.

Experimental results depict the gradual rise in execution time of the PkNC protocol. However, it decreases substantially regardless of *k* (the number of nearest neighbours). But, the primary drawback of this protocol emerges as the dataset increases. The execution time rises again in linear manner with increasing instances in dataset, largely because of the practical limitations on threading for parallel computation. Liu et al. (2020) [34] have investigated training of decision trees in outsourced environment. They asserted that encrypted dataset cannot be divided by the cloud based on best attribute and hence, they have proposed a new method which is splitting-free decision tree training.

However, the prominent defining factor is that problem domain of this work deals with k-NN classification, which does not require a separate training phase that is needed for decision tree classification. Also, the scheme proposed by the authors uses an additive secret-sharing method for privacy preservation. This induces more computational cost with the inclusion of share reconstruction. Moreover, experimentations show that the designed protocols' cost of communication and computation rises along with length of vector. Noteworthy observation is that protocols in study [34] were evaluated on relatively small datasets sizes, containing 24, 100, 120, and 958 instances, respectively. The protocols proposed in study [35] and [36] are more efficient than the pioneer protocol in [29], but they result in class labels corresponding to *k* nearest records instead of providing the final class of query. Thus, this is not the exact expected result for outsourced privacy-preserving *k*NN classification issue [37]. It also reveals the *k* nearest class labels to the querying user, which does not satisfy the privacy requirements as stated in study [29]. Moreover, it cannot protect all the intermediate information. The distribution of the inner products, which is used to describe the distance between two vectors like the Euclidean distance, is leaked to one of the cloud servers.

Examining the proposed scheme for a variety of datasets is an important experimental step toward deciding the range of classification tasks that potentially can be performed by any privacy-preserving approach. Until now, all of the existing schemes have experimented with only integer datasets (i.e. they can handle only integer values). This is the reason that in [38], Du et al. scheme's accuracy is not good enough for the real number datasets. In fact, the accuracy of this scheme severely drops with this Heart Disease dataset.

A privacy-preserving k-NN query scheme (QS) based on a secure multi-party computation mechanism was modeled by Xian Guo et al. in [3] to address security concerns when malicious attackers control the cloud and query users. This method showed that the scheme has a certain degree of feasibility and reliability. Furthermore, this method showed a better solution for privacy protection and security. However, a privacy-preserving k-NN query scheme was limited in real-world applications.

Hyeong-Jin Kim et al. in [6] implemented a privacy preserving k-NN query processing algorithm (QPA) via secure two-party computation based on encrypted data. In terms of query processing cost, the performance of the model was better than the existing methods. Nevertheless, the model did not solve other types of queries including Top-*k* and k-NN classification due to low-dimensional data. In addition, this model required increased computational cost. Developing high-dimensional data space requires a data dimensionality reduction technique which led to a challenging task.

Zhi Li et al. [39] presented a function secret sharing (FSS) based secure multi party kNN classification scheme (SecKNN). For secure computations, the presented scheme offered low computation and communication cost. The implementation of FSS reduced lot of computational overhead. Nonetheless, the deployment of the scheme on real time applications is limited.

A privacy-preserving kNN query scheme (QS) was employed by Yandong Zheng et al. [10] to return accurate query results and high query efficiency. The scheme achieved low computation cots and the max-heap accelerated the query efficiency. However, the kNN query scheme leaked the relative proximities of various data records.

Hyeong-Jin Kim et al. [22] employed a new Top-*k* query processing algorithm based on a homomorphic encryption system that is efficient and provides security also. Compared with the existing methods, the Top-k algorithm achieved more times better performance concerning query processing time. However, this model was only performed in specific privacy-preserving data mining algorithms.

III. PRIMITIVES

A. Synthetic Minority Over-sampling Technique (SMOTE)

SMOTE, introduced by Chawla et al [40] in 2002, addresses imbalanced class issues in machine learning. By synthesizing minority class samples through interpolation among existing instances, it counters bias favoring majority classes. Randomly selecting instances, it identifies *k* nearest neighbours and generates synthetic examples along the connecting line segments. This method improves the capacity of classifier for making accurate predictions by providing robust coverage of the minority class space. SMOTE generates synthetic data points, reducing model bias towards

the majority class. Particularly beneficial for imbalanced datasets where the minority class is underrepresented. Interpolation among existing minority class instances maintains diversity. Contrasts with simpler methods like random oversampling that may lead to overfitting. SMOTE introduces new instances near original minority class data points. Synthetic samples serve as plausible representations, reducing overfitting risk and aiding model generalization.

B. Paillier Cryptosystem

Paillier cryptosystem [28] is additively homomorphic and allows calculations upon encrypted values directly, eliminating the requirement to decrypt. It's extensively employed in safeguarding privacy, especially in situations requiring the secure processing of sensitive information while maintaining confidentiality. This scheme is capable of providing semantic security. Fundamentally, Paillier encryption operates on principles of modular operations and large prime numbers. Its security hinges on computing difficulty of factoring the product of two large prime numbers.

Consider *Epk* as encryption function associated with a public key *pk* represented by (N, g), where N is the product of two large prime numbers, and g is a generator in $Z^*_{N^2}$. Similarly, *Dsk* is the decryption function corresponding to the secret key *sk*. Following properties of Paillier encryption scheme [28] withstand for any two plaintext values a and b belonging to Z_N:

1) Homomorphic addition: It provides the addition operation on encrypted values, producing a sum which is also encrypted.

$$D_{sk}\left(E_{pk}(x+y)\right) = D_{sk}\left(E_{pk}(x) * E_{pk}(y)\ mod\ N^2\right) \quad (1)$$

2) Scalar multiplication homomorphism: It provides multiplication operation *x*y* and yields $E_{pk}(x*y)$ when an encrypted value $E_{pk}(x)$ is raised to the power with a scalar value *y*.

$$D_{sk}\left(E_{pk}(x * y)\right) = D_{sk}\left(E_{pk}(x)^y mod\ N^2\right) \quad (2)$$

IV. Methodology for Privacy Preserved Classification

This section elaborates on the operations of several sub-protocols that serve as the foundational components for enhancing the efficiency of computing the *k* nearest neighbours. By performing all operations on Cloud Server 1 (C_1) and utilizing Cloud Server 2 (C_2) for specific tasks with randomized and shuffled data, a robust privacy-preserving architecture can be established. As shown in Fig. 1, we operate within a genuine-but-curious scenario, where the two involved cloud platforms $C_1$and C_2 are non-colliding and adhere strictly to the protocol specifications. C_2 hosts *sk* (secret key) and does not share it with anyone whereas C_1 , C_2 and the querying user know the public key *pk*.

User data is encrypted and stored securely on C_1. *k*NN operations, including distance calculation and classification, are performed entirely on C_1, ensuring that sensitive information remains within a single secure environment.

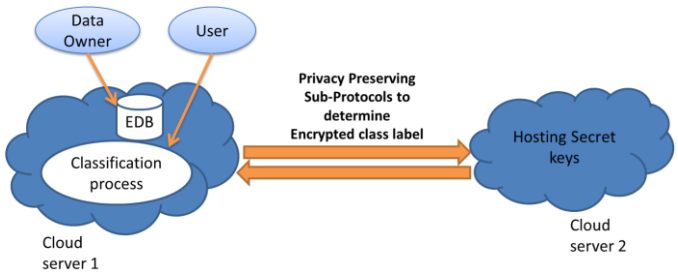


Fig. 1. Two cloud architecture setup.

For operations requiring additional computational resources, such as multiplication or comparison, C_1sends encrypted data in a randomized format to C_2. This randomized data prevents the exposure of sensitive information during the transmission and execution of these operations on C_2. Upon receiving the encrypted data, C_2 performs the necessary operations and returns the results to C_1. The results are de-randomized on C_1, ensuring that the true outcomes are obtained without compromising on data privacy and confidentiality.

The utilization of *k*NN within this two-cloud architecture facilitates privacy-preserving data mining operations in cloud environments. By encrypting data and performing all encrypted operations on C_1, sensitive information remains protected. Role of C_2 is specific to performing operations on randomized and shuffled data therefore, minimizing the risk of data breaches and unintended knowledge gain. The secure interaction between $C_1$and C_2 ensures that privacy is maintained throughout the outsourced classification process.

A. Privacy Preserving Euclidean Distance Protocol

Encrypted squared Euclidean distance is computed by this protocol. These encrypted distances are determined by computing difference between an encrypted user query, $E_{pk}(q)$ and each encrypted dataset instance, denoted as $E_{pk}(t_i)$. Here, i is between 1 and *n*, and *n* represents total instances in dataset. Both $E_{pk}(t_i)$ and $E_{pk}(q)$ have *m* number of attributes. C_2 holds *sk* (secret key) and does not share it with anyone where as C_1 , C_2 and the querying user know the public key *pk*.

The protocol employs parallelization via multiprocessing to expedite results. Additionally, it employs randomization for all intermediate operations necessitating interactions with C_2. In this process, the encrypted dataset values are randomized with an encrypted random number using the Paillier additive property [28], and the obtained result is later de-randomized. This approach guarantees that even if certain data points undergo decryption on C_2, they are presented in a randomized manner, thereby preventing complete exposure of any data point to C_2.

Algorithm-A: PPED(E_{pk}(X),E_{pk}(Y))→$\{E_{pk}(d_1),..,E_{pk}(d_n)\}$

Require: C_1 has E_{pk} (X) and E_{pk} (Y); C_2has *sk*

On C_1:

1. for *i = 1* to *n* do
2. for *j = 1* to *m* do
3. $E_{pk}\ (x_{ij} - y_j) \leftarrow E_{pk}\ (x_{ij}) * E_{pk}\ (y_j)^{N-1}$ mod N^2

(parallelization is used to compute attribute-wise differences concurrently)

4. end for
5. Generate random number $r \in Z_N$
6. $u \leftarrow \sum_{j=1}^{m} E_{pk}\ (x_{ij} - y_j)$
7. send $R \leftarrow u * E_{pk}\ (r) \bmod N^2$ to C_2

On C_2:

8. $u' \leftarrow D_{sk}(R)$
9. $v \leftarrow u' * u' \bmod N$
10. $v' \leftarrow E_{pk}\ (v)$
11. send v' to C_1

On C_1:

12. $r' = r * r$
13. $p = u^{2r} \bmod N^2$
14. $p' \leftarrow v' * E_{pk}(r')^{N-1} \bmod N^2$
15. $E_{pk}(d_i) \leftarrow E_{pk}\ ((x_i - y)^2) \leftarrow p' * p^{N-1} \bmod N^2$

(parallelization is used to concurrently compute the encrypted squared Euclidean distances for all instances)

16. end for
17. return $\{E_{pk}(d_1), \ldots, E_{pk}(d_n)\}$

A vector $E_{pk}(Y)$ having user's encrypted query attributes, and a data-frame E_{pk} (X) having attribute-wise encrypted instances from the dataset are used as inputs for the PPED protocol. Using PPED protocol, C_1 and C_2 jointly compute a vector having encrypted distances corresponding to each encrypted dataset instance.

This protocol implements parallelism in two phases. In the first phase the attribute-wise difference between each attributes of the user query and corresponding attribute of a given dataset instance is computed concurrently. In the second (outer) phase, the encrypted squared difference $E_{pk}(d_i)$ (i. e. $E_{pk}((x_i - y)^2)$) is concurrently computed for all instances of the dataset. During implementation this concurrency is achieved by using threading in Python. Thus, efficiency is improved significantly through these concurrent executions. Moreover, with additional computing resources such as multi-core processors, the PPED protocol can also be run in parallel to simultaneously compute the encrypted squared differences. We use parallelization for independently computing the attribute-wise differences for each i^{th} instance and also for overall execution of PPED algorithm across n instances as each squared distance can be independently computed for all n instances. At the end of PPED protocol, the resulting vector of encrypted distances is only available to C_1 however, these distances remain encrypted.

B. Privacy Preserving Shuffle Protocol (PPSP)

In order to get the k nearest neighbours for the encrypted user query, we need to find the k minimum encrypted distances from amongst the vector of encrypted squared differences generated by PPED protocol. Since, these distance values are encrypted, the k minimum distances cannot be found directly by C_1. The immediate solution is to send the vector of encrypted squared differences to C_2 so that C_2 can decrypt them with the secret key and then the squared differences could be compared in plaintext to get the required k minimum distances. However, this will reveal all the original distance values to C_2 and C_2 also gets to know which dataset records correspond to the selected k minimum distances. So, another solution which avoids this data leakage issue is to randomize the original distances at C_1 using additive homomorphic property and then send these randomized encrypted squared differences to C_2 for comparison. This solves the data leakage issue as the original distances are not revealed to C_2 but C_2 still gains knowledge about which k records from the dataset are selected as the nearest neighbours.

Algorithm-B: PPSP (D) → D'

Require: C_1 has $D \leftarrow \{E_{pk}\ (d_1 + r), \ldots, E_{pk}\ (d_n + r)\}$

On C_1:

1. $n \leftarrow$ *length_of (D)*
2. for $i = n$-1 to 1 do
3. Generate a random integer j , where $0 \leq j \leq i$
4. $temp = D[i]$
   $D[i] = D[j]$
   $D[j] = temp$
5. end for
6. return $D' \leftarrow$ *securely permuted vector of randomized encrypted squared differences*

Although, $C_1$and C_2 are non-colliding but revealing such data access patterns to C_2 can be potentially malicious. Hence, we propose a privacy preserving shuffle protocol (PPSP) that performs random permutation with the randomized encrypted squared differences before sending them to C_2 for comparison. Since, PPSP applies the random permutation directly on encrypted data, at the end of the protocol C_1 does not gain any information about the randomized encrypted squared differences. Moreover, C_2 remains unaware about the sequence of the randomized encrypted squared differences it receives from C_1 for comparison, as intermediate steps are not revealed. Thus, by utilizing proposed PPSP protocol before determining the k minimum encrypted distances, C_2 does not gain any knowledge about which k records from the dataset get selected as the target nearest neighbours and data access patterns are preserved.

C. Privacy Preserving k-Minimum Distances (PPkMD) Protocol

The objective of PPkMD protocol is to determine the encrypted k nearest neighbours of the encrypted user query such that the corresponding original dataset records are not revealed to either of the clouds (i.e.C_1 or C_2). Also, the intermediate results must be either encrypted or such that they must not lead C_1 or C_2 to gain any knowledge about the original values to avoid disclosure of data access patterns. The protocol takes a vector 'v' as input and each element of v is an object having three encrypted values namely, encrypted dataset record identifier $E_{pk}(id_i)$, encrypted distances (i.e. squared difference) $E_{pk}(d_i)$ and corresponding encrypted class label $E_{pk}(c_i)$. So, $v = \{(E_{pk}(id_1), E_{pk}(d_1), E_{pk}(c_1)), \ldots, (E_{pk}(id_n), E_{pk}(d_n), E_{pk}(c_n))\}$

The protocol begins with C_1 generating random integer r from Z_N, and randomizes vector v by homomorphically adding $E_{pk}(r)$ to $E_{pk}(id_i)$, $E_{pk}(d_i)$ and $E_{pk}(c_i)$ of each element of v This gives us an encrypted randomized vector, v'. This v' vector is shuffled using $PPSP_m$ protocol before it is transmitted to C_2. $PPSP_m$ is a variant of above proposed PPSP protocol used for shuffling the vector v', where $v'[i]$= $(E_{pk}(id'_i), E_{pk}(d'_i), E_{pk}(c'_i))$ and $1 \leq i \leq n$. Thus, $PPSP_m$ receives v' and shuffles it such that position of each element $v'[i]$ is changed. Then, the shuffled vector V is sent to C_2.

C_2 decrypts V to get a plaintext but randomized vectors V'. Now, C_2 constructs a min-heap with the randomized distances, $V'[i].d'$, where $1 \leq i \leq n$ and each node in the heap comprises of ($V'[i].id'$, $V'[i].d'$, $V'[i].c'$) i.e. an element of vectors V'. Since, the randomized distance value present at the root node of the min-heap is always the smallest value, we pop the root node from the heap to get the first amongst the k nearest neighbours. Similarly, we pop the heap to get all the remaining nearest neighbours and store them in vector K_{min}. As the min-heap is built with randomized distance values and each node in the heap structure has only randomized values, C_2 does not gain any information about original values. Also, since the randomized elements are already shuffled, therefore C_2 neither learns about their order nor it is able to determine which k records from the dataset were selected as the nearest records to the query. Moreover, the identifiers are also randomized and shuffled which avoids revealing any data access patterns. C_2 then encrypts the vector K_{min} to get encrypted vector K_{min}' and sends it to C_1.

Then, C_1 de-randomizes K_{min}' using the paillier additive property [28] to get the original encrypted k nearest elements in vector v_{min}. Since, every step at C_1 involves only encrypted data, no information is revealed to C_1.

Algorithm-C: PPkMD (v) → v_{min}

Requires: C_1 holds v= $\{(E_{pk}(id_1),E_{pk}(d_1),E_{pk}(c_1)),\ldots, (E_{pk}(id_n), E_{pk}(d_n), E_{pk}(c_n))\}$ and C_2 holds the secret key sk.

On C_1:

1. Generate random integer $r \in Z_N$ and encrypt it, $E_{pk}(r)$
2. Build randomized vector v' by adding $E_{pk}(r)$ to each element of v :
3. for i = 1 to n do
4. $E_{pk}(id'_i) = E_{pk}(id_i) * E_{pk}(r) \bmod N^2$
5. $E_{pk}(d'_i) = E_{pk}(d_i) * E_{pk}(r) \bmod N^2$
6. $E_{pk}(c'_i) = E_{pk}(c_i) * E_{pk}(r) \bmod N^2$
7. end for
8. So we have, encrypted randomized vector as, v'= $\{(E_{pk}(id'_1),E_{pk}(d'_1),E_{pk}(c'_1)),\ldots,(E_{pk}(id'_n), E_{pk}(d'_n), E_{pk}(c'_n))\}$
9. $V \leftarrow PPSP_m(v')$ to shuffle all elements in v'
10. Send shuffled vector V to C_2

On C_2:

11. Decrypt all elements in V using sk such as,
12. for i = 1 to n do
13. $V'[i] \leftarrow (D_{sk}(V[i].id'), D_{sk}(V[i].d'), D_{sk}(V[i].c'))$
14. end for
15. Construct a *min-heap* based on randomized distances $V'[i].d'$, where $1 \leq i \leq n$ and each node in the heap comprises of ($V'[i].id'$, $V'[i].d'$, $V'[i].c'$)
16. for i = 1 to k do
17. $K_{min}[i] \leftarrow$ pop the root node from the *min-heap*
18. end for
19. Vector K_{min} is encrypted using pk such as,
20. for i = 1 to k do
21. $K_{min}'[i] \leftarrow (E_{pk}(K_{min}[i].id'), E_{pk}(K_{min}[i].d'), E_{pk}(K_{min}[i].c'))$
22. end for
23. Send encrypted vector K_{min}' to C_1

On C_1:

24. Receive K_{min}' from C_2 and get the de-randomized vector v_{min} :
25. for i = 1 to k do
26. $E_{pk}(id_{\min\_i}) = K_{min}'[i].id' * E_{pk}(r)^{N-1} \bmod N^2$
27. $E_{pk}(d_{\min\_i}) = K_{min}'[i].d' * E_{pk}(r)^{N-1} \bmod N^2$
28. $E_{pk}(c_{\min\_i}) = K_{min}'[i].c' * E_{pk}(r)^{N-1} \bmod N^2$
29. end for
30. So, we have the encrypted k nearest neighbours in v_{min} as,
31. return v_{min} = $\{(E_{pk}(id_{\min\_1}),E_{pk}(d_{\min\_1}),E_{pk}(c_{\min\_1})),\ldots, (E_{pk}(id_{\min\_k}), E_{pk}(d_{\min\_k}), E_{pk}(c_{\min\_k}))\}$

D. Privacy Preserving Frequency Counting (PPFC) Protocol

The list of encrypted class labels of the dataset is also outsourced to C_1 along with the *EDB*. V=($E_{pk}(c_1)$,…., $E_{pk}(c_w)$) denotes the encrypted class labels list held by C_1.Hence, we have definite class labels (i.e. w). Also, at the end of PPkMD protocol, C_1 holds the encrypted class labels corresponding to the k- nearest records. Let these class labels be denoted as, U= ($E_{pk}(c_1)$,…., $E_{pk}(c_k)$). The goal of PPFC protocol is to compute the frequency of occurrence for each class label in *EDB* in privacy preserved manner i.e. $E_{pk}(f(c_j))$, where $1 \leq j \leq w$.

$PPSP_f$ is another variant of the proposed PPSP protocol used for shuffling vector G_i, where $1 \leq i \leq k$, which comprises of encrypted randomized class label difference values. Then, the shuffled matrix G' is sent to C_2. This ensures that C_2 does not learn anything about which randomized difference value in G' corresponds to which class label. The inverted matrix I received from C_2 is then de-shuffled using the reverse permutation protocol $PPSP'_f$. Finally, the column-wise homomorphic addition of matrix I' gives the encrypted occurrence frequency of class label c_j , where $1 \leq j \leq w$.

Algorithm-D: PPFC (U,V) →F=$\{E_{pk}(f(c_1)),\ldots E_{pk}(f(c_w))\}$

Requires: C_1 holds U= $\{E_{pk}(c_{\min\_1}),..,E_{pk}(c_{\min\_k})\}$ and V= $\{E_{pk}(c_1),..,E_{pk}(c_w)\}$

On C_1:

1. for $1 \leq i \leq k$
2. for $1 \leq j \leq w$
3. $G_{i,j} = E_{pk}(c_j) * E_{pk}(c_{\min\_i})^{N-1}$
4. Generate a random integer $t_{i,j} \in Z_N$
5. $G'_{i,j} = G_{i,j}{}^{t_{i,j}}$
6. end for
7. $G'_i \leftarrow PPSP_f(G'_i)$ to shuffle all elements of G'_i
8. end for
9. Send shuffled matrix G' to C_2

On C_2:
10. for $1 \le i \le k$
11. for $1 \le j \le w$
if $D_{sk}(G'_{i,j}) = 0$
$I_{i,j} = E_{pk}(1)$
otherwise, $I_{i,j} = E_{pk}(0)$
end if
12. end for
13. end for
14. Send matrix I to C_1

On C_1:
15. for $1 \le i \le k$
16. $I'_i \leftarrow$PPSP$'_f(I_i)$ to de-shuffle all elements of I_i
17. end for
18. for $1 \le j \le w$
19. $F[j] \leftarrow E_{pk}(f(c_j)) = \prod_{i=1}^{k} I'_{i,j}$
20. end for

E. Privacy Preserving Max-Frequency (PPMF) Protocol

The PPFC protocol yields a vector *F*, that has encrypted occurrence (counts) frequencies of all class labels of given dataset. The objective of PPMF protocol is to determine which these encrypted frequency values is the largest. The class label corresponding to the largest encrypted randomized frequency will be the final class label for the user's query. So, PPMF protocol can be similar to the proposed PP*k*MD protocol where C_1 prepares a randomized version of the vector F, shuffles it using another suitable variant of PPSP protocol and sends it to C_2; each element is a pair of randomized encrypted class label and corresponding randomized encrypted frequency $<E_{pk}(c_j + r), E_{pk}(f(c_j) + r)>$, where $1 \le j \le w$. C_1 also sends the randomizing factor, *r*, to the querying user at this stage. C_2 decrypts the received vector and now builds a max-heap based on the decrypted but randomized and shuffled frequency values. Each node in the max-heap comprises of the randomized class label and its corresponding randomized frequency value. Since, the randomized frequency value present at the root node of the max-heap is always the largest value; we pop the root node from the heap to get the maximum frequency and its corresponding class label, both randomized. This is the final but randomized class label, $(c_{final} + r)$ for the user query. C_2 sends this randomized final class label to the querying user.

F. Privacy Preserving k-NN Classifcation (PPkC) Protocol

This protocol serves as the base protocol for performing outsourced k-NN classification. It utilizes the above proposed privacy preserving protocols as building blocks for classifying user queries. The querying user is expected to encrypt all query attributes $(E_{pk}(y_1), \ldots, E_{pk}(y_m))$ and send it to C_1. Let us suppose that the encrypted database (EDB) at C_1 is denoted by E_{pk}(X) and the encrypted user query is E_{pk}(Y). With these inputs, the PP*k*C protocol starts its execution.

Algorithm-E: PP*k*C $(E_{pk}(X), E_{pk}(Y)) \rightarrow (E_{pk}(c_1), .., E_{pk}(c_k))$

Requires: C_1 has E_{pk}(X) and receives E_{pk}(Y)
1. $\{E_{pk}(d_1), .., E_{pk}(d_n)\} \leftarrow$ PPED$(E_{pk}(X), E_{pk}(Y))$
2. $v = \{(E_{pk}(id_1), E_{pk}(d_1), E_{pk}(c_1)), \ldots, (E_{pk}(id_n), E_{pk}(d_n), E_{pk}(c_n))\}$
3. $v_{min} \leftarrow$PP*k*MD (v)
4. $U = \{E_{pk}(c_{\min\_1}), .., E_{pk}(c_{\min\_k})\}$ and
5. $V = \{E_{pk}(c_1), .., E_{pk}(c_w)\}$
6. $F \leftarrow$ PPFC (U,V)
7. for $1 \le i \le w$
8. $F'[i] = < E_{pk}(c_i), E_{pk}(f(c_i)) >$
9. User receives $(c_{final} + r) \leftarrow$ PPMF (F')
10. With *r* received from C_1, the user computes the final class label as, $(c_{final} + r) - r$

At the end of PPMF protocol, the querying user receives the final randomized class label, $(c_{final} + r)$ from C_2. With r received from C_1, the user de-randomizes $(c_{final} + r)$ to determine the final class label, c_{final}.

V. PROTOCOL ANALYSIS

Although we focus on building an efficient approach for outsourced *k*NN classification, in this section we also highlight the effectiveness, security and total privacy preservation provided by the proposed protocols. We have guaranteed that the final result of all the proposed privacy preserving protocols remains encrypted. Additionally, C_2 works with only random and shuffled values that bear no connection to the original data. Furthermore, all computations performed on C_2 are consistently sent back to C_1 in encrypted format. Hence, at no stage the original data is revealed to C_1 or C_2. The complexities of the proposed protocols employed in the proposed PP*kC* protocol is presented in Table I.

TABLE I. COMPLEXITIES OF PROPOSED PROTOCOLS

Protocols	PPED	PPSP	PP*k*MD	PPFC
Complexity	O(*m logN*)	O(*n*)	O(*k logn*)	O(*kwn*)

A. PPED Analysis

PPED protocol is carried out with randomization to prevent the sum of attribute-wise differences (i.e. *u*) from getting revealed at C_2. The sum of attribute-wise differences is randomized using the Paillier additive property [28] at C_1 and the randomized value is sent to C_2 for squaring. C_2 decrypts the randomized value, computes square of the randomized values and then encrypts the square again before sending it to C_1. C_1 receives the encrypted square of randomized value and de-randomizes the square through mathematical formulae and homomorphic properties to get the encrypted square of the original *u* value. Hence, the resulting encrypted square of *u* is only available to C_1. Also, the randomizing factor *r* is only known to C_1 so, C_2 does not gain any information about the original value of *u*.

Parallelization is employed in two phases; firstly for computing the attribute-wise difference of each i^{th} instance and also for independently computing the *n* squared distances. With parallelization, assuming ideal conditions, these

computations can be done in O(m) time for the attribute-wise difference and O(n) time for the actual squared distance. The de-randomizing step takes O($nlogN$) time across all n instances, N being the . So with parallelization, the overall complexity could be reduced to O($mlogN$) if the operations are fully parallelized.

B. PPkMD Analysis

The encrypted vector v is randomized with an encrypted random factor $E_{pk}(r)$ and then shuffled using $PPSP_m$ protocol to get vector V at C_1. C_2 then builds the min-heap with the decrypted distances but they are randomized and shuffled distance values so, C_2 does not gain any information about the original distances and access patterns since C_2 takes decisions based on randomized and shuffled values and hence, no extra information is leaked at C_2. Once C_2 determines the randomized k nearest neighbours, C_2 encrypts them and sends to C_1. Now, since paillier cryptosystem is semantically secure, the cipher texts received by C_1 are not the same as the ones which were sent to C_2. Hence, C_1 cannot determine which k distances amongst the sent n distances are received as nearest distances. Ultimately, no knowledge is acquired by C_1 and C_2 about the original data during PPkMD protocol. Since, min-heap is built with O($logn$) and k minimum neighbours are to be extracted, the overall complexity of the PPkMD is O($klogn$).

VI. Experimental Results and Performance Analysis

The various experiments were performed in Google Colab environment with an Intel® 2 GHz system having 4 cores, RAM of 8 GB and 3 MB Cache Size. We utilized the python homomorphic encryption (i.e. phe) library for implementing the Paillier cryptosystem in [28] which is required in the proposed protocols. Existing privacy preserving solutions also use the same cryptosystem so, the performance of the proposed PPkN protocol can be easily compared with them.

We compare the performance of proposed PPkC protocol with the recent and state-of-the-art work in [33], [34], [35], [41] and [43]. The state-of-the-art privacy preserving solutions in [33], [34] and [35] have used datasets the same UCI KDD archive's Car Evaluation dataset [42] in their experimentation. To clearly showcase the improved performance of the proposed PPkC protocol, we firstly conducted experimentation using the same Car Evaluation dataset [42] having 1728 records and six attributes.

For extensive performance evaluation of proposed PPkC protocol with huge dataset and comparison with the most recent work in studies [41] and [43] we used a suitable scaled version of the Car Evaluation dataset in experimentation having 10000 records and six attributes. All the above mentioned recent solutions have used different hardware specifications while performing the performance evaluation of their privacy preserving protocols.

We encrypted both datasets firstly keeping the key size as 512 bits and then as 1024 bits (i.e. K=512/1024), and also varied the values for the nearest neighbours i.e. k and the number of records i.e. n to evaluate the performance of proposed PPkN protocol.

A. Experimental Analysis

1) Performance of proposed protocols with varying key size (K): The below figures illustrate the execution time (in seconds) required by each of the proposed component protocols namely PPED, PPkMD, PPFC, PPMF along with the total execution time taken by PPkC while using datasets encrypted with key size (K) as 512 and 1024 and k= 5. The execution time of PPSP is inclusive in time taken by above mentioned protocols. The protocols are listed on the x-axis, while the y-axis represents the execution time in seconds.

Fig. 2 illustrates the execution time required by all protocols when the Car Evaluation dataset (dataset-1) is encrypted with a key size of 512 and 1024 bits. It is clearly observed that the PPED requires more time as compared to other component protocols with relatively insignificant time requirements.

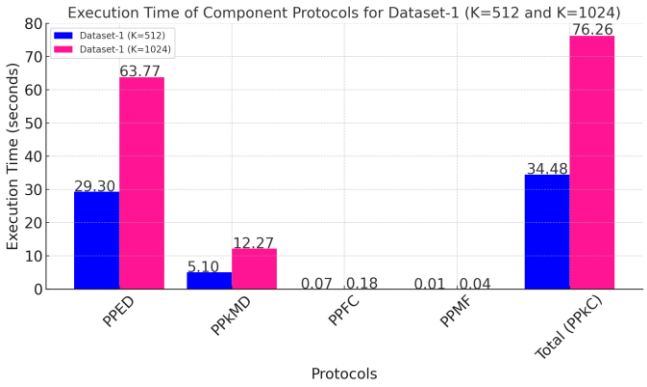


Fig. 2. Execution time of proposed protocols with encrypted Car Evaluation dataset (K= 512, 1024, n=1724).

Fig. 3 illustrates the execution time required by all protocols when the scaled Car Evaluation dataset (dataset-2) is encrypted with a key size of 512 and 1024 bits. As the number of data records are more in this scaled dataset, the execution time taken by all the component protocols is relatively more. However, the growth in time required by PPkMD, PPFC, PPMF protocols is insignificant.

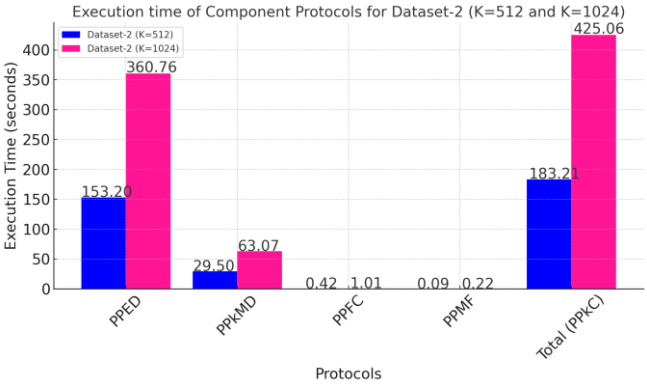


Fig. 3. Execution time of proposed protocols with encrypted Scaled Car Evaluation dataset (K= 512, 1024, n=10000).

TABLE II. SUMMARY OF EXECUTION TIME (SEC) OF COMPONENT PROTOCOLS WITH BOTH DATASETS

Protocols	PPED	PP*k*MD	PPFC,	PPMF	Total (PP*k*C)
Dataset-2 (K= 512)	153.2	29.5	0.42	0.09	183.21
Dataset-2 (K= 1024)	360.76	63.07	1.01	0.22	425.06
Dataset-1 (K= 512)	29.3	5.1	0.07	0.01	34.48
Dataset-1 (K= 1024)	63.77	12.27	0.18	0.04	76.26

Table II shows the summary of execution time incurred by all proposed component protocols during the user query classification with both Car Evaluation dataset and its scaled version having 1724 and 10000 records, respectively, encrypted under key sizes (K) of 512 and 1024 bits.

TABLE III. DATA TRANSFERRED DURING QUERY CLASSIFICATION USING PP*k*C

K (bits)	Data Transferred (MB)				
	k= 5	*k*= 10	*k*= 15	*k*= 20	*k*= 25
512	18.366	25.827	33.355	40.822	48.0
1024	35.587	50.217	64.834	79.474	94.224

Table III shows the data transferred (in Megabytes) during user query classification using the proposed PP*k*C protocol in the two cloud setup with the Car Evaluation dataset encrypted under key sizes (K) 512 and 1024 bits. The table presents the data transferred for various values of *k* i.e. number of neighbours considered.

2) Performance of proposed protocols with varying number of nearest neighbours (k): We examined the execution time required by each of the proposed component protocols and also the total execution time taken by PP*k*C algorithm while varying values of number of neighbours (i.e. *k*) with encrypted Car Evaluation dataset using key size of 512. Across all component protocols a consistent pattern of constant execution times is maintained as the value of *k* is increased from 5 to 25. Hence, the total execution time of proposed PP*k*C protocol remains almost constant when *k* is changed from 5 to 25. Fig. 4 shows this merit of consistent pattern of constant execution times for all proposed protocols while varying *k*.

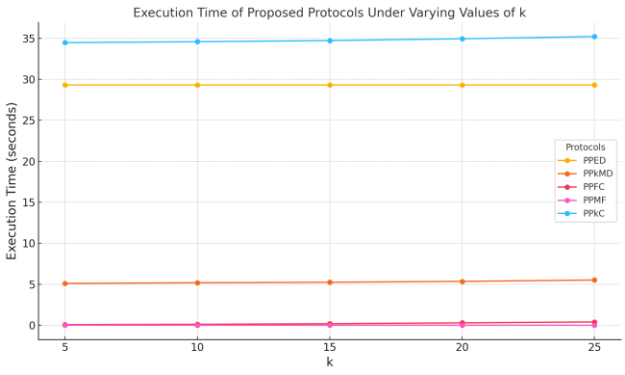


Fig. 4. Constant execution time of proposed protocols under varying values of *k*.

TABLE IV. SUMMARY OF EXECUTION TIME (SEC) OF PROPOSED COMPONENT PROTOCOLS UNDER VARYING VALUES OF *K*

	PPED	PP*k*MD	PPFC	PPMF	PP*k*C
k= 5	29.3	5.1	0.07	0.01	34.48
k= 10	29.3	5.18	0.11	0.01	34.59
k= 15	29.3	5.24	0.18	0.01	34.73
k= 20	29.3	5.35	0.29	0.01	34.95
k= 25	29.3	5.51	0.4	0.01	35.22

Table IV clearly indicates that increase in the number of neighbours considered for query classification (i.e. *k*) does not affect the execution time of proposed PP*k*C protocol which is a significant achievement. On other hand, when compared with recent privacy preserving solutions, the execution time of protocols in [34] and [41] grows linearly along with increasing value of *k*. Although the execution time of protocol in [33] remains almost constant while varying *k* from 5 to 25, still the time required is significantly more. This is discussed in detail in the comparative analysis section.

B. Comparative Analysis

The existing recent privacy preserving solutions in [33], [34], [35], [41] and [43] are compared with proposed PP*k*C protocol. The performance of proposed PP*k*C protocol is examined in terms of its execution time by varying the number of records (*n*) and the number of nearest neighbours considered (*k*) during the outsourced classification. For fair analysis, the execution time of PP*k*C protocol is compared with execution time of protocols in [33], [34] and [35] under above stated varying parameters and using the UCI KDD archive's Car Evaluation dataset [42] having 1728 records, 6 attributes and 4 unique classes. Size of encryption the key (K) used in [33], [34] and [35] is 1024 bits and hence, we maintain the same in our experiment.

Additionally, for extensive performance evaluation with much larger dataset, the comparative analysis on the execution time of proposed PP*k*C protocol and that of the most recent protocols in [41] and [43] is made under same varying parameters while using the SMOTE [40] based scaled version of the Car Evaluation dataset having 10000 records and 6 attributes. Size of the encryption key (K) used in [41] and [43] is 512 bits and hence, to maintain fairness we use the same key size in experiment with the scaled dataset.

1) Analysis with the car evaluation dataset: The state-of-the-art prior work in [33], [34] and [35] used the Car Evaluation dataset [42] encrypted with key size (K) of 1024 bits in their experimentations. Hence, for fairness of comparison we have also used the same encrypted dataset in experiments with the proposed PP*k*C approach. The results on the execution time and performance of proposed PP*k*C protocol under varying parameter of *n* and *k* are compared with state-of-the-art prior work. Table V shows the execution time required by proposed PP*k*C protocol as compared to other state-of-the-art protocols when varying the nearest neighbours i.e. *k*, from 5 to 25.

TABLE V. EXECUTION TIME (SEC) OF PP*K*C AND OTHER STATE-OF-THE-ART PROTOCOLS WITH VARYING VALUES OF *K* (WITH *N*=1724, *K*=1024)

	k= 5	*k*= 10	*k*= 15	*k*= 20	*k*= 25
proposed PP*k*C	76.26	76.61	76.9	77.37	77.82
Park et al. (2020) [33]	249.6	249.6	249.6	249.6	249.6
Liu et al. (2019) [34]	181.14	375.18	560.52	728.46	923.28
Wu et al. (2018) [35]	53.34	56.58	60.3	63.18	65.82

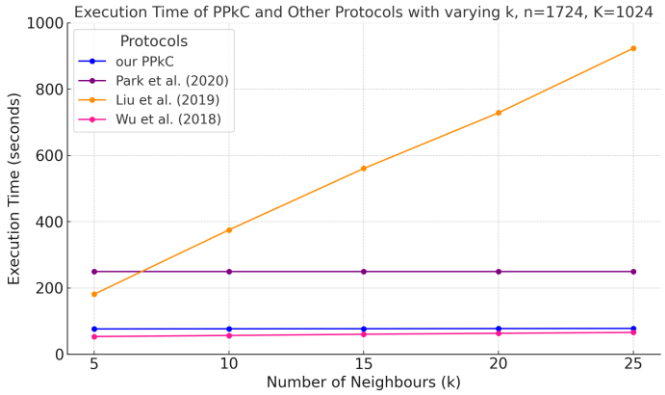


Fig. 5. Comparison on execution time of PP*k*C and existing state-of-the-art protocols with varying *k* using Car evaluation dataset.

Fig. 5 shows the analysis of execution time on the encrypted Car evaluation dataset with key size 1024 bits under varying values *k*. The running time of proposed PP*k*C varies from 76.26 to 77.82 seconds when the number of neighbours are changed from 5 to 25, respectively. Since, execution time of proposed approach remains almost constant so, we can significantly establish that the performance of proposed PP*k*C protocol is not much affected by changes in *k*. When *k*=25, the time taken for execution by PP*k*C protocol is 77.82 seconds which shows that it performs 11.86 times (i.e. 91.57 %) better than the SKC protocol in [34], 3.21 times (i.e. 68.82 %) better than the P*k*NC protocol in [33] and just 1.18 times less better than the PPKC protocol in [35]. As indicated by Table III, the memory usage of the PP*k*C protocol increases gradually with an increase in value of *k* but, so is the case with the other compared protocols. In fact, except protocol in [35] all the other compared protocols require more memory than proposed PP*k*C protocol when using key size of 1024 bits and with varying values of *k*.

Table VI shows the execution time required by proposed PP*k*C protocol as compared to other state-of-the-art protocols when varying the number of records i.e. *n*, from 500 to 1724.

TABLE VI. EXECUTION TIME (SEC) OF PP*K*C AND OTHER STATE-OF-THE-ART PROTOCOLS WHILE VARYING *N* (WITH *K*=25, *K*=1024)

	n= 500	*n*= 1000	*n*= 1500	*n*= 1724
our PP*k*C	22.58	45.12	67.66	77.82
Park et al. (2020) [33]	72.2	144.4	216.6	249.6
Liu et al. (2019) [34]	267.77	535.54	803.31	923.28
Wu et al. (2018) [35]	19.08	38.16	57.24	65.82

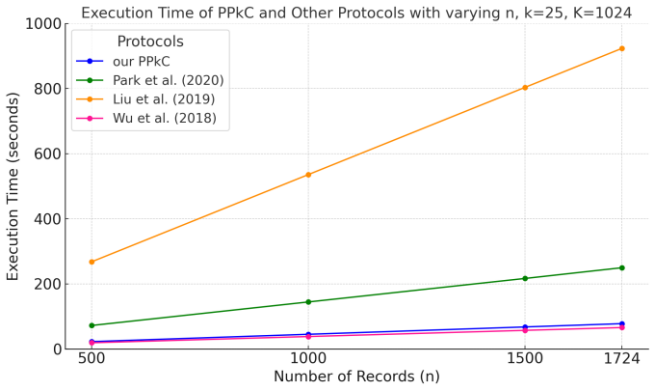


Fig. 6. Comparison on execution time of PP*k*C and existing state-of-the-art protocols with varying *n* using Car evaluation dataset.

Fig. 6 shows the analysis of execution time on the encrypted Car evaluation dataset with key size 1024 bits under varied number of records i.e. *n*, from 500 to 1724. The running time of proposed PP*k*C varies from 22.58 to 77.82 seconds when *n* is changed from 500 to 1724, respectively. Since, execution time drops significantly with proposed PP*k*C approach even while varying the number of records so, we can clearly establish that the performance of proposed protocol is much better than that of P*k*NC protocol and SKC protocol in [33] and [34], respectively. When *n*=1724, the time taken for execution by PP*k*C protocol is 77.82 seconds which shows that it again performs 11.86 times (i.e. 91.57 %) better than the SKC protocol in [34], 3.21 times (i.e. 68.82 %) better than the P*k*NC protocol in study [33] and just 1.18 times less better than the PPKC protocol in study [35]. However, protocol in [35] only aims at determining the class labels corresponding to *k* nearest records instead of providing the final class for user's query. It also reveals the *k* nearest class labels to the querying user, which does not satisfy the privacy requirements as stated in study [29].

2) Analysis with the scaled Car Evaluation dataset: In the literature survey, we observed that the performance of many existing privacy preserving classification protocols has depleted when they were tested with huge datasets. Specifically, the execution time of even the most recent protocols in [41] and [43] grows linearly while varying the number of records (*n*) due to the linear growth in computational cost. So, for extensive performance evaluation of proposed PP*k*C protocol we conducted experiments with the SMOTE [40] based scaled version of the Car Evaluation dataset which is a much larger dataset having 10000 records. Table VII shows the execution time required by PP*k*C protocol as compared to the most recent protocols in [41] and [43] when varying the nearest neighbours i.e. *k*, from 5 to 20.

Fig. 7 shows the comparative analysis on execution time of proposed PP*k*C with the most recent protocols in [41] and [43] using the scaled Car evaluation dataset encrypted with key size of 512 bits under varying values *k*. When *n*=10000 and the number of neighbours are changed from 5 to 20, the running time of proposed PP*k*C varies from only 183.21 to 184.68 seconds, respectively whereas the running time of [41] ranges from 60.32 to 202.12 seconds. Since, execution time of

proposed approach remains almost constant with scaled dataset also, we can significantly establish that even with huge datasets the performance of proposed PP*k*C protocol is not much affected when *k* is increased. Same is the case with the protocol in [43], its run time is also almost independent of *k*. However, the runtime of PP*k*C protocol is nearly 5 times better than that of protocol in [43]. When *k*=20, the time taken for execution by proposed PP*k*C protocol is 184.68 seconds which shows that it performs 9.96 % better than the protocol in study [41]. Also, it is worth observing that the execution time of protocol in [41] grows linearly with increasing value of *k* whereas it remains almost constant for proposed PP*k*C protocol across all values of *k*.

TABLE VII. EXECUTION TIME (SEC) OF PPKC AND RECENT EFFICIENT PROTOCOLS WITH VARYING VALUES OF *K* (*K*= 512)

	with *n*= 10000		with *n*= 6000	
	proposed PP*k*C	Kim et al. (2022) [41]	proposed PP*k*C	Wang et al. (2024) [43]
k= 5	183.21	60.32	103.24	600.26
k= 10	183.93	98.22	104.53	600.33
k= 15	184.32	135.87	104.77	601.67
k= 20	184.68	202.12	104.94	602.88

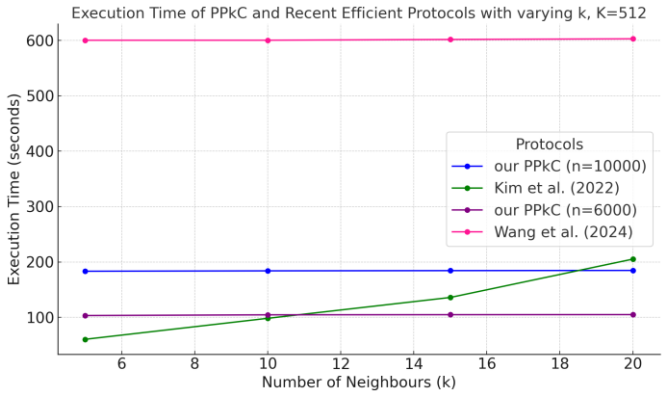


Fig. 7. Comparative analysis on execution time with varying *k* using the scaled dataset.

Table VIII shows the execution time required by proposed PP*k*C protocol as compared to the most recent protocols in [41] and [43] when varying the number of records i.e. *n*, from 2000 to 10000.

TABLE VIII. EXECUTION TIME (SEC) OF PPKC AND RECENT EFFICIENT PROTOCOLS WITH VARYING VALUES OF *N* (WITH *K*=10, *K*= 512)

	Proposed PP*k*C	Kim et al. (2022) [41]	Wang et al. (2024) [43]
n= 2000	39.12	22.44	240
n= 5000	87.1	56.11	480
n= 10000	183.93	98.22	1200

Fig. 8 shows the analysis of execution time of proposed PP*k*C protocol with the most recent protocols in [41] and [43] while using the scaled Car evaluation dataset encrypted with key size of 512 bits under varied number of records i.e. *n*, from 2000 to 10000. The running time of proposed PP*k*C varies from 39.12 to 183.93 seconds when *n* is changed from 2000 to 10000, respectively. Since, execution time drops significantly with proposed PP*k*C approach while using the scaled dataset also so, we can clearly establish that the performance of proposed protocol is much better than that of the protocol in [43]. When *n*=10000, the time taken for execution by proposed PP*k*C protocol is 183.93 seconds which shows that it again performs 6.52 times (i.e. 84.67 %) better than the protocol in [43] and just 1.87 times less better than the protocol in [41] with increasing value of *n*.

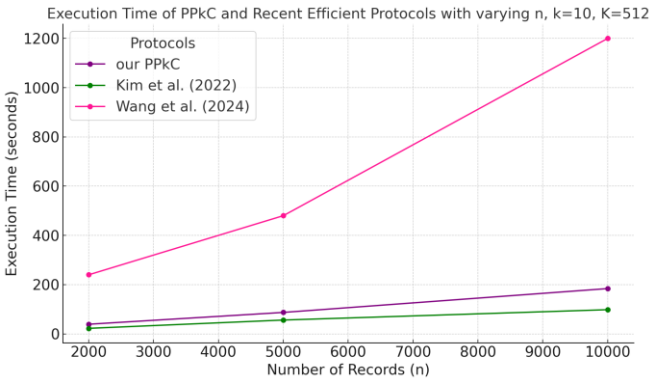


Fig. 8. Comparative analysis on execution time with varying *n* using the scaled dataset.

VII. CONCLUSION AND FUTURE SCOPE

In this paper, we have proposed efficient privacy-preserving *k*NN classification approach, named as PP*k*C protocol and its component protocols that leveraging partial homomorphic encryption (PHE). Our endeavor focused on demonstrating the feasibility and efficacy of PHE in safeguarding sensitive data while allowing for *k*NN classification in outsourced environments.

First and foremost, it is noteworthy that proposed protocols are preserving privacy of user's query, dataset values and the final class label. The protocol analysis shows that no information is ever disclosed and no knowledge can be potentially gained by both the clouds (C_1 and C_2) during execution of any of the component protocols for performing the outsourced *k*-NN classification on encrypted data. In the protocol analysis and implementation, we underscore that the proposed enhanced privacy preserving component protocols fully adhere to the privacy requirements outlined earlier in this paper. Notably, both cloud servers, $C_1 and\ C_2$, are kept oblivious to the identities of the database records associated with the computed nearest neighbours of the user query. Moreover, the intermediate data available to either of the clouds consist of encrypted random values or random numbers only. Also, the privacy preserving shuffling protocol eliminates the risk of C_2 understanding the data accessing patterns.

Furthermore, we explored the possibility of using the heap structure firstly to determine the *k* minimum distances and their corresponding class labels and then for finding the class label with maximum occurrence frequency. With this we were able to significantly reduce the computational overhead involved in classifying the encrypted user's query on

encrypted data and hence enhanced the efficiency of the overall PP*k*C protocol. This approach proved instrumental in optimizing performance with real-world datasets and also particularly in scenarios involving scaled datasets.

Through the experimental investigations, we have drawn several noteworthy conclusions. In the comparative analysis on execution time using the Car evaluation dataset and its scaled version encrypted with key size 1024 bits and 512 bits, respectively it is observed that the running time of proposed PP*k*C remains almost constant while varying values of *k* from 5 to 25. Even while varying *n* the execution time drops significantly with proposed PP*k*C approach with both the dataset. Hence, we established that the performance of proposed PP*k*C protocol is independent of variation in *k* and is much better than that of other recent protocols while varying *k* and *n*.

In our future work, we plan to utilize fully homomorphic encryption (FHE) schemes for working in an encrypted environment since it gives access to a wide range of operations thereby minimizing communication costs incurred in a two-cloud setup. However, its computational overhead must be considered as well and efforts must be taken to improve the same.

REFERENCES

[1] D. Zissis and D. Lekkas, “Addressing Cloud Computing Security Issues,” Future Generation Computer Systems, Vol. 28, No. 3, pp. 583-592, 2012.

[2] M. Zhang, Y. Zhang, Y. Jiang and J. Shen, "Obfuscating EVES Algorithm and Its Application in Fair Electronic Transactions in Public Clouds," in *IEEE Systems Journal*, vol. 13, no. 2, pp. 1478-1486, June 2019.

[3] X. Guo, Y. Li, Y. Jiang, J. Wang, J. Fang, “Privacy-Preserving k-Nearest Neighbor Classification over Malicious Participants in Outsourced Cloud Environments,” in *Cryptography*, vol. 7, no. 4, p. 59, 2023.

[4] R. Barona and E. A. M. Anita, "A survey on data breach challenges in cloud computing security: Issues and threats," *2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT)*, Kollam, India, 2017, pp. 1-8, doi: 10.1109/ICCPCT.2017.8074287.

[5] M. Zhang, Y. Chen and J. Lin, "A Privacy-Preserving Optimization of Neighborhood-Based Recommendation for Medical-Aided Diagnosis and Treatment," in *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10830-10842, July, 2021.

[6] H.J. Kim, H. Lee, Y. K. Kim and J.W. Chang, “Privacy-preserving k NN query processing algorithms via secure two-party computation over encrypted database in cloud computing,” in *The Journal of Supercomputing*, vol. 78, no. 7, pp.9245-9284, 2022.

[7] D. Oh, I. Kim, K. Kim, S. M. Lee and W.W. Ro, “Highly secure mobile devices assisted with trusted cloud computing environments,” in *ETRI Journal*, vol. 37, no. 2, pp.348-358, 2015.

[8] J. Raja and M. Ramakrishnan, “Confidentiality-preserving based on attribute encryption using auditable access during encrypted records in cloud location,” in *The Journal of Supercomputing*, vol. 76, no. 8, pp.6026-6039, 2020.

[9] A. Ahmad, M. Ahmad, M. A. Habib, S. Sarwar, J. Chaudhry, M. A. Latif, S. H. Dar, and M. Shahid, “Parallel query execution over encrypted data in database-as-a-service (DaaS),” in *The Journal of Supercomputing*, vol. 75, pp.2269-2288, 2019.

[10] Y. Zheng, R. Lu, S. Zhang, J. Shao and H. Zhu, "Achieving Practical and Privacy-Preserving kNN Query over Encrypted Data," in *IEEE Transactions on Dependable and Secure Computing*, (Early Access), pp. 1-13, March, 2024.

[11] A. Alabdulkarim, M. Al-Rodhaan, T, Ma, Y. Tian, “PPSDT: A Novel Privacy-Preserving Single Decision Tree Algorithm for Clinical Decision-Support Systems Using IoT Devices” in *Sensors*, vol. 19, no.1, 2019.

[12] P. Centonze, “Security and Privacy Frameworks for Access Control Big Data Systems,” in *Computers, Materials & Continua*, vol. 59, no. 2, pp. 361-374, 2019.

[13] D. Patel, K. Srinivasan, C. Y. Chang, T. Gupta and A. Kataria, “Network anomaly detection inside consumer networks—a hybrid approach,” in *Electronics*, vol. 9, no. 6, pp.923, 2020.

[14] M. M. Salim,I. Kim, U. Doniyor, C. Lee and J. H. Park, “Homomorphic encryption based privacy-preservation for IoMT,” in *Applied Sciences*, vol. 11, no. 18, p.8757, 2021.

[15] N. B. A. Ghani, M. Ahmad, Z. Mahmoud and R. M. Mehmood, “A Pursuit of Sustainable Privacy Protection in Big Data Environment by an Optimized Clustered-Purpose Based Algorithm,” in *Intelligent Automation & Soft Computing*, vol. 26, no. 6, 2020.

[16] M. L. Yiu, G. Ghinita, C. S. Jensen and P. Kalnis, “Enabling search services on outsourced private spatial data,” in *The VLDB Journal*, vol. 19, pp.363-384, 2010.

[17] A. Boldyreva, N. Chenette, Y. Lee and A. O’neill, “Order-preserving symmetric encryption,” in Advances in Cryptology-EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, Proceedings 28, pp. 224-241, Springer Berlin Heidelberg, 2009.

[18] A. Boldyreva, N. Chenette, and A. O’Neill, “Order-preserving encryption revisited: Improved security analysis and alternative solutions,” in *Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference*, CA, USA, Proceedings 31, pp. 578-595, Springer Berlin Heidelberg, 2011.

[19] Y. Qi and M. J. Atallah, "Efficient Privacy-Preserving k-Nearest Neighbor Search," *2008 The 28th International Conference on Distributed Computing Systems*, Beijing, China, pp. 311-319, 2008.

[20] M. Shaneck, Y. Kim and V. Kumar, “Privacy preserving nearest neighbor search,” in *Machine Learning in Cyber Trust: Security, Privacy, and Reliability*, Springer US, pp. 247-276, 2009.

[21] J. Vaidya and C. Clifton, “Privacy-preserving top-k queries,” in *21st International Conference on Data Engineering (ICDE'05)*, IEEE, pp. 545-546, April, 2005.

[22] H.J. Kim, Y.K Kim, H.J. Lee and J.W. Chang, “Privacy-Preserving Top-k Query Processing Algorithms Using Efficient Secure Protocols over Encrypted Database in Cloud Computing Environment,” in *Electronics*, vol. 11 no. 18, p.2870, 2022.

[23] W. K. Wong, D. W. L. Cheung, B. Kao and N. Mamoulis, “Secure kNN computation on encrypted databases,” in *Proceedings of the 2009 ACM SIGMOD International Conference on Management of data*, pp. 139-152, June, 2009.

[24] H. Hu, J. Xu, C. Ren and B. Choi, “Processing private queries over untrusted data cloud through privacy homomorphism,” *2011 IEEE 27th International Conference on Data Engineering*, Hannover, Germany, pp. 601-612, 2011.

[25] Y. Zhu, R. Xu and T. Takagi, “Secure k-NN computation on encrypted cloud data without sharing key with query users,” in *Proceedings of the 2013 international workshop on Security in cloud computing*, pp. 55-60, May, 2013.

[26] Y. Elmehdwi, B. K. Samanthula and W. Jiang, “Secure k-nearest neighbor query over encrypted data in outsourced environments,” in *2014 IEEE 30th International Conference on Data Engineering*, pp. 664-675, March, 2014.

[27] H. I. Kim, H. J. Kim and J. W. Chang, “A secure kNN query processing algorithm using homomorphic encryption on outsourced database,” in *Data & Knowledge Engineering*, vol. 123, pp.101602, 2019.

[28] P. Paillier, “Public key cryptosystems based on composite degree residuosity classes,” in *Eurocrypt*, pp. 223–238, 1999.

[29] B. K. Samanthula, Y. Elmehdwi, and W. Jiang, “k- Nearest Neighbor Classification over Semantically Secure Encrypted Relational Data,” in *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, 2015.

[30] B. K. Samanthula, Y. Elmehdwi, and W. Jiang, "Secure k- Nearest Neighbor Query over Encrypted Data in Outsourced Environment," in *IEEE ICDE*, pp. 664- 675, 2014.

[31] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *ACM STOC*, pp. 169–178, 2009.

[32] Y. Zhu, X. Li, J. Wang, and J. Li, "Cloud-assisted secure biometric identification with sub-linear search efficiency," in *Soft Computing*, vol. 24, p. 5885–5896, 2019.

[33] J. Park and D. H. Lee, "Parallelly running k-nearest neighbor classification over semantically secure encrypted data in outsourced environments," in *IEEE Access*, vol. 8, p. 64617–64633, 2020.

[34] L. Liu, J. Su, X. Liu, R. Chen, K. Huang, R. H. Deng, and X. Wang, "Toward highly secure yet efficient knn classification scheme on outsourced cloud data," in *IEEE Internet of Things Journal*, vol. 6, pp. 9841–9852, 2019.

[35] W. Wu, J. Liu, H. Rong, H. Wang, and M. Xian, "Efficient k-nearest neighbor classification over semantically secure hybrid encrypted cloud database," in *IEEE Access*, vol. 6, pp. 41771–41784, 2018.

[36] W. Wu, U. Parampalli, J. Liu, and M. Xian, "Privacy preserving knearest neighbor classification over encrypted database in outsourced cloud environments," in *World Wide Web*, vol. 22, p. 101–123, 2018.

[37] Gaikwad VS, Walse KH, Thakare VM, "Review of the state-of-the-art methods for privacy preserved classification in outsourced environment," in *Proc. Int. Conf. Innovative Trends in Information Technology (ICITIIT)*, Kottayam, India, Feb. 2020, pp 1–6.

[38] J. Du and F. Bian, "A privacy-preserving and efficient k-nearest neighbor query and classification scheme based on k-dimensional tree foroutsourced data," in *IEEE Access*, vol. 8, pp. 69333–69345, 2020.

[39] Z. Li, H. Wang, S. Zhang, W. Zhang and R. Lu, "SecKNN: FSS-Based Secure Multi-Party KNN Classification Under General Distance Functions," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp.1326-1341, 2024.

[40] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," in *Journal of Artificial Intelligence Research*, vol. 16, p. 321–357, 2002.

[41] Y. K. Kim, H. J. Kim, H. Lee and J.W. Chang, "Privacy-preserving parallel kNN classification algorithm using index-based filtering in cloud computing," in *PLoS One*, vol. 17, no. 9, 2022.

[42] B. Z. M. Bohanec. (1997). *Car Evaluation Data Set*, UCI Machine Learning Repository. Accessed: May. 24, 2023. [Online]. Available: https://archive.ics.uci.edu/ml/datasets/Car+Evaluation.

[43] H. Wang, Y. Zhao, Z. Cai and H. Zhao, "Privacy-Preserving kNN Classification Query Scheme for Encrypted Data in Outsourced Environments for Smart Grid," *4th International Conference on Computer Communication and Artificial Intelligence (CCAI)*, Xi'an, China, 2024, pp. 162-169.

Modeling the Impact of Robotics Learning Experience on Programming Interest Using the Structured Equation Modeling Approach

Nazatul Aini Abd Majid[1], Noor Faridatul Ainun Zainal[2], Zarina Shukur[3],
Mohammad Faidzul Nasrudin[4], Nasharuddin Zainal[5]
Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia (UKM), 43600 UKM Bangi, Selangor, Malaysia[1, 2, 3, 4]
Fakulti Kejuruteraan dan Alam Bina, Universiti Kebangsaan Malaysia (UKM), 43600 UKM Bangi, Selangor, Malaysia[5]

***Abstract*—Proficiency in programming is crucial for driving the Fourth Industrial Revolution. Therefore, interest in programming needs to be instilled in students starting from the school level. While the use of robotics can attract students' interest in programming, there is still a lack of research modeling, the impact of robotic learning experiences on programming interest using a structural equation modeling (SEM) approach. This study aims to analyze the structural relationship between interest in programming and learning experiences using a specially developed robotics module based on Kolb's experiential learning model and the programming development phases. An experiment involving 76 primary and secondary school students was conducted using the robotics module. Data were collected through a questionnaire containing 12 questions for five constructs: engagement, interaction, challenge, competency, and interest. These constructs, which are latent variables, formed the model using the partial least squares-SEM technique through the SmartPLS 4.0 software. The evaluation of the structural model found that the variables of engagement and competency had a significant impact on interest in programming, while interaction and challenge received low values. The developed model has moderate predictive power, indicating that interest in programming can be moderately predicted based on students' experiences using robots.**

***Keywords*—Programming; robotics; Structural Equation Modeling (SEM); experiential learning; student engagement**

I. Introduction

Mastery of programming skills is essential for advancing the Fourth Industrial Revolution; however, fostering a genuine interest in programming among students at the school level continues to pose a considerable challenge. One effective way to enhance students' interest in programming is by integrating technology in interactive environments, such as using Turtle Graphics for vector-based graphics [1] and incorporating robots to provide hands-on learning experiences. Robotics education has emerged as an engaging avenue for introducing students to programming concepts and cultivating computational thinking (CT) skills [2] Additionally, a study by [3] demonstrated that integrating CT with Educational Robotics (ER) significantly enhances students' CT and programming skills. Given that robotic learning has the potential to significantly boost interest in programming, this approach can contribute to the increase of Science, Technology, Engineering, and Mathematics (STEM) graduates, a current national priority for many governments worldwide, including the United States [4], the UK [5] and Malaysia. Despite these efforts, Malaysia has not yet met its target ratio of 60:40 for students enrolling in STEM versus non-STEM programs [6].

STEM teachers require educational tools that are affordable, hands-on, conceptually engaging, syllabus-aligned, interactive, extendable, and suitable for extracurricular activities. While some schools have adopted available robotic kits, they face challenges such as a lack of syllabus-related modules and the need for more extendable resources to maximize the kits' use. Moreover, many schools are unable to use robotic kits due to funding constraints, limiting their ability to foster interest in STEM. To address these issues, our research has developed robot prototypes called AkalBot, designed with affordability and educational value in mind, selecting Arduino as the main component. The accompanying learning module includes essential knowledge in computational thinking, such as algorithms, to make robotics an accessible and effective tool for enhancing programming interest and supporting STEM education in Malaysia. However, there remains a notable gap in the literature concerning the comprehensive assessment of how robotics learning experiences influence students' programming interest. This study seeks to address this gap by employing structural equation modeling (SEM) to analyze the intricate relationships between programming interest and robotics learning experiences, drawing on Kolb's experiential learning model as a theoretical framework.

Kolb's experiential learning theory provides a theoretical framework for understanding how students acquire and internalize knowledge through concrete experiences, reflective observation, abstract conceptualization, and active experimentation [7]. Applied to robotics education, this theory suggests that hands-on activities with robots offer students opportunities to engage in concrete experiences, reflect on their learning, conceptualize abstract programming concepts, and apply their knowledge in practical contexts [8]. This study aims to investigate the structural relationships between programming interest and robotics learning experiences. Specifically, it seeks to assess how student engagement, interaction, challenge, competency, and interest within the context of robotics education impact programming interest after using the robotic module based on Kolb's model and our robot, AkalBot. The remainder of this paper reviews related work (Section II), details

the research methodology, including the experimental design and data analysis techniques (Section III), presents the results of the structural model analysis (Section IV), discusses the findings (Section V), and offers conclusions (Section VI).

II. A Review of Related Work

The use of robotics as a tool to engage students with programming and technology concepts has been extensively studied, emphasizing its potential to promote critical thinking and creativity. For instance, LEGO Mindstorms has been shown to enhance creativity [9], while LEGO WeDo kits have been explored for their role in fostering CT. A study investigating the effects of LEGO® WeDo and the Scratch programming platform on CT skills, grit, and programming abilities among undergraduate educational science students revealed notable outcomes. Using a quasi-experimental design with a pretest-posttest approach, the six-week intervention involved 246 participants (aged 18–23, mean age 20.5 ± 3.37, with a balanced gender distribution). The findings demonstrated that participants using LEGO® WeDo experienced significant improvements in CT skills, exhibited higher levels of grit, and gained a deeper understanding of Internet of Things (IoT) project creation. This study underscores the educational advantages of tangible robotic tools over purely visual programming platforms [10].

Building on these findings, the development of a robotic module tailored for Malaysian students seeks to replicate these educational benefits by introducing a low-cost robotic prototype aligned with the Malaysian school curriculum. The objective is to leverage similar hands-on, tangible tools to actively engage students in STEM learning, fostering deeper understanding and sustaining their interest in pursuing STEM programs. To ensure its effectiveness, survey feedback from STEM teachers was utilized to identify the core requirements for the module, which include being engaging, curriculum-based, easy to understand, and cost-effective [11].

To address this challenge, a customizable module was developed using Arduino as the microcontroller and Google's Blockly as the visual editor, with potential for further enhancement. A study assessed Malaysian students' perceptions of their competency and interest in STEM after engaging with a STEM module and building a robotic prototype. Conducted at the National Science Centre, Malaysia, this activity aimed to address the under-enrollment in STEM programs. The module, based on Kolb's experiential learning theory, incorporated five key activities: watching videos, reading materials, assembling components, using Blockly for programming, and playing a robotic game. The primary goal was to boost STEM interest through robotics and educational games. Evaluated through qualitative and quantitative case studies with students aged 11 to 15, the results showed a positive response, with significant increases in students' interest in STEM, aligning with the Malaysia Education Blueprint 2013-2025 [12]

In recent years, robots and visual editors have gained significant attention for teaching programming and robotics. AelE: A Versatile Tool for Teaching Programming and Robotics Using Arduino, highlights the role of programming in developing problem-solving and abstract thinking skills. Arduino boards, popular for their open hardware design and educational resources, are commonly programmed through text-based environments like Arduino IDE or block-based tools such as mBlock and Scratch. However, these tools often face challenges, such as the need for specific syntax knowledge and limited sensor support. To address these, AelE was developed as a block-based tool designed to simplify programming for students. The tool has been successfully used in diverse educational settings, including secondary schools, adult education, and prison programs. Students across these contexts, regardless of prior knowledge, responded positively to AelE, which was found to effectively support various learning environments and project types, demonstrating its versatility and broad appeal [13].

Despite the growing body of research on robotics in education, there is still a significant gap in understanding how robotics learning experiences impact students' interest in programming. This study aims to fill this gap by utilizing SEM to explore the complex relationships between students' programming interest and their robotics learning experiences, with Kolb's experiential learning model serving as the theoretical foundation.

III. Materials and Methods

The methods to model the impact of robotics learning experience on programming interest using the structured equation modeling approach consists of six main steps. An explanation of each step is given below.

A. Step 1: Forming Variables to Model the Impact

In order to form variables to model the impact of learning experience, existing variables that have been used to analyze learning experiences have been investigated. Five variables have been used to model the impact of interaction, engagement and challenge towards interest and competency in the subject area [14]. They have designed hands-on activities for virtual computer laboratories based on Kolb's experiential learning cycle. The study in [15] have further used the variables to quantitatively analyzed for identifying the impact of the experiential activity. The details of the variables that been used to model the impact of using the educational robotic is given below:

- Interaction (ACT): This construct assesses the degree of collaboration among students during robotics exercises. Working in pairs, students engage in completing tasks, tackling new challenges, and jointly reflecting on their learning experiences.
- Engagement (ENG): This construct evaluates students' readiness and enthusiasm to participate in and complete robotics activities. High engagement is evident through active involvement, enthusiasm, and persistence, which are essential for deep and effective learning experiences in programming.
- Challenge (CHA): This construct gauges the perceived difficulty of the robotics activities from the students' perspective. By assessing the complexity and challenge level, this measure helps to understand how the tasks encourage cognitive development, problem-solving, and critical thinking skills.

- Competency (CMP): This construct focuses on the learning outcomes that students perceive they have achieved through robotics activities. Unlike interaction, engagement, and challenge, which evaluate the learning process, competency reflects the end results, indicating students' mastery of programming concepts and their confidence in applying these concepts.
- Interest (INT): This construct measures the increase in students' interest and curiosity in programming due to robotics activities. Like competency, this construct evaluates the outcomes of the learning experience, showing how effectively the activities have stimulated and maintained students' interest in programming.

These variables were integrated to form the research model as shown in Fig. 1. By integrating these variables into a cohesive framework, we can gain valuable insights into the multifaceted nature of learning experiences and their impact on students' academic outcomes. This framework provides a structured approach for examining the interplay between key factors that shape students' learning trajectories, laying the groundwork for subsequent analyses using structural equation modeling (SEM) techniques. Seven hypotheses were developed:

Hypothesis 1 (H1). Challenge is positively related to students' competency.

Hypothesis 2 (H2). Challenge is positively related to students' interest.

Hypothesis 3 (H3). Competency is positively related to students' interest.

Hypothesis 4 (H4). Engagement is positively related to students' competency.

Hypothesis 5 (H5). Engagement is positively related to students' interest.

Hypothesis 6 (H6). Interaction is positively related to students' competency.

Hypothesis 7 (H7). Interaction is positively related to students' interest.

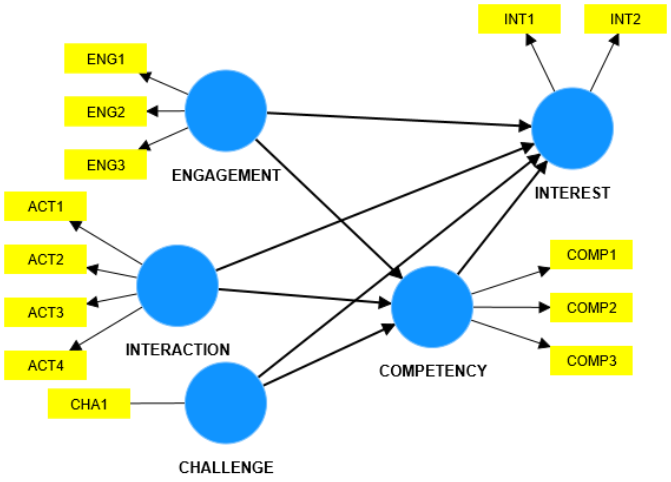


Fig. 1. Research model.

B. Step 2: Developing Robotic Module Based on the Selected Variables and Kolb's Learning Model

The working principle of AkalBot is based on the integration of three main components: modules, robot prototypes, and a blockly editor. The robotic kit leverages Kolb's experiential learning theory as the foundation for its modules, which also integrate computational skills like algorithms.

The first component is module design. The module design captures experience as a resource for learning and development [7] through interactive games using robot prototypes. The modules are structured according to the four phases of Kolb's learning theory:

1) Concrete Experience (CE): Students begin with hands-on exercises, such as programming robots, to gain practical experience.

2) Reflective Observation (RO): Students provide feedback on a series of tasks, reflecting on their experiences from the CE phase.

3) Abstract Conceptualization (AC): Students develop strategies to win specified games based on provided theoretical concepts.

4) Active Experimentation (AE): Students implement their strategies to achieve game objectives.

These phases are designed to promote deep learning and engagement by cycling through practical exercises, reflection, strategy formulation, and experimentation.

The second component is robot prototypes. AkalBot (Fig. 2) features low-cost robot prototypes designed with affordability and accessibility in mind, making the robotic kit an attractive option for schools and higher education institutions. The core component of these robots is the Arduino microcontroller board, known for its low cost, ease of use, and flexibility. Arduino can interact with a variety of components such as buttons, motors, LEDs, and GPS modules. The study in [16] highlights several advantages of using Arduino in educational robotics. One of the key strengths is the ability to load experimental scripts directly onto the board's memory, allowing the Arduino to operate independently without the need for continuous interfacing with computers or external software. This feature provides complete independence, portability, and accuracy in experiments. Additionally, Arduino benefits from a large community that supports its use by offering numerous hardware add-ons and hundreds of free scripts for various projects, making it an accessible and versatile tool for educational purposes. Arduino is particularly suitable for educational purposes due to the abundance of available resources, hardware add-ons, and free scripts for various project ideas.

The third key component of AkalBot is its utilization of a block-based editor, which is a visual programming tool developed by Google. Modified blocks within this platform form AkalBlok (Fig. 3), facilitating a drag-and-drop interface that enables students to program the robots without the need to delve into intricate programming languages. This visual approach aims to captivate primary and secondary students, enticing them to explore the realms of robotics and programming. Within the AkalBlok platform, students

encounter specific blocks tailored for programming Arduino-related components, neatly categorized into three main types: Arduino Parts, Arduino Sensor, and Arduino Motor.

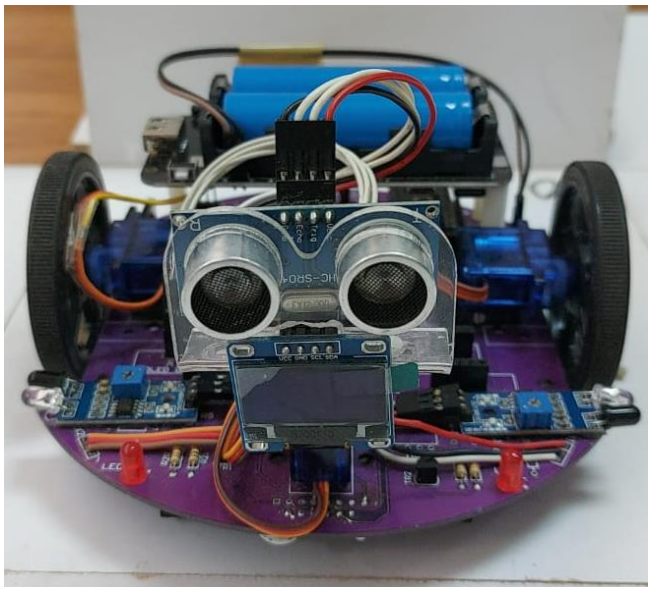


Fig. 2. A robotic prototype named AkalBot.

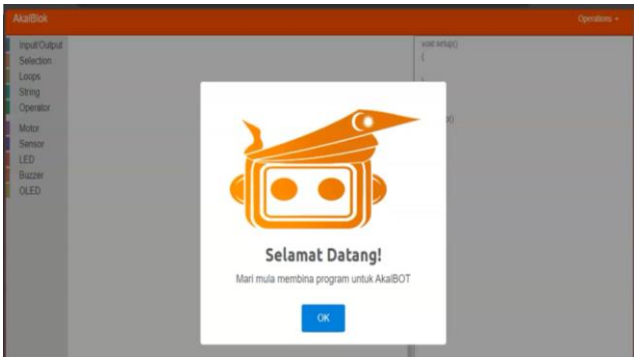


Fig. 3. A block-based editor named AkalBot.

AkalBot's overall design revolves around game-based activities, wherein students apply control over robot prototypes using the block-based editor to create programs. This innovative design framework embraces experiential learning theory, effectively harnessing hands-on experiences as a facilitator for learning and development. By integrating these elements, AkalBot emerges as a comprehensive and immersive educational tool, adept at augmenting students' programming skills and cultivating their interest in the subject matter.

C. Step 3: Setting Up an Experiment with Students

In this study, the population consisted of 76 primary and secondary school students who participated in an experiment designed to assess the impact of a robotics learning module on their interest in programming. The robotics module, developed based on Kolb's experiential learning model, guided the students through different programming development phases. Data were collected during the experiment through a questionnaire, which consisted of 12 questions focused on five key constructs: engagement, interaction, challenge, competency, and interest. These constructs were used as latent variables to form the structural model, which was analyzed using partial least squares structural equation modeling (PLS-SEM) through SmartPLS 4.0 software. The experiment consisted of five sessions, each lasting three hours, designed to evaluate the impact of robotics learning on students' programming interest and skills.

1) Session 1: Pre-Test and Introduction (20 minutes): Activity: Students answered pre-test questions to assess their initial knowledge of basic robotics and programming concepts. This session aimed to establish a baseline for their understanding and skills.

2) Session 2: Introduction to Robotic Kit and a Blok-based Editor (30 minutes): Activity: Students were introduced to the AkalBot robotic kit and the AkalBlok programming environment. This session included a detailed explanation of how to use the kit and the drag-and-drop interface of AkalBlok to program the robots.

3) Session 3: Hands-On Robotic Assembly and Initial Programming (60 minutes): Activity: Students engaged in the assembly of robot prototypes and performed initial programming exercises. This session followed the Concrete Experience (CE) phase of Kolb's learning theory, where students learned through hands-on activities.

4) Session 4: Reflective Observation and Strategy Planning (60 minutes): Activity: Based on their hands-on experiences, students reflected on their activities and provided feedback. This session corresponded to the Reflective Observation (RO) phase, where students analyzed their experiences and planned strategies for upcoming tasks.

5) Session 5: Implementation and Experimentation (60 minutes): Activity: Students implemented their strategies and engaged in further programming to accomplish specific tasks using the robots. This session combined the Abstract Conceptualization (AC) and Active Experimentation (AE) phases, encouraging students to apply theoretical concepts in practical scenarios.

D. Step 4: Collecting Data and Analyzing Model

The empirical data utilized in this study are considered primary as they were directly gathered through a survey conducted among students. To assess the effectiveness of the robotic educational experience, data collection encompassed a combination of quantitative and qualitative methodologies. The subsequent steps were followed:

1) Surveys and Questionnaires: Students filled out surveys and questionnaires to provide feedback on their learning experiences, engagement, and interest levels throughout the experiment.

2) Observation: Instructors observed student interactions with the robotic kit. The measurement model is foundational to structural equation modeling (SEM), offering a robust assessment of the reliability and validity of the constructs under investigation. In addition to assessing convergent validity through factor loadings, composite reliability (CR), and average variance extracted (AVE), discriminant validity is a

critical aspect that ensures the distinctiveness of the constructs [17].

1) Factor loading: Factor loading examines the strength of the relationship between observed variables and their corresponding latent constructs. High factor loadings (> 0.70) indicate that the observed variables effectively capture the underlying constructs [17].

2) Composite Reliability (CR): CR assesses the internal consistency of a set of indicators for each latent construct. CR values exceeding 0.70 indicate satisfactory reliability, implying that the indicators consistently measure the underlying construct [18].

3) Average Variance Extracted (AVE): AVE quantifies the proportion of variance captured by a construct's indicators relative to measurement error. AVE values > 0.50 indicate adequate convergent validity, suggesting that the observed variables collectively represent the latent construct effectively [19].

4) Discriminant validity (Heterotrait-monotrait ratio): Discriminant validity examines whether the constructs are empirically distinct from one another. The heterotrait-monotrait (HTMT) ratio compares the correlations between constructs (heterotrait correlations) with the average correlations within constructs (monotrait correlations). A threshold value of 0.90 is suggested for HTMT ratios to ensure discriminant validity [20]. It measures how much more strongly items within the same construct are related to each other compared to items across different constructs.

Analyzing the structural model is a crucial step in SEM using SmartPLS, as it helps to understand the relationships between constructs and validate the hypothesized paths. This step involves evaluating various metrics such as path coefficients (β), standard errors (SE), t-values, p-values, effect sizes (f^2), variance inflation factors (VIF), and predictive relevance (Q^2 Predict). The following provides a detailed explanation of each component within the context of SmartPLS:

1) Path Coefficients (β): Path coefficients represent the strength and direction of the relationships between constructs, ranging from -1 to +1. Positive values indicate positive relationships, while negative values indicate negative relationships. High absolute values indicate stronger relationships. For example, a path coefficient of 0.45 between robotics learning experience and programming interest suggests a moderate positive relationship [21].

2) Standard Error (SE): The standard error measures the precision of the estimated path coefficients, indicating how much the estimated coefficient would vary from the true population value. Smaller SE values indicate more precise estimates. For instance, an SE of 0.07 for a path coefficient of 0.45 suggests that the estimate is quite precise [22].

3) t-value: The t-value assesses the statistical significance of the path coefficients, calculated by dividing the path coefficient by its standard error ($t = \beta / SE$). A higher absolute t-value indicates stronger evidence against the null hypothesis. Typically, a t-value greater than 1.96 is considered significant at the 0.05 level. For example, a t-value of 6.43 indicates a highly significant relationship [23].

4) p-value: The p-value indicates the probability that the observed relationship is due to chance. A p-value less than 0.05 is typically considered statistically significant. For example, a p-value <0.001 suggests a very low probability that the relationship occurred by chance, thus confirming the significance of the path coefficient [17].

5) Effect Size (f^2): The f^2 effect size measures the impact of a specific exogenous variable on an endogenous variable, calculated based on the change in the R^2 value when the exogenous variable is included in the model. Effect size values are interpreted as follows:

a) Small effect: $f^2 = 0.02$

b) Medium effect: $f^2 = 0.15$

c) Large effect: $f^2 = 0.35$ For instance, an f^2 of 0.20 indicates a medium effect, suggesting that robotics learning experience has a moderate impact on programming interest [24].

6) Variance Inflation Factor (VIF): The VIF assesses multicollinearity among the exogenous constructs. High multicollinearity can inflate the standard errors and affect the reliability of the path coefficients. VIF values greater than 5 indicate significant multicollinearity. A VIF of 1.15 suggests low multicollinearity, indicating that the estimates are reliable [17].

7) Explained Variance (R^2): R^2 quantifies the proportion of variability in the dependent variable explained by the independent variables in the model. A high R^2 value indicates that a large portion of the variability in the dependent variable is captured by the predictors, suggesting a robust model fit. Conversely, a low R^2 suggests that the predictors fail to explain much variability in the dependent variable. According to [24] R^2 values can be categorized as follows:

a) Weak: R^2 values between 0.01 and 0.25

b) Moderate: R^2 values between 0.26 and 0.49

c) High: R^2 values of 0.50 and above

8) Predictive Relevance (Q^2 Predict): PLS Predict assesses the model's predictive power by generating predictions for new data and comparing them with actual observed values. The key metrics include:

a) Q^2 Predict: Indicates the predictive relevance of the model for a specific endogenous construct. A Q^2 Predict value greater than 0 indicates predictive relevance [25].

b) RMSE (Root Mean Squared Error): Evaluates the accuracy of the predictions. Lower RMSE values indicate better predictive performance.

c) MAE (Mean Absolute Error): Measures the average magnitude of the prediction errors. Lower MAE values indicate more accurate predictions.

9) Decision based on Statistical Analysis: The decision indicates whether the hypothesis is supported. If the p-value is less than 0.05 and the path coefficient (β) is in the hypothesized

direction, the hypothesis is typically considered supported. For instance, if β is 0.45, t-value is 6.43, and p-value <0.001, the hypothesis that robotics learning experience positively affects programming interest is supported [23].

IV. Results

A. Measurement Model

The measurement model was evaluated to determine the reliability and validity of the constructs used in this study. Table I presents the factor loadings, composite reliability (CR), and average variance extracted (AVE) for the constructs: Engagement (ENG), Interaction (ACT), Challenge (CHA), Competency (COMP), and Interest (INT).

TABLE I. Factor Loadings, Composite Reliability (CR), and Average Variance Extracted (AVE) for Engagement, Interaction, Challenge, Competency, and Interest Constructs

Construct	Items	Factor Loading	CR	AVE
ENG	ENG1The activity was enjoyable. ENG2 The activity was interesting.	0.916 0.905	0.795	0.829
ACT	ACT1 Asking questions to other students. ACT2 Observing other students. ACT3 Discussions with other students. ACT4 Interacting with other students.	0.715 0.742 0.819 0.741	0.751	0.571
CHA	CHA 1 The activity was challenging.	1.000		
COMP	COMP1 I felt that I learned important skills COMP1 I felt a sense of accomplishment after completing the activity. COMP1 The activity improved my competency in the subject area.	0.798 0.807 0.824	0.738	0.656
INT	INT1 The activity increased my curiosity and interest in this area. INT2 The activity encouraged me to learn more about this topic.	0.901 0.858	0.724	0.774

The Engagement construct was assessed through two items: "The activity was enjoyable" (ENG1) and "The activity was interesting" (ENG2), achieving high factor loadings of 0.916 and 0.905, respectively. With a composite reliability (CR) of 0.795 and an average variance extracted (AVE) of 0.829, these results demonstrate strong internal consistency and convergent validity, confirming reliable measurement of Engagement in this study.

The Interaction construct, measured by four items with factor loadings ranging from 0.715 to 0.819, yielded a CR of 0.751 and an AVE of 0.571. While these figures are acceptable, the lower factor loadings suggest the need for item refinement to better capture the essence of interaction in robotics learning.

The Challenge construct was represented by a single item, "The activity was challenging" (CHA1), which showed a perfect factor loading of 1.000. However, reliance on a single item may not fully encompass the multifaceted nature of challenges encountered by students.

For the Competency construct, three items achieved factor loadings between 0.798 and 0.824, resulting in a CR of 0.738 and an AVE of 0.656. These values indicate satisfactory reliability and validity, effectively reflecting students' perceived learning outcomes from robotics activities.

Lastly, the Interest construct comprised two items: "The activity increased my curiosity and interest" (INT1) and "The activity encouraged me to learn more" (INT2), with factor loadings of 0.901 and 0.858, respectively. The CR was 0.724 and the AVE 0.774, confirming robust internal consistency and good convergent validity, indicating effective measurement of increased interest and curiosity in programming.

In summary, while Engagement and Interest exhibited strong psychometric properties, some constructs, particularly Interaction, may benefit from item refinement. Overall, these findings affirm the model's effectiveness in capturing critical dimensions of the robotics learning experience and its influence on programming interest.

B. Structural Model

The structural model, as shown in Fig. 4, was assessed to test the hypothesized relationships among the constructs. Table II presents the results of the hypothesis testing, and Table III displays the R^2 values for the endogenous latent constructs.

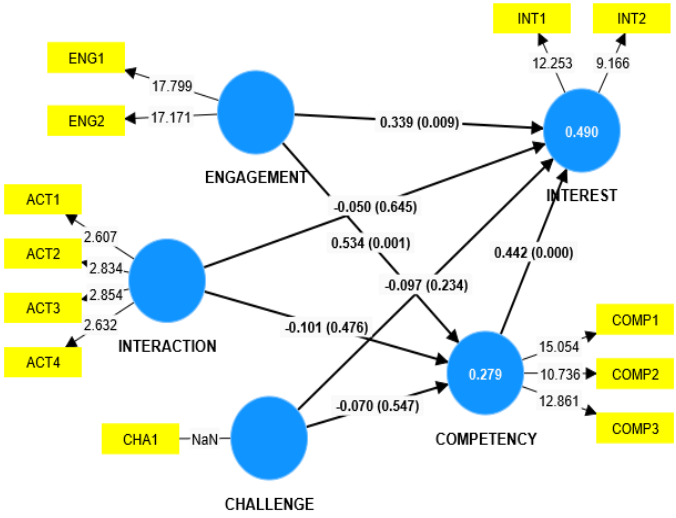


Fig. 4. Structural model analysis using SmartPLS.

TABLE II. HYPOTHESIS TESTING- RESULTS OF STRUCTURAL MODEL (SIGNIFICANT AT $P^{***} < 0.001$, $P^{**} < 0.01$, $P^{*} < 0.05$)

Hypothesis	β,	*t*-Value	*p*-Value	f^2	*VIF*	Decision
H1	-0.070	0.603	0.547	0.006 small	1.059	Not Supported
H2	-0.097	1.189	0.234	0.017 small	1.066	Not Supported
H3	0.442	4.226	0.000	0.276 medium	1.386	Supported***
H4	0.534	3.223	0.001	0.331 medium	1.194	Supported**
H5	0.339	2.602	0.009	0.142 small	1.588	Supported**
H6	-0.101	0.712	0.476	0.012 small	1.151	Not Supported
H7	-0.050	0.461	0.645	0.004 small	1.165	Not Supported

TABLE III. THE R^2 VALUE FOR THE ENDOGENOUS LATENT CONSTRUCTS

Constructs	R^2	Results
Competency	0.279	Weak
Interest	0.490	Moderate

Following this assessment, the study aimed to explore the structural relationships between programming interest and learning experiences within the robotics module using a structural equation modeling (SEM) approach. The analysis indicated that the challenge component did not significantly impact students' perceived competency (H1: $\beta = -0.070$, $p = 0.547$) or their interest in programming (H2: $\beta = -0.097$, $p = 0.234$). This finding underscores a misalignment between the difficulty of tasks and the students' readiness, suggesting that merely increasing challenge levels may not lead to improved learning outcomes unless accompanied by appropriate scaffolding.

Conversely, the hypothesis that competency positively impacts interest (H3: $\beta = 0.442$, $p < 0.001$) was strongly supported, confirming that students who perceive themselves as competent in programming exhibit a higher level of interest.

Engagement also emerged as a significant predictor of both competency (H4: $\beta = 0.534$, $p < 0.01$) and interest (H5: $\beta = 0.339$, $p < 0.01$). These results underscore the dual role of engagement in educational settings, as it not only enhances learning outcomes but also fosters a deeper interest in programming. Engaging and enjoyable activities can captivate students' attention, encouraging active participation and sustained motivation.

However, interaction did not significantly affect competency (H6: $\beta = -0.101$, $p = 0.476$) or interest (H7: $\beta = -0.050$, $p = 0.645$), suggesting that the quality of peer interactions may need enhancement to effectively contribute to learning outcomes. Effective scaffolding and support during collaborative tasks are crucial to maximizing the potential benefits of interaction.

The model demonstrated moderate predictive power, with R^2 values of 0.490 for interest and 0.279 for competency, indicating that it explains a reasonable portion of variance in both constructs.

V. DISCUSSION

The hypothesis testing revealed that engagement and competency had a significant positive effect on students' interest in programming, while the constructs of interaction and challenge showed lower influence. The findings suggest that the developed model has moderate predictive power, indicating that students' experiences with robotics can moderately predict their interest in programming. Overall, this study provides valuable insights into how engagement and competency influence students' interest in programming through robotics. The results suggest that creating engaging learning experiences, aligned with students' skill levels, is essential for fostering interest in programming and preparing students for the demands of the Fourth Industrial Revolution.

In terms of active involvement, students were deeply engaged, especially when the robot successfully moved toward a slipper. This engagement was driven by the necessity to program the robot, as it would not move without the students' input. For example, Fig. 5 depicts a group of students discussing the development of a program during the coding phase.

Fig. 5. A group of students engaged in discussion while developing a program during the coding phase.

Regarding enthusiasm, students were excited to tackle the tasks, primarily because the activity required problem-solving. The problems were presented in the form of a game, specifically making the robot knock over a slipper. This game was inspired by a traditional Malaysian game in which a player uses a slipper to topple a stack of slippers. By adapting the game to involve robots, students had the opportunity to explore programming while also appreciating a traditional Malaysian concept. This fusion of elements likely contributed to the increased enthusiasm among the students. Feedback from students supports this:

"I was very happy to use robots in this programming learning session because I could understand the subject more deeply."

"I was excited and curious to code for this robot."

Persistence was another notable aspect, with students showing determination to complete the tasks despite challenges. Some groups encountered difficulties in making the robot move as intended, requiring them to repeatedly adjust program values, such as the delay. The robot's movement varied depending on factors like battery power, tire condition, and servo motor settings. Through a series of tests, students eventually understood the relationship between the program and the robot's output. They also applied computational thinking techniques,

such as pattern recognition. Feedback reflecting this persistence includes:

"It was fun yet tiring because of the repeated errors, but we got to learn something new in the end."

"I felt skeptical at first about whether we would manage to finish, but as I worked with my group, I became confident we could succeed."

Beyond engagement, the Interaction construct also demonstrated satisfactory factor loadings, indicating that students actively interacted with their peers during the activity. This was evident from responses like:

"I feel happy because I got to discuss different ideas and solutions with other students."

"I enjoyed this programming learning. Robots and friends made the activities fun."

"I felt confused and worried that I wouldn't be able to contribute to my team, but as the instructor helped us out, I felt more connected."

The structural model results reveal that engagement and perceived competency play a crucial role in fostering students' interest in programming and robotics. Significant relationships were found between engagement and competency (H4) and between engagement and interest (H5). These findings suggest that when students are actively engaged in learning activities, they are more likely to feel competent, which in turn increases their interest in the subject. Additionally, the significant link between competency and interest (H3) indicates that as students perceive an improvement in their skills, their curiosity and eagerness to learn more also grow, reinforcing the positive cycle between competence and interest.

However, the study also found that interaction did not have a significant impact on either competency or interest. Despite the common belief that peer discussions and collaborative learning enhance educational outcomes, the results indicate that these interactions did not translate into measurable improvements in students' competency. Although students enjoyed discussing ideas and solutions with their peers, as reflected in qualitative feedback, these exchanges may not have been sufficiently focused or impactful to deepen their engagement with the subject matter. To enhance the effectiveness of interactions in future implementations, it may be necessary to structure these activities more intentionally, ensuring that they promote meaningful cognitive engagement and skill development rather than just social interaction.

Conversely, the hypotheses examining the impact of challenge on both competency (H1) and interest (H2) were not supported. This suggests that the level of difficulty presented by the activities did not significantly contribute to students' perceptions of their skills or their interest in the subject. While challenges are necessary for learning, they must be carefully balanced to avoid discouragement. Student responses, such as the view that programming was complicated and difficult or that the activity was interesting but challenging, underscore the importance of making challenges approachable. Maintaining this balance is crucial for sustaining engagement and fostering positive learning outcomes. These findings highlight the need for well-designed, appropriately challenging activities to enhance students' perceived competency and sustain their interest in STEM education.

The study's findings highlight the importance of carefully structuring interactions and challenges to enhance competency and interest effectively. Without adequate support, these elements may fail to produce the desired outcomes. Creating meaningful learning experiences in programming requires thoughtful technology integration, including appropriate applications, media, systems, and approaches. Misaligned or improper use of technology can hinder students' confidence and problem-solving skills. A well-designed framework that incorporates contextual and meaningful learning objectives is essential for optimizing technology integration [26]. Furthermore, technologies such as augmented reality (AR) can support STEM-based activities [27] and be seamlessly integrated into such a framework.

Despite these insights, the study has limitations. The relatively lower factor loadings for the Interaction construct indicate that the measurement of this construct could benefit from refinement. Additionally, the reliance on a single item for the Challenge construct may not fully capture the multifaceted nature of the challenge experienced by students. Future research should address these limitations by developing more comprehensive measures for these constructs and exploring their impact in different educational contexts

VI. Conclusions

In conclusion, this study highlights the critical factors influencing students' interest in programming through robotics education. To enhance engagement, educators must focus on creating interactive and enjoyable learning experiences that actively involve students. Incorporating hands-on robotics activities can significantly stimulate curiosity and motivation, leading to improved learning outcomes. Additionally, fostering students' perceived competency in programming is essential; scaffolded learning activities and continuous feedback should be implemented to reinforce their skills and confidence. While interaction and challenge play vital roles in the learning process, they must be carefully structured with adequate support to avoid overwhelming students. Thus, educators should ensure that challenges are appropriate to students' skill levels, enabling meaningful interactions that enhance learning without causing disengagement.

A significant limitation of this study was the students' tendency to hasten through the reflection phase, which limited opportunities for deeper learning. To address this, future iterations of the module could include additional activity cycles with structured reflection phases, allowing students to analyze algorithms and their outcomes to better understand cause-and-effect relationships. Incorporating guided reflection tasks, supported by AI tools such as ChatGPT, could further enhance this process by fostering thoughtful analysis and encouraging meaningful insights.

As advancements in AI continue to reshape education, future modules could also introduce a dedicated phase for students to explore AI concepts and applications. While this presents an exciting opportunity to align with emerging technological

trends, it also raises challenges related to resource allocation and the need for specialized teacher training. By addressing these aspects, robotics education can adopt a forward-looking approach, equipping students with essential skills for navigating and contributing to the evolving technological landscape, while maintaining a structured and engaging learning environment.

ACKNOWLEDGMENT

The author acknowledges the Prototype Development Research Grant (PRGS), grant number PRGS/1/2021/ICT01/UKM/02/2, funded by the Ministry of Higher Education (MOHE), Malaysia.

REFERENCES

[1] A. Peremol, R. Latih, and M. Abu Bakar, "MyJavaSchool: Students' Perceptions and Motivation for Computer Programming," Asia-Pacific Journal of Information Technology and Multimedia, vol. 8, no. 2, pp. 71–78, Dec. 2019, e-ISSN: 2289-2192.

[2] L. Holland, "Robotics education: Engaging students in programming and computational thinking," J. STEM Educ., vol. 11, no. 2, pp. 45–58, 2020.

[3] R. N. Jawawi et al., "Enhancing computational thinking and programming skills through educational robotics: A longitudinal study," Comput. Educ., vol. 183, pp. 104728, 2022.

[4] H. Susilo et al., "Increasing STEM graduates: Strategies and challenges," Int. J. STEM Educ., vol. 3, no. 1, p. 12, 2016.

[5] S. Ziaeefard et al., "STEM education in the UK: Status and challenges," Brit. J. Educ. Technol., vol. 47, no. 6, pp. 1234–1246, 2016.

[6] A. Nasa and S. Anwar, "STEM education in Malaysia: Achievements and prospects," Malaysian J. Educ., vol. 40, no. 2, pp. 87–102, 2016.

[7] D. A. Kolb, Experiential Learning: Experience as the Source of Learning and Development. Prentice Hall, 1984.

[8] D. A. Kolb and A. Y. Kolb, "Learning styles and learning spaces: Enhancing experiential learning in higher education," Acad. Manag. Learn. Educ., vol. 4, no. 2, pp. 193–212, 2005.

[9] M. Masril, B. Hendrik, H. T. Fikri, A. H. Hazidar, B. Priambodo, E. Naf'an, I. Handriani, Z. P. Putra, and A. K. Nseaf, "The Effect of Lego Mindstorms as an Innovative Educational Tool to Develop Students' Creativity Skills for a Creative Society," J. Phys. Conf. Ser., vol. 1339, Int. Conf. Computer Science and Engineering (IC2SE), pp. 012082, Apr. 2019

[10] N. Pellas, "Assessing Computational Thinking, Motivation, and Grit of Undergraduate Students Using Educational Robots," J. Educ. Comput. Res., vol. 62, no. 2, pp. 620–644, 2024.

[11] N. F. A. Zainal, R. Din, M. F. Nasrudin, S. Abdullah, A. H. A. Rahman, N. H. S. Abdullah, K. A. Z. Ariffin, S. M. Jaafar, and N. A. Majid, "Robotic Prototype and Module Specification for Increasing the Interest of Malaysian Students in STEM Education," Int. J. Eng. Technol., vol. 7, no. 3.25, pp. 286–290, 2018, doi: 10.14419/ijet.v7i3.25.17583.

[12] N. F. A. Zainal et al., "Primary and Secondary School Students' Perspective on Kolb-Based STEM Module and Robotic Prototype," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 4-2, pp. 1394–1401, Sept. 2018, doi: 10.18517/ijaseit.8.4-2.6794.

[13] G. P. Fernández and C. Cossio-Mercado, "AelE: A Versatile Tool for Teaching Programming and Robotics Using Arduino," Proc. Latin Am. Comput. Conf. (CLEI), Buenos Aires, Argentina, 2024, pp. 1–10, doi: 10.1109/CLEI64178.2024.10700288.

[14] A. Konak, C. Clark, and M. Nasereddin, "Exploring the impact of interaction, engagement, and challenge on students' learning experiences," J. Inform. Technol. Educ.: Res., vol. 13, pp. 141–154, 2014.

[15] T.-C. Huang, C.-C. Chen, and Y.-W. Chou, "Animating eco-education: To see, feel, and discover in an augmented reality-based experiential learning environment," Comput. Educ., vol. 96, pp. 72–82, 2016.

[16] A. D'Ausilio, "Arduino: The advantages and potential applications in educational robotics," J. Educ. Robotics, vol. 4, no. 1, pp. 25–36, 2012.

[17] J. F. Hair et al., A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 2nd ed. SAGE Publications, 2017.

[18] R. P. Bagozzi and Y. Yi, "On the evaluation of structural equation models," J. Acad. Market. Sci., vol. 16, no. 1, pp. 74–94, 1988.

[19] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," J. Market. Res., vol. 18, no. 1, pp. 39–50, 1981.

[20] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," J. Acad. Market. Sci., vol. 43, no. 1, pp. 115–135, 2015.

[21] W. W. Chin, "The partial least squares approach to structural equation modeling," Modern Methods for Business Research, vol. 295, no. 2, pp. 295–336, 1998.

[22] J. Henseler, C. M. Ringle, and R. R. Sinkovics, "The use of partial least squares path modeling in international marketing," Adv. Int. Market., vol. 20, pp. 277–319, 2009.

[23] J. F. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a silver bullet," J. Market. Theory Pract., vol. 19, no. 2, pp. 139–152, 2011.

[24] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, 2nd ed. Lawrence Erlbaum Associates, 1988.

[25] S. Geisser, "A predictive approach to the random effect model," Biometrika, vol. 61, no. 1, pp. 101–107, 1974.

[26] N. F. Husin, H. M. Judi, and S. A. Hanawi, "Meaningful Programming Learning Using Technology Integration: Implementation and Application Level," Asia-Pacific Journal of Information Technology and Multimedia, vol. 10, no. 2, pp. 77–94, Dec. 2021.

[27] N. A. A. Nordin, N. A. Majid, and N. F. A. Zainal, "Mobile Augmented Reality Using 3D Ruler in a Robotic Educational Module to Promote STEM Learning," Bull. Electr. Eng. Informat., vol. 9, no. 6, pp. 2499–2506, 2020, doi: 10.11591/eei.v9i6.2067.

Lampung Batik Classification Using AlexNet, EfficientNet, LeNet and MobileNet Architecture

Rico Andrian, Rahman Taufik, Didik Kurniawan, Abbie Syeh Nahri, Hans Christian Herwanto
Department of Computer Science, University of Lampung, Bandar Lampung, Indonesia

***Abstract*—This study explores the application of image recognition technology based on Convolutional Neural Network (CNN) to classify Lampung batik motifs. Four CNN architectures are employed, namely AlexNet, EfficientNet, LeNet, and MobileNet. The dataset consist of ten motif classes, including Siger Ratu Agung, Sembagi, Jung Agung, Kembang Cengkih, Granitan, Abstract, Sinaran, Tambal, Kambil Sicukil, and Sekar Jagat. It comprises a total of 1000 images of Lampung Batik motifs, which were enhanced using preprocessing techniques such as rotation, shifting, brightness adjustment, and zooming. The classification results show that AlexNet achieves an accuracy of 95.33%, EfficientNet achieves 98.00%, LeNet achieves 99.33%, and MobileNet achieves 98.00%. The best accuracy result was achieved by the LeNet architecture, attributed to its suitability for small datasets. While some classification errors occurred due to similarities in patterns and variations in image positions, employing more advanced methods to better distinguish between similar motifs could address these challenges. This study highlights the effectiveness of CNN architectures in supporting the recognition of Lampung Batik motifs, contributing to the understanding and preservation of Indonesia's cultural heritage.**

Keywords*—*Lampung Batik; image classification; convolutionl neural network; AlexNet; EfficientNet; LeNet; MobileNet

I. INTRODUCTION

Batik is a fundamental part of Indonesia's cultural identity and has been officially recognized by UNESCO as part of the nation's rich cultural heritage. This traditional art form is created through a unique process involving the application of wax and canting to produce intricate patterns on cloth, resulting in works of art with high aesthetic and cultural value [1]. Each region in Indonesia presents its cultural philosophy through different batik motifs, including Lampung Batik. Lampung Batik motifs include images of people, animals, sea creatures, buffaloes, elephants, ships, houses, trees of life and supporting elements such as coffee leaves, cloves, pepper and betel leaves, representing Lampung's cultural identity [2].

However, despite its cultural significance, recognizing Lampung Batik motifs based on their colour, pattern, and texture remains challenging for the human eye, especially when motifs share similar visual elements. This difficulty underscores the importance of employing technology to simplify identification, enabling broader public access to knowledge about Lampung Batik motifs and aiding in their preservation.

In recent years, advancements in computer vision, particularly Convolutional Neural Networks (CNN), have offered robust solutions for image classification tasks. CNN use artificial neural networks to process and analyze images, producing significant results in digital image recognition [3][4]. Numerous CNN architectures have been developed, such as AlexNet, EfficientNet, LeNet, and MobileNet, each with unique advantages [5]. AlexNet is a breakthrough that has combined ConvsNet and dropout regularization techniques [6]. Another architecture is EfficientNet, a CNN model developed by Google in 2019, specifically for object recognition or image classification. EfficientNet currently has eight models, from EfficientNet-B0 to EfficientNet-B7, with increasingly higher levels of accuracy [7] [8]. LeNet is a convolutional neural network (CNN) architecture initially developed for image processing tasks. The architecture comprises six layers: three convolutional layers, two pooling layers, and one fully connected layer [9]. MobileNet uses a technique called separable convolution to reduce the number of model parameters [10].

Previous studies on regional batik image recognition have applied machine learning and deep learning techniques to identify distinct motifs from various regions in Indonesia. One approach used the AlexNet architecture to classify Lamongan batik motifs, achieving an accuracy of 98% on a dataset of 790 images divided into three categories [11]. The EfficientNet-B2 architecture, fine-tuned for optimal performance, was applied to classify Papuan batik motifs [12]. The dataset consisted of 213 images divided into four classes: Raja Ampat, Cendrawasih, Asmat, and Tifa Honai. This approach achieved an accuracy of 72%. Research on Lampung Batik classification has also explored machine learning approaches. One study employed the K-Nearest Neighbor (KNN) algorithm combined with the Gray Level Co-occurrence Matrix (GLCM) for feature extraction [13]. Using a dataset of 100 images divided into four categories with 25 images per class, the method achieved the highest accuracy of 97.96% with an orientation angle of 135° and k = 7. Another study expanded the dataset by including non-Lampung motifs, specifically Parang Kusumo and Parang Rusak, and utilized a backpropagation artificial neural network, achieving an accuracy of 92% [14].

However, existing studies on Lampung Batik motifs are limited by small and less diverse datasets and a need for more exploration into more advanced architectures or methods. This study explores the application of image recognition techniques using CNN architectures, including AlexNet, EfficientNet, LeNet, and MobileNet, for classifying Lampung Batik motifs. The dataset includes ten motif classes: Siger Ratu Agung, Sembagi, Jung Agung, Kembang Cengkih, Granitan, Abstract, Sinaran, Tambal, Kambil Sicukil, and Sekar Jagat. The study aims to investigate the potential of CNN-based image recognition in identifying Lampung Batik motifs, contributing

to the understanding and preserving Indonesia's cultural heritage.

II. Research Method

This study uses the AlexNet, EfficientNet-B4, LeNet, and MobileNet architectures to classify Lampung Batik images with a dataset generated through augmentation techniques. The research process is detailed in Fig. 1.

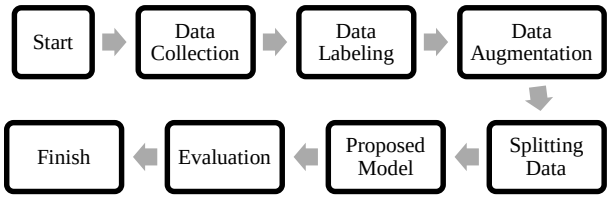


Fig. 1. Research method.

A. Dataset Collection

The dataset used is 1000 images of Lampung Batik motifs with ten classes. Images for each class are separated and saved in a folder named according to each class. The machine will then read the dataset at the beginning of the process, the images of Lampung Batik motifs, and the class names in each folder.

B. Data Labeling

Data labelling in a dataset is the process of adding information or labels to each example of data. This labelling functions to identify or categorize data so that machine learning or deep learning models can understand and process information more effectively. Labelling data in a dataset can involve different tasks, depending on the data analysis goals to be achieved [15].

C. Data Augmentation

This study employs data augmentation techniques such as rotation, shifting [16], and zooming, with the image size adjusted to 224 x 224 pixels. [17]. These augmentation techniques were selected to enhance dataset diversity by generating new variations of the existing dataset and altering objects' position, scale, and orientation [18].

D. Split Data

Data division is carried out by dividing the data into three primary subsets, namely training data, validation data, and test data. Training data is needed as the primary material for training data [19]. The training data itself takes up about 70% of the entire image. Data validation uses data equal to 15% of the whole picture. Test data is used to test a model's performance and success rate. The test data equals 15% of the entire image [20].

E. AlexNet, EfficientNet, LeNet, and MobileNet Architecture Training

The training model uses four architectures, namely AlexNet, EfficientNet, LeNet, and MobileNet, with a dataset of 100 images for each type of Lampung batik motif. Model training using hyperparameters such as epoch, batch size, and learning rate. The hyperparameter values used are in Table I.

TABLE I. Hyperparameters

Hyperparameter	AlexNet	EfficientNet	LeNet	MobileNet
Epoch	10	10	20	20
Batch-size	8	8	32	32
Optimizer	Adam	Adam	Adam	Adam
Learning-rate	0.0001	0.0001	0,001	0,001

Table I contains the hyperparameter values applied in this research. The hyperparameters in this study were determined through experimentation using various advanced callback libraries, including ReduceLROnPlateau and EarlyStopping [21]. ReduceLROnPlateau is a technique that reduces the learning rate when there is a stagnation or slowdown in performance improvement during the training process [22].

F. Evaluation

Performance evaluation in this study is a crucial stage to assess the effectiveness and accuracy of the developed model or algorithm [23]. This process evaluates how effectively the model can accurately predict unseen test data. Metrics such as F1-score, precision, accuracy, and recall are used to measure its performance [24].

III. Result and Discussion

This section presents the results and analysis of Lampung Batik image classification using CNN and explains the evaluation and implementation of the classification process. This section reviews the model's accuracy and evaluation metrics for Lampung Batik image recognition.

A. Dataset Collection

The dataset used in this research consists of 10 classes, each containing 100 images. The batik motifs can be seen in Fig. 2, and the diversity of each motif can be seen in Fig. 3.

B. Dataset Augmentation

The original dataset, consisting of 50 images per class stored in Google Drive, was expanded through augmentation techniques, including rotation, shifting, brightness adjustment, and zooming. These augmentations were applied with specific parameters: a 100° rotation, a 0.1 shift, brightness ranging from 0.05 to 2.0, and a 20% zoom. As a result, the dataset increased to 100 images per class. The final number of images for each class after augmentation is presented in Table II.

Fig. 2. Lampung Batik motifs.

Fig. 3. Lampung Batik motifs diversity.

TABLE II. DATASET AUGMENTATION LAMPUNG BATIK

Name Class	Amout Dataset
Batik Sembagi	100
Batik Granitan	100
Batik Jung Agung	100
Batik Sekar Jagat	100
Batik Siger Ratu Agung	100
Batik Kambil Sicukil	100
Batik Kembang Cengkih	100
Batik Sinaran	100
Batik Tambal	100
Batik Abstrak	100

C. AlexNet Achitecture Model

The AlexNet architectural model has 11 layers, consisting of five convolution layers, three max-pooling layers, two fully connected layers, and one output layer [25]. AlexNet is a CNN architecture that emphasizes the depth of its model, with training parameters reaching 70 million [26]. The dataset is fed to the first layer and read by the model. Multiple image samples are processed in a convolutional layer. The convolution layer functions to retrieve and help the model understand the characteristics of Lampung Batik motifs by using filters and the ReLu activation function. The filters in the convolution layer are matrix arrays that help adjust the image pixel values to fit the model. The ReLU activation function converts negative pixel values to zero while leaving positive pixel values unchanged. The pooling layer in this model is tasked with extracting essential features from the previous layer (convolution layer) [27]. AlexNet uses max-pooling as the pooling layer type. The fully connected layer in this model connects one feature to another of the Lampung Batik motif image. The connected features will be arranged to form a pattern that matches the arrangement of the features. Subsequently, the resulting output will be processed using softmax activation to determine the prediction of the image to one of the ten classes of Lampung Batik motifs.

D. EfficientNet Architecture Model

The EfficientNet-B4 architecture has a different type and number of layers than AlexNet, with only about 17 million parameters. The layers in EfficientNet-B4 consist of MBConv, an advancement of the layers used in the MobileNet architecture. The EfficientNet-B4 architecture consists of 10 blocks forming its primary structure, which includes fully connected, where this block is responsible for extracting abstract features in images [28]. The output from the previous block process will be processed and added with average pooling and flattening, which then results in a one-dimensional array or allows the model to recognize objects and patterns so that classification of Lampung Batik images is obtained in the form of classes of Lampung Batik motifs.

E. LeNet Architecture Model

LeNet-5 is a CNN-based multilayer network that represents an advancement over earlier versions of LeNet. It features additional layers and more adjustable parameters compared to its predecessors, enhancing its capacity for feature extraction and learning [29]. LeNet-5 has six layers: the input layer that receives the image, two convolutional layers for extracting features in the image, two pooling or subsampling layers for reducing image dimensions by half, and fully-connected layers. LeNet-5 is often used in more complex pattern recognition, such as facial or object recognition.

F. MobileNet Architecture Model

MobileNet Architecture is designed to provide high performance with limited power sources [30]. This architecture uses Depthwise Separable Convolution to reduce the parameters and calculations required to train and run the model. MobileNet can provide comparable or even more performance in some tasks with small model sizes and slight complexity. MobileNet architecture comprises an input layer, a standard convolutional layer, depthwise separable convolutional layers, a fully connected layer, and an output layer.

G. Model Evaluation

Evaluation of the AlexNet, EfficientNet, LeNet, and MobileNet architectural models to classify Lampung Batik images using precision, recall, accuracy and F1-score values.

Table III presents the precision, recall, and f1-score values for the AlexNet architecture. Each class has an excellent precision value, namely reaching 100%, except for the Kembang Cengkih, Batik Tambal, Batik Jung Agung, and Batik Kambil Sicukil classes; the Kembang Cengkih Batik class has the lowest precision value, namely 62.00%. The recall value reached 100% in each class, except for the Kembang Cengkih Batik, Garnitan Batik and Sekar Jagat Batik classes. The Kembang Cengkih Batik class has the lowest recall value, 62.00%.

Table IV presents the EfficientNet performance, where all batik classes achieved a precision score of 100%, except for the Batik Kambil Sicukil and Batik Jung Agung classes. The Jung Agung Batik class has the lowest precision value, 80.00%. The Kambil Sicukil Batik class has the lowest recall value, 93.00%. The Kambil Sicukil Batik class has a precision value of 92.86%. This was caused by 1 FP value occurring in the Kambil Sicukil Batik class, which should have been included in the Jung Agung Batik class. The model predicts incorrectly because there are similarities in the Jung motif pattern found in Batik Kambil Sicukil and Batik Jung Agung.

TABLE III. CONFUSION MATRIX ALEXNET ARCHITECTURE

Batik Motif Class	Results Model		
	Precision	Recall	F1-score
Batik Sembagi	100%	100%	100%
Batik Siger Ratu Agung	100%	100%	100%
Batik Granitan	100%	96.00%	98.00%
Batik Kambil Sicukil	94.00%	100%	97.00%
Batik Tambal	82.00%	100%	90.00%
Batik Sinaran	100%	100%	100%
Batik Jung Agung	93.00%	100%	97.00%
Batik Kembang Cengkih	62.00%	62.00%	62.00%
Batik Abstrak	100%	100%	100%
Batik Sekar Jagat	100%	80.00%	89.00%
Accuracy		95.33%	
Error		4.67%	

TABLE IV. CONFUSION MATRIX EFFICIENTNET ARCHITECTURE

Batik Motif Class	Results Model		
	Precision	Recall	F1-score
Batik Sembagi	100%	100%	100%
Batik Siger Ratu Agung	100%	100%	100%
Batik Granitan	100%	94.74%	97.30%
Batik Kambil Sicukil	92.86%	93.00%	92.93%
Batik Tambal	100%	100%	100%
Batik Sinaran	100%	100%	100%
Batik Jung Agung	80.00%	100%	88.89%
Batik Kembang Cengkih	100%	93.75%	96.67%
Batik Abstrak	100%	100%	100%
Batik Sekar Jagat	100%	80.00%	89.00%
Accuracy		98.00%	
Error		2.00%	

TABLE V. CONFUSION MATRIX LENET ARCHITECTURE

Batik Motif Class	Results Model		
	Precision	Recall	F1-score
Batik Sembagi	100%	100%	100%
Batik Siger Ratu Agung	100%	100%	100%
Batik Granitan	100%	100%	100%
Batik Kambil Sicukil	100%	100%	100%
Batik Tambal	100%	100%	100%
Batik Sinaran	100%	100%	100%
Batik Jung Agung	94.00%	100%	97.00%
Batik Kembang Cengkih	100%	100%	100%
Batik Abstrak	100%	100%	100%
Batik Sekar Jagat	100%	93.00%	97.00%
Accuracy		99.33%	
Error		0.67%	

Table V presents the LeNet performance, where Batik Jung Agung has the lowest precision value of 94.00%, and the other classes achieve a precision value of 100%. The recall value for the Batik Sekar Jagat class has the lowest recall value, 93.00%, while the other classes get a recall value of 100%.

TABLE VI. CONFUSION MATRIX MOBILENET ARCHITECTURE

Batik Motif Class	Results Model		
	Precision	Recall	F1-score
Batik Sembagi	100%	100%	100%
Batik Siger Ratu Agung	100%	100%	100%
Batik Granitan	100%	100%	100%
Batik Kambil Sicukil	100%	100%	100%
Batik Tambal	100%	100%	100%
Batik Sinaran	100%	94.00%	97.00%
Batik Jung Agung	89.00%	100%	94.00%
Batik Kembang Cengkih	100%	100%	100%
Batik Abstrak	96.00%	92.00%	94.00%
Batik Sekar Jagat	100%	100%	100%
Accuracy		98.00%	
Error		2.00%	

Table VI presents the MobileNet performance, where Batik Abstract gets a precision value of 96.00%, and Batik Jung Agung gets the lowest precision value of 89.00%. In comparison, the other classes get a precision value of 100%. For the recall value, the Batik Sinaran class gets 94.00%. Batik Abstract records the lowest recall value of 92.00%, except for Batik Sinaran and Batik Abstract, all classes get a recall value of 100%.

H. Performance Comparison Between Architectures

The differences among the four architectures can be seen in Table VII. AlexNet is an 11-layer architecture with 70 million parameters for processing complex features. EfficientNet, on the other hand, consists of 10 blocks that form its primary structure, with a total of 17 million parameters to ensure efficient computation. LeNet comprises 6 layers, including an input layer for receiving images, two convolutional layers for extracting features, two pooling layers for reducing image dimensions, and fully connected layers for classification. MobileNet includes input layers, convolutional layers, depth-separable convolutional layers, fully connected layers, and output layers to support lightweight computations. MobileNetV1 contains 28 layers, incorporating depth-separable convolutions, whereas MobileNetV2 improves upon this with 53 layers, introducing inverse residuals and linear bottlenecks to enhance efficiency and performance on mobile and embedded devices.

In addition, Table VII presents an accurate comparison between the four architectures. LeNet achieves the highest accuracy for Lampung Batik classification by effectively extracting essential features through convolution and pooling layers, which preserve the spatial information crucial for image recognition. In previous Lampung Batik studies, LeNet outperforms KNN and Backpropagation due to its efficiency in recognizing patterns and resistance to overfitting. Unlike KNN,

which only measures distances in feature space, and Backpropagation, which flattens images and loses spatial information, LeNet delivers superior performance for image classification tasks. Therefore, this study addresses the limitations of smaller and less diverse datasets in previous research by exploring four CNN architectures and employing augmentation techniques to enhance dataset quantity and accuracy.

TABLE VII. RESULT COMPARISON BETWEEN ARCHITECTURES

Architecture	Layer	Parameters	Accuracy
AlexNet	11	70m	95.33%
EfficientNet	10	17m	98.00%
LeNet	6	60k	99.33%
MobileNet	53	3.4m	98.00%

IV. CONCLUSION

The study concludes that the AlexNet, EfficientNet, LeNet, and MobileNet architectures effectively classify ten Lampung Batik motif classes, including Siger Ratu Agung, Sembagi, Jung Agung, Kembang Cengkih, Granitan, Abstract, Sinaran, Tambal, Kambil Sicukil, and Sekar Jagat. The accuracy achieved by AlexNet is 95.33%, EfficientNet-B4 is 98.00%, MobileNet is 98.00%, and LeNet achieves the highest accuracy at 99.33%. The dataset was enhanced using augmentation techniques, including rotation, shifting, brightness adjustment, and zooming, to generate 1000 images to train and evaluate the models. However, the study is limited by the similarity of specific Lampung Batik motifs, occasionally leading to misclassification. Future research could leverage advanced architectures and methods to differentiate motifs with similar patterns better, further enhancing classification accuracy.

ACKNOWLEDGMENT

Experiments in this study were conducted using NVIDIA Tesla K80 and Tesla K20, facilitated by the Department of Computer Science, University of Lampung.

REFERENCES

[1] E. Steelyana, "Batik, A Beautiful Cultural Heritage that Preserve Culture and Supporteconomic Development in Indonesia," *Binus Bus. Rev.*, vol. 3, no. 1, p. 116, 2012, doi: 10.21512/bbr.v3i1.1288.

[2] R. Andrian, B. Hermanto, and R. Kamil, "The Implementation of Backpropagation Artificial Neural Network for Recognition of Lampung Batik Motive," J. Phys. Conf. Ser., vol. 1338, no. 1, 2019, doi: 10.1088/1742-6596/1338/1/012062.

[3] S. Dargan, M. Kumar, M. R. Ayyagari, and G. Kumar, "A Survey of Deep Learning and Its Applications: A New Paradigm to Machine Learning," Arch. Comput. Methods Eng., vol. 27, no. 4, pp. 1071–1092, 2020, doi: 10.1007/s11831-019-09344-w.

[4] T. Liu, S. Fang, Y. Zhao, P. Wang, and J. Zhang, "Implementation of Training Convolutional Neural Networks," 2015.

[5] S. Patel, "A comprehensive analysis of convolutional neural network models," Int. J. Adv. Sci. Technol., vol. 29, no. 4, pp. 771–777, 2020.

[6] A. Nasihin, H. Akbar, G. Firmansyah, and B. Tjahjono, "Analysis of Drowsiness Detection based on Images Using Convolutional Neural Network," Astonjadro, vol. 13, no. 2, pp. 378–388, 2024, doi: 10.32832/astonjadro.v13i2.14888.

[7] Ü. Atila, M. Uçar, K. Akyol, and E. Uçar, "Plant leaf disease classification using EfficientNet deep learning model," *Ecol Inform*, vol. 61, Mar. 2021, doi: 10.1016/j.ecoinf.2020.101182.

[8] E. Anggraini, C. Suryanti, T. Nurbella, and M. Sholihin, "Arsitektur Untuk Klasifikasi Jenis Batik Lamongan.," *Cybernetics*, vol. 6, pp. 54–60, 2022.

[9] D. Fitriati, "PERBANDINGAN KINERJA CNN LeNet 5 DAN EXTREME LEARNING MACHINE PADA PENGENALAN CITRA TULISAN TANGAN ANGKA," J. Teknol. Terpadu, vol. 2, no. 1, 2016, doi: 10.54914/jtt.v2i1.45.

[10] E. I. Haksoro and A. Setiawan, "Pengenalan Jamur Yang Dapat Dikonsumsi Menggunakan Metode Transfer Learning Pada Convolutional Neural Network," J. ELTIKOM, vol. 5, no. 2, pp. 81–91, 2021, doi: 10.31961/eltikom.v5i2.428.

[11] E. Anggraini, C. Suryanti, T. Nurbella, and M. Sholihin, "Alexnet Arsitektur Untuk Klasifikasi Jenis Batik Lamongan," vol. 6, no. 02, pp. 54–60, 2022.

[12] S. Aras, A. Setyanto, and Rismayani, "Deep Learning Untuk Klasifikasi Motif Batik Papua Menggunakan EfficientNet dan Transfer Learning," Insect (Informatics Secur. J. Tek. Inform., vol. 8, no. 1, pp. 11–20, 2022, doi: 10.33506/insect.v8i1.1865.

[13] R. Andrian, M. A. Naufal, B. Hermanto, A. Junaidi, and F. R. Lumbanraja, "K-Nearest Neighbor (k-NN) Classification for Recognition of the Lampung Batik Motifs," J. Phys. Conf. Ser., vol. 1338, no. 1, 2019, doi: 10.1088/1742-6596/1338/1/012061.

[14] R. Andrian, B. Hermanto, and R. Kamil, "The Implementation of Backpropagation Artificial Neural Network for Recognition of Lampung Batik Motive," J. Phys. Conf. Ser., vol. 1338, no. 1, 2019, doi: 10.1088/1742-6596/1338/1/012062.

[15] D. A. Sriatna, R. Andrian, and R. Safei, "Implementation of Convolutional Neural Network for Classification of Density Scale and Transparency of Needle Leaf Types," *Indonesian Journal of Artificial Intelligence and Data Mining*, vol. 7, no. 1, p. 1, Nov. 2023, doi: 10.24014/ijaidm.v7i1.26258.

[16] C. Shorten and T. M. Khoshgoftaar, "A survey on Image Data Augmentation for Deep Learning," *J Big Data*, vol. 6, no. 1, pp. 1–48, Dec. 2019, doi: 10.1186/s40537-019-0197-0.

[17] F. Kong and R. Henao, "Efficient Classification of Very Large Images with Tiny Objects," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2022-June, pp. 2374–2384, 2022, doi: 10.1109/CVPR52688.2022.00242.

[18] L. F. Sánchez-Peralta, A. Picón, F. M. Sánchez-Margallo, and J. B. Pagador, "Unravelling the effect of data augmentation transformations in polyp segmentation," Int. J. Comput. Assist. Radiol. Surg., vol. 15, no. 12, pp. 1975–1988, 2020, doi: 10.1007/s11548-020-02262-4.

[19] L. Alzubaidi et al., "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," *J Big Data*, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00444-8.

[20] X. Han, Y. Zhong, L. Cao, and L. Zhang, "Pre-trained alexnet architecture with pyramid pooling and supervision for high spatial resolution remote sensing image scene classification," *Remote Sens (Basel)*, vol. 9, no. 8, Aug. 2017, doi: 10.3390/rs9080848.

[21] S. Tripathy, R. Singh, and M. Ray, "Automation of Brain Tumor Identification using EfficientNet on Magnetic Resonance Images," Procedia Comput. Sci., vol. 218, no. 2022, pp. 1551–1560, 2022, doi: 10.1016/j.procs.2023.01.133.

[22] R. Mahesh et al., "Transformative Breast Cancer Diagnosis using CNNs with Optimized ReduceLROnPlateau and Early Stopping Enhancements," Int. J. Comput. Intell. Syst., vol. 17, no. 1, 2024, doi: 10.1007/s44196-023-00397-1.

[23] H. A. Shah, F. Saeed, S. Yun, J. H. Park, A. Paul, and J. M. Kang, "A Robust Approach for Brain Tumor Detection in Magnetic Resonance Images Using Finetuned EfficientNet," *IEEE Access*, vol. 10, pp. 65426–65438, 2022, doi: 10.1109/ACCESS.2022.3184113.

[24] R. Ghawi and J. Pfeffer, "Efficient Hyperparameter Tuning with Grid Search for Text Categorization using kNN Approach with BM25 Similarity," *Open Computer Science*, vol. 9, no. 1, pp. 160–180, Jan. 2019, doi: 10.1515/comp-2019-0011.

[25] D. M. Belete and M. D. Huchaiah, "Grid search in hyperparameter optimization of machine learning models for prediction of HIV/AIDS test results," Int. J. Comput. Appl., vol. 44, no. 9, pp. 875–886, 2022, doi: 10.1080/1206212X.2021.1974663.

[26] M. Avşar and K. Polat, "Classifying Alzheimer's disease based on a convolutional neural network with MRI images," *Journal of Artificial Intelligence and Systems*, vol. 5, no. 1, pp. 46–5, 2023, doi: 10.33969/ais.2023050104.

[27] A. E. Maxwell, T. A. Warner, and L. A. Guillén, "Accuracy assessment in convolutional neural network-based deep learning remote sensing studies—part 2: Recommendations and best practices," Jul. 01, 2021, MDPI AG. doi: 10.3390/rs13132591.

[28] L. Alzubaidi et al., Review of deep learning: concepts, CNN architectures, challenges, applications, future.

[29] J. Zhang, X. Yu, X. Lei, and C. Wu, "A Novel Deep LeNet-5 Convolutional Neural Network Model for Image Recognition," *Comput. Sci. Inf. Syst.*, vol. 19, no. 3, pp. 1463–1480, 2022, doi: 10.2298/CSIS220120036Z.

[30] B. J. B. Nair, B. Arjun, S. Abhishek, N. M. Abhinav, and V. Madhavan, "Classification of Indian Medicinal Flowers using MobileNetV2," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2024, pp. 1512–1518. doi: 10.23919/INDIACom61295.2024.10498274.

Optimization of DL Technology for Auxiliary Painting System Construction Based on FST Algorithm

Pengpeng Xu*, Guo Chen
Engineering Training Center, Shandong Huayu University of Technology, Ezhou, 253000, China

***Abstract*—The continuous development of computers has brought about the emergence of many image processing software, but these software have relatively limited functions and cannot learn and create works according to the prescribed style. To make it easier for ordinary people to create artistic style paintings, this study proposes the construction of an auxiliary painting system based on finite state transducer algorithm-optimized deep learning technology. The results demonstrated that when there were 12 images, the accuracy of the optimized convolutional neural network model in extracting image features increased by 1.1% compared to before optimization. When the number of images was 1, the optimized model reduced the image feature extraction time by 15.1s compared to before optimization. Compared with other algorithms, the accuracy of extracting image style information based on a convolutional neural network was the highest at 80% under different iteration times. The research algorithm has improved the accuracy and time of extracting image style information.**

***Keywords*—Finite state transducer; deep learning; CNN; auxiliary painting; style transfer**

I. Introduction

As a visual art, painting can stimulate people's imagination and creativity. Through the observation and practice of painting, people can cultivate their creativity, form a unique way of thinking and problem-solving ability [1]. In recent years, with the rapid development of industrial automation and intelligent technology, spraying, as a key link in the field of industrial manufacturing, has gradually received widespread attention. In the field of modern industrial manufacturing, spraying technology as a key surface treatment process, its accuracy and efficiency are directly related to the final quality of products and market competitiveness [2-3]. However, the traditional spraying system has many problems in the construction process, such as low spraying accuracy, serious material waste and high manual operation cost. In recent years, the development of intelligent spraying robots and automated spraying systems has provided a new direction to solve these problems. In the automatic development of spraying system, Fuzzy SynST Technology (FST) can effectively optimize the spraying process through state conversion, avoid repetitive programming, and reduce human error [4-5]. And automatically diagnose and adjust faults such as nozzle blockage to improve construction efficiency. In the spraying system, FST is prone to lack of control accuracy due to complex environment, and it is difficult to cope with changeable construction scenarios [6]. Deep learning (DL) optimizes spraying paths and parameters through big data analysis and adaptive learning to improve construction efficiency and quality. At the same time, DL can adjust the spraying strategy in real time to better respond to environmental changes and reduce human intervention [7]. In view of this situation, in order to enable most ordinary people to integrate the style of painting art into their works, this study proposed a deep learning technology based on FST algorithm optimization, and innovatively constructed an auxiliary spraying system (APS) based on FST and DL, aiming to improve the intelligence level of the auxiliary spraying system. This study innovatively optimized the Convolutional Neural Network (CNN) model based on the FST, using FST as the output layer of the model and constructing APS based on the TensorFlow framework. The main contribution is the proposal of APS construction based on FST-optimized DL technology, which has significant implications for the successful transfer of painting styles in images.

The research structure has six sections. Section II is a review of the current research status of DL and FST algorithms. Section III is a study on APS based on FST-optimized DL technology. Section IV is the experimental verification of the proposed research method. Discussion is given in Section V. Section VI is a summary of the research content.

II. Related Works

DL is a ML method based on artificial neural networks that can perform nonlinear transformations and feature extraction on complex data [8]. Yu K et al. proposed a DL-based auxiliary diagnosis scheme for breast cancer to solve the problem of low diagnostic efficiency of breast cancer due to the lack of high-quality medical resources in remote areas. This scheme was based on DL model for transfer learning to gain a diagnostic model. This method improved the diagnostic efficiency of breast cancer to 98.19%, and could be used for auxiliary diagnosis in hospitals in remote areas [9]. Zhou X et al. proposed a smart automatic tagging scheme based on deep Q-network to improve the accuracy of Human Activity Recognition (HAR) in healthcare Internet of Things. This scheme identified fine-grained patterns by extracting advanced features from sequential motion data. This method better solved the problem of insufficient sample labeling [10]. Wan S et al. proposed a real-time HAR method based on DL model to solve the problem that traditional methods cannot recognize complex and real-time human activities. This method utilized CNN for local feature extraction and preprocessed the data through denoising, normalization, and other methods. This method was

superior to other traditional methods and improved the accuracy of HAR [11]. Chohan M et al. proposed a DL-based plant disease detection model to promptly detect various diseases caused by bacteria, fungi, and viruses in plants. This model could use images of plant leaves to detect plant diseases, improving the accuracy of image detection of diseased plants, with an accuracy rate of up to 98.3% [12]. Chowdhury M E H et al. proposed a DL architecture based on EfficientNet to classify tomato diseases to lower down the adverse influences of diseases on plants and weaken the drawbacks of continuous human monitoring. This method could improve the segmentation accuracy of leaf images and has shown excellent performance in the ten class classification of images, with an accuracy of 99.89% [13].

Compared with other data structures, FST has higher spatial efficiency and query performance when processing large-scale string collections. Abro WA et al. proposed a model combining weighted FST and BERT architecture to reduce the cost and time of collecting high-quality labeled data. This model utilized weighted FST to enhance the fine-tuning of BERT-like architecture. Compared with other models, this model had a higher recall rate and F1 score, which can reduce the need for massive supervised data [14]. Mohammadghuliha M et al. constructed a frequency controllable acoustic sensor for guided wave detection in order to simplify the hardware of phased array systems and reduce the cost of guided wave based systems. FSAT was made by patterning spiral electrodes on a piezoelectric plate. The generation of directional guided waves in the main structure of the converter has been significantly improved, reducing the cost of the system [15]. Dolatian et al. designed a type of finite state machine with two deterministic FSTs to address the issue of limited state processing not fully capturing the productivity of unbounded replication. This sensor was easy to design and debug in practice, and had linguistic motivation in the origin semantics of the transducer. This sensor could capture almost all processes, which can be found in online repetitive databases [16]. Martin K et al. proposed a bidirectional motion device based on FST to eliminate the descriptive costs of bidirectional motion, non-determinism, and scanning, especially the cost of converting to deterministic or non-deterministic finite automata. This method was more powerful in bidirectional motion than unidirectional motion under deterministic conditions [17]. Somerset W. E. et al. proposed a novel bending ultrasonic transducer for high-pressure environments to handle the issue of pressure imbalance caused by the internal air cavity of traditional transducers on the vibrating membrane of the transducer. The internal chamber of the transducer was filled with an incompressible fluid in the form of non-volatile oil. This method could achieve stable ultrasound measurement [18].

In summary, literature in [8] and [9] have made some progress in the field of medical image recognition, but they are still limited in real-time adaptability and accuracy in dealing with complex industrial scenes. Literature in [10] and [11] improve the recognition accuracy through human activity recognition, but it is difficult to cope with the high environmental variability in the spraying system. The plant disease recognition model proposed in literatures in [12] and [13] performs better under high noise data, but it is insufficient in extracting complex spray features. Literature in [14] combined FST and BERT to improve the recall rate, but the acquisition cost of large-scale data is high. Literatures [15] to [18] has optimized the sensor design, but it still needs to be improved in the stability and diversity of industrial spraying. DL reduces manual intervention through automatic feature extraction of neural networks and is suitable for diverse data scenarios. FST has advantages in optimizing state transition and processing big data, and can effectively improve the spatial efficiency of the algorithm. Therefore, this paper proposes the research of APS construction based on FST optimization DL technology.

III. APS Construction based on FST-Optimized DL Technology

A. Optimizing DL Technology based on FST Algorithm

A painting mainly consists of two parts, namely the content and style of the painting. Among them, painting styles have diversity, and each painter has their own unique style, expressing emotions through elements such as color and lines. Even if the content of the painting is the same, the effects displayed by different painting styles are also different [19]. Compared with traditional ML methods, the most significant advantage of DL is its ability to automatically extract and learn meaningful feature hierarchies from raw data. This hierarchical structure simulates the hierarchical organization of the human brain's neural network, where each layer can capture features of different complexity and abstraction levels [20-21]. CNN is a DL model that can automatically learn the features of images without the need for manual design or selection of feature extractors. CNN uses convolutional and pooling layers to extract local features of images and perform dimensionality reduction, thereby reducing the number of parameters and computational complexity. CNN has advantages such as high efficiency in image recognition [22-23]. Therefore, to integrate the painting styles of famous masters into daily painting works, this study extracts the style information features of images based on CNN. The structure of CNN mainly consists of convolutional layers, activation functions, pooling layers, fully connected layers, output layers, etc. The process of extracting image style features using CNN is shown in Fig. 1.

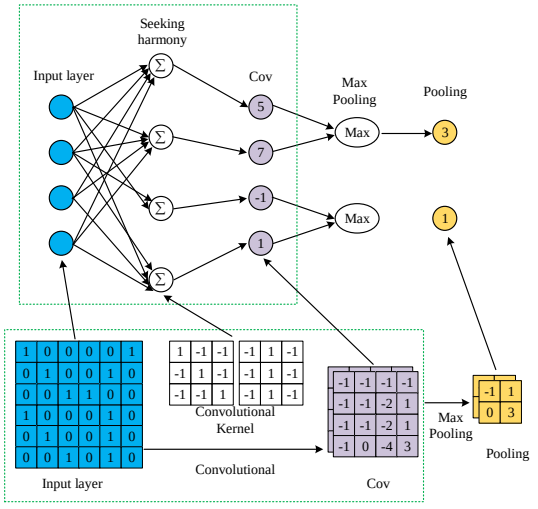


Fig. 1. Flow chart of CNN extracting image style features.

Among them, the input layer receives raw image data. The convolutional layer convolves the input image with the convolutional kernel, introducing nonlinearity by applying activation functions, enabling the network to learn complex features. The pooling layer reduces computational complexity by reducing the feature map size, by selecting the maximum or average value within the pooling window. The fully connected layer transforms the extracted feature maps into the final output. The first step in extracting the style information features of an image is to perform convolution operations, where attention should be paid to the position step size of each slide. The basic idea of the Adam algorithm is to keep an adaptive Learning Rate (LR) for each model parameter during the training process, so that parameter updates can more accurately control the step size [24]. Therefore, this study uses the Adam parameter update method combined with the First-Order Moment Estimation (1OME) and Second-Order Moment Estimation (2OME) of the loss function for calculation. The Adam parameter update steps are shown in Fig. 2.

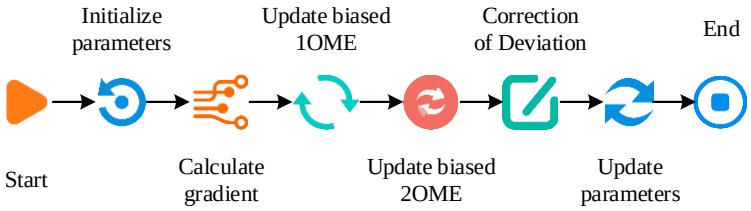


Fig. 2. Adam parameter update steps.

Firstly, the 1OME m_t is corrected using the correction formula shown in Eq. (1).

$$\hat{m}_t = \frac{m_t}{1-\beta_1^t} \tag{1}$$

In Eq. (1), β_1 is the 1OME attenuation coefficient. $\hat{m}_t$ is the corrected 1OME. t is the number of updated steps. Secondly, the 2OME v_t is corrected, and its correction expression is Eq. (2).

$$\hat{v}_t = \frac{v_t}{1-\beta_2^t} \tag{2}$$

In Eq. (2), β_2 is the 2OME attenuation coefficient. $\hat{v}_t$ is the corrected 2OME. Finally, the model parameters were updated based on the corrected $\hat{m}_t$ and $\hat{v}_t$. The formula for updating model parameters θ_{t+1} is Eq. (3).

$$\theta_{t+1} = \theta_t - \frac{\ell \hat{m}_t}{\sqrt{\hat{v}_t} + \varepsilon} \tag{3}$$

In Eq. (3), ℓ is the LR. θ_t is the parameter model before the update. ε is a hyperparameter. When performing convolution processing on each convolutional channel, different filters are used, and the calculation process is Eq. (4).

$$c_i = F\left(K_i * X + b_i\right) \tag{4}$$

In Eq. (4), K_i and b_i are the convolution kernels and biases of the i-th channel. X is the input data. c_i is the convolution result of the i-th channel. $F(\cdot)$ is a non-linear activation operation in the convolution process. The activation function of CNN is ReLU. ReLU trains in the negative area. When a neuron with a gradient of 0 appears, the gradient of this neuron and subsequent neurons will always be 0 and will no longer respond to any data, causing the correlated parameters never being updated [25]. To solve the problem of neuronal necrosis in ReLU function, this study improves ReLU using exponential linear units, and the improvement process is Eq. (5).

$$ELU(x) = \begin{cases} x, & x>0 \\ \alpha\cdot(\exp(x)-1), & x\le 0 \end{cases} \tag{5}$$

In Eq. (5), x is the input value, α is the predefined hyperparameter, and $\exp(\cdot)$ is the exponential function operation. The composition of CNN includes a max pooling layer, which discards non max information and may lose some detail information. Average Pooling (AveP) considers the mean value of all values in the pooling window, which is smoother than Maximum Pooling (MaxP) and can preserve more detailed information. The calculation of mixed pooling and AveP is shown in Fig. 3.

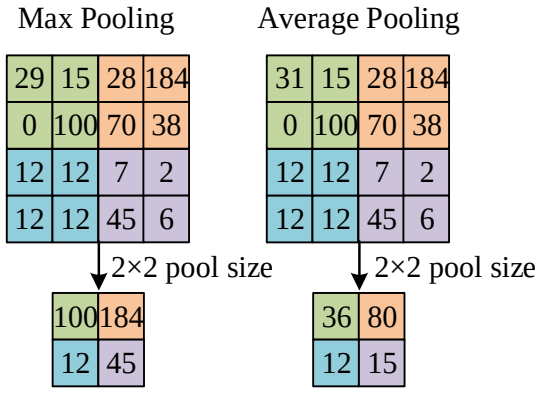


Fig. 3. Mixed pooling and AveP calculation.

The calculation of AveP G_{ij} is Eq. (6).

$$G_{ij} = \frac{1}{p\times p}\cdot\left(\sum_{i=1}^{p}\sum_{j=1}^{p} M_{ij}\right) + b \tag{6}$$

In Eq. (6), M denotes the feature map of the pooling operation, b is the bias of each channel, and $p\times p$ is the

size of the pooling region. To solve the problem of feature weakening caused by using only the max pooling layer for feature processing, this study adopts a mixed pooling method to pool the features. The calculation of mixed pooling is Eq. (7).

$$G_{ij} = \frac{1}{2}\left(\frac{1}{p \times p} \cdot \left(\sum_{i=1}^{p}\sum_{j=1}^{p} M_{ij}\right) + \max_{(p\times p)i=1,\, j=1} M_{ij}\right) + b \quad (7)$$

In Eq. (7), $\max_{(p\times p)i=1,\, j=1} M_{ij} + b$ represents the MaxP operation. To transform the image style information features extracted by CNN into a series of string states containing semantic information, this study optimizes DL technology based on FST and uses FST as the output layer of the model. The formula for the time complexity O of FST is Eq. (8).

$$O = n \times m \quad (8)$$

In Eq. (8), n is the text length and m is the pattern length. The optimization steps are as follows: Firstly, the number of states in FST and the transition relationship between states are determined. Secondly, in the output layer of the CNN model, a node layer with an equal number of FST states is created. Finally, the image feature information extracted based on the FST algorithm is transformed into a string.

B. Construction of APS

After optimizing DL technology based on FST, this study constructs APS based on the optimized model. TensorFlow is an open-source ML framework dedicated to automatic differentiation of various data flow graphs and computation of deep neural networks. This framework provides multiple advanced Application Programming Interfaces (APIs), making building and training DL models relatively simple. At the same time, it also maintains great depth and flexibility to meet the needs of researchers exploring complex models. Therefore, this study constructs APS based on the TensorFlow framework. The APS constructed mainly consists of two parts. Part 1 is the front-end page: The main functions of the system's front-end include uploading images that require style fusion, selecting the desired style, style conversion buttons, and outputting images after style conversion is completed. The process of requesting front-end image style conversion is shown in Fig. 4.

The other part is the backend of the system. The backend of APS mainly has three modules: Uniform Resource Locator (URL) request forwarding, logical functionality, and style conversion. The task of Module 1 is to pass the URL request link transmitted by the frontend to a specific function for execution. The task of Module 2 is to preprocess, transcode, encode, and store uploaded images. The task of Module 3 is to convert the style of uploaded images and return the converted images to the user. The relationship between the three modules in the APS backend is shown in Fig. 5.

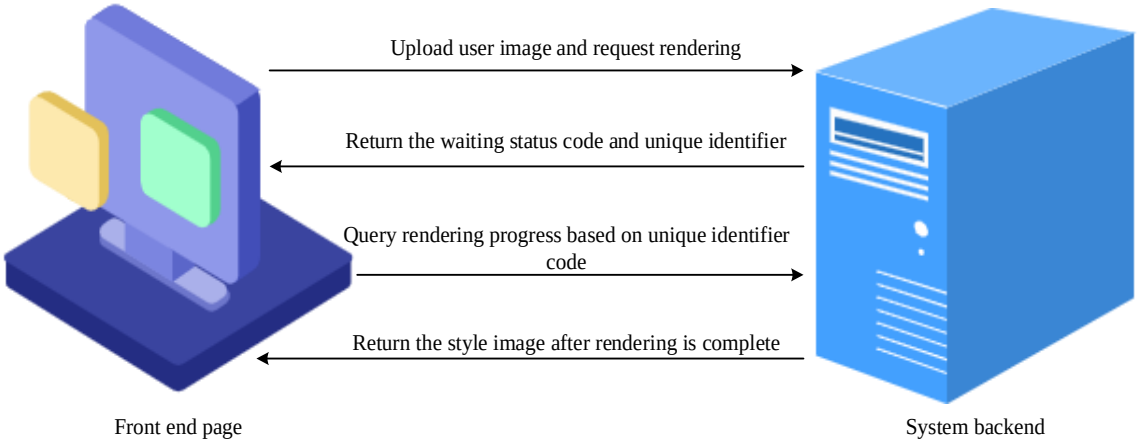


Fig. 4. Process of front-end image style conversion request.

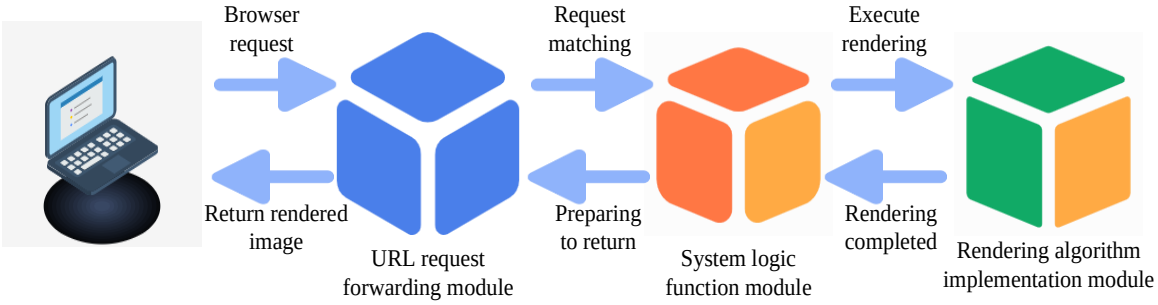


Fig. 5. The relationship between the three modules in the background of the APS.

The core module of the system backend is to extract image feature information. Due to various noises, interferences, and deformations that may exist in the original image, directly using the original image for DL model training may lead to a decrease in model accuracy. As a result, this study requires preprocessing of the original images to enhance the training effectiveness and recognition accuracy. The image data preprocessing steps are shown in Fig. 6.

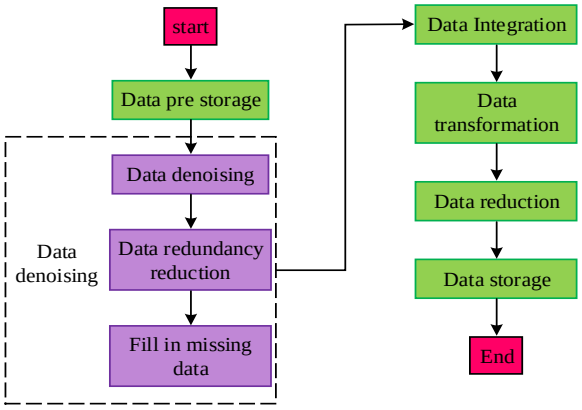


Fig. 6. Image data preprocessing steps.

Standardizing image data can adjust images of different sizes and resolutions to the same range, facilitating subsequent processing and analysis. Data standardization processing can be divided into normalization processing and z-score processing. The difference in comparison results of different data sets is due to the diversity of the characteristics of data sets and the number of samples. The performance of the algorithm on different data sets depends on the characteristics of the data, such as the resolution of the image, the complexity of the background, and the clarity of the target style. Normalizing the data can balance the weights of various dimensional features and avoid the interference of features with large or small numerical scales on the model. Among them, normalization processing can be divided into minimax normalization and mean normalization. The calculation of minimax normalization is Eq. (9).

$$\begin{cases} X = \dfrac{X_{old} - \min(X_{old})}{\max(X_{old}) - \min(X_{old})}, [0,1] \\ X = \dfrac{2\left(X_{old} - \min(X_{old})\right)}{\max(X_{old}) - \min(X_{old})} - 1, [-1,1] \end{cases} \quad (9)$$

In Eq. (9), X_{old} is the original dataset. $\max(X_{old})$ and $\min(X_{old})$ take extreme values for each column feature of the original dataset. Mean normalization maps the values of features to the range of [0,1], eliminating the influence of dimensionality on the eventual result, making different features comparable, and allowing features with potentially large distribution differences to have the same weight impact. The expression of mean normalization is Eq. (10).

$$X = \frac{X_{old} - mean(X_{old})}{\max(X_{old}) - \min(X_{old})} \quad (10)$$

In Eq. (10), $mean(X_{old})$ defines taking the mean of each column feature of the original dataset. Standardizing data using z-score involves scaling the data to a distribution centered around 0 with a standard deviation of 1. This method preserves the original data information without changing the distribution type of the original data, making the different features of the original data comparable. The formula for z-score is shown in Eq. (11).

$$\mu \ X = \frac{X_{old} - \mu}{\sigma} \quad (11)$$

In Eq. (11), μ is the vector of the mean of each column feature of the original dataset. σ is the vector of the standard deviation of each column feature in the original dataset. To better evaluate the detection model's performance, this study utilizes the $F-Score$ method for evaluation, and the formula for $F-Score$ is Eq. (12).

$$F-Score = \left(1+\beta^2\right)\frac{Precision \cdot Recall}{\beta^2 \cdot Precision + Recall} \quad (12)$$

In Eq. (12), $Recall$ represents the recall rate of abnormal data in the results. $Presion$ is the accuracy of abnormal data in the result. β is the degree of importance to the outcome. When β =1, it indicates that both have the same impact on the result. At this point, $F-Score$ is expressed as Eq. (13).

$$F-Score = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall} \quad (13)$$

IV. Analysis of APS Effect based on FST Algorithm Optimization of DL Technology Construction

A. Experimental Parameter Setting and Performance Verification

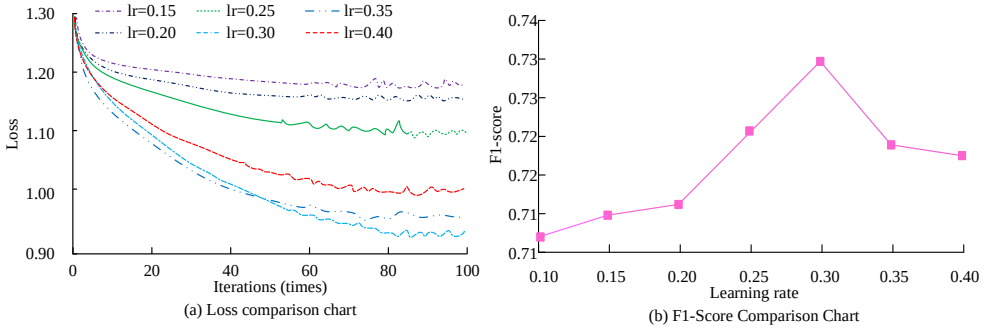
The software selected for the experiment is Python v3.5.2, and the learning framework is TensorFlow. The operating system is Windows 10, the memory is 128GB, the CPU is Intel Core (TM) i7-6700CPU @3.40GHz, and the GPU is NVIDIA GeForce GTX 750 Ti. Table I provides information on the backend functions of the system.

The size of the LR directly affects the convergence speed and state of the CNN model. Excessive LR may cause the model to oscillate near the optima and fail to converge. If the LR is too low, it may lead to slow convergence speed of the model, and even get stuck in local optimal solutions. Therefore, to obtain the best LR, this study set the LR to different values and evaluated it through the loss value and F1 Score. The statistical results are displayed in Fig. 7. In Fig. 7(a), when iterating up to 70 times, the loss curves for different LRs tend to stabilize. When the LR = 0.3, the loss value of the model is minimized. When the LR < 0.3, the loss value decreases as the LR increases. When the LR > 0.3, the loss value grows with the growth of the LR. In Fig. 7(b), when the LR is 0.3, the F1 Score value is optimal, and when the LR is < 0.3, the F1 Score value rises with the sire of the LR. When the LR is > 0.3, the F1 Score value decreases as the LR increases.

The maximum tree depth parameter (max_depth) controls the complexity of the decision tree. However, if this value is set too small, the CNN model may underfit, resulting in poor performance. When the max_depth is set too high, it may cause overfitting issues. Therefore, to obtain the optimal x_depth, this study sets the x_depth to different values and evaluates it based on the loss value and F1 Score. The statistical results of the loss value and F1 Score are shown in Fig. 8. In Fig. 8(a), when the iteration reaches 48 times, the loss curves of different max_depth tend to be stable. When the max_depth=3, the loss value of the model is the smallest; When the max_depth<3, the loss value descends with the rise of the max_depth; When the max_depth>0.3, the loss value grows with the increase of LR. In 8 (b), when the max_depth=3, the F1 Score value is optimal; When the max_depth<3, the F1 Score value grows with the increase of the max_depth; When the max_depth>3, the F1 Score value decreases with the rise of the max_depth.

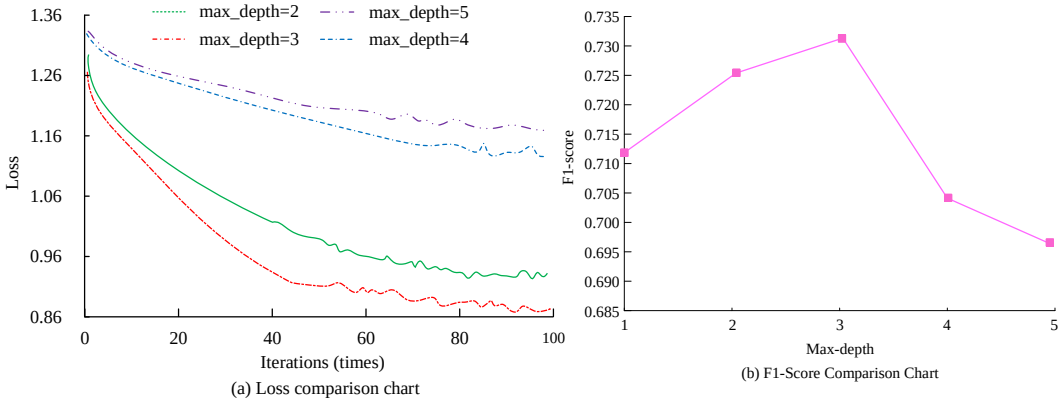
TABLE I. SYSTEM BACKEND FUNCTION SETTINGS

Serial number	Function Name	Module to which it belongs	Function Introduction
1	path	URL request forwarding module	Filter and match the links sent by the front-end
2	open/write	System logic function module	Provide read and write functionality for images
3	json	System logic function module	Responsible for processing JSON related formatted data
4	base64	System logic function module	Base64 encoding and decoding of images
5	get_unique_key	System logic function module	Generate a unique key for each user image
6	apply_async	System logic function module	Asynchronous execution of rendering process
7	settings	System logic function module	Access and modify some system settings options
8	check_img	System logic function module	Check image format
9	pool_exec	System logic function module	Provide scheduling and execution of process pools
10	style_rendering	Style conversion implementation module	Render the received image into the specified style



(a) Loss comparison chart (b) F1-Score Comparison Chart

Fig. 7. Comparison of loss values and F1 Score at different LRs.



(a) Loss comparison chart (b) F1-Score Comparison Chart

Fig. 8. Comparison between loss values and F1 Score under different max_depth.

B. APS Quality Analysis based on CNN

This study compares the recall rate and F1 Score value of image features pooled using a Maximum-Median-Mixed Pooling (MMMP) strategy with other pooling approaches. The statistical results are shown in Table II. Single Pooling Strategies (SPS) are lower than Mixed Pooling Strategies (MPS). In the SPS, the maximum recall rate and F1 Score value of the SPS are the highest, at 79.58% and 0.7350, respectively. In the MPS, the two values of the MMMP are the highest, at 81.3% and 0.7408. The two value of the three MPSs are lower than those of the MMMP strategy and the average-median-MPS, which are 80.25% and 0.7362.

TABLE II. COMPARISON OF DIFFERENT POOLING STRATEGIES

Pooling strategy	Recall (%)	F1 Score
Maximum-single	0.7958	0.7350
Average-single	0.7846	0.7328
Middle value single	0.7909	0.7335
Maximum-average-mixed	0.7966	0.7357
Average-median-mixed	0.8058	0.7370
Maximum-intermediate-mixed	0.8103	0.7408
Three mixed	0.8025	0.7362

The results of comparing the accuracy of extracting image style information based on CNN with other algorithms under different iteration times are shown in Fig. 9. The accuracy of extracting image style information using different algorithms increases with the increasing number of iterations. The accuracy of CNN in extracting image style information is higher than other algorithms, with an accuracy of 80%. The highest accuracy of the four layer Deep Neural Network algorithm (DNN) is 68.9%, because the algorithm requires numerous parameters and computational resources, which lifts the difficulty of training and tuning. The highest accuracy rates of User-based Collaborative Filtering Algorithm (UserCF), Content-based Algorithm (CBF), Probability-based Matrix Factorization (PFM), and Item-based Collaborative Filtering Algorithm (ItemCF) are 58.6%, 68.8%, 68.8%, and 67.9%, respectively.

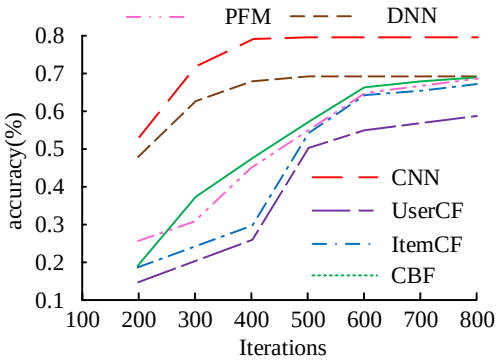
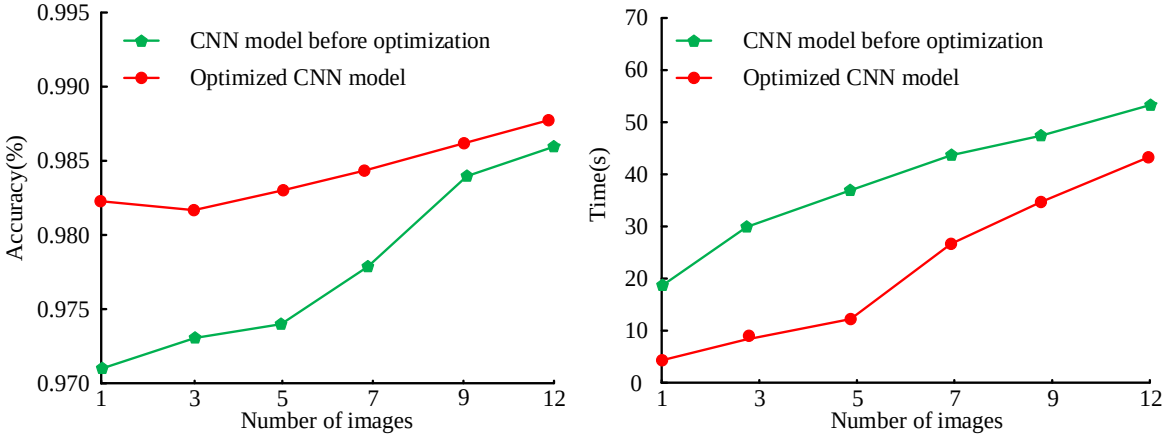


Fig. 9. The accuracy of extracting image features using different models.

In the case of different numbers of images, this study compares the accuracy and time of extracting image features based on the optimized CNN model. Fig. 10 shows the comparison results. In Fig. 10 (a), the accuracy of the optimized CNN in extracting image features increases with the increase of the number of images. When there are 12 images, the highest accuracy is 98.3%, which is 1.1% higher than before optimization. In Fig. 10(b), the running time of the pre-optimized model for extracting image features increases with the rise of the amount of images, while the optimized time decreases. When the image is 1, the optimized CNN takes a minimum of 4.7 seconds, which is 15.1 seconds shorter than before optimization. The proposed algorithm is more suitable for complex and detailed image style data sets, because the algorithm can effectively extract and process the style details in the image through the hybrid pooling strategy and the optimization of the FST layer, and improve the accuracy and efficiency of the model.



(a) The accuracy before and after optimizing the CNN model

(b) The running time before and after optimizing the CNN model

Fig. 10. Comparison of the accuracy and time of extracting image features.

In this paper, we propose an auxiliary spray system (APS) based on finite state sensor (FST) algorithm to optimize deep learning (DL) technology, and realize automatic image style extraction through convolutional neural network (CNN) model. Compared with the optimized model, it shows higher accuracy and speed in processing multiple images. When the number of images is 12, the accuracy of feature extraction reaches 98.3%, and the running time is reduced to 4.7 seconds. In addition, the maximum-median-mixed pooling (MMMP) method was used in the pooling strategy, and the recall rate and F1 score reached 81.3% and 0.7408, respectively, which was superior to the single pooling strategy. The experiment also verified the performance of CNN under different learning rate (LR) and max_depth Settings, with the best parameter configurations being LR=0.3 and max_depth=3.

V. Discussion

In this paper, a deep learning technology based on FST algorithm optimization is proposed. The accuracy of the model is increased by 1.1% when processing 12 images, and the processing time of a single image is shortened by 15.1 seconds, which is better than the existing methods and meets the requirements of rapid response in the field of industrial spraying. Compared with the scheme used in the literature [8] for the auxiliary diagnosis of breast cancer, this method has achieved a breakthrough in image processing speed. Although the literature [9] and [10] perform well in the identification of human activity (HAR), there are shortcomings in dealing with complex industrial spraying tasks; The APS model designed in this study is more suitable for the changeable construction environment. In addition, compared with the real-time HAR method in literature [11], MMMP pooling strategy is superior in terms of recall rate and F1 score, which highlights its high efficiency in image feature extraction. In terms of image style information extraction, the accuracy of this model reached 80%, which was higher than the plant disease detection model proposed in literatures [12] and [13]. At the same time, although literature [14] combines weighted FST and BERT architecture to perform well in terms of recall rate and F1 score, this study reduces the dependence on large-scale labeled data and simplifies the data preprocessing process through CNN optimization. In general, the introduction of FST optimization deep learning technology not only improves the accuracy and processing speed of image feature extraction in APS, but also shows broad application prospects in the field of industrial spraying.

VI. Conclusion

To optimize the accuracy and efficiency of the spraying system to improve product quality and market competitiveness, reduce human error and adapt to the changing construction environment, so as to achieve intelligent and efficient spraying process, reduce operating costs and reduce material waste. This study proposed APS based on FST-optimized DL technology. After optimizing DL technology based on FST algorithm, this study constructed APS based on the optimization model. The experiments indicated that when the max_depth and LR of the model were set to 0.3 and 3, the loss value and F1 Score value of the CNN were optimal. Compared with the pre-optimized CNN, the accuracy and time of extracting image features by the optimized CNN were 98.3% and 4.7s, under different numbers of images. Compared with other pooling strategies, the MMMP strategy used in this study had the best pooling effect on image features, with recall and F1 Score values of 81.3% and 0.7408. The research model has been effectively applied in assisting painting, and compared to existing models, this model has higher efficiency in extracting features. However, CNN has a large number of layers and parameters, requiring a significant amount of computation time and storage space, thus requiring high computational resources. Future research will focus on the computational efficiency of the system to reduce the computing resource requirements and further improve the performance of the assisted painting system (APS) in image style conversion. Specifically, image style recognition is enhanced by improving the feature extraction accuracy of convolutional neural network (CNN). Adjust the learning rate (LR) and maximum tree depth (max_depth) to get the best model parameters. The hybrid pooling strategy is used to optimize image feature processing to improve the recall rate and accuracy of the system.

References

[1] Ilyaevna P U, Bahodirovich T I, Davlatovich A X, Mahmudovich T M. DERMATOSCOPIC PAINTING SOME COMMON DERMATOSES. World scientific research journal, 2023, 16(2): 107-120.

[2] Cimini B A, Chandrasekaran S N, Kost-Alimova M, Miller L, Goodale A, Fritchman B, Carpenter A E. Optimizing the Cell Painting assay for image-based profiling. Nature protocols, 2023, 18(7): 1981-2013.

[3] Bakhtiyorovich K I, Shodikulovich T A. The Role of Painting in the Folk Art of Surkhandarya. International Journal of Human Computing Studies, 2021, 3(2): 26-28.

[4] Rakhmatullaevna U L. Aesthetic role of folk traditions in the development of miniature painting of the east[C]//Archive of Conferences. 2020, 8(1): 34-35.

[5] Wahyuni R, Erdiyanti E. Meningkatkan Kemampuan Motorik Halus Anak Melalui Finger Painting Menggunakan Tepung Singkong. Murhum: Jurnal Pendidikan Anak Usia Dini, 2020, 1(1): 28-40.

[6] Shlezinger N, Whang J, Eldar Y C, Dimakis A G. Model-based deep learning. Proceedings of the IEEE, 2023, 111(5): 465-499.

[7] Janiesch C, Zschech P, Heinrich K. Machine learning and deep learning. Electronic Markets, 2021, 31(3): 685-695.

[8] Saxe A, Nelli S, Summerfield C. If deep learning is the answer, what is the question?. Nature Reviews Neuroscience, 2021, 22(1): 55-67.

[9] Yu K, Tan L, Lin L, Cheng X, Yi Z, Sato T. Deep-learning-empowered breast cancer auxiliary diagnosis for 5GB remote E-health. IEEE Wireless Communications, 2021, 28(3): 54-61.

[10] Zhou X, Liang W, Kevin I, Wang K, Wang H, Yang L T, Jin Q. Deep-learning-enhanced human activity recognition for Internet of healthcare things. IEEE Internet of Things Journal, 2020, 7(7): 6429-6438.

[11] Wan S, Qi L, Xu X, et al. Deep learning models for real-time human activity recognition with smartphones. mobile networks and applications, 2020, 25(2): 743-755.

[12] Chohan M, Khan A, Chohan R, Katpar S H, Mahar M S. Plant disease detection using deep learning. International Journal of Recent Technology and Engineering, 2020, 9(1): 909-914.

[13] Chowdhury M E H, Rahman T, Khandakar A, Ayari M A, Khan A U, Khan M S, Ali S H M. Automatic and reliable leaf disease detection using deep learning techniques. AgriEngineering, 2021, 3(2): 294-312.

[14] Abro W A, Qi G, Aamir M, Ali Z. Joint intent detection and slot filling using weighted finite state transducer and BERT. Applied Intelligence, 2022, 52(15): 17356-17370.

[15] Mohammadgholiha M, Palermo A, Testoni N, Moll J. De Marchi L. Finite element modeling and experimental characterization of piezoceramic frequency steerable acoustic transducers. IEEE Sensors Journal, 2022, 22(14): 13958-13970.

[16] Dolatian H, Heinz J. Computing and classifying reduplication with 2-way finite-state transducers. Journal of Language Modelling, 2020, 8(1): 179-250.

[17] Martin K, Andreas M, Mereghetti C, Palano B S. Iterated uniform finite-state transducers: descriptional complexity of nondeterminism and two-way motion. Journal of Automata, Languages and Combinatorics, 2023, 28(3): 59-88.

[18] Somerset W E, Feeney A, Kang L, Li Z, Dixon S. Design and dynamics of oil filled flexural ultrasonic transducers for elevated pressures. IEEE Sensors Journal, 2022, 22(13): 12673-12680.

[19] Kumar V, Kalita K, Chatterjee P, Zavadskas E K, Chakraborty S A. SWARA-CoCoSo-based approach for spray painting robot selection. Informatica, 2022, 33(1): 35-54.

[20] Shorten C, Khoshgoftaar T M, Furht B. Deep Learning applications for COVID-19. Journal of big Data, 2021, 8(1): 1-54.

[21] Mohammed A, Kora R. A comprehensive review on ensemble deep learning: Opportunities and challenges. Journal of King Saud University-Computer and Information Sciences, 2023, 35(2): 757-774.

[22] Li Z, Liu F, Yang W, Peng S, Zhou J. A survey of convolutional neural networks: analysis, applications, and prospects. IEEE transactions on neural networks and learning systems, 2021, 33(12): 6999-7019.

[23] P. Preethi and H. R. Mamatha, "Region-Based Convolutional Neural Network for Segmenting Text in Epigraphical Images," Artif Intell Appl, 2023, 1(2): 119-127.

[24] Khan A H, Cao X, Li S, Katsikis V N, Liao L. BAS-ADAM: An ADAM based approach to improve the performance of beetle antennae search optimizer. IEEE/CAA Journal of Automatica Sinica, 2020, 7(2): 461-471.

[25] Parhi R, Nowak R D. Near-minimax optimal estimation with shallow ReLU neural networks. IEEE Transactions on Information Theory, 2022, 69(2): 1125-1140.

BackC&P: Augmenting Copy and Paste Operations on Mobile Touch Devices Through Back-of-device Interaction

Liang Chen[1]
School of Software Engineering, Chengdu University of Information Technology, Chengdu, China[1]
Sichuan Province Engineering Technology Research Center of Support Software of Informatization Application, Chengdu, China[1]

***Abstract*—As more and more complex applications, e.g. photo editing software and slideshow editing software, can be used on mobile touch devices, some simple operations, such as copying and pasting, are used more frequently by ordinary mobile users. However, the existing touch techniques are far from perfectly supporting these simple operations on mobile devices. In this paper, a new interactive technique BackC&P, which takes advantage of back-of-device touch input to augment copy and paste operations on mobile devices, is presented. The results of a user study that evaluated the usability of BackC&P are also presented. The findings indicate that BackC&P was about twice as fast as the currently used technique on mobile touch devices when used to complete the copy-and-paste tasks, with no significant decrease in accuracy.**

***Keywords*—Back-of-device interaction; copy and paste operations; mobile touch devices; touch interaction**

I. INTRODUCTION

Various mobile touch devices have already been widely used in our everyday lives and enable users to manipulate user interfaces with a variety of touch interactions that previous feature phones cannot support [1]-[5]. Direct touch interaction has become the mainstream interactive technology on a mobile device mainly because it provides users with better performance and experience through natural, easy-to-use, and intuitive touch gestures.

Despite the numerous advantages, direct touch interaction still has many limitations that require further improvements, especially when it is applied to mobile devices. Due to the small screen size of mobile devices, touch interaction design for mobile user interfaces is usually tedious and time-consuming. Taking the copy operation as an example, the current technique utilizes a long-press action applied on the target to trigger the copy menu, and then utilizes a tap action applied on the pop-up copy menu to complete the copy of the target. Obviously, the long-press action is already very time-consuming; acquiring the copy menu takes even more time. Similar issues exist in the paste operation as well. In the meanwhile, however, as the computing power of mobile devices continues to increase, more and more complex applications, e.g. image editing software, slideshow editing software, and storytelling software, have already been available to mobile users. Apparently, simple operations such as copying and pasting are often used in these mobile applications. Therefore, how to further improve these simple and frequently used operations on mobile touch devices is an important research topic that HCI researchers should pay more attention to and explore.

The author's previous work in [6] explored the use of back-of-device touch input for promoting front-of-device touch interactions on mobile devices, for instance, to enhance mobile text entry or to augment the zooming operations in a map application. In this paper, the author extends the use of BackAssist [6] to enhance the copy and paste operations on mobile touch devices. The prototype BackC&P utilizes the back-of-device touch input provided by BackAssist to switch the current system mode to the copy mode or paste mode. In the copy mode, a front-of-device tap on the target will complete the copy of the target; in the paste mode, a front-of-device tap on the destination will complete the paste of the target.

The purpose of BackC&P is to take advantage of back-of-device touch input to improve the user performance of completing copy and paste operations on mobile touch devices. The results of the user study indicate that BackC&P was approximately twice faster than the currently used technique on mobile devices, and there was no significant increase in the error rate.

The reminder of this paper is as follows. The paper begins with a review of a series of important research literature on back-of-device interaction in Section II. After that, the interaction design of the technique BackC&P is introduced in Section III. Then, a user study comparing user performance between using BackC&P and the currently used technique is described in Section IV, followed by a detailed comparative analysis of efficiency and accuracy in Section V. Finally, some of the research results in terms of efficiency and accuracy are discussed in Section VI. Finally, the paper is concluded in Section VII.

II. RELATED WORK

The research area that is most relevant to this research is back-of-device interaction. As its name suggests, back-of-device interaction makes use of various input units on the rear of a device to complete multifarious interactive tasks, such as text entry, target acquisition, mobile authentication, and so on. It can be used either as an exclusive manipulation technique or together with other interactive techniques, thus bringing many

benefits that can improve user performance and experience in many aspects.

A. Exclusive Manipulation via Back-of-device Interaction

When it comes to back-of-device interaction, the first reaction is that it can address the occlusion problem and the fat finger problem. One of the best-known examples is NanoTouch [7] presented by Baudisch and Chu. It enables users with back-of-device touch input to interact with digital contents that are displayed on the tiny screen of a very small handheld device.

Back-of-device interaction can also be used for promoting one-handed mobile interaction. Yang et al. [8] augmented a PDA with cursor manipulation by attaching an optical sensor on the rear of the device. With the onscreen cursor, which was controlled by back-of-device input, a user could acquire the targets located in the places where the thumb could not reach. Hasan et al. [9] also explored one-handed back-of-device cursor interaction. Their findings indicated that compared with absolute mode cursor input, relative mode cursor input achieved better performances in both positioning the cursor and selecting the targets. Fan and Coutrix [10] explored the effect of asymmetry between preferred and non-preferred hands on user performance. Their study found that the preferred hand performed better in target acquisition tasks, but for steering tasks, they found little performance difference between preferred and non-preferred hands.

Mobile text entry is another research hotspot in back-of-device interaction. With a back-attached keyboard, RearType [11] allowed users to input text on a tablet by operating the physical keyboard on its rear. In order to keep mobile devices to their original form factor, Sandwich Keyboard [12] utilized a back-adhered multi-touch sensor to substitute the back-attached physical keyboards. In addition, Buschek et al. [13] added a machine-learning algorithm to Sandwich Keyboard to reduce the typing errors. Cui et al. proposed BackSwipe [14] which enabled a user to enter text or trigger a command by drawing a word-gesture on the back of a mobile device.

Researchers have also explored employing back-of-device interaction to support other mobile manipulation scenarios. For example, Luca et al. [15], Leiva et al. [16], and Kulshreshtha and Arif [17] explored realizing mobile device authentication through back-of-device interaction to address the problem of shoulder surfing. For another example, Granell and Leiva [18], [19] utilized the built-in gyroscope and accelerometer to implement tap-based back-of-device interaction, which could be used to control camera and game applications. Furthermore, Shimon et al. [20] investigated user-defined back-of-device gestures for a series of frequently used tasks on mobile devices. They found that for the vast majority of the tasks, participants had varying mental models when designing back-of-device gestures to complete them.

Although back-of-device interaction used as an exclusive input technique can make many achievements, e.g. addressing hand occlusion and “fat fingers”, supporting touch manipulation on tiny displays, and so on, it still has some limitations. On one hand, although back-of-device input addresses hand occlusion, the performance may not be as efficient as that of front-of-device touch input [21]. The results of a user study [22] show that compared with front-of-device touch input, back-of-device touch input achieves more accurate but much slower performance in conducting pointing tasks on a mobile device. On the other hand, when a user acquires onscreen targets by tapping, back-of-device touch interaction tends to be inferior to its front-of-device counterparts because the user’s operating fingers are occluded by the device itself [23], thereby failing to provide the user with visual clues of the operating fingers which are very important for accurately acquiring the targets. Therefore, combining back-of-device interaction with other interaction techniques rather than using it alone may better exert its strengths.

B. Hybrid Manipulation with Back-of-device Interaction

Many researchers have conducted studies on combining back-of-device interaction with other interactive techniques to augment mobile device manipulation.

Corsten et al. [24] presented BackXPress, which made use of back-of-device pressure input to switch between different quasi-modes for augmenting front-of-device touch interaction. Chen et al. [6] presented BackAssist, which utilized the combinations of on and off states of the two fingers resting on the rear of a mobile device to augment mobile text entry and zooming operations in a mobile map application. Huang et al. [25] proposed TapNet, which could identify taps on a smartphone while simultaneously recognizing various tap properties, such as direction and location. With TapNet, users could utilize back-of-device or edge tapping with other forms of interaction, such as tilt and touch, to complete tasks on their mobile devices.

One-handed mobile interaction was augmented by two-sided touch interaction as well. InfiniTouch [26] enabled touch input across the entire device surface of a smartphone while maintaining the standard smartphone form factor. Through a machine learning technique, InfiniTouch could identify all fingers during single-handed interaction. Le and colleagues also investigated fingers’ comfortable area [27] and safe area [28] for one-handed smartphone interaction, which could guide the design of interactions on the back and edges.

LucidTouch [29] took advantage of a technique, which was named pseudo-transparency, to overlay the video images of the user’s hands, which were behind the device and could not be seen by the user, onto the screen of the device. With the augmented visual feedback, users could manipulate the targets on a mobile device’s screen more accurately compared with the other back-of-device interaction techniques without such visual feedback.

C. Back-of-device Interaction for Copy and Paste Operations

Among the above-mentioned studies on back-of-device interaction, several involve the copy and paste operations. In [20], participants were asked to create gestures to complete the copy and paste tasks. However, the results of their study showed that there was little consensus on the gestures designed by the participants for these two tasks. When designing gestures, some participants mimicked keyboard shortcuts, and completed copy and paste operations by

respectively drawing "C" and "V" on the back of the device. Cui et al. [14] proposed using word-gesture interaction to trigger commands. According to their design, a user could complete the copy operation by input "copy" or "replicate" on the device's back. However, they did not implement their design on a real device. In study [26], several use cases were demonstrated. For instance, with InfiniTouch [26], a user could swipe down with the index finger to copy and swipe down with the middle finger to paste. However, their study did not verify the usability of the technique through experiments.

III. BACK-OF-DEVICE INTERACTION AUGMENTED COPY-AND-PASTE

The copy and paste operations are frequently used on various electronic devices. Compared with the techniques used on desktop computers, the current technique used on mobile devices is apparently more time-consuming, as illustrated in Fig. 1. For example, the long-press action is used for triggering the copy menu and even for triggering the paste menu until the tap action replaces it to complete the same task.

The author's previous work in [6] explored making use of the two resting fingers, the index finger and the middle finger of the holding hand, on the rear of a mobile device to generate back-of-device touch input for augmenting the front-of-device touch interaction by the other hand. The hardware of the prototype, BackAssist, was built by attaching two off-the-shelf smartphones in a back-to-back fashion. Similar hardware prototypes were also utilized in many previous studies [12], [13]. The appearance of the prototype is shown in Fig. 2. The results of the user study indicate that the back-of-device input of BackAssist is easy-to-learn and can be efficiently and accurately used by ordinary mobile users [6]. Some applications enhanced by BackAssist have also been developed. For example, utilize the back-of-device input to switch between the lowercase page and the uppercase page of a soft keyboard [6].

In this paper, the author extends the use of BackAssist and explores utilizing the combinations of on and off states of the two fingers, respectively resting on Zone 1 and Zone 2 (see Fig. 2), for augmenting copy and paste operations on a mobile device. The interaction technique is named BackC&P.

With BackC&P, back-of-device input can be used for switching the current system mode to the copy mode or the paste mode, thus saving the time for the operations compared with those of currently used techniques. In the present implementation, the system modes are controlled by the back-of-device inputs, as shown in Table I. In order to complete a copy operation, the user first lifts up his/her finger on Zone 1 to switch the current system mode to the copy mode, and then taps the target by the other hand to copy the target, as shown in Fig. 3(b). Similarly, to complete a paste operation, the user first raises the finger on Zone 2 to switch the system mode to the paste mode, and then taps the desired position to paste the copied target there, as shown in Fig. 3(c). With BackC&P, there is no pop-up copy menu or paste menu, so the time for acquiring the copy menu or the paste menu is also saved. To sum up, theoretically, BackC&P can tremendously reduce the time for completing copy and paste operations compared with the existing techniques used on mobile touch devices.

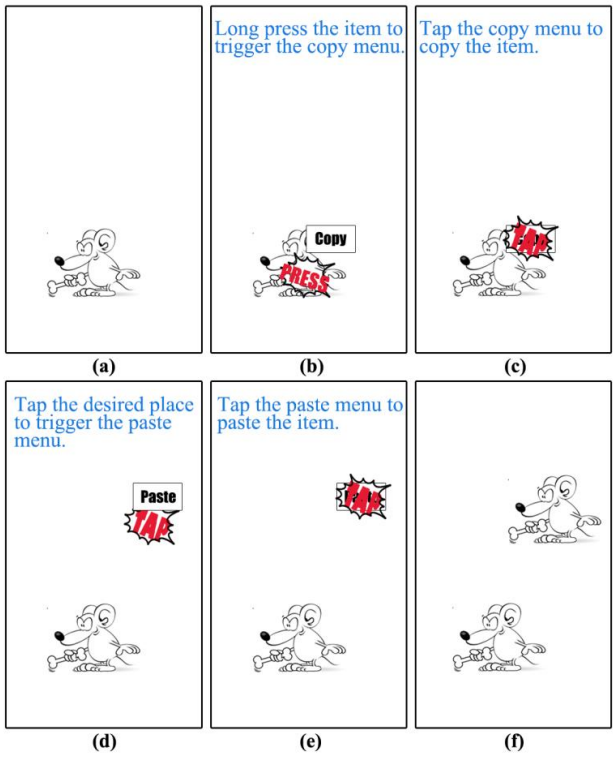


Fig. 1. A diagram demonstrates how to perform copy and paste operations with the currently used technique on a mobile touch device.

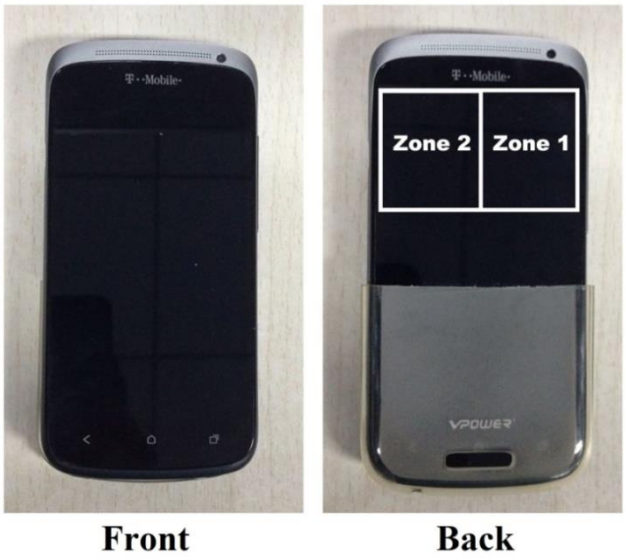


Fig. 2. The appearance of the hardware prototype.

TABLE I. THE MODES GENERATED BY BACK-OF-DEVICE INPUT

	Zone 1 without index finger on	**Zone 1 with index finger on**
Zone 2 without middle finger on	Usual Mode I	Paste Mode
Zone 2 with middle finger on	Copy Mode	Usual Mode II

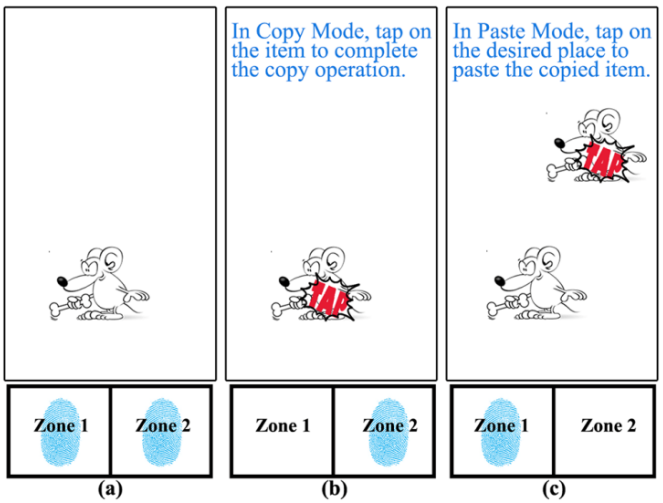


Fig. 3. A diagram of how to perform copy and paste operations with BackC&P. The blue fingerprints in the picture indicate that the corresponding finger(s) is/are on the specific Zone(s).

It should be noted that BackC&P can only save the time for the copy operation and the paste operation rather than the time for the navigation phase. The navigation time is the time that is taken to navigate from the copy position to the paste position. It may include the time for scrolling off-screen contents into the screen, the time for switching from one application to another, and so on. Usually, during a complete copy-and-paste operation, navigating to the desired place to paste the copied target may take the user a lot of time [30], [31]. Sometimes, the navigation time is much longer than the sum of the copy time and the paste time.

IV. User Study

Based on the previous analysis on the procedures of copy and paste operations on mobile devices, BackC&P is able to improve a user's performance at least in terms of the completion time. In order to verify the theoretical analysis, a user study was conducted to compare users' performances in using BackC&P and the currently used technique. Specifically, the author hoped to figure out whether BackC&P could improve users' performance in conducting copy-and-paste tasks. And if so, to what extent? In addition, the author wanted to get a more complete understanding of BackC&P. For instance, besides the completion time, were there other aspects of copy and paste operations on mobile devices affected by BackC&P? Finally, the author hoped to get the participants' first impressions on BackC&P.

A. Participants

Ten participants were recruited from a local university, ranging in age from 22 to 30. The participants' average age was 24.8 (SD = 2.10). All participants were right-handed people and they were all skilled in manipulating mobile touch devices.

B. Apparatus

The hardware prototype described in study [6] was used in this study. The experimental software was written in Java and Android SDK.

C. Task and Procedure

A copy-and-paste task was designed to simulate real copy-and-paste tasks on a mobile device for the user study. In order to minimize the impact of the navigation phase on the completion time, in the copy-and-paste task, the target to be copied and the destination to paste the copied target were presented in a single display. Therefore, the participants did not need to search for an off-screen destination by scrolling through the screen view or switching to another application.

The copy-and-paste task could be conducted by both BackC&P and the currently used technique which the author called it the traditional technique in this study. In real practice on current mobile devices, the paste menu could be triggered either by a long-press action or by a tap action, so both methods were enabled to activate the paste menu although the participants were encouraged to trigger the paste menu by tapping upon the destination, which could reduce the time for the paste operation.

Each trial began with displaying a start button below the inactivated target. The distance between the center of the target and the center of the start button was 370 pixels. After the participant successfully acquired the start button, timing started and the target, a blue circle in the center of the display, was activated at the same time. The participant then conducted the copy operation. Once the target was successfully copied, four circles with the radius of 10 pixels larger than that of the target would be rendered in the four locations around the target, respectively in its northwest, northeast, southeast and southwest. The four circles represented the potential locations for pasting the copied target. The real location for pasting the target was called the destination. The destination was highlighted in green while the other three circles, serving as distractors, were rendered in grey. Finally, the participant pasted the target in the destination.

Before the study began, each participant was required to fill out a pre-study questionnaire to gather demographics. Then a brief introduction about the copy-and-paste task and a training session about how to perform the copy-and-paste task were given. After that, the participant was allowed to practice performing the tasks. When he or she felt skilled enough, ten blocks of trials would be given to complete. Short breaks were permitted between trials or blocks. At the conclusion of the study, each participant was asked to fill out a post-study questionnaire to collect subjective feedbacks.

D. Experimental Design

In the copy-and-paste task, three target sizes (radius = 30, 50, 70 pixels; respectively similar to the sizes of keys of the virtual keyboard, app icons, and thumbnails of pictures on a smartphone), two target-destination (from the center of the target to the center of the destination) distances (224 and 335 pixels, as shown in Fig. 4), and four potential locations for the destination were used. As a result, there were totally 24 (Size × Distance × Destination) different tasks for each interaction technique.

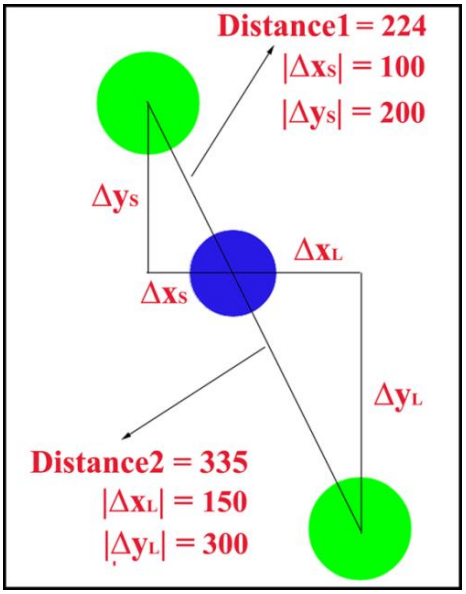


Fig. 4. The two target-destination distances for the task (the subscript 'S' denotes short and the subscript 'L' denotes long).

A within-subjects design was utilized for the experiment. Each participant conducted the copy-and-paste tasks using both BackC&P and the traditional technique. The order of using the two techniques was counterbalanced. For each technique, there were totally 10 blocks of trials. Each block contained all the 24 different copy-and-paste tasks and these tasks would appear in a random order.

To sum up, the experiment design was as follows:

10 participants ×
2 Techniques ×
10 blocks ×
3 Sizes ×
2 Distances ×
4 Destinations
= 4800 trials.

V. Results and Analysis

A. Completion Time Analysis

The completion time is the time that is taken between the acquisition of the start button and the completion of pasting the copied target. It includes the copy time and the paste time. The copy time is defined as the time between the selection of the start button and the completion of copying the target. The paste time is defined as the time between the completion of the copy operation and the completion of pasting the copied target.

Before conducting the data analysis, the records that were marked as error ones were removed from the dataset. The grand mean of the completion time of the adjusted data was 2.10 seconds (SD = 1.06 seconds).

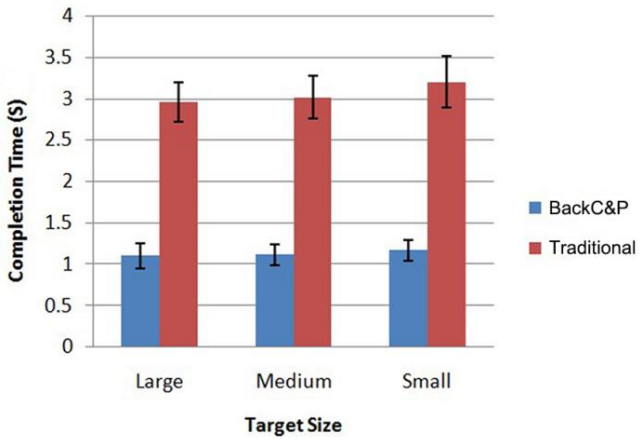


Fig. 5. Mean completion times of both techniques for each target size.

After the data adjustment, a repeated measures ANOVA was applied to the collected records. The result demonstrated a significant difference for Technique ($F(1,9) = 666.272$, $p < 0.001$), with the mean completion times of 1.13s for BackC&P and 3.06s for the traditional technique. BackC&P was almost twice faster than the traditional technique. One thing should be pointed out was that in the pre-study questionnaires nine participants chose the older method, which utilized the long-press action, when they answered the question "How do you trigger the paste menu on your smartphone?" However, after they were encouraged to use the tap action to trigger the paste menu in the study, only eight of the 2400 trials were completed by using the long-press actions. Therefore, if the participants utilized their frequently used method in the study, the difference in the completion times would have been even greater.

A significant main effect for Size ($F(2,18) = 17.813$, $p < 0.001$) was also found. Post hoc analysis indicated that the completion time of small targets (30 pixels) was significantly different from those of medium (50 pixels) and large targets (70 pixels). This was in line with the author's expectation that it would take more time to copy and paste a target whose size was much smaller than the fingertip of the operating finger. In addition, there was a significant interaction between Technique and Size ($F(2,18) = 12.526$, $p < 0.001$). A post hoc test indicated that BackC&P performed significantly better than the traditional technique in all three target sizes. Fig. 5 illustrates the mean completion times of both techniques for each target size.

The author also calculated the mean completion time of the trials that were operated by BackC&P and marked as error ones. The result was 2.60s, which was still shorter than that (3.06s) of the correct trials which were conducted by the traditional technique.

B. Copy Time Analysis

The grand mean copy time of the adjusted dataset was 1.16s (SD = 0.77s). A repeated measures ANOVA revealed a significant main effect for Technique ($F(1,9) = 616.068$, $p < 0.001$), with mean copy times of 0.48s and 1.81s for BackC&P and the traditional technique respectively. A significant main effect for Size ($F(2,18) = 9.506$, $p < 0.01$) was found as well.

Post hoc analysis indicated that the copy time of small targets was significantly different from those of medium and large targets. There was a significant interaction between Technique and Size ($F(2,18) = 6.151$, $p < 0.01$). Post hoc analysis showed that BackC&P performed significantly better than the traditional technique in all three target sizes. Fig. 6 shows the mean copy times of both techniques for each target size.

C. Paste Time Analysis

The grand mean paste time of the adjusted data was 0.95s (SD = 0.33s). A repeated measures ANOVA revealed a significant difference for Technique ($F(1,9) = 321.630$, $p < 0.001$), with mean paste times of 0.65s and 1.24s for BackC&P and the traditional technique respectively. A strong main effect for Size ($F(2,18) = 45.612$, $p < 0.001$) was also observed. Post hoc analysis indicated that the paste time of each target size was significantly different from those of the others. In addition, there was a significant interaction between Technique and Size ($F(2,18) = 20.731$, $p < 0.001$). Post hoc analysis showed that BackC&P performed significantly better than the traditional technique in all three target sizes. Fig. 7 shows the mean paste times of both techniques for each target size.

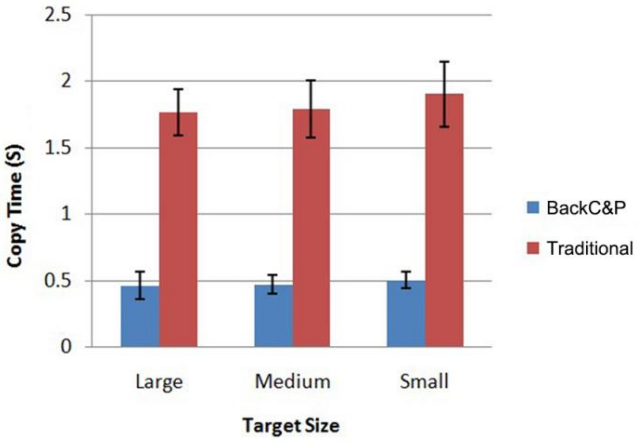


Fig. 6. Mean copy times of both techniques for each target size.

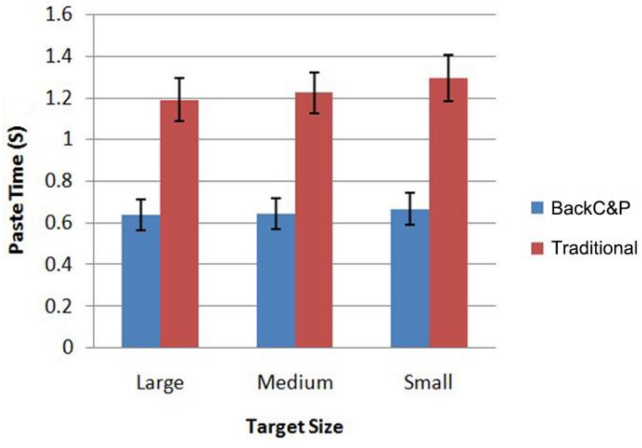


Fig. 7. Mean paste times of both techniques for each target size.

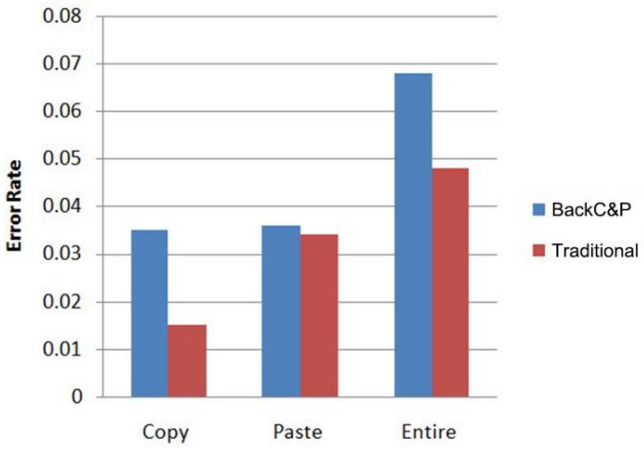


Fig. 8. Error rates of the copy operation, the paste operation, and the whole copy-and-paste operation.

D. Entire Error Analysis

There were totally 276 trials marked as error ones, in which participants made either copy errors or paste errors, or both. The grand mean error rate was 5.8%.

A repeated measures ANOVA showed no significant difference for Technique ($F(1,9) = 3.447$, $p = 0.096$), with mean entire error rates of 6.8% and 4.8% for BackC&P and the traditional technique respectively. Also, no significant main effect for Size ($F(2,18) = 2.059$, $p = 0.157$) was found. Fig. 8 shows the error rates of the copy operation, the paste operation, and the whole copy-and-paste operation.

E. Copy Error Analysis

There are four types of errors, which may occur during a copy operation, when using BackC&P, as shown in Table II. For the traditional technique, there are two types of errors: pressing outside the target and missing the copy menu.

There were totally 122 trials marked with copy errors, of which 85 trials was performed by BackC&P and 37 trials by the traditional technique. The number of copy errors of each error type of BackC&P was listed in Table II. Note that, there were two trials which committed both Copy Error I and Copy Error II. For the traditional technique, seven errors belonged to pressing outside the target while 30 errors pertained to tapping outside the copy menu.

The grand mean of the copy error rate was 2.5%. A repeated measures ANOVA revealed a significant difference for Technique ($F(1,9) = 9.618$, $p < 0.05$), with mean copy error rates of 3.5% and 1.5% for BackC&P and the traditional technique respectively. No significant main effect for Size ($F(2,18) = 1.696$, $p = 0.211$) was found.

F. Paste Error Analysis

There are four types of errors, which may occur during a paste operation using BackC&P, as shown in Table III. For the traditional technique, there are three types of errors: pressing outside the destination (Traditional Paste Error Type I, abbreviated TPET I), tapping outside the destination (TPET II), and missing the paste menu (TPET III).

TABLE II. THE COPY ERROR TYPES OF BACKC&P

Error Type	Descriptions	Error Number
Copy Error I	Hit the target on the front screen while the back-of-device input is in the Usual Mode II.	68
Copy Error II	Hit the target on the front screen while the back-of-device input is in the Paste Mode.	7
Copy Error III	Hit the target on the front screen while the back-of-device input is in the Usual Mode I.	0
Copy Error IV	Miss the target on the front screen.	12

TABLE III. THE PASTE ERROR TYPES OF BACKC&P

Error Type	Descriptions	Error Number
Paste Error I	Hit the destination on the front screen while the back-of-device input is in the Usual Mode II.	76
Paste Error II	Hit the destination on the front screen while the back-of-device input is in the Copy Mode.	5
Paste Error III	Hit the destination on the front screen while the back-of-device input is in the Usual Mode I.	1
Paste Error IV	Miss the destination on the front screen.	6

Fig. 9. The summary of answers collected from the post-questionnaires.

There were totally 168 trials marked with copy errors, of which 86 trials was conducted by BackC&P and 82 trials by the traditional technique. The number of paste errors of each error type of BackC&P was listed in Table III. Note that, there were two trials which committed both Paste Error I and Paste Error II. For the traditional technique, two errors belonged to TPET I, 24 errors belonged to TPET II, and the other 65 errors belonged to TPET III.

The grand mean paste error rate was 3.5%, which was higher than the grand mean copy error rate. A repeated measures ANOVA demonstrated no significant difference for Technique ($F(1,9) = 0.047$, $p = 0.834$), with mean paste error rates of 3.6% and 3.4% for BackC&P and the traditional technique respectively. In addition, no significant main effect for Size ($F(2,18) = 0.714$, $p = 0.503$) was found.

G. User Feedback

At the end of the study, a post-study questionnaire was answered by each participant. The purpose of the questionnaire was to collect the participants' first impressions on the interaction technique BackC&P.

From the post-study questionnaires, positive feedback on BackC&P was received from the participants that six of the ten participants chose BackC&P as their preferred technique for completing the copy-and-paste tasks. The other four participants treated the two techniques equally. None of participants specifically chose the traditional technique as their preferred technique.

In the post-study questionnaire, each participant was also asked to rate the items on a scale from 1 to 7, with 7 being the strongly agree. The summary of the collected results from the questionnaires is illustrated in Fig. 9. It can be seen that, on the whole, the participants deemed that BackC&P was easy to learn, easy to operate, comfortable to use, and less time-consuming.

VI. DISCUSSIONS

From the user study, the author found that BackC&P outperformed the traditional copy-and-paste technique on mobile devices in terms of efficiency. BackC&P achieves this mainly for two reasons. To begin with, BackC&P requires less front-of-device touch interactions for item acquisition than the traditional technique does. It accomplishes a copy-and-paste task with only two front-of-device touch actions, a tap to acquire the target and another tap to acquire the destination. As for the traditional technique, it needs four item acquisitions on the frontal touchscreen to complete the same task. In addition, BackC&P does not utilize the action of long-press, which is particularly time-consuming compared to interactions such as tapping [32], thereby tremendously saving the time for the copy operation.

In terms of error rate, the author found that for BackC&P, the most majority of the errors in copy and paste operations were caused by unsuccessfully lifting up the dedicated finger on the rear rather than by lifting the wrong finger on the rear, or by unsuccessfully acquiring the target or destination on the front screen. The author speculates that this might be due to the participants' attempt to finish the tasks in a shorter time. As copy and paste operations used in daily life are not as many and intensive as in the user study, these types of errors may be far less in actual use.

Also in terms of errors, the author found that for the traditional technique, the participants committed many more errors in acquiring the paste menu than acquiring the copy menu. The author deems that this difference is mainly due to the different mechanisms by which they trigger the two types of menus. For the copy operation, the user long-presses the target to trigger the copy menu, so he or she has more time to prepare to acquire the copy menu compared with the time to prepare to acquire the paste menu which is triggered by tapping. That is, acquiring a menu by a tap action following another tap action is less accurate than acquiring a menu by a tap action following a long-press action. It is interesting and meaningful to conduct a more comprehensive study in the future to investigate on the user performance in completing various tasks that require successive touch actions. The results

will provide us with more insights into designing better mobile touch user interfaces.

VII. CONCLUSION

Direct touch input enables users to interact with mobile devices with spontaneous and easy-to-use touch gestures. However, its limitations, e.g. time-consuming, still exist and negatively affect user experiences, especially in some frequently used simple tasks, e.g. copy and paste operations. In this paper, BackC&P, a mobile interactive technique which augments the copy and paste operations through the assistance of back-of-device touch input, is presented. The results of the user study indicate that with BackC&P users' efficiency in conducting copy and paste operations was tremendously improved on a mobile touch device, nearly two times faster than the currently used technique, and the accuracy was not significantly degraded during the entire process.

The current technique supports to copy and paste individual items, such as an image, a word, a chat message, a web link, etc. In the future, the author will explore extending the current technique to copy and paste a series of continuous items, such as several continuous words or sentences.

ACKNOWLEDGMENT

The author would like to express gratitude to the participants who participated in the user study. This research is funded by the Scientific Research Foundation of CUIT (No.KYTZ202274) and the National Natural Science Foundation of China (No. 62172081).

REFERENCES

[1] M.Jain and R. Balakrishnan, "User learning and performance with bezel menus," in Proceedings of the 2012 CHI conference on Human Factors in Computing Systems (CHI), 2012, pp.2221-2230.

[2] B. Poppinga, A. S. Shirazi, N. Hence, W. Heuten, and S. Boll, "Understanding shortcut gestures on mobile touch devices in Proceedings of the 16th international conference on Human computer interaction with mobile devices and services (MobileHCI), 2014, pp.173-182.

[3] K. Schramm, C. Gutwin, and A. Cockburnl, "Supporting Transitions to Expertise in Hidden Toolbars," in Proceedings of the 2016 CHI conference on Human Factors in Computing Systems (CHI), 2016, pp.4687-4698.

[4] T. Han, J. Liu, K. Hasan, M. Fan, J. Kim, J. Li, X. Fan, F. Tian, E. Lank, and P. Irani, "PinchList: Leveraging Pinch Gestures for Hierarchical List Navigation on Smartphones," in Proceedings of the 2019 CHI conference on Human Factors in Computing Systems (CHI), 2019, Paper No.: 501, pp.1 - 13.

[5] Z. Xu, Y. Meng, X. Bi, and X. Yang, "Phrase-Gesture Typing on Smartphones," in Proceedings of the annual ACM symposium on user interface software and technology (UIST), 2022, Article 55, pp.1–11.

[6] L. Chen, D. Chen, and X. Chen, "BackAssist: Augmenting Mobile Touch Manipulation with Back-of-Device Assistance," IEICE Trans. Inf. & Syst., vol. E101-D, no. 6, pp. 1682-1685, June 2018.

[7] P. Baudisch and G. Chu, "Back-of-device interaction allows creating very small touch devices," in Proceedings of the 27th international conference on Human Factors in Computing Systems (CHI), 2009, pp. 1923- 1932.

[8] X. D. Yang, P. Irani, P.Boulanger, and W. Bischof, "One-handed behind-the-display cursor input on mobile devices," CHI EA, 2009, pp. 4501-4506.

[9] K. Hasan, X. D. Yang, H. N. Liang, and P. Inrani, "How to position the cursor?: an exploration of absolute and relative cursor positioning for back-of-device input," in Proceedings of the 14th international conference on Human computer interaction with mobile devices and services (MobileHCI), 2012, pp. 103-112.

[10] Z. Fan and C. Coutrix, "Impact of Hand Used on One-Handed Back-of-Device Performance," Proceedings of the ACM on Human-Computer Interaction, Vol. 4, Issue ISS, Article No.: 188, pp. 1–19, November 2020.

[11] J. Scott, S. Izadi, L. Rezai, D. Ruszkowski, X. Bi, and R. Balakrishnan, "Reartype: text entry using keys on the back of a device," In Proceedings of the 12th international conference on Human computer interaction with mobile devices and services (MobileHCI), 2010, pp. 171–180.

[12] O. Schoenlenben and A. Oulasvirta, "SandwichKeyboard: fast tenfinger typing on a mobile device with adaptive touch sensing on the back side," In Proceedings of the 15th international conference on Human computer interaction with mobile devices and services (MobileHCI), 2013, pp.175-178.

[13] D. Buschek, O. Schoenleben, and A. Oulasvirta, "Improving accuracy in back-of-device multitouch typing: a clustering-based approach to keyboard updating," In Proceedings of the 19th international conference on Intelligent User Interfaces (IUI), 2014, pp.57-66.

[14] W. Cui, S. Zhu, Z. Li, Z.Xu, X.Yang, I. Ramakrishnan, X. Bi, "Back-Swipe: Back-of-device Word-Gesture Interaction on Smartphones," in Proceedings of the 2021 CHI conference on Human Factors in Computing Systems (CHI), 2021, Article No.: 196.

[15] A. D. Luca, E. von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich, "Back-of-device authentication on smartphones," in Proceedings of the 31st international conference on Human Factors in Computing Systems (CHI), 2013, pp. 2389-2398.

[16] L. A. Leiva and Alejandro Catala, "BoD taps: an improved back-ofdevice authentication technique on smartphones," in Proceedings of the 16th international conference on Human computer interaction with mobile devices and services (MobileHCI), 2014, pp. 63-66.

[17] S. Kulshreshtha and A. S. Arif, "Woodpecker: Secret Back-of-Device Tap Rhythms to Authenticate Mobile Users," in Proceedings of the 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2020, pp. 2727-2733.

[18] E. Granell and L. A. Leiva, "Less Is More: Efficient Back-of-Device Tap Input Detection Using Built-in Smartphone Sensors," in Proceedings of the 2016 ACM International Conference on Interactive Surfaces and Spaces (ISS), 2016, pp. 5-11.

[19] E. Granell and L. A. Leiva, "βTap: back-of-device tap input with built-in sensors," in Proceedings of the 19th international conference on Human computer interaction with mobile devices and services (MobileHCI), 2017, Article No. 52.

[20] S. Shimon, S. Smith, N. John, G. Fahimi, and J. Ruiz, "Exploring User-Defined Back-Of-Device Gestures for Mobile Devices", in Proceedings of the 17th international conference on Human computer interaction with mobile devices and services (MobileHCI), 2015, pp. 227-232.

[21] J. O. Wobbrock, B. A. Myers, and H. H. Aung, "The performance of hand postures in front- and back-of-device interaction for mobile computing," Int. J. Hum.-Comput. Stud., vol. 66, no. 12, pp. 857-875, December 2008.

[22] L. Chen, D. Chen, and X. Chen, "A Comparison Study on Front- and Back-of-Device Touch Input for Handheld Displays," IEICE Trans. Electron., vol. E101-C, no. 11, pp. 880-883, November 2018.

[23] D. Wigdor, D. Leigh, C. Forlines, S. Shipman, J. Barnwell, R. Balakrishnan, and C. Shen, "Under the table interaction," in Proceedings of the annual ACM symposium on user interface software and technology (UIST), 2006, pp.259-268.

[24] C. Corsten, B. Daehlmann, S.Voelker, and J. Borchers, "BackXPress: Using Back-of-Device Finger Pressure to Augment Touchscreen Input on Smartphones," in Proceedings of the 2017 CHI conference on Human Factors in Computing Systems (CHI), 2017, pp.4654-4666.

[25] M. Huang, Y. Li, N. Nazneen, A. Chao, and S. Zhai, "TapNet: The Design, Training, Implementation, and Applications of a Multi-Task Learning CNN for Off-Screen Mobile Input," in Proceedings of the 2021

CHI conference on Human Factors in Computing Systems (CHI), 2021, Article No.: 282.

[26] H. Le, S. Mayer, and N. Henze, "InfiniTouch: Finger-Aware Interaction on Fully Touch Sensitive Smartphones, " in Proceedings of the annual ACM symposium on user interface software and technology (UIST), 2018, pp. 779-792.

[27] H. Le, S. Mayer, P. Bader,and N. Henze, "Fingers' Range and Comfortable Area for One-Handed Smartphone Interaction Beyond the Touchscreen," in Proceedings of the 2017 CHI conference on Human Factors in Computing Systems (CHI), 2018, Paper No.: 31.

[28] H. Le, S. Mayer, B. Steuerlein, and N. Henze, "Investigating Unintended Inputs for One-Handed Touch Interaction Beyond the Touchscreen," In Proceedings of the 21th international conference on Human computer interaction with mobile devices and services (MobileHCI), 2019, Article No.: 34.

[29] D. Wigdor, C. Forlines, P. Baudisch, J. Barnwell, and C. Shen, "Lucid-Touch: A See-Through Mobile Device," in Proceedings of the annual ACM symposium on user interface software and technology (UIST), 2007, pp. 269–278.

[30] O. Chapuis and N. Roussel, "Copy-and-paste between overlapping windows," in Proceedings of the 25th international conference on Human Factors in Computing Systems (CHI), 2007, pp.201-210.

[31] S. D. Zhao, F. Chevalier, W. T. Ooi, C. Y. Lee, and A. Aharwal, "AutoComPaste: Auto-completing text as an alternative to copy-paste," in Proceedings of the International Working Conference on Advanced Visual Interfaces (AVI), 2012, pp.365-372.

[32] E. Oh, J. Hong, M. Cho, J. Choi, "Study on Behavioral Characteristics of 3D Touch in Smartphone," Journal of the Ergonomics Society of Korea, vol.35, no.6, pp.551-568, December 2016.

A Review: PTSD in Pre-Existing Medical Condition on Social Media

Zaber Al Hassan Ayon[1], Nur Hafieza Ismail*[2], Nur Shazwani Kamarudin[3]
Faculty of Computing, University Malaysia Pahang Al-Sultan Abdullah, 26600 Pekan, Pahang, Malaysia[1, 2, 3]

***Abstract*—Post-Traumatic Stress Disorder (PTSD) is a multifaceted mental health condition, particularly challenging for individuals with pre-existing medical conditions. This review critically examines the intersection of PTSD and chronic illnesses as expressed on social media platforms. By systematically analyzing literature from 2008 to 2024, the study explores how PTSD manifests and is managed in individuals with chronic conditions such as cancer, heart disease, and autoimmune disorders, with a focus on online expressions on platforms like X (formally known as Twitter) and Facebook. Findings demonstrate that social media data offers valuable insights into the unique challenges faced by individuals with both PTSD and chronic illnesses. Specifically, natural language processing (NLP) and machine learning (ML) techniques can identify potential PTSD cases among these populations, achieving accuracy rates between 74% and 90%. Furthermore, the role of online support communities in shaping coping strategies and facilitating early interventions is highlighted. This review underscores the necessity of incorporating considerations of pre-existing medical conditions in PTSD research and treatment, emphasizing social media's potential as a monitoring and support tool for vulnerable groups. Future research directions and clinical implications are also discussed, with an emphasis on developing targeted interventions.**

Keywords*—*PTSD; mental health; social media; natural language processing; health informatics

I. INTRODUCTION

Mental health disorders, including conditions such as PTSD, depression, and anxiety, represent a substantial global public health challenge. The World Health Organization (WHO) estimates that one in four individuals will experience a mental disorder at some point in their lives, underscoring the widespread impact of these conditions on physical health and overall well-being [1]. Among these disorders, PTSD stands out due to its association with severe psychiatric comorbidities, including depression, anxiety, and an elevated risk of suicide, as well as its potential to exacerbate pre-existing physical health conditions [2].

PTSD is commonly understood to develop following exposure to traumatic events, such as warfare, natural disasters, or severe interpersonal violence, including sexual assault. Based on our analysis recent research has expanded this understanding to include PTSD triggered by serious medical challenges, such as chronic illnesses (e.g., cancer, heart disease, kidney failure, and lung disease) and complications during childbirth. Notably, studies suggest that up to 30% of individuals who experience life-threatening medical conditions may develop PTSD, highlighting the significant psychological toll of such experiences [3, 4, 5].

The onset of PTSD in medical contexts can be attributed to several factors, including the emotional shock of receiving a serious diagnosis, the physical and psychological demands of treatment, and the pervasive fear of death or disability. These experiences can lead to profound feelings of helplessness, loss of control, and vulnerability, all of which are key contributors to the development of PTSD [4, 6, 7]. Despite the growing recognition of PTSD in medical settings, there remains a critical need to understand how individuals with pre-existing medical conditions navigate and manage their PTSD symptoms.

In recent years, social media has emerged as a valuable tool for individuals with PTSD to seek support, share experiences, and access information. The impact of social media uses on PTSD symptoms, particularly in individuals with pre-existing medical conditions, is not yet fully understood [8]. The spontaneous and candid nature of social media posts provides a unique lens into individuals' thoughts, feelings, and behaviors, potentially revealing early signs of PTSD.

Advancements in artificial intelligence (AI), particularly in ML and NLP, have enabled the development of sophisticated algorithms capable of detecting patterns indicative of PTSD in social media data. These technologies hold promise for identifying PTSD cases with considerable accuracy, facilitating early intervention and personalized treatment approaches [9, 10]. During our analysis of the research works, the ethical implications and privacy concerns associated with using social media data for mental health research warrant careful consideration.

This article aims to provide a comprehensive overview of the intersection between PTSD and pre-existing medical conditions, focusing on the role of social media and ML in the identification and management of PTSD. By synthesizing current research, this review seeks to inform future research directions and clinical practices, ultimately improving outcomes for individuals grappling with both PTSD and chronic medical conditions.

To further underscore the significance of this study, the motivations include addressing the critical gap in understanding the interplay between PTSD and chronic medical conditions. This research aims to provide actionable insights that inform both clinical practices and the development of supportive technologies for affected individuals. This work highlights the transformative potential

*Corresponding Author

of social media analytics in mental health care, offering novel avenues for early intervention and monitoring.

II. Mental Health Disorders

Mental disorders, as defined by the WHO, involve significant disturbances in cognition, emotional regulation, or behavior, leading to distress or impairment in daily functioning [1]. These conditions, which encompass a wide range of disorders, adversely affect cognitive abilities, emotions, and social interactions. Accurate and timely assessments are critical for proper diagnosis and intervention. Traditionally, mental health screening has relied on self-report questionnaires designed to identify specific symptoms or attitudes related to social interactions [11].

The recognition of mental illness through diverse data sources and algorithms has been a significant focus of recent research, with AI playing a pivotal role. ML models, trained on various datasets, including self-reported questionnaires and EEG (Electroencephalogram) data, have been employed to predict mental health disorders such as depression and PTSD. Early studies utilized datasets annotated by domain experts, while more recent research has explored the potential of social media data in detecting mental illness [12, 13, 14].

Technological advancements have revolutionized psychiatric research, enabling the rapid collection and analysis of vast datasets through mobile phones, sensors, and social media platforms. ML, particularly in the context of advanced statistical and probabilistic methods, has proven effective in detecting mental health conditions [15]. A study on mental health recognition the authors employed ML techniques to analyze bipolar disorder using the Mood Disorder Questionnaire, while another study achieved 98.6% accuracy in detecting stress levels from bio-signals using supervised ML [11, 16]. Similarly, another study demonstrated a model for assessing psychiatric distress using EEG signals, employing algorithms such as Support Vector Machine (SVM), Logistic Regression (LR), and Naive Bayes (NB), with notable accuracy rates in stress detection [17].

In addition to ML, deep learning (DL) techniques have emerged as powerful tools in predicting depression risk. Context-DNN (Context Deep Neural Network) models, for instance, have been used to estimate the likelihood of depression [18]. Social media platforms, as a repository of user-generated content, have become valuable resources for observing mental states and psychiatric disorders. Studies have utilized platforms such as Reddit to analyze mental illness-related content through DL approaches, diagnosing chronic mental disorders like panic, bipolar disorder, and ADHD (attention deficit hyperactivity disorder) [19].

Other research has focused on detecting various mental illnesses, including schizophrenia, bipolar disorder, and PTSD, using data from platforms such as X, Facebook, and Weibo [18, 20]. Recent advancements in Large Language Models (LLMs) [86] have shown promise in recognizing mental health disorders from social media interactions, opening new possibilities for early identification and intervention [21]. LLMs are being explored as a tool to identify potential mental health concerns by analyzing text and speech patterns [22]. LLMs can be trained on large datasets of social media posts to identify patterns of language use associated with specific mental health conditions [23]. Regardless of the recent advancement of LLM in mental health identification, research and development are crucial to ensure accuracy and reliability before these tools can be integrated into clinical practice.

The expansion of social media has created unparalleled opportunities for mental health research, offering real-time insights into individuals' mental states. Advances in NLP and ML have enabled the identification of patterns in social media data that are indicative of mental health conditions, such as depression, anxiety, and PTSD. Studies have demonstrated the potential of these technologies to reveal linguistic markers and behavioral patterns associated with mental health issues, with predictive accuracy [6, 24]. Despite these advancements, the use of social media data for mental health research raises ethical concerns, including privacy issues, the risk of misdiagnosis, and potential stigmatization. The representativeness of social media data and the accuracy of self-reported mental health statuses remain areas of debate. Nonetheless, the integration of social media analysis into mental health research offers significant potential for early detection and intervention, potentially transforming the field of mental health care in the digital age.

Recent research has underscored the efficacy of combining social media data with LLMs for the diagnosis of mental health disorders, particularly in the early stages. The reluctance of many individuals to undergo mental health evaluations, coupled with the growing use of social media to share personal experiences, presents a unique opportunity for early diagnosis through social media analysis. The spontaneous and candid nature of social media expressions, when analyzed by sophisticated language models, can reveal subtle indicators of mental health issues that might otherwise go undetected. This approach holds significant promise for revolutionizing early intervention strategies in mental health care, potentially leading to improved outcomes through timely diagnosis and treatment initiation.

III. PTSD in Pre-Medical Conditions

PTSD is a complex psychiatric condition that arises from exposure to traumatic events or prolonged distressing circumstances [25]. Traditionally associated with combat veterans and survivors of violence or natural disasters, PTSD also manifests in patients with pre-existing medical conditions, posing significant challenges for both patient care and treatment outcomes. The intersection of PTSD and chronic illness is an increasingly important area of study, with far-reaching implications for healthcare practices and economics.

The prevalence of PTSD is substantial, with approximately 3.5% of U.S. adults affected annually, and lifetime prevalence reaching 8% among adolescents aged 13-18 [26]. Globally, data from the World Mental Health Survey Consortium reveal that over 70% of the population has experienced at least one traumatic event, highlighting the widespread potential for PTSD development [27]. In the medical context, patients diagnosed with conditions such as cancer, heart disease, and

chronic respiratory illnesses are at heightened risk for PTSD, with the psychological burden of these conditions creating fertile ground for trauma-related stress responses [28, 29]. This bidirectional relationship, where PTSD exacerbates physical symptoms and impairs treatment outcomes, underscores the importance of recognizing and addressing PTSD within medical populations [30].

The Coronavirus disease (COVID-19) pandemic has further emphasized the link between PTSD and medical conditions, with survivors of severe infections displaying PTSD symptoms, particularly among those with risk factors like a history of psychiatric disorders or experiences of delirium during illness [28]. The pandemic itself is a traumatic event capable of inducing PTSD, as evidenced by studies showing high prevalence rates due to factors such as lockdowns, economic instability, and social isolation [21, 31].

Another critical area of concern is childbirth-related PTSD (CB-PTSD). Approximately 6% of women experience CB-PTSD, affecting about eight million women globally in 2022 [32, 33]. High-risk factors include medically complicated deliveries, obstetrical complications, and maternal near-miss incidents [34, 35]. Racial and ethnic disparities exacerbate these risks, with Black and Latin women nearly three times more likely to exhibit acute stress responses to childbirth [32]. Overall, about 20% of high-risk individuals are likely to develop CB-PTSD [32].

The Diagnostic and Statistical Manual of Mental Disorders, 5th edition (DSM-5), identifies core PTSD symptoms such as intrusive memories, avoidance, negative alterations in cognition and mood, and heightened arousal [36]. In medical contexts, these symptoms may manifest as flashbacks to painful procedures, avoidance of necessary treatments, and negative health beliefs, complicating medical management [37, 38]. Early detection and trauma-informed interventions are thus crucial in these settings to prevent misdiagnosis and ensure comprehensive care [30].

While effective treatments for PTSD, including psychotherapy and pharmacotherapy, are available, co-occurring conditions such as depression and substance use disorders complicate recovery. Addressing both psychological and physiological aspects of trauma through integrated care approaches is essential for improving patient outcomes [39].

The interplay between PTSD and pre-existing medical conditions warrants ongoing research and clinical focus. Future studies should aim to develop tailored interventions for specific medical populations, explore the neurobiological mechanisms of medical trauma-induced PTSD, and assess the long-term effectiveness of integrated care models. Advancing our understanding in this area will contribute to more compassionate and effective care for those grappling with the dual challenges of medical conditions and PTSD [40].

IV. Mental Health Assessment for Diagnosis

Mental health assessment is a fundamental component of diagnosing and managing psychological and psychiatric disorders, requiring a multifaceted approach that integrates neuroimaging, physiological and laboratory analyses, clinical interviews, psychometric tools, and increasingly, social media data analysis [41]. This comprehensive methodology provides a nuanced understanding of the interplay between neurobiological, physiological, psychosocial, and digital behavioral factors underlying mental health conditions.

Neuroimaging techniques, particularly functional magnetic resonance imaging (fMRI) and positron emission tomography (PET), have become essential in identifying the neural substrates associated with various psychiatric disorders. For example, depressive disorders often involve reduced activity in the prefrontal cortex and increased amygdala activation, while schizophrenia is linked to anomalies in frontal and temporal lobe function [42]. These neurobiological insights are crucial for developing targeted and personalized therapeutic interventions [40].

Physiological and laboratory analyses complement neuroimaging by identifying underlying medical conditions that may contribute to psychiatric symptoms, such as thyroid dysfunction or nutritional deficiencies [43]. Comprehensive medical evaluations, including hematological profiles, endocrine function tests, and genetic analyses, are instrumental in guiding effective treatment strategies tailored to individual needs [43, 44].

Clinical interviews and standardized psychometric instruments remain central to mental health assessment. These methods allow clinicians to systematically gather detailed information on an individual's symptoms, personal and familial history, and functional impairments across various domains of life. The mental status examination, a critical component of the clinical interview, evaluates cognitive and behavioral domains such as affect, thought processes, and memory functions [45], offering crucial insights into the individual's psychological state and potential neuropsychiatric impairments.

Recently, the analysis of social media data has emerged as a promising addition to mental health assessment. The widespread use of social media platforms provides researchers and clinicians with real-time, naturalistic data on individuals' thoughts, emotions, and behaviors. This digital footprint can offer valuable insights into mental health trajectories and conditions.

NLP and ML algorithms have been developed to analyze social media content for markers of mental health conditions. For instance, changes in social media activity, linguistic style, and emotional expression have been used to predict the onset of depression with considerable accuracy [6]. Similarly, researchers have demonstrated the potential to diagnose PTSD from X data [24].

The integration of social media data analysis into mental health assessment offers several advantages:

- Early detection: Social media analysis can identify subtle changes in behavior or language indicative of emerging mental health issues before clinical symptoms appear.
- Continuous monitoring: Unlike traditional assessments, social media provides a continuous stream of data,

allowing for dynamic and responsive monitoring of mental health.

- Ecological validity: Social media reflects individuals' behaviors in natural environments, offering potentially more valid insights than clinical settings.
- Reach and accessibility: Social media analysis can extend mental health screening to populations that may not access traditional mental health services.

Nevertheless, the use of social media data in mental health assessment also presents significant ethical and practical challenges, including concerns about privacy, consent, data security, and the potential for misinterpretation. Additionally, biases in social media use and algorithmic analysis could lead to disparities in assessment and diagnosis [46, 47].

The integration of social media data with traditional assessment methods requires careful validation and robust ethical guidelines. Ongoing research is focused on refining algorithms, establishing normative data, and developing best practices for the responsible use of social media data in mental health assessment [46].

V. PTSD Diagnosis on Social Media

The advent of social media has markedly transformed how individuals express and manage mental health conditions, including PTSD. While traditional diagnostic methods remain essential, social media platforms offer novel avenues for researchers and clinicians to explore the lived experiences of those with PTSD. This is particularly crucial given the high prevalence of PTSD among veterans, with 15-20% affected, highlighting the need for innovative approaches to address this critical issue [5].

Historically, PTSD identification in populations such as cancer survivors has relied on questionnaires, but these are time-consuming and impractical for large-scale studies. Methods like fMRI, though informative, are cost-prohibitive for widespread use. An alternative approach involves analyzing public social media posts, which offer quick, accessible data from a broad audience. A pioneer study on PTSD in cancer patients reports that approximately 60% of adults use online resources for health information, and social media platforms allow individuals to discuss health concerns more openly than in face-to-face interactions [20]. Previous studies have utilized platforms like Reddit to detect early indicators of mental health disorders, while others have analyzed Twitter data to understand language patterns among PTSD patients with a history of cancer [7, 46, 47].

The challenge of accurately diagnosing PTSD, particularly in cancer survivors, is compounded by the lack of measurable data, a gap that motivates the collection of social media data for analysis. Various statistical methods, including correlations, chi-square tests, and regression analyses, have been employed to evaluate mental health datasets, revealing variables closely associated with mental health diagnoses [48]. ML algorithms, both supervised and unsupervised, have proven effective in tracking mental illness symptoms with high diagnostic accuracy. For instance, linear discriminant analysis has been used to explore social media content, identifying topics relevant to mental health [7, 24].

Recent studies highlight the potential of social media analysis to identify symptoms like anger associated with PTSD, particularly within the veteran community. This method shows promise as a preventative measure, enabling early detection and timely intervention. The complex nature of military service, including exposure to combat and the difficulty in distinguishing combatants from non-combatants, contributes to the high prevalence of PTSD among veterans, underscoring the urgency of exploring new strategies like social media analysis for supporting military personnel's mental health [6].

Advanced ML techniques, such as recurrent neural networks (RNN), deep neural networks (DNN), and convolutional neural networks (CNN), are increasingly employed for text processing in mental health research. Sentiment analysis on X data, for example, has been suggested for understanding the context of communication and dialogue related to mental health [49].

In a novel approach, recent research has explored the detection of CB-PTSD using LLMs like Bio_ClinicalBERT and BioGPT, which have outperformed ChatGPT in clinical tasks. This study reveals that approximately 6% of the global childbearing population, or over eight million women annually, develop CB-PTSD, significantly impacting mothers and their children. The generative AI model such as Open AI text embedding (ADA), by analyzing maternal narratives, achieved an F1 score of 0.81 in identifying PTSD, indicating its potential to generalize to other mental health disorders [27].

As mental health research continues to evolve, the integration of social media data analysis holds significant potential for enhancing our understanding of PTSD. Leveraging user-generated content on these platforms allows researchers to gain deeper insights into PTSD symptoms, triggers, and coping mechanisms. This real-time, granular data can complement traditional survey methods, facilitating the early identification of mental health issues and the development of personalized interventions. Additionally social media analysis can inform public health initiatives, guiding resource allocation and outreach programs to address the mental health needs of vulnerable populations, particularly veterans and active-duty military personnel.

VI. Text Classification in PTSD Identification

Accurately classifying and diagnosing PTSD in medical settings remains a formidable challenge, with significant implications for patient outcomes and healthcare resource allocation. PTSD, a prevalent psychiatric disorder, especially among military personnel and veterans, manifests in severe symptoms that drastically impair quality of life [4].

This review addresses the complexities of PTSD classification and diagnosis by exploring key processes, starting with the identification of robust data sources, such as clinical records, screening questionnaires, and social media content. These diverse data sources provide a comprehensive foundation for analyzing PTSD symptoms. Following data collection, precise annotation is crucial, as it involves

accurately labelling symptoms essential for training effective models. Feature selection further refines the dataset, ensuring that the most relevant PTSD indicators are highlighted, thus enhancing model accuracy.

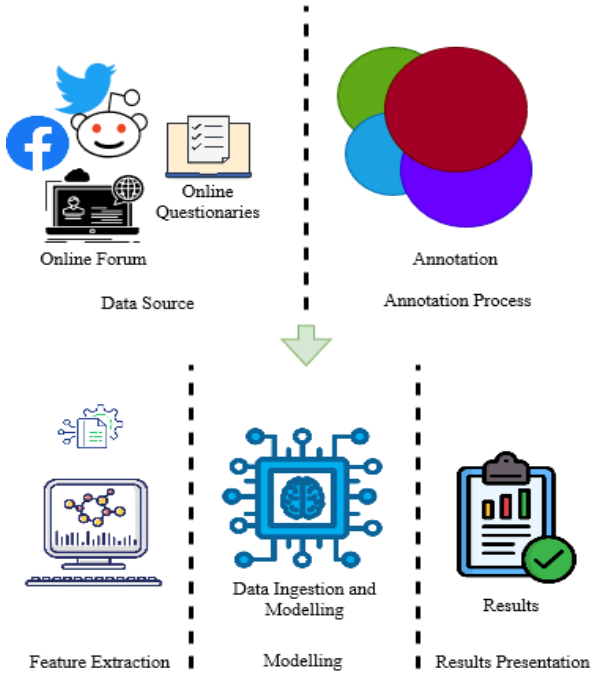


Fig. 1. Generic representation of PTSD identification from social media data.

Fig. 1 depicts a general approach followed by the reviewed studied related to identification of mental health disorder from social media data. As data source most of the studies. All most every study mentioned about human annotation via domain experts. Finally descriptive or inferential model training and feature extraction processes were followed to get class probability distribution.

Advanced modelling techniques, particularly ML algorithms, are then applied to predict PTSD presence. These models undergo rigorous testing to ensure robustness, with results critically analyzed to evaluate their effectiveness in medical settings. This process not only offers insights into the practical application of these models but also identifies potential areas for further refinement and research, ultimately contributing to more accurate PTSD diagnoses and improved patient care.

A. Data Sources

In recent years, researchers have utilized a range of data collection methods to explore the intersection of PTSD, pre-existing medical conditions, and social media engagement. This review synthesizes the key data sources employed in this burgeoning field, critically examining their strengths, limitations, and overall contributions to advancing our understanding of this complex and multifaceted issue. By integrating findings from diverse methodologies, this review seeks to provide a comprehensive overview of how these data sources have informed current research and to identify potential avenues for future inquiry.

1) Questionnaires: Several studies have employed online self-administered screening questionnaires to evaluate the prevalence of PTSD symptoms among individuals with pre-existing medical conditions who are active on social media platforms [24, 50]. These questionnaires are designed to collect comprehensive data, including demographic information, medical history to identify pre-existing conditions, and responses to validated PTSD screening tools such as the PTSD Checklist for Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-5) also known as PTSD Checklist Fifth Edition (PCL-5) Additionally, they include questions regarding social media usage and online behavior, enabling researchers to examine the relationship between PTSD symptoms and social media engagement.

The primary advantage of this approach is its capacity to generate quantitative data on the prevalence of PTSD symptoms and to explore the potential correlation between these symptoms and social media use. Even though it is important to acknowledge the methodological limitations inherent in this approach, particularly the risk of self-selection bias and the potential for underreporting or overreporting of symptoms within online environments. These factors must be carefully considered when interpreting the results to ensure the validity and reliability of the findings.

2) Online discussion sites: Numerous studies have investigated online discussion sites, including mental health forums and support groups, to gain insights into the experiences of individuals dealing with PTSD alongside pre-existing medical conditions [51, 52]. Key data sources for these studies include Reddit communities (subreddits) focused on PTSD and chronic illnesses, established mental health support forums, and condition-specific forums where mental health discussions are prevalent. These platforms provide rich qualitative data that allow for a nuanced analysis of personal narratives and coping mechanisms. The anonymity inherent to these platforms poses challenges in verifying the authenticity of the reported experiences.

3) Social media platforms: Individuals with chronic conditions are more likely to engage with health-related content on social media, while those with mental health conditions tend to engage less frequently [53]. An expanding body of research has focused on analyzing the social media activity of individuals who publicly discuss their mental health issues, including PTSD, in conjunction with pre-existing medical conditions [6, 54]. These studies typically investigate X posts using relevant hashtags, public Facebook groups dedicated to PTSD and chronic illness support, and Instagram posts with captions referencing both PTSD and other medical conditions.

This methodological approach provides valuable insights into how individuals publicly navigate their experiences with PTSD and pre-existing medical conditions on social media platforms. Researchers must also carefully consider ethical concerns related to privacy and consent when utilizing

publicly available data, as these factors are critical to maintaining the integrity and ethical standards of the research [55].

The triangulation of diverse data sources has emerged as a best practice in this field, enabling researchers to obtain a comprehensive understanding of how PTSD manifests and is discussed within the context of pre-existing medical conditions on social media platforms [56, 57]. This multi-faceted approach facilitates both the quantitative assessment of symptom prevalence and the qualitative analysis of lived experiences and online behaviors.

Despite the benefits of these methods, researchers face several challenges when utilizing these data sources. First, representativeness is a significant concern; social media users may not accurately reflect the broader population of individuals with PTSD and pre-existing medical conditions [58]. For instance, Biernesser et al. found that social media data often over represent younger, more technologically savvy demographics, potentially leading to skewed results [58]. Second, the quality of data is a critical issue, as the reliability and validity of self-reported information on social media platforms can be questionable. This necessitates rigorous verification and cross-referencing of data, as highlighted by a study conducted by Torous et al., which emphasized the need for robust data cleaning and validation processes in mental health research using social media data [59].

Ethical considerations also play a crucial role, particularly in balancing the need for research with privacy concerns and informed consent. Golder et al. proposed a framework for ethical social media research in health contexts, emphasizing the importance of protecting user privacy and obtaining appropriate consent [60]. Additionally, technological barriers must be considered; the rapid evolution of social media platforms and their algorithms can impact data collection and analysis methods, requiring researchers to continuously adapt their approaches. Staying informed about platform changes and their implications for data accessibility and analysis is essential [61].

Future research in this domain would benefit from the development of standardized protocols for social media data collection and analysis, alongside the exploration of innovative approaches to integrating online and offline data sources. Such integration could yield a more comprehensive understanding of PTSD in the context of pre-existing medical conditions. Conway and O'Connor on their study suggest that combining traditional clinical data with social media insights could enhance the robustness and generalizability of findings [62]. By critically examining these diverse data sources and their applications, researchers can refine their methodologies and contribute meaningfully to the expanding body of literature at the intersection of mental health, chronic illness, and digital spaces.

B. Data Annotation

Data annotation is pivotal in the analysis of social media content for PTSD and other mental health conditions, playing a crucial role in ensuring the validity and reliability of research findings. This process involves several key methods and tools, each contributing uniquely to the field. A fundamental aspect of data annotation is the identification and labelling of specific PTSD symptoms in social media posts. Researchers utilize a variety of techniques for this task, ranging from NLP and ML algorithms to manual coding by trained clinicians and keyword-based approaches [6, 24, 63]. These methods are designed to detect symptoms such as re-experiencing, avoidance, negative alterations in cognition and mood, and heightened arousal, with each approach balancing considerations of efficiency, accuracy, and scalability.

Another critical component of this process is establishing the ground truth for data collection, which involves validating annotated data against reliable sources. This validation can be achieved through clinical verification via interviews, self-reported PTSD symptom measures, or comparisons with clinician-diagnosed cases [49, 64]. Human annotators continue to play an essential role in this process, providing a nuanced understanding and insights that may be difficult to capture through automated methods alone. Expert annotators, such as mental health professionals, offer high-quality annotations based on clinical expertise, while trained lay annotators and crowdsourcing platforms provide scalable alternatives, albeit with the necessity of rigorous quality control [9, 65].

To deepen the analysis, researchers frequently incorporate additional tools and measures. Depression survey scores, such as the Patient Health Questionnaire-9 (PHQ-9), are often used alongside PTSD assessments to evaluate symptom severity and understand comorbidities [6, 66]. The Linguistic Inquiry and Word Count (LIWC) tool has also gained prominence for its ability to analyze linguistic patterns in social media posts, offering valuable insights into the emotional and cognitive processes associated with PTSD [49, 63].

Recently, the advent of LLMs as annotators has introduced new possibilities in data annotation for PTSD research. LLMs such as GPT-3 and Bidirectional Encoder Representations from Transformers (BERT) show considerable promise in automating symptom detection and efficiently processing vast amounts of data [67, 68, 69]. However, their use raises important considerations. Ethical concerns related to privacy and consent, the inherent lack of clinical expertise in these models, limitations in understanding broader contextual nuances, and issues of reliability and transparency present significant challenges. While LLMs offer potential benefits in terms of scalability and efficiency, their application in mental health contexts requires careful validation against established clinical standards and ongoing scrutiny to ensure ethical and accurate annotations.

In conclusion, the process of data annotation for PTSD research on social media is continuously evolving, with each method presenting distinct strengths and limitations. A balanced approach that integrates human expertise with technological advancements appears most promising. As the field advances, researchers must skillfully navigate the complexities of various annotation methods, striving for a harmonious integration that ensures both efficiency and clinical relevance in the pursuit of understanding PTSD through social media data.

C. Feature Selection

In the context of analyzing PTSD in individuals with pre-existing medical conditions on social media, feature selection is critical for identifying the most relevant characteristics that enhance the effectiveness of predictive modelling. Researchers utilize a range of techniques to distil meaningful features from the extensive data available on social media platforms. Commonly extracted textual features include word frequency, n-grams, and sentiment scores derived from posts and comments, which provide insights into the language patterns associated with PTSD [24]. Temporal patterns of social media activity, such as posting frequency and the time-of-day posts are made, have also proven significant in detecting PTSD, offering a behavioral dimension to the analysis [6].

In addition to these features, researchers frequently incorporate user profile information and engagement metrics, which may serve as potential indicators of PTSD symptoms. Advanced approaches further enhance the analysis by leveraging NLP techniques to capture semantic and contextual features, such as topic modelling and word embeddings, allowing for a deeper understanding of the content and its relevance to PTSD [69].

The primary challenge in feature selection lies in balancing the richness of these features with the risk of overfitting, particularly given the complex and multifaceted nature of PTSD and its interactions with pre-existing medical conditions. To address this, dimensionality reduction techniques like Principal Component Analysis (PCA) and t-SNE are often employed. These methods help manage high-dimensional feature spaces by condensing the data while preserving the most critical information [70].

Recent studies have explored the use of automated feature selection methods, including wrapper and embedded techniques, which optimize the feature set for detecting PTSD in the context of comorbid conditions. These methods offer a systematic approach to refining feature selection, thereby improving model accuracy and robustness [71].

By carefully selecting and refining features, researchers can build more effective models that not only predict PTSD but also account for the complexity of its interactions with other medical conditions, ultimately contributing to more accurate and meaningful insights in mental health research.

D. Modeling

The modelling approaches employed in studying PTSD among individuals with pre-existing medical conditions on social media encompass a broad spectrum of techniques, ranging from traditional statistical methods to cutting-edge ML and DL algorithms.

Statistical methods have long served as the cornerstone of research in this field, providing foundational tools for analysis. LR remains a widely favored approach due to its interpretability and its capability to quantify the relationship between various features and the likelihood of PTSD [24]. Additionally, survival analysis techniques, particularly Cox proportional hazards models, are frequently used to explore the temporal dynamics of PTSD development in individuals with pre-existing conditions, identifying key risk factors over time [16]. Multilevel modelling has gained prominence for its ability to account for the nested structure of social media data—such as posts within users and users within platforms—thereby accommodating the hierarchical nature of the data and enhancing the accuracy of the analysis.

ML methods have also been pivotal in advancing PTSD detection and risk assessment. SVMs, known for their effectiveness in handling high-dimensional feature spaces, have been successfully applied to classify social media users with PTSD [13, 14]. Random Forests and Gradient Boosting Machines offer robust performance by managing complex interactions between features, making them particularly valuable in assessing the interplay between PTSD and co-existing medical conditions [41] [85]. Ensemble methods, which combine the strengths of multiple algorithms, have demonstrated superior accuracy and generalizability in PTSD prediction models [12].

The rise of DL has introduced powerful tools for analyzing the unstructured and complex nature of social media data in PTSD research. CNNs have been utilized to detect PTSD-related language by capturing local patterns in text data, demonstrating their efficacy in this domain [17]. RNNs, especially Long Short-Term Memory (LSTM) networks, excel in modeling temporal dependencies in social media activity, making them well-suited for identifying patterns associated with PTSD [23] Transformer-based models, such as BERT and its variants, have emerged as particularly effective in understanding the nuanced contexts in which PTSD expressions occur in social media posts. These models, when fine-tuned on domain-specific data, can capture subtle linguistic cues indicative of PTSD [19]. Additionally, the use of graph neural networks is gaining traction, as they can model the complex relationships between users, posts, and symptoms in social networks, offering a novel perspective on understanding PTSD within the dynamics of online social interactions [34].

Recently, LLMs have revolutionized PTSD research on social media by providing advanced capabilities for feature extraction and modelling. Pre-trained on vast text corpora, these models bring a sophisticated understanding of language and context, which is essential for identifying PTSD. Researchers have explored several applications of LLMs in this area. For instance, fine-tuning approaches adapt pre-trained models like BERT to the specific task of detecting PTSD in social media texts, capturing subtle linguistic and contextual nuances associated with PTSD symptoms [22]. Another approach leverages LLMs as feature extractors, utilizing the rich representations learned by these models as inputs for other ML algorithms [10]. Recent studies, such as those by Yang et al. have developed frameworks using ChatGPT and LLaMA-2 to automate PTSD assessments from clinical interviews, highlighting the potential of LLMs to enhance diagnostic accuracy [23]. Additionally, a group of researchers introduced innovative text augmentation methods using LLMs to address data imbalance issues in PTSD diagnosis, further demonstrating the versatility and impact of these models [72].

In summary, the evolution of modeling approaches in PTSD research on social media reflects a dynamic interplay between traditional and modern techniques. By integrating statistical methods, ML, DL, and LLMs, researchers can achieve a more nuanced and comprehensive understanding of PTSD in individuals with pre-existing medical conditions, ultimately advancing the field's ability to accurately detect and model this complex disorder. Fig. 2 depicts the general approach followed by many studies to implement AI modeling with NLP.

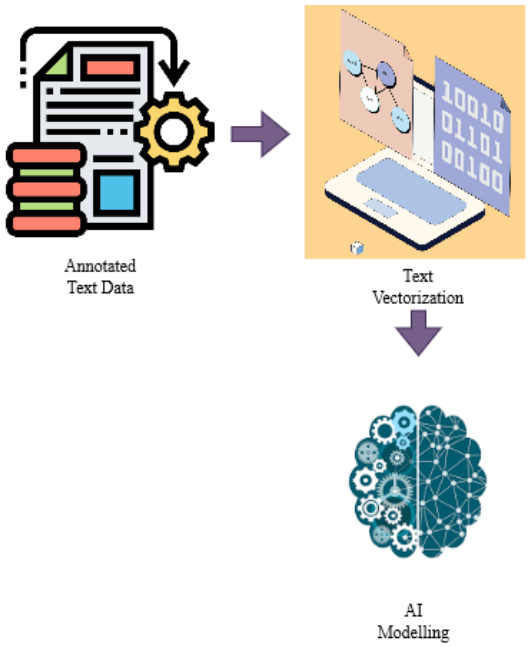


Fig. 2. Generic artificial intelligence predictor modelling.

E. Results

The study of PTSD in individuals with pre-existing medical conditions using social media data has yielded significant insights through various modeling approaches. Statistical methods, including survival analyses, have identified critical time windows for intervention following diagnoses of conditions like chronic pain and autoimmune disorders, emphasizing the need for timely support [73, 74, 75]. Traditional ML models, such as SVMs and Random Forests, have demonstrated strong performance, with accuracy rates between 75-85% and AUC scores exceeding 0.90 in some cases [24, 76, 77]. The variability in performance across different conditions indicates that these models require further tuning for condition-specific applications. DL techniques, such as CNNs, LSTMs, and Transformer-based models like BERT, have advanced PTSD detection by capturing nuanced language patterns in social media posts, achieving precision rates up to 88% and F1 scores between 0.85-0.90 [9, 37]. The "black box" nature of these models presents challenges for clinical application due to difficulties in interpretability [78].

Sentiment analysis tools, such as the LIWC tool and the VADER (Valence Aware Dictionary for Sentiment Reasoning) tool, have shown promise in identifying mental health conditions. LIWC has revealed significant differences in the linguistic style of individuals experiencing emotional distress compared to those who are not, suggesting its utility in mental health detection [19]. VADER, known for its computational efficiency and extensive word corpus, has been used effectively to predict depression risk based on sequential social media messages, demonstrating the evolving nature of sentiment analysis in this field [79]. Feature engineering methods, including bag-of-words and N-grams, combined with these sentiment analysis tools, have achieved accuracy rates ranging from 74% to 82%, suggesting that text-based screening tools hold substantial potential for identifying individuals at risk of PTSD or related mental health conditions [79, 80].

LLMs, such as GPT-3 and text-embedding-ada-002, have shown impressive accuracy in detecting PTSD, with F1 scores and accuracy rates up to 0.82 and 83%, respectively [81, 82]. Despite the progress, challenges remain, particularly with the "black box" nature of advanced models, computational demands, and privacy concerns [83, 84]. Traditional ML and sentiment analysis tools provide a good balance of accuracy and interpretability but often lack the depth to capture complex PTSD manifestations. DL models and LLMs offer superior performance in detecting nuanced expressions of trauma but suffer from interpretability and ethical concerns, which limit their practical use in clinical settings. The integration of these methods with a focus on improving interpretability and ethical use is crucial for advancing PTSD detection and intervention strategies.

VII. Conclusion and Future Work

This review has examined the intersection of PTSD, pre-existing medical conditions, and social media behavior, highlighting the significant advancements in the field from basic keyword analysis to the application of sophisticated ML and LLMs. These developments demonstrate substantial potential for the early detection and intervention of PTSD among individuals with chronic health conditions.

Despite these advancements, several critical knowledge gaps persist. First, there is currently no consensus on best practices for data collection, annotation, and analysis in social media-based PTSD research, particularly in the context of comorbid conditions. Additionally, most of the existing research relies on cross-sectional data, leaving the temporal dynamics of PTSD development in individuals with pre-existing conditions inadequately understood. Furthermore, a significant disconnect exists between insights derived from social media and their application in clinical practice, limiting the practical utility of research findings. The specific interactions between certain medical conditions and PTSD manifestations on social media are also not sufficiently studied. Comprehensive ethical guidelines for the use of AI in mental health detection on social media are lacking, raising concerns about privacy, consent, and the responsible use of predictive models.

To address these gaps, future research should prioritize the following areas. First, establishing clear guidelines for data collection, annotation, and analysis is essential to enhance the reproducibility and comparability of studies across the field. Collecting users single post and training an inferential model for prediction might not give the model full understanding of

sarcasm, jokes, humor due incomplete reasoning over the dataset. Second, designing long-term studies that track PTSD development in individuals with pre-existing conditions, using continuous social media data, will provide deeper insights into the temporal dynamics of PTSD. Third, combining social media data with electronic health records and data from wearable devices can offer a more comprehensive understanding of PTSD in the context of comorbid conditions.

Fourth, creating adaptive models that account for individual differences and specific interactions between pre-existing conditions and PTSD is crucial for enhancing the accuracy and relevance of predictive tools. Fifth, developing methods to make advanced models, particularly LLMs, more interpretable for clinical application is vital for their effective integration into healthcare settings. Sixth, expanding research to include diverse cultural contexts will help in understanding varying PTSD manifestations and social media usage patterns across different populations. Lastly, establishing robust ethical frameworks for the use of AI in mental health contexts is necessary to address issues of consent, privacy, and the responsible deployment of predictive models.

In conclusion, while social media analysis offers unprecedented opportunities for understanding PTSD in the context of pre-existing medical conditions, realizing its full potential requires addressing these significant knowledge gaps. Future research should focus on standardization, longitudinal studies, and the development of ethical, interpretable AI models that can be effectively integrated into clinical practice. Interdisciplinary collaboration will be crucial in translating these research insights into tangible improvements in mental health care for individuals living with both PTSD and chronic medical conditions.

ACKNOWLEDGMENT

This research was fully funded by UMPSA Research Grant Scheme under grant RDU220350, UMPSA.

REFERENCES

[1] Post-traumatic stress disorder." Proceedings of WHO Conference (WHO), World Health Organization (Switzerland), July 5, 2024, pp. 1-2

[2] Bisson, J. I., Cosgrove, S., Lewis, C., & Roberts, N. P., “Post-Traumatic Stress Disorder,” *BMJ*, h6161-h6161, 2015. https://doi.org/10.1136/bmj.h6161.

[3] Vieweg, W. V. R., Julius, D. A., Fernandez, A., Beatty-Brooks, M., Hettema, J. M., & Pandurangi, A. K., “Posttraumatic Stress Disorder: Clinical Features, Pathophysiology, and Treatment,” *Elsevier BV*, 119(5), 2006, pp. 383-390. https://doi.org/10.1016/j.amjmed.2005.09.027.

[4] Iribarren, J., Prolo, P., Neagos, N., & Chiappelli, F., “Post-Traumatic Stress Disorder: Evidence-Based Research for the Third Millennium,” *Hindawi Publishing Corporation*, 2(4), 2005, pp. 503-512. https://doi.org/10.1093/ecam/neh127.

[5] Forbes, D., Lloyd, D., Nixon, R. D., Elliott, P., Varker, T., Perry, D., Bryant, R. A., & Creamer, M., “A Multisite Randomized Controlled Effectiveness Trial of Cognitive Processing Therapy for Military-Related Posttraumatic Stress Disorder,” *Elsevier BV*, 26(3), 2012, pp. 442-452. https://doi.org/10.1016/j.janxdis.2012.01.006.

[6] Choudhury, D., Counts, M., & Horvitz, S., “Social Media as a Measurement Tool of Depression in Populations,” *Proceedings of the 5th Annual ACM Web Science Conference*, ACM, 2013, pp. 47–56.

[7] Paul, M., & Dredze, M., “You Are What You Tweet: Analyzing Twitter for Public Health,” *Proceedings of the International AAAI Conference on Web and Social Media*, AAAI, 2021, pp. 265–272. https://doi.org/10.1609/icwsm.v5i1.14137.

[8] Ding, N., Li, L., Song, K., Huang, A., & Zhang, H., “Efficacy and Safety of Acupuncture in Treating Post-Traumatic Stress Disorder,” *Wolters Kluwer*, 99(26), 2020, pp. e20700-e20700. https://doi.org/10.1097/md.0000000000020700.

[9] Gkotsis, G., Oellrich, A., Velupillai, S., Liakata, M., Hubbard, T. J. P., Dobson, R. J. B., & Dutta, R., "Characterisation of mental health conditions in social media using Informed Deep Learning", Proceedings of Scientific Reports (Nature Publishing Group), King’s College London (United Kingdom), 2017, pp. 46813-46813.

[10] Benton, A., Mitchell, M., & Hovy, D., “Multitask Learning for Mental Health Conditions with Limited Social Media Data,” *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 1, Long Papers*, 2017, pp. 152-162.

[11] Jadhav, R., Chellwani, V., Deshmukh, S., & Sachdev, H., "Mental disorder detection: Bipolar disorder scrutinization using machine learning", Proceedings of the 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Thakur College of Engineering and Technology (India), 2019, pp. 1-6.

[12] Zhang, T., Schoene, A. M., Ji, S., & Ananiadou, S., "Natural language processing applied to mental illness detection: a narrative review", Proceedings of NPJ Digital Medicine (Springer Nature), University of Manchester (United Kingdom), 2022, pp. 46-46.

[13] Zhang, Z., Lin, W., Liu, M., & Mahmoud, M., "Multimodal deep learning framework for mental disorder recognition", Proceedings of the 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020), Arizona State University (USA), May 2020, pp. 1-4.

[14] Leightley, D., Williamson, V., Darby, J., & Fear, N. T., "Identifying probable post-traumatic stress disorder: applying supervised machine learning to data from a UK military cohort", Proceedings of the Journal of Mental Health (Taylor & Francis), King’s College London (United Kingdom), 2019, pp. 34-41.

[15] Galatzer-Levy, I. R., Karstoft, K. I., Statnikov, A., & Shalev, A. Y., "Quantitative forecasting of PTSD from early trauma responses: A machine learning application", Proceedings of the Journal of Psychiatric Research (Elsevier), New York University School of Medicine (USA), 2014, pp. 68-76.

[16] Rahman, R. A., Omar, K., Mohd Noah, S. A., Danuri, M. S. N. M., & Al-Garadi, M. A., "Application of machine learning methods in mental health detection: A systematic review", Proceedings of IEEE Access (IEEE), University of Malaya (Malaysia), 2020, pp. 183952-183964.

[17] Lin, H., Jia, J., Guo, Q., Xue, Y., Li, Q., Huang, J., Cai, L., & Feng, L., "User-level psychological stress detection from social media using deep neural network", Proceedings of the 22nd ACM International Conference on Multimedia, Tsinghua University (China), November 2014, pp. 507-516.

[18] Baek, J.-W., & Chung, K., "Context deep neural network model for predicting depression risk using multiple regression", Proceedings of IEEE Access (IEEE), Chung-Ang University (South Korea), 2020, pp. 18171-18181.

[19] Shing, H. C., Nair, S., Zirikly, A., Friedenberg, M., Daumé III, H., & Resnik, P., "Expert, crowdsourced, and machine assessment of suicide risk via online postings", Proceedings of the Fifth Workshop on Computational Linguistics and Clinical Psychology: From Keyboard to Clinic, University of Maryland (USA), 2020, pp. 182-192.

[20] Ismail, N. H., Liu, N., Du, M., He, Z., & Hu, X., “Using Deep Neural Network to Identify Cancer Survivors Living with Post-Traumatic Stress Disorder on Social Media,” *Proceedings of the Creative Commons License Attribution 4.0 International Conference*, Texas A&M University, Florida State University, February 21-23, year, pp. 626-632.

[21] Messman, B. A., Rafiuddin, H. S., Slavish, D. C., Weiss, N. H., & Contractor, A. A. "Examination of Daily-Level Associations between Posttraumatic Stress Disorder Symptoms and COVID-19 Worries." *Psychological Trauma: Theory, Research, Practice and Policy* 14(3), February 21-23, 2022, pp. 497-506. https://doi.org/10.1037/tra0001170

[22] Lawrence, H. R., Schneider, R. A., Rubin, S. B., Matarić, M. J., McDuff, D. J., & Jones Bell, M., "The Opportunities and Risks of Large Language Models in Mental Health," *JMIR Mental Health*, vol. 11, JMIR Publications, 2024, pp. e59479-e59479. https://doi.org/10.2196/59479.

[23] Yang, K., Zhang, T., Kuang, Z., Xie, Q., Huang, J., & Ananiadou, S., "MentaLLaMA: Interpretable Mental Health Analysis on Social Media with Large Language Models," *Proceedings of the ACM Web Conference 2024*, ACM, 2024, pp. 4489-4500. https://doi.org/10.1145/3589334.3648137.

[24] Coppersmith, G., Dredze, M., & Harman, C., "Quantifying Mental Health Signals in Twitter," *Proceedings of the Workshop on Computational Linguistics and Clinical Psychology: From Linguistic Signal to Clinical Reality*, 2014.

[25] Ernala, S. K., Birnbaum, M. L., Candan, K. A., Rizvi, A. F., Sterling, W. A., Kane, J. M., & De Choudhury, M., "Methodological gaps in predicting mental health states from social media: Triangulating diagnostic signals", Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Georgia Institute of Technology (USA), 2019, pp. 1-16.

[26] Dai, H. J., Wang, Y., Trivedi, R., & Dai, L., "Deep learning for automated recognition of PTSD in social media", Proceedings of the IEEE International Conference on Bioinformatics and Biomedicine (BIBM), National Yang-Ming University (Taiwan), November 2017, pp. 834-839.

[27] Benjet, C., Bromet, E., Karam, E. G., Kessler, R. C., McLaughlin, K. A., Ruscio, A. M., Shahly, V., Stein, D. J., Petukhova, M., Hill, E., Alonso, J., Atwoli, L., Bunting, B., Bruffaerts, R., Caldas-de-Almeida, J. M., de Girolamo, G., Florescu, S., Gureje, O., Huang, Y., … Koenen, K. C. "The Epidemiology of Traumatic Event Exposure Worldwide: Results from the World Mental Health Survey Consortium." *Psychological Medicine* 46(2), February 21-23, 2016, pp. 327-343. https://doi.org/10.1017/S0033291715001981

[28] Janiri, D., Carfì, A., Kotzalidis, G. D., Bernabei, R., Landi, F., & Sani, G., "Posttraumatic Stress Disorder in Patients After Severe COVID-19 Infection," *American Medical Association*, 78(5), 2021, pp. 567-567. https://doi.org/10.1001/jamapsychiatry.2021.0109.

[29] Smith, G., "Evidence for Pharmacotherapy of Posttraumatic Stress Disorder," *Capnography Journal*, 8(8), 2003, pp. 1-5. https://doi.org/10.1521/capn.8.8.1.27930.

[30] Stubbe, D., "Optimizing Empathy: Physician Self-Care as a Crucial Component of Trauma-Informed Treatment," *Focus Journal*, 15(4), 2017, pp. 432-434. https://doi.org/10.1176/appi.focus.20170033.

[31] Yunitri, N., Chu, H., Kang, X. L., Jen, H., Pien, L., Tsai, H., Kamil, A. R., & Chou, K., "Global Prevalence and Associated Risk Factors of Posttraumatic Stress Disorder During COVID-19 Pandemic: A Meta-Analysis," *Elsevier BV*, 126, 2022, pp. 104136-104136. https://doi.org/10.1016/j.ijnurstu.2021.104136

[32] Bartal, A., Jagodnik, K. M., Chan, S. J., & Dekel, S., "AI and narrative embeddings detect PTSD following childbirth via birth stories", Proceedings of Scientific Reports (Nature Publishing Group), Harvard Medical School (USA), 2024, pp. 54242-54242.

[33] Forte, G., Favieri, F., Tambelli, R., & Casagrande, M. "COVID-19 Pandemic in the Italian Population: Validation of a Post Traumatic Stress Disorder Questionnaire and Prevalence of PTSD Symptomatology." *Int. J. Environ. Res. Public Health* 17, February 21-23, 2020.

[34] Dekel, S., Stuebe, C., & Dishy, G. "Childbirth Induced Posttraumatic Stress Syndrome: A Systematic Review of Prevalence and Risk Factors." *Front Psychol* 8, February 21-23, 2017.

[35] Yildiz, P. D., Ayers, S., & Phillips, L. "The Prevalence of Posttraumatic Stress Disorder in Pregnancy and After Birth: A Systematic Review and Meta-Analysis." *J Affect Disord* 208, February 21-23, 2017, pp. 634-645.

[36] Mak, I. W. C., Chu, C. M., Pan, P. C., Yiu, M. G. C., & Chan, V. L. "Long-Term Psychiatric Morbidities Among SARS Survivors." *General Hospital Psychiatry* 31(4), February 21-23, 2009, pp. 318-326. https://doi.org/10.1016/j.genhosppsych.2009.03.001

[37] Liu, N., Zhang, F., Wei, C., Jia, Y., Shang, Z., Sun, L., Wu, L., Sun, Z., Zhou, Y., Wang, Y., & Liu, W. "Prevalence and Predictors of PTSS During COVID-19 Outbreak in China Hardest-Hit Areas: Gender Differences Matter." *Psychiatry Research* 287(112921), February 21-23, 2020, pp. 1-7. https://doi.org/10.1016/j.psychres.2020.112921

[38] American Psychiatric Publishing. "Diagnostic and Statistical Manual of Mental Disorders: DSM-5." *Institution Name (Country)*, February 21-23, 2013.

[39] Shalev, A., Liberzon, I., & Marmar, C. "Post-Traumatic Stress Disorder." *N Engl J Med* 376, February 21-23, 2017, pp. 2459-2469.

[40] Mota, N., Bolton, S. L., & Enns, M. W. "Course and Predictors of Posttraumatic Stress Disorder in the Canadian Armed Forces: A Nationally Representative, 16-Year Follow-Up Study: Cours et Prédicteurs du Trouble de Stress Post-Traumatique dans les Forces Armées Canadiennes: Une Étude de Suivi de 16 Ans Nationalement Représentative." *Can J Psychiatry* 66, February 21-23, 2021, pp. 982-995.

[41] Mori, R., Lakhanpaul, M., & Verrier-Jones, K., "Diagnosis and Management of Urinary Tract Infection in Children: Summary of NICE Guidance," *BMJ*, 335(7616), 2007, pp. 395-397. https://doi.org/10.1136/bmj.39286.700891.ad.

[42] Hong, J., Huang, Y., Ye, J., Wang, J., Xu, X., Wu, Y., Li, Y., Zhao, J., Li, R., Kang, J., & Lai, X., "3D FRN-ResNet: An Automated Major Depressive Disorder Structural Magnetic Resonance Imaging Data Identification Framework," *Frontiers Media*, vol. 14, May 13, 2022. https://doi.org/10.3389/fnagi.2022.912283.

[43] Kalia, M., "Neurobiological Basis of Depression: An Update," *Elsevier BV*, vol. 54, no. 5, May 1, 2005, pp. 24-27. https://doi.org/10.1016/j.metabol.2005.01.009

[44] Segal, A., Parkes, L., Aquino, K., Kia, S. M., Wolfers, T., Franke, B., Hoogman, M., Beckmann, C. F., Westlye, L. T., Andreassen, O. A., Zalesky, A., Harrison, B. J., Davey, C. G., Soriano-Mas, C., Cardoner, N., Tiego, J., Yücel, M., Braganza, L., Suo, C., … Chopra, S., "Regional, Circuit and Network Heterogeneity of Brain Abnormalities in Psychiatry

[45] Taylor, M. A., *The Neuropsychiatric Mental Status Examination*, Springer Nature, Jan. 1, 1981. https://doi.org/10.1007/978-94-011-7391-9.

[46] Choudhury, D., Counts, M., & Horvitz, S., "Social Media as a Measurement Tool of Depression in Populations," *Proceedings of the 5th Annual ACM Web Science Conference*, ACM, 2013, pp. 47–56.

[47] Coppersmith, G., Dredze, M., & Harman, C., "Quantifying Mental Health Signals in Twitter," *Proceedings of the Workshop on Computational Linguistics and Clinical Psychology: From Linguistic Signal to Clinical Reality*, 2014.

[48] James, J., Harris, Y. T., Kronish, I. M., Wisnivesky, J. P., & Lin, J. J. "Exploratory Study of Impact of Cancer-Related Posttraumatic Stress Symptoms on Diabetes Self-Management Among Cancer Survivors." *Psycho-Oncology* 27, February 21-23, 2018.

[49] Wongkoblap, A., Vadillo, M. A., & Ćurčin, V., "Researching Mental Health Disorders in the Era of Social Media: Systematic Review," *JMIR Publications*, 19(6), 2017, pp. e228-e228. https://doi.org/10.2196/jmir.7215.

[50] Paul, M., & Dredze, M., "You Are What You Tweet: Analyzing Twitter for Public Health," *Proceedings of the International AAAI Conference on Web and Social Media*, AAAI, 2021, pp. 265–272. https://doi.org/10.1609/icwsm.v5i1.14137.

[51] Pennebaker, J. W., Boyd, R. L., Jordan, K., & Blackburn, K., "The Development and Psychometric Properties of LIWC2015," *University of Texas at Austin*, 2015. https://doi.org/10.15781/T29G6Z.

[52] Kilpatrick, D. G., Resnick, H. S., Milanak, M. E., Miller, M. W., Keyes, K. M., & Friedman, M. J., "National Estimates of Exposure to Traumatic Events and PTSD Prevalence Using DSM-IV and DSM-5 Criteria: *DSM-5* PTSD Prevalence," *Journal of Traumatic Stress*, vol. 26, no. 5, 2013, pp. 537-547. https://doi.org/10.1002/jts.21848.

[53] Mueser, K. T., Rosenberg, S. D., Jankowski, M. K., Hamblen, J. L., Descamps, M., & McHugo, G. J., "A Cognitive-Behavioral Treatment Program for Posttraumatic Stress Disorder in Persons with Severe

Mental Illness," *American Journal of Psychiatric Rehabilitation*, vol. 7, no. 2, 2004, pp. 107-146. https://doi.org/10.1080/15487760490476183.

[54] Tarsitani, L., Tarolla, E., Berardelli, I., & Pasquini, M., "The Association between Post-Traumatic Stress Disorder and Chronic Medical Illnesses," *Journal of Psychosomatic Research*, vol. 124, 2019, p. 109748. https://doi.org/10.1016/j.jpsychores.2019.109748.

[55] Ayangunna, E., Shah, G., Kalu, K., Shankar, P., & Shah, B., "Variations in Pattern of Social Media Engagement between Individuals with Chronic Conditions and Mental Health Conditions," *Informatics (MDPI)*, vol. 11, no. 2, 2024, p. 18. https://doi.org/10.3390/informatics11020018.

[56] Feliciano, M., "An Overview of PTSD for the Adult Primary Care Provider," *Elsevier BV*, vol. 5, no. 7, July 1, 2009, pp. 516-522. https://doi.org/10.1016/j.nurpra.2008.12.009.

[57] Zhang, T., Schoene, A. M., Ji, S., & Ananiadou, S., "Natural language processing applied to mental illness detection: a narrative review", Proceedings of NPJ Digital Medicine (Springer Nature), University of Manchester (United Kingdom), 2022, pp. 46-46.

[58] Naslund, J. A., Bondre, A., Torous, J., & Aschbrenner, K. A., "Social Media and Mental Health: Benefits, Risks, and Opportunities for Research and Practice," *Springer Science+Business Media*, vol. 5, no. 3, Apr. 20, 2020, pp. 245-257. https://doi.org/10.1007/s41347-020-00134-x.

[59] Sinnenberg, L., Buttenheim, A. M., Padrez, K., Mancheno, C., Ungar, L., & Merchant, R. M., "Twitter as a Tool for Health Research: A Systematic Review," *American Journal of Public Health*, vol. 107, no. 1, 2017, pp. e1-e8. https://doi.org/10.2105/AJPH.2016.303512.

[60] Biernesser, C., Sewall, C. J. R., Brent, D., Bear, T., Mair, C., & Trauth, J., "Social Media Use and Deliberate Self-Harm Among Youth: A Systematized Narrative Review," *Children and Youth Services Review*, vol. 116, 2020, p. 105054. https://doi.org/10.1016/j.childyouth.2020.105054.

[61] Torous, J., Firth, J., Huckvale, K., Larsen, M. E., Cosco, T. D., Carney, R., & Christensen, H., "The Emerging Imperative for a Consensus Approach Toward the Rating and Clinical Recommendation of Mental Health Apps," *The Journal of Nervous and Mental Disease*, vol. 206, no. 8, 2018, pp. 662-666. https://doi.org/10.1097/NMD.0000000000000864.

[62] Golder, S., Ahmed, S., Norman, G., & Booth, A., "Attitudes Toward the Ethics of Research Using Social Media: A Systematic Review," *Journal of Medical Internet Research*, vol. 19, no. 6, 2017, p. e195. https://doi.org/10.2196/jmir.7082.

[63] Conway, M., & O'Connor, D., "Social Media, Big Data, and Mental Health: Current Advances and Ethical Implications," *Current Opinion in Psychology*, vol. 9, 2016, pp. 77-82. https://doi.org/10.1016/j.copsyc.2016.01.004.

[64] Fiesler, C., & Proferes, N., "'Participant' Perceptions of Twitter Research Ethics," *Social Media + Society*, vol. 4, no. 1, 2018, p. 2056305118763366. https://doi.org/10.1177/2056305118763366.

[65] Resnik, P., Armstrong, W., Claudino, L., Nguyen, T., Nguyen, V. A., & Boyd-Graber, J., "Beyond LDA: Exploring Supervised Topic Modeling for Depression-Related Language in Twitter," in *Proceedings of the 2nd Workshop on Computational Linguistics and Clinical Psychology: From Linguistic Signal to Clinical Reality*, Association for Computational Linguistics, 2015, pp. 99-107. https://doi.org/10.3115/v1/W15-1211.

[66] Coppersmith, G., Dredze, M., Harman, C., & Hollingshead, K., "From ADHD to SAD: Analyzing the Language of Mental Health on Twitter Through Self-Reported Diagnoses," in *Proceedings of the 2nd Workshop on Computational Linguistics and Clinical Psychology: From Linguistic Signal to Clinical Reality*, Association for Computational Linguistics, 2015, pp. 1–10. https://doi.org/10.3115/v1/W15-1201.

[67] Saha, K., Sugar, B., Torous, J., Abrahao, B., Kıcıman, E., & De Choudhury, M., "A Social Media Study on the Effects of Psychiatric Medication Use," in *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 13, 2019, pp. 440-451. AAAI Press. https://doi.org/10.1609/icwsm.v13i01.3262.

[68] Kroenke, K., Spitzer, R. L., & Williams, J. B. W., "The PHQ-9: Validity of a Brief Depression Severity Measure," *Journal of General Internal Medicine*, vol. 16, no. 9, 2001, pp. 606-613. https://doi.org/10.1046/j.1525-1497.2001.016009606.x.

[69] Gao, S., Gera, R., & Schmid, D., "Using Large Language Models for Mental Health Assessment on Social Media," *arXiv*, 2022. https://arxiv.org/abs/2206.12093.

[70] Kshirsagar, R., Morris, R., & Bowman, S. R., "Detecting and Explaining Crisis," *arXiv*, 2021. https://arxiv.org/abs/2103.01513.

[71] Preoţiuc-Pietro, D., Eichstaedt, J., Park, G., Sap, M., Smith, L., Tobolsky, V., Schwartz, H. A., & Ungar, L., "The Role of Personality, Age, and Gender in Tweeting About Mental Illnesses," in *Proceedings of the 2nd Workshop on Computational Linguistics and Clinical Psychology: From Linguistic Signal to Clinical Reality*, 2015, pp. 21-30.

[72] Tadesse, M. M., Lin, H., Xu, B., & Yang, L., "Detection of Depression-Related Posts in Reddit Social Media Forum," *IEEE Access*, vol. 7, 2019, pp. 44883-44893.

[73] Reece, A. G., Reagan, A. J., Lix, K. L., Dodds, P. S., Danforth, C. M., & Langer, E. J., "Forecasting the Onset and Course of Mental Illness with Twitter Data," *Scientific Reports*, vol. 7, no. 1, 2017, p. 13006. https://doi.org/10.1038/s41598-017-12961-9.

[74] Wu, Y., Chen, J., Mao, K., & Zhang, Y., "Automatic Post-Traumatic Stress Disorder Diagnosis via Clinical Transcripts: A Novel Text Augmentation with Large Language Models," *2023 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, IEEE, 2023.

[75] Asmundson, G. J. G., & Katz, J., "Understanding the Co-Occurrence of Anxiety Disorders and Chronic Pain: State-of-the-Art," *Depression and Anxiety*, vol. 26, no. 10, Wiley, 2009, pp. 888-901. https://doi.org/10.1002/da.20600.

[76] Boscarino, J. A., "Posttraumatic Stress Disorder and Physical Illness: Results from Clinical and Epidemiologic Studies," *Annals of the New York Academy of Sciences*, vol. 1032, no. 1, New York Academy of Sciences, 2004, pp. 141-153. https://doi.org/10.1196/annals.1314.011.

[77] Neria, Y., Nandi, A., & Galea, S., "Post-Traumatic Stress Disorder Following Disasters: A Systematic Review," *Psychological Medicine*, vol. 38, no. 4, Cambridge University Press, 2008, pp. 467-480. https://doi.org/10.1017/S0033291707001353.

[78] Mitchell, A. J., Vaze, A., & Rao, S., "Clinical Diagnosis of Depression in Primary Care: A Meta-Analysis," *The Lancet*, vol. 374, no. 9690, Elsevier, 2015, pp. 609-619. https://doi.org/10.1016/S0140-6736(09)60879-5.

[79] Orabi, A., Buddhitha, P., Hitchman, G., & Mahoney, T., "Deep Learning for Depression Detection of Twitter Users," *Proceedings of the Fifth Workshop on Computational Linguistics and Clinical Psychology: From Keyboard to Clinic*, Association for Computational Linguistics, 2018, pp. 88-97.

[80] Moreno, M. A., Egan, K. G., Bare, K., Young, H., Cox, E., & Borzekowski, D. L., "Internet Safety Education for Youth: Stakeholder Perspectives," *BMC Public Health*, vol. 13, BioMed Central, 2013, pp. 1-8. https://doi.org/10.1186/1471-2458-13-543.

[81] Leiva, V., & Freire, A., "Towards Suicide Prevention: Early Detection of Depression on Social Media," *Proceedings of the International Conference on Internet Science*, Springer, 2017, pp. 428-436.

[82] He, Q., Veldkamp, B. P., Glas, C. A. W., & de Vries, T., "Automated Assessment of Patients' Self-Narratives for Posttraumatic Stress Disorder Screening Using Natural Language Processing and Text Mining," *Assessment*, vol. 24, no. 2, SAGE Publications, 2017, pp. 157-172. https://doi.org/10.1177/1073191115602551.

[83] Bartal, A., Jagodnik, K. M., Chan, S. J., Babu, M. S., & Dekel, S., "Identifying women with postdelivery posttraumatic stress disorder using natural language processing of personal childbirth narratives", Proceedings of American Journal of Obstetrics & Gynecology MFM (Elsevier), Harvard Medical School (USA), 2023, pp. 100834.

[84] Radwan, A., Amarneh, M., Alawneh, H., Ashqar, H. I., AlSobeh, A., & Magableh, A. A. A. R., "Predictive Analytics in Mental Health Leveraging LLM Embeddings and Machine Learning Models for Social Media Analysis," *International Journal of Web Services Research*, vol. 21, no. 1, 2024, pp. 1–22. https://doi.org/10.4018/ijwsr.338222.

[85] Marcus, G., "The Next Decade in AI: Four Steps Towards Robust Artificial Intelligence," *arXiv preprint arXiv:2002.06177*, arXiv, 2020.

[86] Carlini, N., Tramer, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., ... & Song, D., "Extracting Training Data from Large Language Models," *arXiv preprint arXiv:2012.07805*, arXiv, 2021.

CIPHomeCare: A Machine Learning-Based System for Monitoring and Alerting Caregivers of Cognitive Insensitivity to Pain (CIP) Patients

Rahaf Alsulami[1], Hind Bitar[2], Abeer Hakeem[3], Reem Alyoubi[4]
Information Systems Department, King Abdulaziz University, Jeddah, Saudi Arabia[1, 2]
Information Technology Department, King Abdulaziz University, Jeddah, Saudi Arabia[3]
Pediatric Department, King Abdulaziz University Hospital, Jeddah, Saudi Arabia[4]

***Abstract*—Congenital Insensitivity to Pain (CIP) patients, particularly infants, are vulnerable to self-injury due to their inability to perceive pain, which can lead to severe harm, such as biting their hands. This research introduces "CIPHomeCare," a wearable monitoring solution designed to prevent self-injurious behaviors in CIP patients aged 6 to 24 months. The primary focus of this study is developing and applying machine learning algorithms to classify hand-biting behaviors. Using accelerometer data from the STEVAL-BCN002V1 sensor, which is a motion sensor, several machine learning models—K-Nearest Neighbors (KNN), Random Forest (RF), Naive Bayes (NB), Linear Discriminant Analysis (LDA), and Logistic Regression (LR)—were trained to differentiate between normal and harmful behaviors. To address data imbalance due to the infrequency of biting events, oversampling techniques such as SMOTE, Borderline-SMOTE, ADASYN, K-means-SMOTE, and SMOTE-ENN were employed to enhance classification performance. Among the algorithms, KNN achieved the highest accuracy (98%) and a sensitivity of 72%, highlighting its effectiveness in detecting harmful hand motions. The findings suggest that machine learning, in combination with wearable technology, can provide accurate, personalized monitoring and timely intervention for CIP patients, paving the way for broader clinical applications and real-time prevention of self-injury. The real-time processing capability of the system enables immediate alerting of caregivers, allowing for timely intervention to prevent injuries, thus improving their quality of life.**

Keywords*—Cognitive insensitivity to pain patients; CIP; machine learning; motion sensors; quality of life; wearable activity recognition

I. Introduction

One of the significant challenges that patients with CIP face is the late detection of injuries, as they are unable to feel pain. For instance, infants with CIP may inadvertently harm themselves while teething, sometimes biting their tongues to the point of cutting off the tip or gnawing on their hands until they bleed [1, 2, 3]. These behaviors can lead to severe self-mutilation or, in extreme cases, amputation [4]. Researchers have noted that due to the lack of pain perception and visible signs of distress, serious injuries can occur, including premature self-extraction of teeth [3, 5]. Therefore, it is crucial to provide patients, particularly infants and their caregivers, with coping strategies for this disorder. Such support can enhance their quality of life (QoL), defined as the impact of a disease, disability, or disorder on an individual's physical and mental well-being over time [6].

While most research on CIP has concentrated on understanding the disorder's characteristics [7, 8], there is a notable lack of studies that focus on developing coping mechanisms, especially in comparison to other conditions like attention deficit hyperactivity disorder. To date, and based on the authors' knowledge, there has been only one significant attempt to address the challenges faced by CIP patients: the design and fabrication of an assistive technology glove that alerts patients to extreme temperature variations in their environment [9]. However, this solution has limitations, as it may not fully address the broader range of self-injurious behaviors these patients experience. The glove primarily targets temperature awareness, leaving other critical aspects of injury prevention unaddressed. This highlights the need for more comprehensive interventions that can provide holistic support for individuals with CIP. It is essential to develop targeted solutions that address their specific needs. One critical area of focus is the issue of finger-biting behaviors, which can lead to severe self-injury and long-term consequences.

Providing a good quality of life for CIP disorder patients is the primary motivation of this research study. CIP disorder holds the potential to worsen the overall health of patients by limiting their capacity to live well and their functional status and productivity. This research focuses on finger-biting behaviors and aims to develop a solution called 'CIPHomeCare,' specifically designed for infants with CIP aged 6 to 24 months and their caregivers during the teething stage. Addressing this behavior is vital, as it not only helps prevent immediate physical harm but also supports the overall emotional and psychological well-being of patients and their families. Equipping caregivers with practical tools to monitor and manage these behaviors is essential; however, a key challenge is determining how to alert caregivers when a child with CIP begins to injure their hands. Specifically, there is a need to detect when a child's biting reaches a predefined limit and notify caregivers of the risk of injury.

Incorporating machine learning can be highly beneficial to address these challenges. Machine learning algorithms can analyze and identify patterns in patient datasets and

correlations that may not be immediately apparent through traditional methods. This facilitates the development of a dynamic threshold that adapts to individual behavior over time, ensuring personalized interventions. Furthermore, machine learning can enhance the estimation accuracy regarding when a child is likely to reach harmful biting levels, enabling caregivers to intervene proactively. By leveraging these advanced analytical techniques, the proposed solution not only improves safety but also empowers caregivers with actionable insights, ultimately contributing to better management of the disorder and enhanced QoL for CIP patients.

To implement this innovative approach, data from typically developing children was used, as no datasets are available specifically for CIP patients. By tracking the frequency of hand-biting behaviors over time, the researchers identified moments when a child might be at risk of self-harm. This data established a baseline for behavior patterns, which was then used to train various machine-learning algorithms. The analysis showed that the K-Nearest Neighbors (KNN) algorithm achieved the highest average accuracy rate of 98% in identifying abnormal hand motions. This predictive capability helps estimate the injury threshold, at which point the proposed solution would alert caregivers. The proactive alarm system is designed to notify caregivers before a child's biting reaches a level that could cause harm, thereby enhancing safety and preventing injuries.

To the best of our knowledge, 'CIPHomeCare' is the first comprehensive solution combining technology and machine learning to address the unique challenges CIP patients face, aiming to improve their quality of life. The remainder of this research is organized as follows: Section II reviews related works, including wearable activity recognition and classification algorithms. Section III provides an overview of the proposed solution. In Section IV, the experimental method is presented. Section V describes the evaluation methods used in this research. Section VI analyzes the results obtained. Discussion is given in Section VII. Finally, the conclusions are presented in Section VIII.

II. Related Work

Recent studies underscore the pivotal role of technology in advancing motion recognition through wearable devices, which are crucial for applications ranging from fall detection in elderly individuals to monitoring hazardous movements and anticipating potential risks. These technologies enable early detection and effective intervention, reducing injury severity and mortality rates in vulnerable populations [10]. Motion recognition technology's ability to analyze data, identify movements, and provide timely alerts has significantly improved patient safety and response times. Given its growing relevance, monitoring and investigating human gestures has become a central focus in commercial and biomedical research [11, 12]. The related work is organized as follows: the first part illustrates the new advancements in hand gesture monitoring technologies, the second part compares the use of one sensor against multiple sensors, and the last part provides insight into the impact of sensor placement on gesture recognition accuracy.

A. Advancements in Hand Gesture Monitoring Technologies

The field of hand gesture monitoring has seen rapid advancements, driven by the need for better rehabilitation tools and performance analysis systems. A notable study [10] introduced an intelligent wristband equipped with polymeric strain gauge sensors capable of detecting eight distinct hand gestures with 98% accuracy using Linear Discriminant Analysis (LDA). This innovation highlights the potential of simple yet highly accurate systems for recognizing complex hand gestures. Expanding on this, another study [13] examined hand gesture recognition in table tennis using multiple algorithms, including Support Vector Machine (SVM), LDA, K-Nearest Neighbor (KNN), Decision Tree (DT), and Naive Bayes (NB). The Decision Tree algorithm stood out, achieving an accuracy of 95%, demonstrating the effectiveness of ensemble methods in sports-related gesture recognition.

Real-time gesture recognition has also been explored, particularly with Inertial Measurement Unit (IMU) sensors. Research from 2018 [14] reported an accuracy range of 72% to 100%, with an average accuracy of 86.99% when using algorithms such as SVM, LDA, Dynamic Time Warping (DTW), and Principal Component Analysis (PCA). These studies collectively illustrate the diversity of approaches used in gesture recognition, each tailored to the specific application domain, highlighting both the potential and challenges of integrating such technologies into everyday use. Thus, this current research study uses real-time gesture recognition and accelerometer-based bracelet-type sensor specified for CIP children's patients.

B. Comparison of Single vs. Multiple Wearable Sensors

While many studies have focused on single-sensor configurations, others have explored using multiple sensors to enhance gesture recognition accuracy. Zhao et al. [15] developed a table tennis stroke classification system using three sensors placed on different body parts, achieving a recognition accuracy of 97.41% with SVM. This illustrates how combining multiple sensors can improve the precision of gesture detection in dynamic environments. In contrast, a study [16] compared single and multiple sensor setups, revealing only a modest difference in accuracy—90% for single sensors compared to 95% for multiple sensors. This finding suggests that the marginal improvement in accuracy with additional sensors may not justify the increased complexity and discomfort in practical applications, mainly when wearable devices are intended for daily use. Research has also shown that an increased number of sensors can interfere with everyday activities, reducing user comfort and compliance [17, 18]. These results emphasize the need to balance accuracy with usability, particularly in contexts like athletics or rehabilitation, where user comfort is paramount. Accordingly, this study considers children's comfort a priority, so only one sensor was used.

C. Impact of Sensor Placement on Gesture Recognition Accuracy

Sensor placement plays a critical role in determining the accuracy of gesture recognition systems. A study in [19] on fall detection using six sensors focused on wrist placement

achieved an accuracy of 96.63% using the K-NN algorithm. This highlights the importance of precise sensor placement in improving recognition rates. Similarly, research in [20] that compared wrist and below-elbow sensor placements for dynamic hand gestures found that wrist placement yielded a higher accuracy of 93.27%, likely due to the more extensive range of motion captured at the wrist. Despite the improved accuracy with multiple sensors, studies also noted that additional sensors can interfere with daily activities [17, 18], underscoring the trade-offs between accuracy and practicality.

Several technological innovations have further enhanced gesture recognition accuracy. For instance, a study [21] introduced an accelerometer-based pen-type device combined with a Feedforward Neural Network and Similarity Matching system to detect primary and complex hand gestures, achieving an accuracy of 98.9%. Other advancements include axis-crossing code algorithms for wrist gestures, achieving accuracies as high as 96.9% and 97.1%, respectively [21]. Additionally, specialized devices, such as a wristband developed for basketball shooting analysis, demonstrated the potential for highly accurate gesture recognition in sports, with up to 98.5% accuracy using the Artificial Neural Network (ANN) algorithm [22]. These studies underscore the importance of sensor placement and algorithmic improvements in achieving high accuracy in gesture recognition, particularly in practical, real-world applications. Hence, this research settles on the wrist as the best placement of the sensor.

Table I summarizes all the related work on gesture recognition. The first column lists the types of sensors used in each paper. The second column lists the algorithms used to classify and evaluate the data. Next, the hardware type is used to process the data. The next column illustrates the sensor's placement. The last column shows the average accuracy of each study. While many wearable solutions target broad applications, focusing on specific, well-defined user groups can enhance effectiveness.

TABLE I. SUMMARY OF THE RELATED WORK

#	Work	Sensor	Model (algorithm)	Computing Hardware	Placement	Accuracy
1	[18]	polymeric strain gauge	SVM, LDA	PC	wrist	98%
2	[23]	MPU9250 includes (6-DOF inertial measurement unit (IMU), 3-DOF magnetometer sensor)	K-NN, SVM, DT, LDA, NB	Not mentioned	wrist	95%
3	[24]	ADIS16448 inertial measurement unit	SVM	PC	upper arm, lower arm, back	97.41%
4	[25]	triboelectric motion sensor	K-NN	PC	Not mentioned	80%
5	[4] method 1	ACC, HR, BVP, skin temperature (ST), galvanic skin response (GSR)	Long short-term memory with deep learning (LSTM-DL)	PC	Wrist	95%
6	[4] method 2	Only ACC	LSTM-DL	PC	wrist	90%
7	[26]	MTw sensor unit	k-NN, SVM, DTW, ANN, Bayesian decision making (BDM), least squares method (LSM)	PC	head, chest, waist, right-wrist, right-thigh, right-ankle	96.63%
8	[27]	3-dimensional accelerometer (ACC), blood volume pulse (BVP), heart rate (HR)	Random Forest (RF)	PC	Hip and wrist	92%
9	[28]	ACC	SVM	mobile application	Hip and wrist	89%
10	[29]	ACC	K-NN, and SVM, LDA, ensemble method (EM)	Not mentioned	Hip or thigh	93%
11	[30]	IMU, electromyography	K-NN, NB, RF, J48	PC	Wrist	93.27%
12	[3]	Accelerometer-based pen-type sensing device	FNN, SM	PC	hand	98.9%
13	[7]	inertial sensor	DTW	PC	wrist	96.9%
14	[16]	IMU	Axis-crossing code matching	Cortex32-M0 level MCU	wrist	97.1%
15	[13]	Mpu9250, Power system, Communication	SVM, K-NN, RF, ANN	PC	wrist	97.4%
16	[31]	accelerometer, gyroscope, compass sensor	SVM, NB, RF, J48, AdaBoost, Hidden Markov Model (HMM)	Not mentioned	wrist	94%
17	[12]	IMU including Accelerometer, Gyroscope	SVM, DTW, LDA, PCA	Not mentioned	wrist	86.99%
18	[32]	IMU	restricted column energy (RCE) neural network, DTW	Field-programmable gate array (FPGA)	hand	98.6%
19	[33]	single patchable six-axis IMU	recurrent neural networks (RNN)	PC	wrist	95.3%
20	Original research	Accelerometer-based bracelet-type sensor device	K-NN, NB, RF, LDA, LR	PC	wrist	98%

In summary, wearable-based gesture recognition systems have significantly improved, with various algorithms and sensor configurations improving accuracy and practicality. Using algorithms like K-NN, Decision Tree, and ANN, combined with appropriate sensor placement, has proven effective in diverse applications such as fall detection, sports

performance analysis, and rehabilitation. While integrating multiple sensors can improve accuracy, single-sensor setups offer comparable performance with greater user comfort, particularly in everyday settings. Moreover, advancements in sensor technology, such as the development of wrist-based devices and novel algorithms, continue to push the boundaries of gesture recognition accuracy. Despite these advancements, challenges remain in real-time applications; balancing accuracy, sensor placement, and user comfort is critical. While previous research has focused on sensor-based systems for fall detection, this current study extends this by concentrating on CIP patients, who present unique challenges in gesture monitoring. The ongoing evolution of motion recognition technologies holds immense potential for improving patient safety and enhancing the quality of life for individuals across various domains.

III. Overview of the Proposed Solution: 'CIPHomeCare'

The proposed solution, 'CIPHomeCare,' comprises three main components, as depicted in Fig. 1. Since it is not within the main scope of the research, the architecture is not illustrated in detail. The first component is a motion/wearable sensor designed to be comfortable for infants and continuously monitor hand motions. It counts instances of biting and collects data on the frequency and intensity of these behaviors. The sensor establishes a baseline for normal behaviors by tracking these movements over time, allowing for better identification of abnormal patterns. The second component is the CIPHomeCore Smart Component, which processes the collected data using the wearable sensor. It trains machine learning models to classify hand motions and estimate when biting behaviors may become dangerous. The last component is the mobile application for caregivers, which is out of this research study's scope. The app provides real-time alerts to caregivers when the system detects a child approaching the predefined injury threshold. The application features an intuitive interface that displays data on the child's hand motions and biting frequency, empowering caregivers with actionable insights.

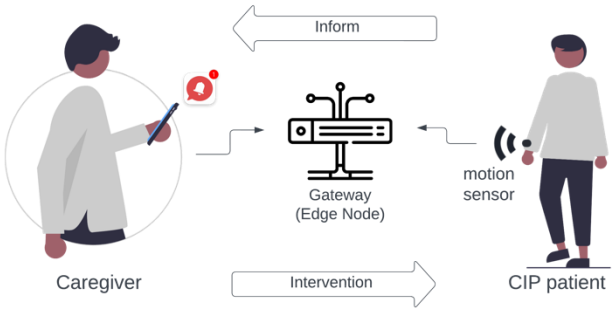


Fig. 1. The architecture of 'CIPHomeCare'.

These components create a comprehensive monitoring solution that enhances safety for CIP patients and supports caregivers in managing the disorder effectively.

IV. Methodology

This research encompasses multiple phases, from the initial selection of the sensor to the final analysis of the results.

Each phase was carefully designed to ensure the accuracy and reliability of data collection and analysis. Fig. 2. It illustrates the proposed workflow, which includes sensor selection, ethical considerations, data collection and processing, handling imbalanced dataset, training machine learning algorithms, and evaluating and comparing different approaches (illustrated in the Evaluation section). Statistical analysis was conducted using Python version 3.11, with libraries such as Pandas (version 2.2.2) for data processing and NumPy (version 1.26.4). The following subsections discuss all stages in detail.

A. Sensor Selection

The STEVAL-BCN002V1 multi-sensor is used to collect the data in this research study. The STEVAL- BCN002V1 is a multi-sensor board based on the BlueNRG-2 SoC Bluetooth Low Energy application processor and includes a 6-DOF inertial measurement unit (IMU). Thus, the child's wrist motions were collected using this sensor. The overall size is as tiny as a coin, so children would not feel uncomfortable wearing the sensor. It was chosen because of its small size, high accuracy, and low power consumption, making it suitable for continuous monitoring of young children without causing discomfort. The high sensitivity of the IMU allows for capturing even subtle hand movements, which is crucial for distinguishing between normal and biting behaviors. The sensor complies with European EMI/EMC and safety directives and standards.

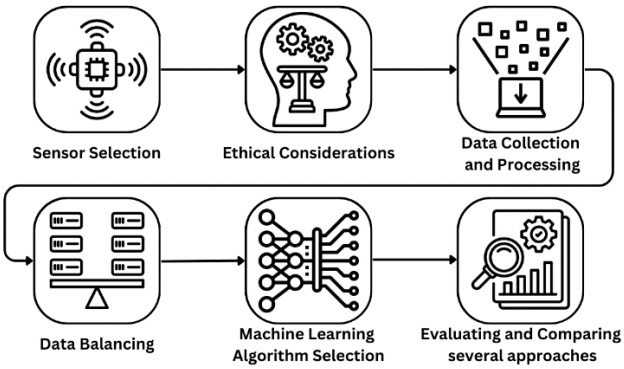


Fig. 2. The proposed workflow of 'CIPHomeCare'.

B. Ethical Considerations

This study followed the ethical principles outlined in the Declaration of Helsinki. Ethical approval was obtained from the Unit of Biomedical Ethics at King Abdulaziz University (No. HA-02-J-008) prior to the initiation of the research. Informed consent was secured from the guardians of all participants involved in the study. Each guardian was provided with detailed information regarding the purpose of the research, the procedures involved, and any potential benefits and risks. The study ensured that participation was voluntary, and participants could withdraw without consequences. To protect the confidentiality of participants,

all data was anonymized and stored securely. Identifiable information was removed to ensure that individual responses could not be traced back to specific participants, and each participant was assigned a random ID number to maintain patient confidentiality. Data access was restricted to authorized personnel only.

Additionally, measures were implemented to minimize potential discomfort or distress to the children during data collection. The type and design of the wearable sensor were selected with the children's comfort in mind, ensuring it was non-intrusive, and the children were monitored to ensure their well-being throughout the study.

C. Data Collection and Processing

This current study utilized a newly collected dataset of children's hand movements, with prior approval from their parents. Data were gathered from the King Abdulaziz University Hospital clinics and Childhood Centers in Jeddah City, Saudi Arabia. The only eligibility criterion was that the child had to be between 6 and 24 months old. This age group is chosen because it gets the most injuries among CIP patients due to their low cognitive ability [2, 3] and to protect them from injuries they could suffer from. The data collection employed an accelerometer-based sensor, which enabled real-time monitoring of the children's hand movements. The sensor was worn on the children's dominant hand. Data were collected daily for a maximum of 35 minutes per child to maintain consistency across participants and ensure comprehensive monitoring without causing fatigue. The data were collected between 9 am and 3 pm since the data is collected from a hospital and childhood center.

Wrist motion data was collected from 41 normal children without CIP health conditions. The children are 19 females and 22 males. The youngest participants were 6 months old, while the oldest were 2. Each child wore a wristband sensor for a maximum of 35 minutes daily. To capture natural behavior, the children were not restrained in their movements and were not instructed to perform any specific actions, providing a realistic baseline for detecting abnormal hand motion (biting motion). The wristband recorded acceleration data across the X-axis, Y-axis, and Z-axis, capturing various wrist motions, including the intensity and frequency of movements. Upon analyzing the acceleration data, significant differences in the peak profiles across the X, Y, and Z axes were observed.

Consequently, the acceleration data from all three axes was selected as this primary motion analysis dataset for subsequent motion recognition and detection. The recorded motion data was then manually classified by the first author (RA) into two categories: normal motion (no hand biting) and abnormal motion (hand biting), and then reviewed by three experts. Two experts, the second and the third co-authors (HB and AH), are from the technology field and have at least seven years of experience in machine learning. The third expert is from the health sector; the last co-author (RA) is a physician with over fifteen years of experience in the pediatric department (neurology division). However, some challenges arose during data collection: children did not frequently bite their hands, leading to an imbalanced dataset. To address this issue, oversampling techniques were employed to ensure a more balanced representation of both motion categories in the analysis phase.

The data processing phase started after labeling the data with the expert's assistance. The processing phase progressed through several stages until the appropriate stage was determined. Initially, we took the data as is and identified the abnormal biting behavior. Unfortunately, if the child bites his hand, the alarm will go off, which is not a practical solution. Then, we set a fixed threshold of 10 seconds to define abnormal biting behavior without accounting for individual differences in pain tolerance. This threshold was used uniformly across all participants. However, this approach led to substandard results, as it failed to consider the natural variability in how different children responded to discomfort.

Given that the data was collected from children, it was crucial to consider individual differences in pain tolerance, which naturally varies among them. Granted, we revised our approach by calculating each child's average biting duration and using it to create a personalized threshold for abnormal behavior detection. We significantly improved the system accuracy compared to a generic threshold. This adjustment resulted in improved accuracy and consistency in detecting abnormal behaviors.

Table II shows a sample of the average biting duration; some results are 0, which means those children did not bite their hands at all during the observation period. Table III illustrates that the children's hand motion dataset consisted of four columns and more than eight million rows. Each row represents a part of the child's hand motion. The four columns represent the acceleration data across the X-axis, Y-axis, and Z-axis, and the last column represents the child's status (label), whether they were biting their hand at the time or not.

TABLE II. AVERAGE BITING DURATION

ID	Average (Sec)
1	2.7975
2	0
3	0
4	1
5	6.2

TABLE III. AVERAGE BITING DURATION STATUS

X(mg)	Y(mg)	Z(mg)	Status
-184	1026	141	0
-110	974	89	0
-121	961	87	0
-126	985	114	0
-138	1011	168	0

D. Data Balancing

As mentioned earlier, children did not frequently bite their hands, which led to an imbalanced dataset. As shown in

Fig. 3, the children's hand motion dataset suffers from a severe skew in the class distribution. This figure highlights the imbalance in the children's hand motion dataset, with a significantly higher proportion of normal hand motion (99.7%) than abnormal hand biting motion (0.3%). This imbalance requires oversampling techniques to ensure balanced training of ML models due to the infrequency and importance of detecting biting events.

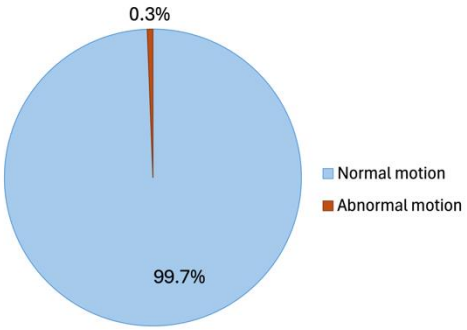


Fig. 3. Class distribution in the children hand motion dataset.

Several oversampling methods were investigated, such as the Synthetic Minority Over-sampling Technique (SMOTE), Borderline-SMOTE, Adaptive Synthetic Sampling (ADASYN), and K-means-SMOTE, to address class imbalance and mitigate overfitting in the collected dataset [34]. Each oversampling technique provides a dataset to be classified. SMOTE has gained significant attention due to its effectiveness and relative simplicity [34]. SMOTE is one of the earliest and most widely used methods, generating synthetic samples by interpolating between nearest neighbors within the minority class in the training set. This approach effectively blends features from original instances with those of randomly selected k-nearest neighbors [35]. An enhancement to SMOTE, known as Borderline-SMOTE [36], focuses on oversampling only those minority instances near the class boundary. Research indicates that Borderline-SMOTE improves classification performance for the minority class more effectively than both SMOTE and random oversampling methods. Another method applied is ADASYN [37], which adjusts the classification boundary by emphasizing more challenging examples. ADASYN employs a weighted approach to generate synthetic samples, prioritizing difficult instances within the minority class, and results from various datasets and evaluation metrics support its effectiveness.

K-means-SMOTE [38, 39] also leverages K-means clustering to identify clusters in the training data with an Imbalance Ratio (IR) below a specified threshold. SMOTE is then applied to these clusters, with the extent of oversampling determined by the sparsity and density of minority class objects. By implementing these four methods, the analysis aimed to effectively balance the dataset and reduce the risk of overfitting in the machine learning models.

In addition to the previously discussed oversampling techniques (SMOTE, Borderline-SMOTE, ADASYN, and K-means-SMOTE), this study also applied the SMOTE-ENN technique to address the class imbalance. SMOTE-ENN combines the Synthetic Minority Over-sampling Technique (SMOTE) with Edited Nearest Neighbors (ENN), providing an enhanced balance of the dataset by generating synthetic samples for the minority class while removing ambiguous samples that could potentially confuse the classifier [40]. This hybrid approach aims to improve the quality of the training set by effectively handling noisy instances, leading to potentially better model performance.

E. Machine Learning Algorithm Selection

Several machine learning algorithms were carefully selected to analyze the collected hand motion data. They were chosen for their proven effectiveness, as illustrated in related work, in similar applications and widespread implementation across various software platforms [16, 33]. The classifier algorithms applied in this work are as follows: the first chosen algorithm is the K-Nearest Neighbors (K-NN). It is a nonparametric, instance-based learning algorithm for classification and regression tasks. K-NN is recognized for its simplicity but can be computationally intensive due to its reliance on distance calculations between test instances and all training examples [41, 42]. The distance metric used in K-NN is typically the Euclidean distance, defined by Eq. (1).

$$\boldsymbol{d}(\boldsymbol{x},\boldsymbol{y}) = \sqrt{\sum_{i=1}^{n}(\boldsymbol{x_i} - \boldsymbol{y_i})^2} \quad (1)$$

This formula calculates the distance $\boldsymbol{d}(\boldsymbol{x},\boldsymbol{y})$ between two points, x and y, in an n-dimensional space, helping the algorithm classify new instances based on proximity to training examples [43].

The second algorithm used is Random Forest (RF), an ensemble-based technique known for its robustness in classification tasks. RF constructs multiple decision trees using randomly sampled subsets of data and features, aggregating results through majority voting [44]. It effectively handles complex interactions and diverse data types, although it can be computationally demanding [45]. The impurity measure used to evaluate the quality of splits in decision trees is often represented by Eq. (2).

$$G = 1 - \sum_{i=1}^{n} p_i^2 \quad (2)$$

In this formula, G denotes the Gini impurity, where pipi represents the probability of a class i within the dataset, allowing the algorithm to assess the homogeneity of splits [43].

Naive Bayes (NB), the third chosen algorithm, employs the Bayesian theorem for classification by calculating the mean and variance of feature variables within clusters. It is particularly effective for high-dimensional data and is recognized for its simplicity and computational efficiency [27,28]. The probability of a class C_k given a feature x is computed as in Eq. (3).

$$P(C_k|x) = \frac{P(x|C_k)\times P(C_k)}{P(x)} \quad (3)$$

This formula illustrates how the algorithm updates the probability of class membership based on observed features, leveraging prior knowledge and likelihood [43].

The fourth chosen algorithm is the Linear Discriminant Analysis (LDA), which finds a linear combination of features that best separates different classes, transforming features into lower-dimensional space to enhance class separability [46]. Although effective, it assumes a standard feature distribution and may struggle with non-linearly separable classes. The within-class scatter matrix is represented in Eq. (4).

$$S_w = \sum_{k=1}^{K} \sum_{x_i \in C_k} (x_i - \mu_k)(x_i - \mu_k)^T \quad (4)$$

In this formula, S_w captures the variance of data points x_i within each class C_k, where μ_k is the mean of class k [43].

The last algorithm used is logistic regression (LR). This algorithm predicts the probability of a target variable by analyzing relationships between independent variables [47]. The logistic function, which models the probability, is Eq. (5).

$$\sigma(z) = \frac{1}{1+e^{-z}} \quad (5)$$

Here, $\sigma(z)$ represents the predicted probability of the target variable, where z is a linear combination of the independent variables, ensuring outputs are constrained between 0 and 1[43].

V. Evaluation

Muraina et al. [48] and Nguyen et al. [49] showed that selecting a 70/30 ratio to be the training/testing ratio impacts and improves the predictive capability of the ML models. Thus, the dataset was split into 70% for learning and 30% for testing to evaluate all classifier models. To determine which machine learning algorithm best estimates hand motion behaviors using the collected dataset, we evaluated a combination of five classification techniques: KNN, RF, NB, LDA, and LR. Along with various oversampling techniques: SMOTE, ADASYN, Borderline-SMOTE, K-means-SMOTE, and the newly added SMOTE-ENN. The effectiveness of these different combinations is compared in terms of three key metrics: accuracy, sensitivity, and specificity. Accuracy is the ratio of the total number of correct predictions to the total number of predictions made [50].

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

Sensitivity refers to the proportion of actual positive cases (the abnormal motion) that the model correctly identifies [50].

$$Sensitivity = \frac{TP}{TP+FN} \quad (7)$$

While specificity measures how accurately the model classifies negative cases (the normal motion), indicating its effectiveness in predicting normal hand motion [50].

$$Specificity = \frac{TN}{TN+FP} \quad (8)$$

VI. Results

The primary objective of this study was to evaluate the performance of several machine learning algorithms in detecting abnormal hand motions (specifically hand biting) in children with CIP using wearable sensors. The findings from the classification algorithms and oversampling techniques reveal valuable insights into the effectiveness of these approaches in addressing data imbalance and accurately classifying hand motions.

Tables IV-IX summarize the performance metrics of the classification algorithms, including accuracy, sensitivity, and specificity, for each oversampling method. Each table details the performance of the various algorithms, with the first column listing the different algorithms, the second column displaying the accuracy results, the third column showing specificity values, and the last column presenting sensitivity values. Table IX displays the result of the original imbalanced dataset.

Initially, a fixed threshold of 10 seconds for pain tolerance across all children led to poor performance as it did not adequately capture individual differences in pain perception. By individualizing the threshold, accounting for differences in average biting duration, the accuracy, sensitivity, and specificity of the models improved significantly, offering a more personalized and effective monitoring mechanism.

TABLE IV. Comparison of Classification Techniques using SMOTE

Techniques	Accuracy	Sensitivity	Specificity
K-NN	0.99	0.69	1.00
RF	0.61	0.69	0.61
NB	0.64	0.62	0.64
LDA	0.56	0.60	0.56
LR	0.56	0.61	0.55

TABLE V. Comparison of Classification Techniques using Borderline-SMOTE

Techniques	Accuracy	Sensitivity	Specificity
K-NN	1.00	0.65	1.00
RF	0.67	0.53	0.67
NB	0.58	0.63	0.58
LDA	0.60	0.64	0.60
LR	0.59	0.64	0.59

TABLE VI. Omparison of Classification Techniques using ADASYN

Techniques	Accuracy	Sensitivity	Specificity
K-NN	0.99	0.69	1.00
RF	0.80	0.44	0.80
NB	0.50	0.61	0.50
LDA	0.60	0.42	0.60
LR	0.60	0.42	0.60

TABLE VII. COMPARISON OF CLASSIFICATION TECHNIQUES USING K-MEANS-SMOTE

Techniques	Accuracy	Sensitivity	Specificity
K-NN	1.00	0.65	1.00
RF	0.61	0.69	0.61
NB	0.64	0.63	0.64
LDA	0.56	0.59	0.56
LR	0.55	0.61	0.55

TABLE VIII. COMPARISON OF CLASSIFICATION TECHNIQUES USING SMOTE-EEN

Techniques	Accuracy	Sensitivity	Specificity
K-NN	0.98	0.72	0.98
RF	0.60	0.69	0.60
NB	0.63	0.64	0.63
LDA	0.56	0.50	0.56
LR	0.55	0.61	0.55

TABLE IX. ORIGINAL DATASET CLASSIFICATION

Techniques	Accuracy	Sensitivity	Specificity
K-NN	1.00	0.63	1.00
RF	1.00	0.00	1.00
NB	1.00	0.00	1.00
LDA	1.00	0.00	1.00
LR	1.00	0.00	1.00

Additionally, Oversampling techniques such as SMOTE, Borderline-SMOTE, ADASYN, K-means-SMOTE, and SMOTE-ENN played a crucial role in addressing class imbalance by generating synthetic samples for underrepresented classes and eliminating noisy data. These methods were particularly effective in enhancing model sensitivity across classifiers like KNN, RF, and NB, limiting the challenges posed by the rarity of abnormal behavior hand-biting in CIP patients.

From the results obtained, K-NN consistently outperformed the other algorithms across all oversampling methods especially with SMOTE-ENN, SMOTE and ADASYN where the sensitivity scores reached 0.72, 0.69 and 0,69, respectively. A sensitivity of 0.72 implies that it flagged the abnormal motion correctly, which means the children's risky motion is detected. Due to its instance-based learning approach, which effectively leveraged high-dimensional data for classifying hand movements. SMOTE-ENN, K-means-SMOTE, and SMOTE specifically contributed to improved sensitivity and specificity, with KNN showing the highest accuracy across all conditions. Similarly, RF demonstrated strong performance, particularly with ADASYN and SMOTE-ENN, indicating its capacity to handle complex data patterns. In contrast, NB maintained moderate accuracy (0.50-0.64), while linear models like LDA and LR struggled with non-linear data separability, yielding lower accuracies of 0.55-0.60.

As mentioned earlier, oversampling techniques were crucial in addressing class imbalance, which significantly enhanced the model's ability to detect rare hand-biting behaviors. SMOTE-based methods improved sensitivity across all algorithms, notably increasing KNN's sensitivity from 0.65 to 0.72 with SMOTE-ENN. However, ADASYN, while boosting RF's sensitivity, reduced its specificity to 0.44, illustrating the trade-off between enhanced detection of abnormal behaviors and increased false positives. This underscores the importance of choosing oversampling techniques aligned with specific clinical goals.

VII. DISCUSSION

To validate the result of this study, we compared our results with similar research studies regarding the performance of oversampling techniques, ML algorithm results, and the integration of wearable sensors with machine learning. These findings align with prior research in healthcare, where oversampling techniques such as SMOTE-ENN have been shown to enhance model performance across various applications, including healthcare fraud detection and diabetic risk prediction. For example, Bounab et al. demonstrated that SMOTE-ENN improved accuracy and reliability by balancing datasets and eliminating noise [51], while Aruleba and Sun found similar benefits in credit risk prediction [52].

In prior research, the application of deep neural networks for emergency department triage demonstrated improved sensitivity and specificity compared to conventional triage models [53]. Similarly, KNN and RF in our study achieved high sensitivity, especially when paired with K-means-SMOTE, reinforcing the idea that careful model selection and oversampling techniques can substantially enhance the ability to identify critical behaviors, which is crucial in clinical settings where missing abnormal events could have severe consequences.

The effectiveness of oversampling methods such as SMOTE and ADASYN was also observed in other domains, including healthcare data privacy and diabetic risk prediction [54]. These studies found that oversampling significantly improved the detection capabilities of models for minority class events, such as high-risk patients, which aligns with our finding that oversampling increased sensitivity and specificity for detecting abnormal hand-biting behaviors. This enhancement in sensitivity, while sometimes compromising specificity, underscores the necessity of selecting an oversampling technique that aligns with specific clinical objectives—whether prioritizing sensitivity for early detection or specificity to reduce false alarms.

Fig. 4 illustrates the sensitivity comparison for each algorithm, demonstrating that KNN outperforms other techniques, such as LDA and LR, and also shows promising results, particularly with the SMOTE technique, and even better performance with K-means-SMOTE. Additionally, NB maintains a relatively consistent accuracy of around 63%.

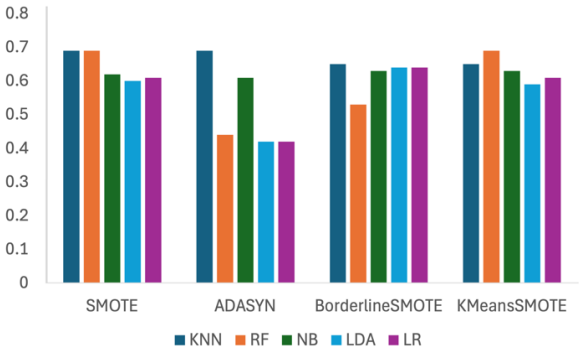


Fig. 4. Sensitivity.

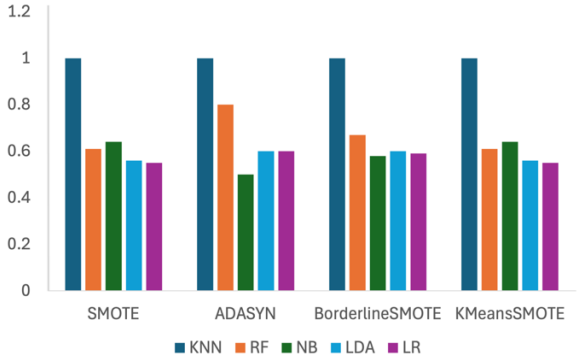


Fig. 5. Specificity.

Fig. 5 presents the specificity comparison across each oversampling technique. Here, KNN achieves the highest specificity again, while RF excels with the ADASYN method, showing comparable results to NB across the other three oversampling techniques. Moreover, while RF demonstrates overall good results, the NB algorithm achieves higher accuracy than LR. This can likely be attributed to the interdependence of the acceleration data across the X, Y, and Z axes; each feature contributes individually to the predictions made by the NB classifier.

Conversely, both LDA and LR underperformed, yielding a low average accuracy of 58% across all oversampling techniques. This highlights the need for careful selection of algorithms in future implementations to enhance detection capabilities for abnormal hand motions in children.

The results are also consistent with the work by Viloria et al., which demonstrated the efficacy of combining methods like SMOTE and random oversampling to address class imbalances in biomedical datasets [30]. Our use of SMOTE and ADASYN parallels these findings by effectively mitigating imbalance issues in hand motion data, thereby improving the models' ability to differentiate between harmful and non-harmful behaviors.

The integration of wearable sensors with machine learning for real-time monitoring, as demonstrated in this study, parallels prior applications in cardiovascular and neurological health monitoring [55]. This technology offers a viable solution for detecting harmful behaviors in CIP patients, enabling timely intervention and improving patient safety.

The high sensitivity achieved by KNN and RF, especially with SMOTE, K-means-SMOTE, and SMOTE-ENN, has important implications for real-world monitoring systems for CIP patients. Detecting abnormal hand motions like hand biting is critical for preventing self-injury in children who cannot feel pain. The wearable sensor system evaluated in this study offers a viable solution for real-time detection and intervention. By incorporating machine learning models that adapt to individual behavior patterns, caregivers can be alerted before harmful behaviors escalate, improving patient safety.

Moreover, the successful application of oversampling methods indicates that similar approaches could be used to detect other critical healthcare behaviors, such as monitoring involuntary movements in patients with neurological disorders. These findings are consistent with prior research on motion classification using wearable sensors. For example, previous studies have demonstrated the effectiveness of KNN and RF in recognizing activities and detecting critical health events when combined with appropriate data augmentation techniques. Additionally, machine learning models in real-time monitoring, similar to wearable devices used in cardiovascular health monitoring, underscores the transformative potential of AI in healthcare applications.

Studies have also validated the effectiveness of machine learning models like KNN and RF in recognizing critical health events across different domains. For example, KNN's success in heart sound analysis with an accuracy of 93.50% [56] and RF's compelling performance in fraud detection and credit risk analysis [57,58] demonstrate their robustness across varied datasets. These findings validate our approach, as KNN and RF were well-suited for highly dimensional accelerometer data, requiring distinguishing subtle variations in hand motion patterns.

Finally, addressing imbalanced datasets in healthcare has consistently been highlighted as a critical issue, especially in applications where the cost of false negatives can be severe. This research study extends previous literature by evaluating multiple oversampling techniques, providing a comprehensive understanding of how these methods can be applied to healthcare datasets with imbalanced classes, such as CIP-related hand-biting data. This emphasizes the importance of a tailored approach to handling imbalance, especially in clinical contexts where false negatives could harm patients [59].

In conclusion, this study demonstrates that KNN, particularly when paired with oversampling techniques like SMOTE-ENN, performs best for detecting abnormal hand motions in children with CIP. These findings support the potential for more effective intervention systems for CIP patients.

VIII. Conclusion, Limitations, and Future Work

This research explores the use of wristband sensors to investigate abnormal hand motions, explicitly focusing on hand biting. We collected and analyzed hand movement data from children to distinguish subtle differences between

normal and abnormal motions. The wristband sensor, equipped with motion detection technology, provides a portable and easily deployable solution. We utilized the STEVAL-BCN002V1 sensor to capture motion acceleration data, which was transmitted via Bluetooth for analysis. Our classification was based on acceleration data from three axes, resulting in an impressive average recognition accuracy of 98% and a sensitivity of 72%, highlighting the system's potential for future applications. The high sensitivity allows for capturing even subtle hand movements, which is crucial for classifying abnormal behaviors in real-world and other future applicability. Our findings underscore the value of detecting subtle differences in hand movements as a proactive measure for monitoring and preventing harmful behaviors. Furthermore, gaining deeper insights into these movements could substantially improve the quality of life for children affected by Congenital Insensitivity to Pain (CIP).

Despite these promising results, several limitations need to be addressed. The dataset used for model training and testing was relatively small, comprising data from only 41 children, which may affect the generalizability of our models to larger and more diverse populations. While we mitigated class imbalance using oversampling techniques, real-world datasets are often more complex and may introduce noise into synthetic samples. Additionally, sensor data were collected over a short period (35 minutes per day), potentially missing key variations in hand motions.

As a future direction, we plan to extend data collection over longer periods to improve model robustness and capture a broader range of motion variations. Future research should also focus on expanding the dataset to include a larger, more diverse population and incorporate additional relevant motions, such as eye rubbing, particularly for CIP patients. Integrating advanced deep learning techniques, such as Convolutional Neural Networks (CNNs), could enhance classification accuracy, especially for more complex motion patterns. Additionally, we will prioritize expanding the dataset and exploring similar behaviors to broaden the applicability of our findings. For CIP patients, even minor advancements could significantly improve their well-being and that of their caregivers. This research could also be extended to other conditions, such as autism, where motion detection is critical in managing behaviors. Another future direction after getting the necessary IRP approval is designing and building the whole system to ensure it is as safe as possible; we will conduct a clinical control trial study in a hospital to measure the system's effectiveness and scalability.

ACKNOWLEDGMENT

We want to express our sincere gratitude to King Abdulaziz University Hospital for their invaluable support in the data collection process for this research. Their assistance and collaboration enabled us to gather the necessary data to advance our study.

This research work was funded by Institutional Fund Projects under grant no (IFPRC-186-140-2020). Therefore, authors gratefully acknowledge technical and financial support from the Ministry of Education and King Abdulaziz University, Jeddah, Saudi Arabia.

REFERENCES

[1] Algahtani, H., N. M. I. A.-Q. M. A. S. A.-B. F. . S. B. [2016], ‘Congenital insensitivity to pain with anhidrosis: A report of two siblings with a novel mutation in (trka) ntrk1 gene in a saudi family’, Journal of the neurological sciences 370, 35–38.

[2] Magadami, R. [2021], private interview.

[3] Schalka, M. M. S., C. M. S. N. P. . C.-A. L. [2006], ‘Congenital insensitivity-to-pain with anhidrosis (cipa): a case report with 4-year follow-up’, 101(6), 769–773.

[4] Ramaraj, S. M., . D. D. [2015], ‘Congenital insensitivity to pain with anhidrosis in twin sisters with sensorineural deafness’, The Indian Journal of Pediatrics 82(8), 755–756.

[5] Behrendt, A., V. K. . W. W. E. [1997], ‘Consequences of serious oral injury associated with the congenital analgia syndrome’, ASDC journal of dentistry for children 64(4), 264–266.

[6] Bottomley, A. [2002], ‘The cancer patient and quality of life’, The oncologist 7(2), 120–125.

[7] Schon, K. R., P. A. P. J. . W. C. G. [2020], ‘Congenital insensitivity to pain overview.’.

[8] Karimi, M., . R. F. A. [2012], ‘A case report of congenital insensitivity to pain and anhidrosis (cipa)’, Iranian journal of child neurology 6(3), 45.

[9] Hanson, B. D., D. A. F. M. S. C. B. S.-. S. G. [2019], ‘Fabrication of a wearable temperature sensing system for cipa patients’, 14th International Conference on Nano/Micro Engineered and Molecular Systems (NEMS) pp. 84–87.

[10] Ferrone, A., M. F. M. L. A. M. C. A. P.-A. . . C. L. [2016], ‘Wearable band for hand gesture recognition based on strain sensors’, 6th IEEE International Conference on Biomedical Robotics and Biomechatronics (BioRob) 6, 1319–1322.

[11] Fukui, R., W. M. G. T. S. M. and Sato, T. [2011], ‘Hand shape classification with a wrist contour sensor: development of a prototype device’, 13th international conference on Ubiquitous computing 13, 311–314.

[12] Sadarangani, G., . M. C. [2016], ‘A wearable sensor system for rehabilitation apllications’, IEEE International Conference on Rehabilitation Robotics (ICORR) pp. 672–677.

[13] Sha, X., W. G. Z. X. R. X. W. S. H.-Z. . Z. Y. [2021], ‘Accurate recognition of player identity and stroke performance in table tennis using a smart wristband’, IEEE Sensors Journal 21(9), 10923–10932.

[14] Wang, Y. T., . M. H. P. [2018], ‘Real-time continuous gesture recognition with wireless wear- able imu sensors’, IEEE 20Th international conference on e-health networking, applications and services (healthcom) 26, 1–6.

[15] Liu, R., W. Z. S. X. Z. H. Q. S. L.-J. . Y. N. [2019], ‘Table tennis stroke recognition based on body sensor network’, In International Conference on Internet and Distributed Computing Systems pp. 1–10.

[16] Sevil, M., R. M. M. Z. H. I. S. S. A.-M. R. . . C. A. [2020], ‘Determining physical activity characteristics from wristband data for use in automated insulin delivery systems’, IEEE Sensors Journal 20(21), 12859–12870.

[17] Ahmadi, M. N., P. K. A. . T. S. G. [2020], ‘Physical activity classification in youth using raw accelerometer data from the hip’, Measurement in Physical Education and Exercise Science 24(2), 129–136.

[18] Manjarres, J., N. P. G. K. P. W. . P. M. [2020], ‘Physical workload tracking using human activity recognition with wearable devices’, sensors 20(1), 39.

[19] Özdemir, A. T. [2016], ‘An analysis on sensor locations of the human body for wearable fall detection devices: Principles and practice’, sensors 16(8), 1161.

[20] Kefer, K., H. C. . F. R. D. [2017], ‘Evaluating the placement of arm-worn devices for recognizing variations of dynamic hand gestures’, Mobile Multimedia 12(34), 225–242.

[21] Xie, R., . C. J. [2016], 'Accelerometer-based hand gesture recognition by neural network and similarity matching', IEEE Sensors Journal 16(11), 4537–4545.

[22] Lian, C., M. R. W. X. Z. Y. P. H. Y.-T. . . L. W. J. [2021], 'Ann enhanced iot wristband for recognition of player identity, and shot types based on basketball shooting motion analysis', IEEE Sensors Journal.

[23] Maselli, F., Chirici, G., Bottai, L., Corona, P. and Marchetti, M. [2005], 'Estimation of mediter- ranean forest attributes by the application of k-nn procedures to multitemporal landsat etm+ images', International Journal of Remote Sensing 26(17), 3781–3796.

[24] Mika, S., Ratsch, G., Weston, J., Scholkopf, B. and Mullers, K.-R. [1999], Fisher discriminant analysis with kernels, in 'Neural networks for signal processing IX: Proceedings of the 1999 IEEE signal processing society workshop (cat. no. 98th8468)', Ieee, pp. 41–48.

[25] Mohamed, A. E. [2017], 'Comparative study of four supervised machine learning techniques for classification', International Journal of Applied 7(2), 1–15.

[26] Nagasako, E. M., O. A. L. . D. R. H. [2003], 'Congenital insensitivity to pain: an update', Pain 101(3), 213–219.

[27] Ng, A. and Jordan, M. [2001], 'On discriminative vs. generative classifiers: A comparison of logistic regression and naive bayes', Advances in neural information processing systems 14.

[28] Nikam, S. S. [2015], 'A comparative study of classification techniques in data mining algorithms', Oriental Journal of Computer Science and Technology 8(1), 13–19.

[29] Peddareddygari, L. R., O. K. . G. R. P. [2014], 'congenital insensitivity to pain: a case report and review of the literature'.

[30] Sheng, B., M. O. M. D. P.-C. B. D. P.-C. J. A.-R. R. M. . Z. Y. [2020], 'A comparison of different machine learning algorithms, types and placements of activity monitors for physical activity classification', 145, 107480.

[31] Sun, Z., Hu, K., Hu, T., Liu, J. and Zhu, K. [2018], 'Fast multi-label low-rank linearized svm classification algorithm based on approximate extreme points', IEEE Access 6, 42319–42326.

[32] Scholkopf, B., . S. A. J. [2018], Learning with kernels: support vector machines, regularization, optimization, and beyond, MIT press.

[33] Schon, K. R., P. A. P. J. . W. C. G. [2017], 'Weighted level set evolution based on local edge features for medical image segmentation', IEEE Transactions on Image Processing 26(4), 1979– 1991.

[34] Tarawneh, A. S., Hassanat, A. B., Altarawneh, G. A., & Almuhaimeed, A. (2022). Stop oversampling for class imbalance learning: A review. *IEEE Access*, *10*, 47643-47660.

[35] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, ''Smote: Synthetic minority over-sampling technique,'' *J. Artif. Intell. Res.*, vol. 16, pp. 321–357, Jul. 2018.

[36] Revathi, M., & Ramyachitra, D. (2021). A modified borderline smote with noise reduction in imbalanced datasets. *Wireless Personal Communications*, *121*(3), 1659-1680.

[37] Dey, I., & Pratap, V. (2023, March). A comparative study of SMOTE, borderline-SMOTE, and ADASYN oversampling techniques using different classifiers. In *2023 3rd international conference on smart data intelligence (ICSMDI)* (pp. 294-302). IEEE.

[38] Douzas, G.; Bacao, F.; Last, F. Improving imbalanced learning through a heuristic oversampling method based on k-means and SMOTE. Inf. Sci. 2018, 465, 1–20.

[39] Rodríguez-Torres, F., Martínez-Trinidad, J. F., & Carrasco-Ochoa, J. A. (2022). An oversampling method for class imbalance problems on large datasets. *Applied Sciences*, *12*(7), 3424.

[40] Bounab, R., Zarour, K., Guelib, B., & Khlifa, N. (2024). Enhancing Medicare Fraud Detection Through Machine Learning: Addressing Class Imbalance With SMOTE-ENN. IEEE Access.

[41] Pawar, P. Y., . G. S. H. [2012], 'A comparative study on different types of approaches to text categorization', International Journal of Machine Learning and Computing 2(4), 423.

[42] Mahesh, B. [2020], 'Machine learning algorithms-a review', International Journal of Science and Research (IJSR).[Internet] 9, 381–386.

[43] GeeksforGeeks. Available online: https://www.geeksforgeeks.org/ (accessed on 28 Sep 2024).

[44] Buskirk, T. D. [2018], 'Surveying the forests and sampling the trees: An overview of classification and regression trees and random forests with applications in survey research.', Survey Practice 11(1), 1–13.

[45] Kefer, K., H. C. . F. R. D. [2017], 'Evaluating the placement of arm-worn devices for recognizing variations of dynamic hand gestures', Mobile Multimedia 12(34), 225–242.

[46] Tharwat, A., Gaber, T., Ibrahim, A. and Hassanien, A. E. [2017], 'Linear discriminant analysis: A detailed tutorial', AI communications 30(2), 169–190.

[47] Logistic Regression—ProQuest. Available online: https://www.proquest.com/openview/e8e7564d6f02ac54d757f3b74422f0ef/1?pq-origsite=gscholar&cbl=30764 (accessed on 25 Aug 2024).

[48] Muraina, I. (2022, May). Ideal dataset splitting ratios in machine learning algorithms: general concerns for data scientists and data analysts. In 7th international Mardin Artuklu scientific research conference (pp. 496-504).

[49] Nguyen, Q. H., Ly, H. B., Ho, L. S., Al-Ansari, N., Le, H. V., Tran, V. Q., ... & Pham, B. T. (2021). Influence of data splitting on performance of machine learning models in prediction of shear strength of soil. Mathematical Problems in Engineering, 2021(1), 4832864.

[50] Itoo, F., Meenakshi, & Singh, S. (2021). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *International Journal of Information Technology*, *13*(4), 1503-1511.

[51] Bounab, R., Zarour, K., Guelib, B., & Khlifa, N. (2024). Enhancing Medicare Fraud Detection Through Machine Learning: Addressing Class Imbalance With SMOTE-ENN. IEEE Access.

[52] Aruleba, I., & Sun, Y. (2024). Effective Credit Risk Prediction using Ensemble Classifiers with Model Explanation. IEEE Access.

[53] Goto, T., Camargo, C. A., Faridi, M. K., Freishtat, R. J., & Hasegawa, K. (2019). Machine learning–based prediction of clinical outcomes for children during emergency department triage. JAMA network open, 2(1), e186937-e186937.

[54] Balasubramanian, S., Kashyap, R., CVN, S. T., & Anuradha, M. (2020, December). Hybrid prediction model for type-2 diabetes with class imbalance. In *2020 IEEE international conference on machine learning and applied network technologies (ICMLANT)*(pp. 1-6). IEEE.

[55] Hamza, M. F. A. B., & Sjarif, N. N. A. (2024). A Comprehensive Overview of Heart Sound Analysis Using Machine Learning Methods. IEEE Access.

[56] Hamza, M. F. A. B., & Sjarif, N. N. A. (2024). A Comprehensive Overview of Heart Sound Analysis Using Machine Learning Methods. *IEEE Access.*

[57] Bounab, R., Zarour, K., Guelib, B., & Khlifa, N. (2024). Enhancing Medicare Fraud Detection Through Machine Learning: Addressing Class Imbalance With SMOTE-ENN. *IEEE Acces.*

[58] Aruleba, I., & Sun, Y. (2024). Effective Credit Risk Prediction using Ensemble Classifiers with Model Explanation. *IEEE Access.*

[59] Dina, A. S., Siddique, A. B., & Manivannan, D. (2022). Effect of balancing data using synthetic data on the performance of machine learning classifiers for intrusion detection in computer networks. IEEE Access, 10, 96731-96747.

A Multi-Person Collaborative Design Method Driven by Augmented Reality

Liqun Gao*
College of Arts and Design, Ningbo University of Finance & Economics, Ningbo, Zhejiang, 315715, China

***Abstract*—The current interior design of commercial buildings is facing innovative challenges, requiring a balance between aesthetics, functionality, and economic benefits. The design industry faces challenges in interdisciplinary integration, lack of standardized processes, and limitations of traditional design methods in complex situations. Although virtual reality technology provides new solutions, its integration difficulty, cost, and operational complexity constrain its widespread application. This study introduces a digitally twin-based augmented reality (AR) collaborative indoor design framework, addressing the decomposition of spatial planning for the complexity inherent in design processes. Subsequently, contextual data in the indoor design process is structured into an indoor design knowledge graph to elucidate information transmission and iterative mechanisms during collaborative design, thereby enhancing the situational adaptability of AR collaborative design. Utilizing a root anchor-based collaborative approach, multiple designers engage in spatial design collaboration within the AR environment. Real-time knowledge and data facilitated by the design knowledge graph contribute to collaborative decision-making, ensuring the quality and efficiency of collaborative design. Finally, exemplified by a complex interior design project for a commercial space, an AR-based collaborative digital twin (DT) interior design system is established, validating the effectiveness and feasibility of the proposed methodology. Through this approach, designers can preview and modify designs in a virtual environment, ultimately reducing errors, shortening design cycles, lowering costs, and enhancing user satisfaction.**

Keywords*—Digital twin; optimized design; interior space; multi-person collaborative design

I. Introduction

In the golden age of commercial building interior design, traditional design concepts are being questioned and new ideas are overturning established principles and paradigms. Commercial buildings, second only to residential buildings in floor area, are the most numerous and widely ranged, touching every aspect of daily urban life [1]. They serve as a window into the socio-economic status of a city, reflecting the material economic life and vibrant cultural character. The interior environment is an essential component of commercial architecture. Analyzing design trends and creating a favorable commercial environment also contributes to urban economic development [2]. Due to the significant costs, long construction cycles, and high public engagement, once completed, commercial interior projects can broadly impact the regional landscape and environment [3]. Consequently, stakeholders demand higher safety, functionality, and economic performance compared to other buildings, leaving no room for error in the design process. However, the interior design industry still faces significant challenges:

1) Interdisciplinary integration and complexity: Interior design involves aesthetics, architecture, environmental psychology, material engineering, and other disciplines. Designers must ensure beauty while guaranteeing functionality and comfort, increasing design complexity. Traditional commercial interior design must consider building types, environmental harmony, landscape coordination, and investment risks.

2) Overreliance on personal experience: Designers' unique styles and experiences mean that designs are often limited by individual capabilities. The lack of standardized design processes leads to inefficiency.

3) Slow feedback and rework: Traditional design processes often require multiple revisions, with each change consuming considerable time and resources, limiting design efficiency.

4) Singular design methods: The complexity of situations hinders the use of precise theories or quantitative methods to demonstrate the scientific aspects of design. Whether it's aesthetics or space and environmental factors, methods for presenting and arguing commercial building interior design solutions are quite singular, urgently requiring a realistic, intuitive, and visual technology method for presentation.

In interior design processes, due to the emphasis on spatial visualization and user experience, the characteristics of virtual reality technology are highly similar, as it is a computer system that presents a virtual world or simulated environment to users. Virtual reality can serve people better by allowing users to experience the architectural environment from all angles and senses from the design's inception. As a result, the integration of interior design with virtual reality technology is gradually being widely applied in the industry.

Firstly, since interior design is a process involving planning, design, and construction, which is costly and irreversible, it cannot afford many errors. Virtual reality technology, with its lifelike presentation, allows for the preview and real-time modification of interior design plans. Designers and users can enter the virtual space at any time, examining their work from any angle, truly feeling the space, scale, materials, textures, details, and sounds, thus resolving issues arising from overlooking errors in two-dimensional design drawings.

Secondly, unlike traditional design media, virtual reality technology describes building interiors dynamically and

interactively with real-time feedback. Users can thus compare and edit interior design elements during the preview, modifying them according to their needs and preferences without professional constraints.

In this context, the rapidly developing virtual reality technology facilitates the expression of interactive interior design, enhancing the realism of the experience and meeting the growing demand for "interactivity" among contemporary users.

However, looking at the current application of virtual reality technology in interior design, imperfections in design methodology can cause issues such as how to integrate virtual reality into the design process, resolve the high computational demands and significant costs in terms of capital and time investment, and overcome the lack of familiarity with operating methods limiting its widespread adoption. These issues hinder the digital evolution of architectural interior design methods and the innovative integration and widespread teaching of virtual reality technology in everyday life. Therefore, this paper proposes an augmented reality-driven method for interior space design. This method allows for the examination and evaluation of design effects at the initial conceptual stage, simulating construction quality before building to ensure control, thereby reducing design time and improving design quality while saving resources.

II. Literature Review

In recent years, the rapid advancements in cutting-edge technologies such as artificial intelligence, big data, and cyber-physical systems have been driving the swift evolution of engineering design. This paper provides a comprehensive review of the current state of research in this domain.

A. Digital Design

Currently, digital design technologies have been widely applied in the field of interior space design, particularly in the planning and innovation of residential, commercial, and exhibition spaces [4]. Design software tools such as SketchUp, AutoCAD, and Revit have become indispensable for designers, supporting complex design requirements such as 3D modeling, virtual reality roaming, and environmental simulation. With the development of big data and artificial intelligence technologies, data-driven interior design has become a research hotspot. By collecting and analyzing designers' creative ideas, user behavior data, and the usage effects of interior spaces, more accurate predictions of the functionality and user experience of interior spaces can be made during the design phase.

In recent years, interior designers have intensified their pursuit of rapidly developing interior space design solutions that are both aesthetically pleasing and practical, meeting consumers' demands for personalized and functional interior spaces. Grübel et al. [5] used digital technology to design multifunctional interior spaces that meet strict requirements for environmental adaptability and user interactivity, achieving a level of functionality and aesthetic design comparable to high-end standards. Lu et al. [6], focusing on home office spaces, explored the application of digital design and analysis technologies in interior space design, combining digital design with user behavior analysis to achieve optimal design outcomes. Künz et al. [7] summarized the development of some advanced digital interior design methods, particularly emphasizing advanced digital design for smart home products beyond traditional furniture and decorative materials. This approach is considered key to improving residents' quality of life fundamentally. Schroeder et al. [8], utilizing digital technology, proposed a data-driven intelligent interior design simulation model based on user experience feature learning. Using personalized design techniques and leveraging user behavior data and spatial layout data, they designed personalized interior environments.

However, as user demands for interior spaces become increasingly personalized and functional, new challenges arise for digital interior space design. How to rapidly design interior spaces that meet specific user needs while ensuring design feasibility and sustainability is a major research direction in the future of digital interior space design.

B. DT-driven Design Patterns

DT technology has been widely applied throughout the entire lifecycle of interior space design, construction, and maintenance. For instance, Coupry et al. [9] designed an interior design visualization technology based on DTs and virtual reality. This system provides an intuitive representation and accurate description of interior space layouts, systematically manages spatial usage data and user interaction data, thereby enhancing design precision. Schott et al. [10] proposed a DT-driven interior design collaboration platform, establishing a stable and reliable communication mode among designers, engineers, and clients throughout the entire design process.

In response, Zhu et al. [11] introduced a comprehensive, precise, real-time interior environment monitoring and analysis system. This technology, by bridging the gap between the actual interior environment and the digital model, enables real-time iteration and optimization of interior design. As interior space design becomes increasingly complex, requiring knowledge from multiple disciplines, Xu et al. [12] identified DT (DT) as one of the most promising enabling technologies for achieving smart buildings and smart cities. Therefore, integrating knowledge from different disciplines in the design process to realize interdisciplinary digital interior space design is a crucial future research trend.

In light of this, Pang et al. [13] proposed a DT-driven method for rapid personalized design of residential and commercial spaces. Wang et al. [14] presented a rapid personalized design method for office space layouts based on DTs. They developed an analysis-decoupling framework based on DTs to provide interior design analysis capabilities and support decision-making for design and solution assessment. Liu, Zheng & Bao [15] discussed the application of DT models as a natural evolution in model-based engineering in interior design. These are important application cases of DTs in the interior space design phase. The application of DT-driven interior space design has been summarized by relevant scholars and proven to be a significant method for enhancing the interior design process. DT technology holds greater efficiency potential in the construction and management of interior spaces.

C. Research Gaps

With the evolution of modern interior design, spatial planning and personalized customization have become increasingly intricate and detailed, posing challenges that current design methods often struggle to address. Despite the ongoing shift of contemporary interior design methods towards three-dimensional modeling and virtual reality technologies, inherent issues persist, as outlined below.

1) Lack of parameterized collaborative design approaches: This implies that manual adjustments are required when spatial functional needs or user preferences change, leading not only to time consumption but also potential design inconsistencies. Introducing parameterized collaborative design approaches can automate design adjustments, saving time and enhancing design consistency and accuracy.

2) Application of DTs in the design process: Furthermore, although DTs have found widespread applications in various domains such as manufacturing and medical simulation, their application in the interior design process remains underexplored. DTs can provide additional information for the design process, including spatial usage simulation, lighting, and acoustic effects, thereby elevating design precision and user satisfaction.

Motivated by these identified research gaps and objectives, this study aims to develop a DT-based intelligent collaborative design method for interior space design. Integrating parameterized collaborative design and DT technology, this approach seeks to enhance the efficiency, precision, and personalization of interior space design. Simultaneously, this research aspires to propel the advancement of interior design by presenting innovative perspectives and methodologies for future endeavors in this field.

III. DT-based Multi-Person Collaborative Design System

To meet the application demands of intricate assembly scenarios, this chapter delves into the intricacies of collaborative scenarios. It introduces an architecture for multi-user collaborative assembly methods based on Augmented Reality (AR) and DT technology. Additionally, it conducts an analysis of collaborative assembly sequences within the DT framework.

A. Multi-Person Collaborative Design Process

In intricate interior space design, the design process typically encompasses multiple complex stages, demanding precision in design execution and necessitating close coordination between these stages. Collaborative design involving multiple individuals can significantly enhance design efficiency, contingent upon efficient task collaboration. The collaborative process relies on the macro-management and swift allocation of tasks by the design administrator. Simultaneously, it is constrained by the understanding of tasks by on-site design personnel and the execution of design operations. Fig. 1 illustrates the collaborative process of complex interior space design. This paper divides the collaborative design process into two parts: single-functional area design collaboration and multi-functional area design collaboration.

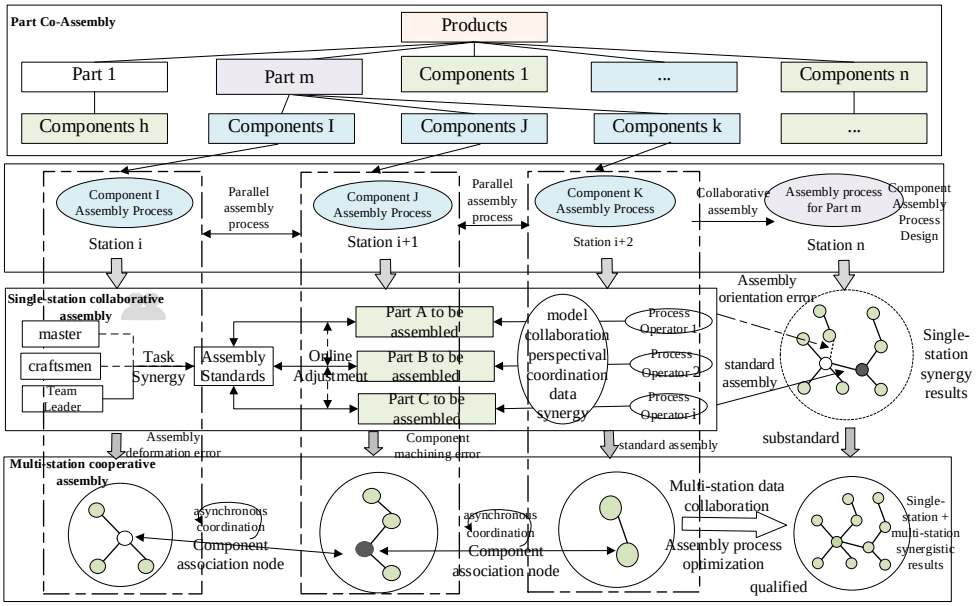


Fig. 1. Collaborative process for designing complex interior spaces.

1) Complex interior space design process in a single functional area: When the design requirements of a space are complex, multiple designers conduct different design operations in the same functional area from different design perspectives. This task collaboration process is termed single-functional area collaborative design. In this design process, senior designers are responsible for formulating design concepts, design managers review design proposals, design task cards are created based on the design process, project managers manage on-site activities, guide and plan the work of designers, and collaborative designers' complete tasks. The collaborative process primarily focuses on the interaction

between project managers and designers, with the project manager being the key decision-maker in collaboration. During the design process, rapid extraction of individual design tasks and collaborative relationships, along with unified and accurate acquisition and expression of information, is crucial for on-site designers to effectively grasp design details. Additionally, due to the tolerance range in design quality standards, it is necessary to systematically coordinate, optimize design parameters based on on-site conditions, and iteratively control the design process to ensure the stability of collaborative design quality.

2) Collaborative design process for complex interior space with multiple functional areas: When the tolerance requirements for space design are high, and there are multiple and interrelated functional areas, not only must design integration errors arising from the collaborative design process between various functional areas be considered, but also the cumulative errors resulting from material selection, furniture layout, and lighting design errors in the design processes of each functional area leading to design inconsistencies. The design process is top-down, controlling from overall design concepts to specific design elements. It macroscopically manages the design process and, based on the relationships and design precision of various functional areas, optimizes the design process into a multi-functional area collaborative design process. Due to the independence of each functional area, information collaboration computation and feedback between functional areas are crucial means to achieve accuracy prediction and process optimization.

B. Multi-person Collaborative Design Approach Incorporating AR

In order to ensure the efficiency of interior space design, this paper optimizes the collaborative design process and establishes a DT-based AR multi-user collaborative design architecture, as depicted in Fig. 2. Within the DT space, the three-dimensional model and design information are initially processed to extract abstract design attribute information and relational information, which is employed for the expression of design knowledge. Subsequently, design semantic information is organized in the format of "Entity-Relation-Entity" and "Entity-Attribute-Value" to construct a design knowledge graph. Object mapping is conducted based on the knowledge graph to build the design twin. Each node in the knowledge graph represents the twin representation of a physical object in the digital space. Based on hierarchy, these representations are categorized into object-level twins and space-level twins. The latter includes both attribute and layout information. The DT serves as the foundation for design management and data collaboration.

The AR-guided scenario serves as a bridge between the physical design space and the DT design space, facilitating guidance and collaboration throughout the design process. The AR system disseminates and visualizes designers' tasks based on the collaborative attribute information of nodes in the design knowledge graph, constructing a collaborative AR space. Model collaboration, perspective coordination, and data collaboration in single-functional area collaboration are achieved through multi-device collaboration and control.

The physical design space acquires design and collaborative information through the AR system, completing collaborative design tasks with visual guidance. To guide different collaborative tasks, the AR system possesses independence and collaboration. Independence ensures the guidance of different design tasks for various functional areas, ensuring effective guidance for single-functional area collaboration. Collaboration involves self-adjustment based on the design conditions of other functional areas during multi-functional area collaboration, ensuring that the overall spatial design meets aesthetic and functional specifications.

The DT space guides the design implementation of the physical space based on design principles, ensuring the standardization and efficiency of the design process through the virtual-to-real mapping process. Changes in the physical space's design drive the evolution of the DT, ensuring the high fidelity of the DT design process through a bidirectional mapping approach.

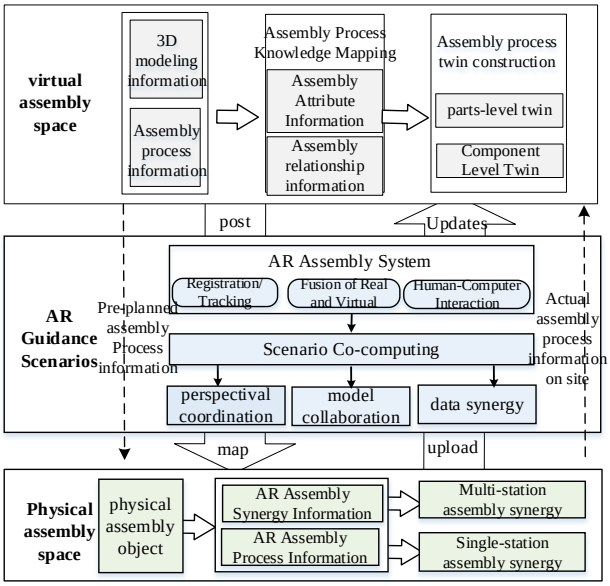


Fig. 2. DT-based multi-person collaborative design architecture for AR.

IV. DT-Driven Linked Design Process

This section provides a DT-driven approach to multi-person collaboration.

A. Process Collaboration

In this section, we employ manufacturing processes as fundamental units to establish an augmented reality-based DT multi-user collaborative interior space design workflow, as illustrated in Fig. 3. The process delineates the transmission and iterative mechanisms of design information between the physical design scenario and the DT space.

In the figure, following the determination of the interior space design scheme, the twin space stores and expresses design information in the form of a knowledge graph, where nodes represent specific design elements, and edges signify relationships between design elements. Each node in the

interior design knowledge graph corresponds to a DT of interior elements or functional zones, serving as an abstract representation of physical objects. The entire knowledge network is capable of describing the entire interior design scheme. The AR system, based on the interior design knowledge graph, can acquire the Design Element Set (DES) for the entire design process. DES is the knowledge expression of the pre-planned design scheme, i.e.

$$DES = \sum_{i=1}^{n}(SAI_i \cup DPI_i \cup DCI_i) \quad (1)$$

where, DES is used for modularized management of the interior space design process. It comprises Scene Asset Information (SAI) for AR scene reconstruction, Design Planning Information (DPI), and Design Cooperation Information (DCI) for design guidance and collaborative processes.

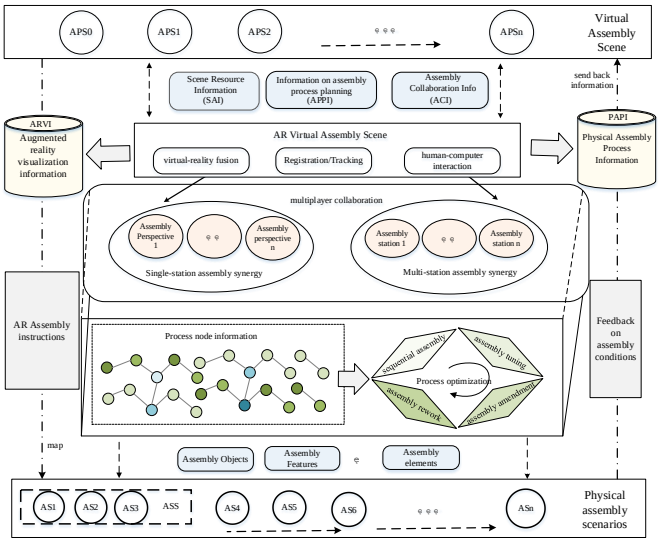


Fig. 3. DT interior space design process collaboration.

Due to the complexity of the interior design processes, we decompose them into various design step combinations for different categories of AR collaborative guidance. Different Design Element Sets (DES) are composed of Design Step Sets (DSS). Designers acquire the corresponding DSS through the system to obtain information on design steps, requirements, features, and elements. Based on specific design tasks, we classify them into two design cooperation categories (DCC): single-functional zone design and multi-functional zone collaborative design. The AR system provides distinct collaborative guidance for different DCC, generating Augmented Reality View Information (ARVI) based on design and model information, formally expressed as

$$ARVI := \{UI \cup MBD \cup ADN\} \quad (2)$$

The Model-Based Definition (MBD) method is employed for AR display of model information in Scene Asset Information (SAI), Design Animation (ADN) for visual expression of Design Planning Information (DPI), and UI information for expressing Design Cooperation Information (DCI) and design property information. Designers implement design steps based on ARVI to advance the DSS process. During the execution of DSS in physical space, the system acquires Physics Design Information (PDI), including Material Information (MI), Design Process Data (DPD), and Design Adjustment Data (DAD), formally expressed as,

$$PDI := \{MI \cup DPD \cup DAD\} \quad (3)$$

PDI is directly fed back to the interior design knowledge graph through human-computer interaction. Through analysis and computation, the system predicts the current state of the design process twin object and performs distributed optimization based on this state. Firstly, DES is optimized, adjusting errors to different degrees based on the actual design situation, facilitating differential optimization processes such as design adjustments, corrections, or rework. Design adjustments mainly address design errors in single-functional zones, while design corrections and rework address overall aesthetics and functionality matching issues in the collaborative processes of multi-functional zones. DCI updates involve the optimization results communicated through the AR system, guiding designers through the UI for process optimization and error indication.

B. Scene Synergy

One primary feature of AR systems is the overlay of computer-generated three-dimensional graphics onto physical space to provide operational guidance, fulfilling a majority of instructional needs. However, in scenarios involving multiple operators, independent AR spaces are incapable of facilitating information sharing and interactive operations. In order to overcome information isolation and enable multi-user collaborative operations, this paper introduces a shared AR space constructed through the method of root anchor point alignment, achieving collaborative scene interactions.

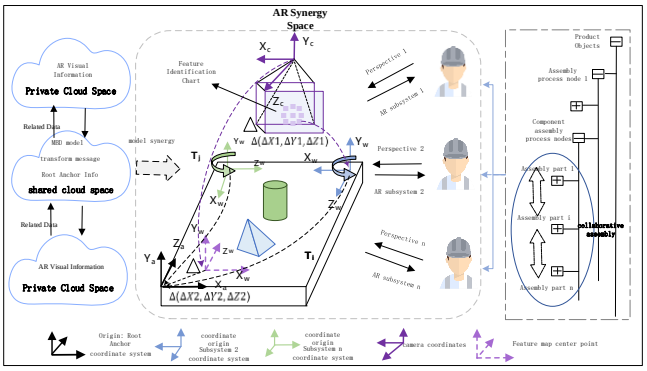


Fig. 4. Scenario collaboration principle.

The AR collaborative system for interior design enables multiple designers to share and collaborate on design concepts within the same physical space. As illustrated in Fig. 4, during the interior design process, designers collaborate by creating their respective AR spaces. Each designer's AR device establishes a unique world coordinate system, with the root anchor point serving as the origin (0, 0, 0) for the coordinate system, and all design element models are loaded as child objects.

The key to establishing a unified coordinate system is aligning the root anchor points of multiple virtual scenes. In this section, the collaborative process is achieved by calculating relative coordinate offsets based on the overlap

point of the physical spaces of two devices. Image-based tracking technology is employed to determine the location information of common points in physical space. To simplify collaborative calculations and enhance system adaptability, feature recognition images are stored in the system. The relative coordinates of the feature recognition image with respect to the root anchor point are utilized for rapid acquisition of common coordinate points between devices through screen recognition of the feature image. These relative coordinates are then employed in the alignment calculation of the root anchor points of the two devices, achieving a unified coordinate system.

Initially, the benchmark device DS for collaborative calibration is determined. Since the camera is in a non-fixed state during the AR scene loading process, the camera coordinates V_{ecp}（X_P， Y_P， Z_P） at the calibration moment are obtained as the central coordinates of the feature recognition image. Considering the camera offset constants for different devices, the actual central coordinates of the feature recognition image are adjusted to V_{ecp}（$X_P + \Delta X_1$， $Y_P + \Delta Y_1$ ， $Z_P + \Delta Z_1$）. To align the root anchor points, the local coordinates relative to the feature recognition image are computed as the coordinate offset, taking into account the coordinate transformation rules of the virtual space. The matrix transformation sequence in its coordinate system involves the Y-axis, then the X-axis, and finally the Z-axis. Thus, based on the transformation rules, the world coordinate system W is transformed to the local coordinate system L, where a and b represent intermediate coordinate systems in the transformation process.

$$Rot_W^L = Rot_{\mathrm{b}}^L Rot_{\mathrm{a}}^{\mathrm{b}} Rot_W^{\mathrm{a}} \tag{4}$$

The local coordinates of the root anchor point under the feature recognition image are obtained through matrix operations as V_{eca}（ΔX_2， $\Delta Y_2, \Delta Z_2$）.

$$V_{eca}=R_W^L \mathrm{Tr}\left(X_P + \Delta X_1\ ,\ Y_P + \Delta Y_1\ ,\ Z_P + \Delta Z_1\right) V_{ecp} \tag{5}$$

During device calibration, the client utilizes AR Core image tracking technology to obtain the spatial coordinates V_{ect}（X_t， Y_t, Z_t） of the recognition image through feature point clouds. Since the offset of the recognized feature point cloud may introduce deviations in calibration results, a collaborative filtering method is employed to eliminate false coordinates caused by positioning offset. Additionally, the data is grouped, and a weighted arithmetic mean is calculated.

$$X' = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{x_i f_i}}{\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{f_i}} = \frac{\mathrm{x_1 f_1 + x_2 f_2 + \cdots + x_n f_n}}{\mathrm{f_1 + f_2 + \cdots + f_n}} \tag{6}$$

Get the final coordinate values of the feature recognition map.

$$V_{ect}= (\ X_t'\ ,\ Y_t', Z_t'\ ) \tag{7}$$

Due to the identical screen coordinates of the two devices, a unified coordinate system can be achieved by determining the same coordinate offset. The client's root anchor point is transformed into the local coordinate system of the feature image, setting the same coordinate offset V_{eca}. Based on the existing coordinate offset and the spatial coordinates of the feature recognition image with rotation anglesV_{ecr}（θ_1， θ_2， θ_3）, the root anchor point coordinates are aligned in the world coordinate system. According to the matrix transformation rules in the world system, the transformation matrix for the root anchor point is obtained by rotating in the z-x-y sequence.

$$R_L^W = Rot(Y, \theta_2)\, Rot(\mathrm{X}, \theta_1)\, Rot(\mathrm{Z}, \theta_3) \tag{8}$$

Get the coordinates of the root anchor point in the world coordinate system.

$$V_{eca2}=Tr\left(X_t^{'}\ ,\ Y_t^{'}\ ,\ Z_t^{'}\right) R_L^W V_{eca} \tag{9}$$

In the equations, $Rot(x,\theta) = \begin{bmatrix} M(x,\theta) & 0 \\ 0 & 1 \end{bmatrix}$ represents a rotation matrix, where $M(k,\theta) = I + \sin\theta R_{\vec{k}} + (1 - \cos\theta) R_{\vec{k}}^2$ is the rotation matrix for any vector $\vec{k}$ rotating counterclockwise around the axis by an angle θ in three-dimensional space. Here, I is the 3×3 identity matrix, and $R_{\vec{k}}$ is the cross-product matrix of $\vec{k}$.

$Tr(x,y,z)=\begin{bmatrix} I & (x,y,z)^{\mathrm{T}} \\ 0 & I \end{bmatrix}$ denotes the translation matrix.

After spatial calibration of different devices, although the root anchor points in each AR space have different numerical values in the world coordinate system, they are aligned in physical space, serving as the origin of the shared AR space's common coordinate system. In the shared coordinate system, AR resources only need to exist as their child objects and ensure local coordinate consistency to achieve spatial coordinate collaboration.

Scene collaboration involves both coordinate collaboration of the shared AR subsystem and collaboration of AR resources. Building on the foundation of root anchor-based coordinate collaboration to construct a shared AR space, a unified loading of AR resources and consistency in resource interaction can be achieved under different assembly perspectives. Collaborative resources are stored in shared cloud storage, and when the MBD model is stored in the shared space, the creation of the AR scene in a procedural form ensures consistency in model loading and removal, monitored through the shared space. In achieving consistency in the interaction process, as transformation information (transform) stores the basic attributes of resources, the system monitors and updates it in real-time to ensure consistency in model interactions, such as movement, rotation, and scaling operations in different spaces.

Through AR scene collaboration, operators can perform assembly based on collaborative perspectives, and the natural AR human-computer interaction ensures effective transmission of collaborative information.

V. CASE STUDY

This paper develops an augmented reality-based multi-user collaborative design system using the aforementioned approach and validates it through a case study of an interior design project.

A. Platform Construction

The establishment of the interior space design management platform primarily aims to provide data services for the design process, encompassing information storage and expression of interior design elements, definition and storage of augmented reality (AR) resources, and integration of collaborative design algorithm services. Firstly, a knowledge graph of interior design is constructed based on the spatial design requirements. This involves utilizing the DT and spatial relationships of design objects to obtain design precision information and design relationships for design nodes. Subsequently, design errors are calculated, facilitating the iterative update of on-site design information.

The design-level DT manages the fundamental information of interior design, while the object-level DT oversees its basic attribute information. The knowledge representation of the interior design DT is illustrated in Fig. 5, encompassing attribute information such as augmented reality (AR) visualization and algorithmic interfaces. The visualization information primarily includes interior design object models and information on interior design elements. Simultaneously, the algorithmic interfaces furnish collaborative design algorithms utilized in the collaborative calculation processes of design.

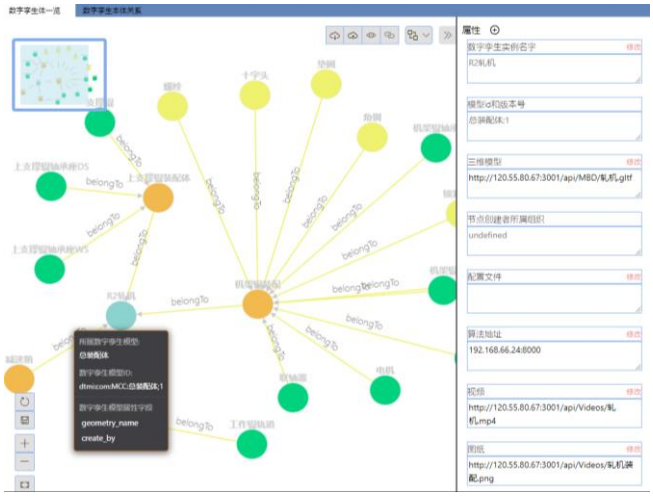


Fig. 5. Interior design DT knowledge expression.

In response to diverse on-site design requirements, the Augmented Reality (AR) system leverages the DT platform to acquire resources, establishing an adaptive AR design environment. Through real-time rendering and AR visualization of design elements, parameters, and tools, the system guides designers in the creative process, thereby reducing cognitive load and enhancing design efficiency.

B. Test Validation

Incorporating Augmented Reality (AR) technology into interior space design can enhance both design efficiency and customer experience. This study explores collaborative work modes in the interior design process by combining smartphones and HoloLens headsets. Using a smartphone as the collaborative reference platform, coupled with Vuforia image tracking technology, synchronization of root anchor points between HoloLens and smartphones within the same AR space is achieved. To enhance the precision of collaboration, recognition images with distinct features are chosen, and stability tests for rotation and scaling are conducted. The collaborative accuracy primarily relies on the alignment of root anchor points across different devices. This is indirectly measured by sending the physical dimensions of the recognition image to each collaborative device and comparing the results with the image tracking outcomes.

Fig. 6. Root anchor synergy process.

As illustrated in Fig. 6, this process accurately tracks the positions of interior design elements under different sizes, distances, and rotation angles. It achieves precise alignment with translation errors approximately 1mm and rotation errors less than 0.5 degrees, providing a reliable reference for the collaborative interior design process. Fig. 6 presents the visual effects of the collaborative interior design scene from different perspectives, namely the smartphone AR perspective and the HoloLens AR perspective. Within the AR collaborative space, design elements are categorized into private information, public information, and associated information. For instance, foundational elements of the design, such as major furniture or structural components, serve as public resources shared by all participants, ensuring consistency in physical space and interactive effects from different perspectives.

Private information is tailored to the specific tasks of individual designers. Different designers may see different AR elements based on their task requirements. Key design objects, like specific furniture or decorative elements, although requiring attention from all designers, may have different details of interest to each designer. By setting element attributes as private, designers can interactively translate and rotate models to comprehensively understand and examine every angle of the design objects.

C. Physical Assembly Process Synergy

This section analyzes the collaborative effects of the physical design process through an on-site interior design implementation experiment. Designers arrived at the actual interior design site and engaged in collaborative design layout activities for the central area of the living room. Given the diverse design objects and the complexity of the design environment, acquiring on-site information proved challenging for the designers. To address this challenge, designers accessed

design element information, including collaborative design tasks and design resources, through the tethering of the DT design platform to assist in the design process. Designers were then able to visualize three-dimensional models and drawings of the design resources using augmented reality (AR).

The collaborative layout design of the central area requires the joint efforts of multiple individuals. During the design preparation phase, designers, designated as A, B, and C, gather design information from various visual perspectives based on their respective roles and responsibilities. It is displayed the AR visual perspectives of designers A, B, and C. Designer A is responsible for overall concept confirmation and design optimization, primarily assisting in layout design. To facilitate effective design guidance, the AR system visualizes the design baseline for this perspective, allowing designer A to comprehend the structural model of the spatial layout. To achieve task collaboration among designers, different forms of visualization for resources are necessary. Since all designers use the central area model as the baseline for their designs, with its attributes set as "Public" for shared visualization, designers B and C can observe the spatial model loaded by designer A in the shared AR space, enabling task collaboration. Designer B, acting as the lead designer, is tasked with central area layout design. The AR system employs design animation to demonstrate layout details, guide the design process, and visualize the effects. Designer C's task is to test the layout's effectiveness and assist in the design process. The system uses Model-Based Definition (MBD) model visualization to help designer C obtain design parameter information. To avoid interference caused by the overlay of visual resources from multiple AR subsystems, the model attributes of the central area are set as "Private," visible only to designer C. Interactions by designer C with the central area do not affect the design animation presentation for designer B

Throughout the entire design process, designers can iteratively update design solutions by uploading real-time design information to the DT space through AR system interactions such as voice commands or gestures. The optimized information is then fed back to the design team via the AR system, completing a closed-loop control of the design.

To validate collaborative design efficiency, designers responsible for other design elements were divided into two groups and subjected to 20 experiments each. The parameters, including design preparation, completion, and documentation, were compared with those of experienced designers focusing on the central area, as summarized in Table I.

TABLE I. COMPARISON OF ASSEMBLY EFFICIENCY FOR DIFFERENT ASSEMBLY CATEGORIES

Assembly category	Preparedness efficiency	Assembly Fluency	Assembly Collaboration Efficiency	Assembly Special Session Completion	Assembly pass rate	Assembly completion efficiency	Assembly process record efficiency
Senior Designer Codesign	100	100	100	100	100	100	100
New Designer Codesign	45	45	40	80	65	30	70
New Designer Codesign	90	80	85	100	95	85	160

From Table I, the following observations can be made: ① New designers utilizing traditional processes and methods for interior design tasks incurred substantial time in design preparation and documentation. Although the design qualification rate exceeded 50%, the design efficiency fell short of meeting the scene's requirements. ② AR-based collaborative design, supported by DTs and AR technology, exhibited overall favorable performance. ③ In the AR collaborative environment, the design collaboration efficiency of new designers was twice that of traditional design, enabling the new team to quickly adapt. ④ Guided and alerted by AR, designers were less prone to overlook design aspects, achieving a 100% completion rate for handling detailed elements in spatial layouts. The overall design qualification rate reached 95%, ensuring the stability of design quality. ⑤ AR's data interaction eliminated communication barriers between physical space and the twin space, and the efficiency of recording design information in the design process even surpassed that of experienced designers. In comparison, it is evident that AR-guided collaborative design based on DTs significantly reduces the cognitive burden on designers and enhances both the stability of design quality and overall design efficiency.

D. Analysis and Discussion

In the digitized process of interior space design, interactive experience and efficiency are crucial considerations. Within the digital design environment, a well-crafted interactive experience significantly impacts the work efficiency of designers and the quality of design outcomes. The user interface of design software should be intuitive, easy to understand, and flexible enough to adapt to the designer's workflow. Efficiency is equally vital in the digital design of interior spaces. The design process should be swift, flexible, and capable of adapting to evolving customer demands and market trends.

Through the experiments described above, the proposed method and developed system demonstrate the following advantages in terms of interactive experience and design efficiency:

1) The design software provides real-time views of spatial models, allowing designers to immediately see how their design choices impact the layout and aesthetic effects of the space. Simultaneously, the software enables designers to effortlessly adjust design parameters and instantly observe the

results of these adjustments. This immediate feedback significantly enhances design efficiency and quality. Furthermore, the design software supports seamless integration with other tools and platforms, such as VR/AR demonstration software, material databases, and 3D printing systems. This facilitates a smoother design process, reducing waiting and conversion times.

2) The software allows for the rapid creation of initial 3D models and 2D floor plans for interior layouts, saving time. While some designs may require adjustments to existing models, at least one-third of the projects need a complete redesign. For instance, forming a preliminary design model in 15 minutes contrasts sharply with the days or even a whole day required for a seasoned designer to conceptualize a design from scratch or make adjustments to an existing model. This results in substantial savings in design costs.

In conclusion, this system provides robust tools for the digitization of interior space design, enhancing both design efficiency and quality while optimizing the user's interactive experience to meet the rapidly changing demands of the market.

VI. Conclusions and Future Work

This research investigates the current status and challenges within the interior space design industry, proposing an intelligent design approach based on DT. We identify interdisciplinary integration challenges in the design process, limitations associated with design knowledge relying on personal experience, and issues stemming from frequent design modifications, lengthy project cycles, and high work intensity imposed by traditional design patterns. To address these challenges, we establish multi-physical information models for interior spaces, systematically describing rule models for design knowledge and experience in a digitized format. Additionally, we achieve intelligent parametric design associations among spatial elements.

This design approach not only enhances design efficiency and quality but also opens new avenues for the intelligence of interior space design. In the future, we aim to refine this design approach, improving the accuracy and reliability of the models, enhancing the intelligence of rule models, strengthening the intelligent parametric design associations among spatial elements, and exploring the application of this method in a broader spectrum of interior design domains. We will also investigate the integration of this design method with advanced digital technologies, such as artificial intelligence and big data, to achieve a higher level of intelligent design.

The primary contribution of this research lies in the proposal and implementation of an innovative interior space design method, with the potential to drive the transformation of the design industry towards intelligence.

References

[1] Liu S, Zheng P, Xia L, et al. A dynamic updating method of digital twin knowledge model based on fused memorizing-forgetting model[J]. Advanced Engineering Informatics, 2023, 57: 102115.

[2] Fu T, Li P, Liu S. An imbalanced small sample slab defect recognition method based on image generation[J]. Journal of Manufacturing Processes, 2024, 118: 376-388.

[3] Fu T, Liu S, Li P. Intelligent smelting process, management system: Efficient and intelligent management strategy by incorporating large language model[J]. Frontiers of Engineering Management, 2024: 1-17.

[4] ZHENG H, LIU S, ZHANG H, et al. 2024. Visual-triggered contextual guidance for lithium battery disassembly: a multi-modal event knowledge graph approach. J Eng Des 2024: 1-26.

[5] GRUBEL J, GATH-MORAD M, AGUILAR L, et al. 2021. Fused twins: A cognitive approach to augmented reality media architecture. In: Media Architecture Biennale 20. 2021: 215-220.

[6] LU W, CHEN J, FU Y, et al. 2023. Digital twin-enabled human-robot collaborative teaming towards sustainable and healthy built environments. J Clean Prod 412: 137412.

[7] KÜNZ A, ROSMANN S, LORIA E, et al. 2022. The potential of augmented reality for digital twins: A literature review. In: 2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR). IEEE, 2022: 389-398.

[8] SCHROEDER G, STEINMETZ C, PEREIRA C E, et al. 2016. Visualising the digital twin using web services and augmented reality. In: 2016 IEEE 14th International Conference on Industrial Informatics (INDIN). IEEE, 2016: 522-527.

[9] COUPRY C, NOBLECOURT S, RICHARD P, et al. 2021. BIM-Based digital twin and XR devices to improve maintenance procedures in smart buildings: A literature review. Appl Sci 11(15): 6810.

[10] SCHOTT E, MAKLED E B, ZOEPPIG T J, et al. 2023. UniteXR: Joint Exploration of a Real-World Museum and its Digital Twin. In: Proceedings of the 29th ACM Symposium on Virtual Reality Software and Technology. 2023: 1-10.

[11] ZHU Z, LIU C, XU X. 2019. Visualisation of the digital twin data in manufacturing by using augmented reality. Procedia Cirp 81: 898-903.

[12] XU X, LU Y, VOGEL-HEUSER B, et al. 2021. Industry 4.0 and Industry 5.0—Inception, conception and perception. J Manuf Syst 61: 530-535.

[13] PANG J, ZHENG P, LI S, et al. 2023. A verification-oriented and part-focused assembly monitoring system based on multi-layered digital twin. J Manuf Syst 68: 477-492.

[14] WANG B, ZHOU H, LI X, et al. 2024. Human Digital Twin in the context of Industry 5.0. Robot Comput Integr Manuf 85: 102626.

[15] LIU S, BAO J & ZHENG P. 2023. A review of digital twin-driven machining: From digitization to intellectualization. J Manuf Syst 67: 361-378.

A Safety Detection Model for Substation Operations with Fused Contextual Information

Chen Bo[1], Zhanghong Yu[2], Yangrun Xi[3], Zhao Lei[4], Ding Yi[5*]
State Grid Beijing Electric Power Company, Beijing 100031, China[1, 2, 3, 4]
Beijing Electric Power Economic Research Institute Co., Ltd., Beijing 100055, China[1, 2, 3, 4]
Nanjing Artificial Intelligence Research of IA, Nanjing 211100, China[5]

***Abstract*—Detecting and regulating compliance at substation construction sites is critical to ensure the safety of workers. The complex backgrounds and diverse scenes of construction sites, as well as the variations in camera angles and distances, make the object detection models face low accuracy and missed detection problems. In addition, the high complexity of existing models creates an urgent need for effective parameter compression techniques to facilitate deployment at the edge server. To cope with these challenges, this study proposes a safety protection detection algorithm that fuses contextual information for substation operation sites, which enhances multi-scale feature learning through a two-path downsampling (TPD) module to effectively cope with changes in target scales. Meanwhile, the Global and Local Context Information extraction (GLCI) module is utilized to optimize the key information learning and reduce the background interference. Furthermore, the C3GhostNetV2 unit is utilized in discerning the interconnections of far-off spatial pixels, while enhancing the network's expressive power and reducing the number of parameters and computational costs. The outcomes of the experiments indicate that the present model improves upon the mAP50 metric by 4.5% compared to the baseline model, and the accuracy of the checks and the recall have seen respective increases of 4.8% and 10.1%, while there has been a reduction in both the count of parameters and the floating-point calculations by 16.5% and 12.6% respectively, which proves the validity and practicability of the method.**

***Keywords*—Object detection; context information; electricity construction operation; model complexity; lightweight**

I. INTRODUCTION

As societal demand for electrical energy continues to rise, there is an increasingly urgent need for power production in China. However, due to a combination of various factors, the frequency of power production accidents in the country remains relatively high, posing a serious threat to urban safety. The power construction process involves a wide range of complex scenarios, including tower assembly, hoisting, excavation work, hot work, edge work, and high-altitude operations. These tasks encompass numerous safety challenges, requiring workers to maintain a high level of vigilance and adhere to standardized procedures to prevent serious accidents [1-2].To ensure that power workers enhance their safety awareness, adopt compliant protective measures and procedures, and ultimately improve on-site safety levels to ensure the normal operation of the power system, there is an urgent need for worksite compliance monitoring and supervision. Traditional manual management methods are costly and inefficient, making it difficult to meet the needs of effective supervision in multi-scenario, around-the-clock power grid operations. Therefore, the application of deep learning algorithms for compliance monitoring at power grid work sites holds significant research value. This research introduces advanced visual technologies to the field of power production and provides substantial support for improving on-site safety levels.

With the tremendous achievements of deep learning algorithms in image recognition and detection [3-5], these algorithms have made significant progress in various applications. Thanks to their high detection accuracy and strong robustness [6-7], deep learning-based object detection algorithms have been widely applied in detecting standardized work clothing. Ren et al. [8] discussed the concept of deep learning-based intelligent substation system monitoring and analyzed the advantages and disadvantages of using traditional methods and deep learning for monitoring. Liu et al. [9] employed the Faster R-CNN algorithm for detecting whether standard work clothing is worn and introduced an L2 regularization term into the loss function to improve the convergence speed of the model during training. The model demonstrated good generalization ability and robustness, with significant improvements in both accuracy and real-time performance compared to the baseline model. Reference [10] employed the lightweight network from MobileNet in the YOLOv2 structure to achieve a certain degree of network compression, reducing the computational complexity of the model and improving its convergence performance, but with lower accuracy in object detection. Xu et al. [11] proposed an improved YOLOv3 algorithm for safety helmet recognition, which enhanced the precision of safety helmet detection, but the detection speed was relatively slow. The study in [12] implemented a real-time video analysis algorithm based on YOLOv4 for monitoring whether workers in industrial facilities wear helmets, safety vests, and safety belts, but it ignored the influence of complex backgrounds and environmental factors on algorithm performance and did not analyze the algorithm's complexity. Du et al. [13] selected the Swin Transformer as the backbone network based on YOLOv5 to extract deeper semantic information and capture more detailed features of safety helmets, but it had false detection issues when the colors were the same. In addition to YOLO, Long et al. [14], Wu et al. [15], and Li et al. [16] proposed safety helmet detection methods based on SSD, which achieved good detection results. Although single-stage object detection algorithms have performed well in terms of real-time performance and efficiency, they still face some challenges, such as the use of dense grids or anchor boxes to generate candidate regions, which can lead to overlapping or

missed detections and relatively poor performance in detecting small objects [17].

Existing detection methods exhibit certain limitations in practical application scenarios. They often focus on specific target detection while neglecting the diverse task requirements in power construction sites. For instance, Shen et al. [18] utilized convolutional neural networks to detect facial features and helmet usage on construction sites. However, this study did not sufficiently address the impact of environmental variations on detection performance. Additionally, the lightweight improvement of YOLOv5 proposed in [19] targets helmet detection only and still has room for improvement in adaptability and scalability in real-world scenarios. Furthermore, the methods in [20, 21] are only effective in environments with simple backgrounds. These approaches, which focus on single categories or specific scenarios, struggle to handle the complexity and variability of power construction environments, limiting their broader applicability in practical settings.

In recent years, research on compliance detection for multiple categories of personal protective equipment (PPE) has increased. For instance, Zhang et al. [22] enhanced YOLOv4's feature extraction network and combined it with PANet to achieve effective detection of helmets and masks. Similarly, [23] utilized synthetic datasets to train an improved YOLOv5 model, successfully applying it to real-time PPE detection in industrial environments. In study [24], an intelligent detection system was designed to notify supervisors when workers failed to wear helmets or vests, improving the efficiency of on-site safety management. Additionally, Gong et al. [25] adopted a key region localization method to optimize PPE detection performance further. While these methods have achieved notable advances in accuracy and detection capability, they still face certain limitations. The complex model structures demand significant hardware resources and result in low detection efficiency, making them challenging to apply in industrial scenarios requiring real-time performance and low power consumption. Therefore, reducing model complexity while maintaining detection accuracy remains a critical research direction in this field.

The aforementioned methods have achieved detection and monitoring of power grid operation scenes with humans as the main objects to some extent, but the detection scenarios and categories are relatively limited, usually focusing on specific categories such as safety helmets or work clothing, with less attention to other scenes. This limits the comprehensiveness and applicability of the algorithms because power grid operation scenes involve various scenarios such as lifting operations, excavation work, hot work, work near edges, and work at heights, requiring more comprehensive detection capabilities. Additionally, the collected images from the power grid industry exhibit characteristics of diverse target types, inconsistent sizes, and complex and variable background environments. In complex backgrounds, the previous algorithms perform poorly in effectively extracting features from targets of different scales, resulting in weak adaptability to environmental changes. This can lead to issues of missed detections and low accuracy in practical applications, reducing the reliability of the algorithms. Furthermore, existing models have high complexity, requiring a reasonable and effective parameter simplification technique as a basis to address the challenges of deployment on remote server devices. Enhancing object detection performance in complex scenarios, improving the detection accuracy of multi-scale objects, and reducing model complexity have become key research focuses in substation safety monitoring. Therefore, this study presents an improved YOLOv7 network. A down-sampling module was designed to enable the model to better learn multi-scale features. Additionally, a Global and Local Context Information extraction (GLCI) module was introduced, allowing the model to effectively capture critical information within complex backgrounds and reduce missed and false detections caused by background interference. Furthermore, structural optimization was implemented to reduce the model's parameter count, enhancing the real-time performance and adaptability of the improved YOLOv7 model while maintaining high detection accuracy. These improvements enable efficient and compliant detection in power production scenarios. Our contributions are summarized as follows:

- We design a global and local context information extraction (GLCI) module, enabling the network to capture both global contextual and local spatial information, effectively addressing the challenge of complex backgrounds in power construction site environments.
- We propose a two path downsampling (TPD) module, which enhances the network's ability to learn features across multiple scales, improving performance on multi-scale target detection tasks.
- We develop a novel C3GhostNetV2 unit, replacing all ELAN-H modules in the neck network and the ELAN modules at the backbone's end. This design expands the receptive field, strengthens model representation, and significantly reduces model complexity, parameter count, and computational cost.

II. Proposed Method

This method consists of three modules: Global and Local Context Information extraction (GLCI) module Two-Path Downsample (TPD) module, and C3GhostNetV2 module. The TPD module enables the network to effectively capture and utilize spatial information from feature maps of different scales. The GLCI module helps the network learn key information more efficiently and reduces background interference. The C3GhostNetV2 unit not only expands the perception range to ensure the model's expressive effectiveness but also reduces the demand for floating-point calculations.

The YOLO series algorithms have high similarity in terms of network structure and module composition. Taking YOLOv7 as an example, Fig. 1 shows the network structure diagram of YOLOv7 with GLCI and TPD inserted and lightweight improvements applied. It mainly includes four components: Input, Backbone, Neck, and Head. The Backbone consists of CBS, C3, and SPPF, which are responsible for extracting information features from input images. After the Backbone, feature maps of three different sizes can be obtained. The Neck module combines the Feature Pyramid Network (FPN) and Pyramid Attention Network (PAN) to fuse the features extracted by

the Backbone. The Prediction Head consists of three prediction layers of different scales, which are responsible for outputting the network's predictions.

In YOLO series networks, the backbone is primarily responsible for feature extraction, transforming input images into high-level feature representations [26], which serve as the basis for subsequent detection. The insertion of the GLCI module enhances the network's learning ability for multi-scale information and its perception of global and local context, addressing the challenges posed by significant scale variations and complex backgrounds. The backbone is where the network learns and perceives information, making it a suitable location for the insertion of the GLCI module. Additionally, placing the GLCI plugin at the end of the backbone allows for effective utilization of high-level information in the feature maps, and the lower resolution of the end feature maps can alleviate the potential computational and memory costs introduced by the plugin. Furthermore, since the proposed GLCI plugin does not change the size of the input and output feature maps, it is not affected by the number of network layers and is applicable to all YOLO series algorithms. Taking YOLOv7 algorithm as an example, as shown in Fig. 1, the feature maps output by the last CBS module in the backbone have a size of 20×20×1024. After being processed by the GLCI plugin, the size and number of channels of the feature maps remain unchanged, meeting the data format requirements of the subsequent network structure. Therefore, it is reasonable to insert the GLCI module at the end of the backbone. Considering that the neck network contains rich information and serves as the direct input to the head network, the TPD module is inserted into the neck network. Finally, the C3GhostNetV2 unit is constructed in the neck network to expand the perception field and maintain the model's expressive power while significantly reducing the number of parameters and computational costs.

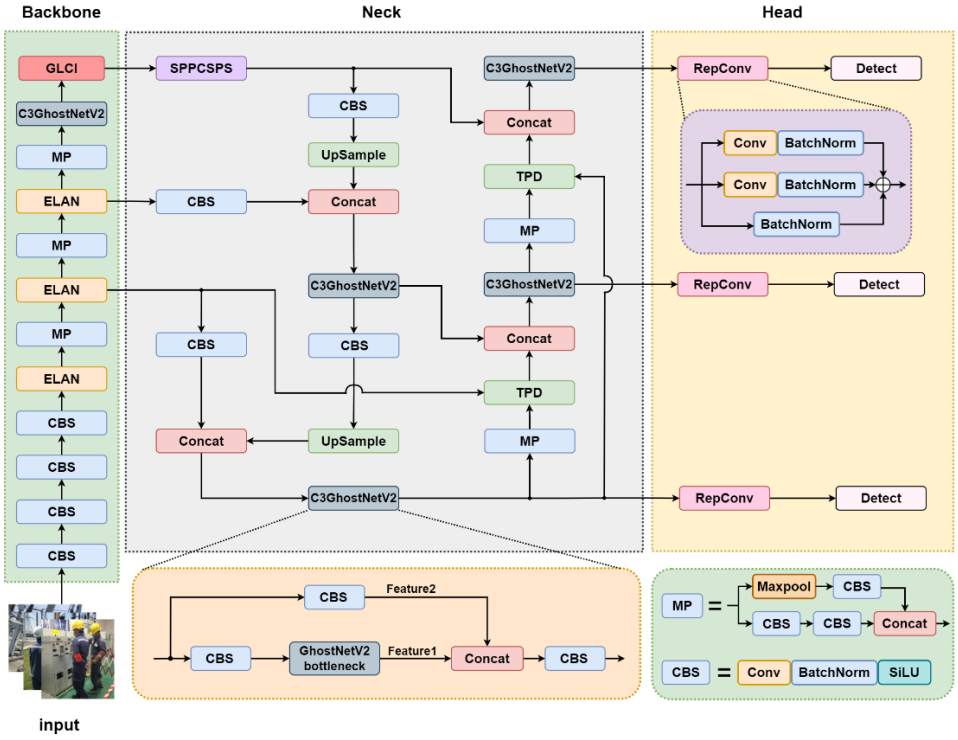


Fig. 1. Schematic diagram of lightweighting methods structure.

A. Global and Local Context Information Extraction Module

To improve network adaptability in complex image backgrounds in real-world power construction site detection tasks, we propose the GLCI module (see Fig. 2). This module consists of two branches: Global and Local Context Extraction. It helps the object detection network learn more crucial information and attenuate background interference. The primary objects to be detected in input images—power construction site workers—are closely tied to their surrounding environments. Incorporating contextual information into the model enhances its understanding of the relationships between detected objects and their scenes, thereby improving detection performance. The global branch of the GLCI module, built on the traditional self-attention mechanism, leverages not only the relationships between keys and queries but also emphasizes the contextual information among input keys. This approach enhances the network's capacity to extract contextual information and improves its ability to learn critical features through the guidance of the learned dynamic attention matrix.

For a feature map X of size $c \times h \times w$, linear processing is applied to yield K=X, Q=X,, and V=XWV, where K denotes the key, Q the query, and V the value, with WV representing a 1×1 embedding convolution. In the spatial domain, group convolution is performed on adjacent keys within a 3×3 grid of $\boldsymbol{K}$, with the number of groups set to 4. This is followed by batch normalization (BN) and ReLU activation, resulting in a feature map $\boldsymbol{K}_1$ of size $c \times h \times w$. Through these operations, encoding is applied to the adjacent keys in the spatial domain, producing K1, which captures the static contextual information between

neighboring keys and is referred to as static contextual keys $\boldsymbol{K}_1$. Subsequently, $\boldsymbol{K}_1$ and $\boldsymbol{Q}$ are concatenated, and two successive 1×1 convolutions generate an attention matrix $\boldsymbol{A}$. This attention matrix $\boldsymbol{A}$ differs from the traditional self-attention mechanism, as it is derived from query features and static contextual features of $\boldsymbol{k}_1$, rather than key/query pairs. Thus, $\boldsymbol{A}$ effectively aggregates contextual information.

$$A = [K^1, Q] W_\theta W_\delta \tag{1}$$

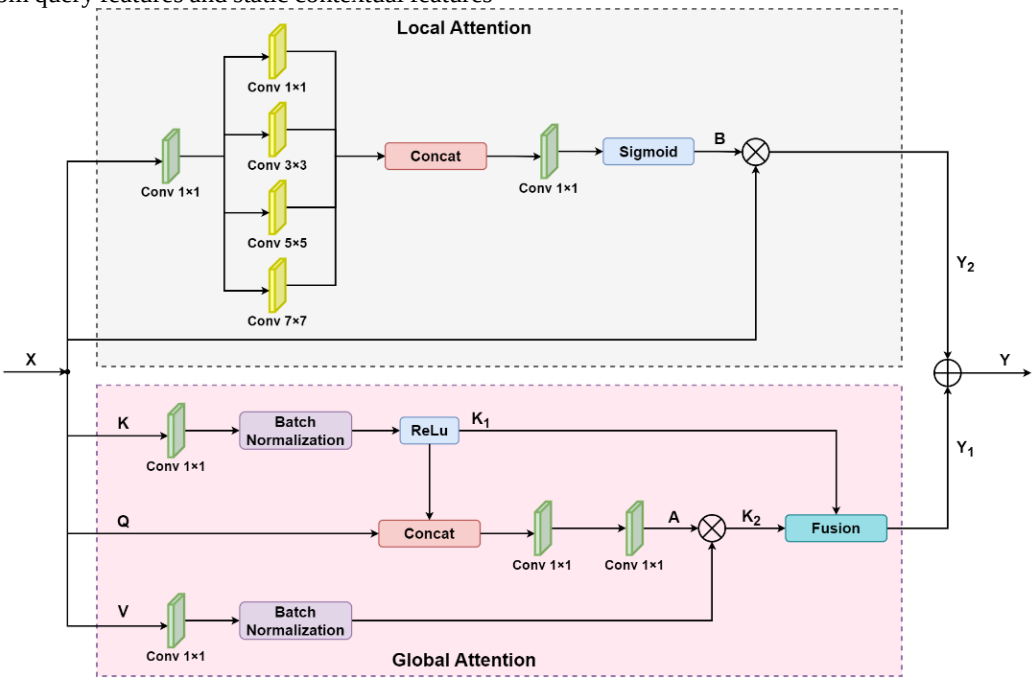


Fig. 2. Structure diagram of GLCI module.

In Eq. (1), W_θ represents a convolution with a ReLU activation function, and W_δ represents a convolution without an activation function. Next, the attention matrix $\boldsymbol{A}$, which aggregates contextual information, is element-wise multiplied with $\boldsymbol{V}$ resulting in a feature map $\boldsymbol{K}_2$ weighted by $\boldsymbol{V}$. Since $\boldsymbol{K}_2$ is obtained through self-attention computation on the input keys and values, it captures the dynamic feature interactions among the inputs and is named the dynamic contextual keys. The fusion of the static contextual keys $\boldsymbol{K}_1$ and the dynamic contextual keys $\boldsymbol{K}_2$ yields the output $\boldsymbol{Y}_1$ of the global attention network.

In the Local Contextual Information (LCI) network, multiple convolution sizes capture spatial information at various scales, enhancing learning and addressing noisy, complex backgrounds. For an input feature map $\boldsymbol{X}$ of size $c \times h \times w$, a 1×1 convolution reduces the channels to 1/16, minimizing parameters. The reduced map is processed by 1×1, 3×3, 5×5, and 7×7 convolutions, concatenated into a tensor of size $1/4\,c \times h \times w$, then passed through a 1×1 convolution to reduce the channels to 1. Applying the sigmoid function produces a local spatial attention map $\boldsymbol{B}$ of size 1×H×W, which is element-wise multiplied with $\boldsymbol{X}$ to generate $\boldsymbol{Y}_2$. The outputs of the Global and Local Contextual Information networks, $\boldsymbol{Y}_1$ and $\boldsymbol{Y}_2$, are summed to produce $\boldsymbol{Y}$, enabling the GLCI module to capture both local and global features and address challenges from complex backgrounds.

B. Two Path Downsampling (TPD) Module

The challenge of handling multiscale data in deep learning lies in efficiently extracting and learning features from data of varying scales, such as different sizes and resolutions. To address the impact of multiscale issues on detection accuracy in images collected from power construction sites, this paper proposes the Two Path Downsampling (TPD) module. This module facilitates information exchange between different feature layers, enabling spatial channel dependencies between different scales and enhancing the performance of feature extraction across different scales. The TPD module's structure is illustrated in Fig. 3.

The TPD module takes two input feature maps: the local feature map F_c with dimensions $c \times h \times w$ and the higher-level feature map F_u with dimensions $1/2c \times 2h \times 2w$. Unlike traditional stride-based convolutional downsampling, this module introduces a lossless downsampling process for the local feature map, preserving its fine-grained details. Additionally, the downsampling process is improved by preserving spatial information before and after downsampling, reducing the loss of detail. Furthermore, the module captures details from the higher-level feature map and incorporates semantic information from the local small-scale feature map, enhancing interdependencies between feature maps at different levels.

The downsampling process consists of two distinct paths. Path 1 involves lossless downsampling of the local feature and an enhanced convolutional downsampling process. The local feature F_c first undergoes feature extraction through average pooling and convolution with stride 1, resulting in the feature map F_{cl} of size $c \times h \times w$. Then, the feature map F_{cl} is

reshaped to generate the pseudo lower-level feature F_{nl} of size $c\times 1/2h\times 1/2w\times 4$, which preserves the local feature without information loss. Subsequently, softmax normalization is applied to obtain the lossless downsampled result F_{snl} of size $c\times 1/2h\times 1/2w\times 4$. Meanwhile, the spatial information of the local feature F_c is preserved by applying a convolution operation with stride 1, resulting in the spatial information feature F_s of size $4c\times h\times w$. Then, a downsampling operation is performed using a convolutional operation with stride 2 to generate the lower-level feature F_{sl} of size $4c\times 1/2h\times 1/2w$,which includes the preserved spatial information. Next, the feature F_{sl} undergoes feature extraction using the BAM [27] attention mechanism, yielding the feature representation F_{bsl}. Finally, the previously preserved spatial information is restored through a reshaping operation, generating the lower-level feature representation F_{el} of size $c\times 1/2h\times 1/2w\times 4$, which includes enhanced spatial information.

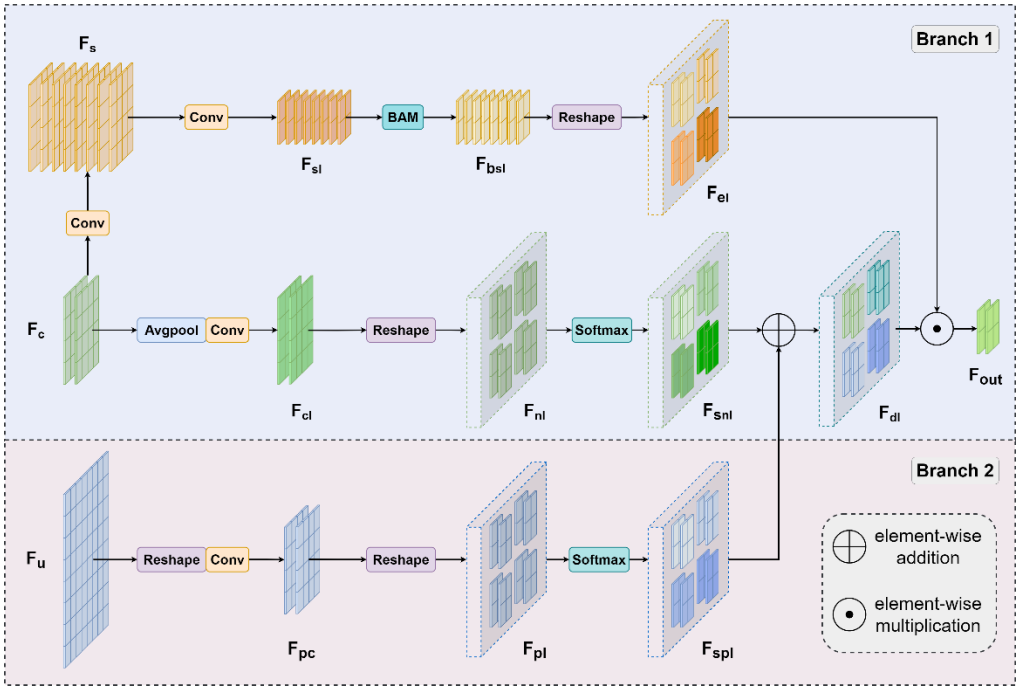


Fig. 3. Structure diagram of TPD module.

Path 2 involves a lossless downsampling process for the higher-level feature. The higher-level feature undergoes downsampling for the first time through reshaping, resulting in a size of $2c\times h\times w$. Then, a convolution operation is applied to halve the number of channels, generating a pseudo local-level feature F_{pc} based on the reconstructed details from the higher-level feature. Subsequently, a second downsampling is performed, yielding a pseudo lower-level feature F_{pl} based on the reconstructed details from the higher-level feature, with a size of $c\times 1/2h\times 1/2w\times 4$. Finally, softmax normalization is applied across the last dimension to obtain the output F_{spl} of Path 2.

The output F_{spl} of Path 2 is element-wise added with the downsampling result F_{snl} of the local feature, resulting in a lower-level feature map of size $c\times 1/2h\times 1/2w\times 4$ that combines the detailed information from both the higher-level and local features. This lower-level feature, denoted as F_{dl}, contains the detailed information from both the higher-level and local feature maps. The equation is as follows:

$$F_{dl} = Softmax(R(Conv(R(F_u)))) + Softmax(R(Conv(Avgpool(F_c)))) \quad (2)$$

Here, $R(\square)$ represents the reshape operation. The lower-level feature map F_{dl} obtained from the fusion in (2) is multiplied and fused with the enhanced lower-level feature F_{el} from Path 1, followed by summation across the last dimension. This yields the output feature map F_{out} of the TPD module, with a size of $c\times 1/2h\times 1/2w$. The equation is as follows:

$$F_{el} = R(BAM(Conv(Conv(F_c)))) \quad (3)$$

$$F_{out} = Sum(F_{dl} \square F_{el}) \quad (4)$$

C. C3GhostNetV2 Module

The original YOLOv7 model has relatively high complexity due to deep layers and multiple convolution operations, leading to many parameters and computational redundancy [28]. To reduce floating-point operations and parameters, this paper introduces the C3GhostNetV2 module. As shown in Fig. 1, the

input feature map is split into two branches: one passes through CBS and the GhostNetV2 bottleneck[29], generating Feature 1, while the other passes through CBS to produce Feature 2. Feature 1 and Feature 2 are then concatenated and processed by CBS to produce the final output.

Fig. 4 illustrates the structure of the GhostNetV2 bottleneck, comprising three steps: First, the input feature map is transformed into a compressed low-dimensional vector through downsampling and convolution. Next, this vector is processed by fully connected layers in vertical and horizontal directions, expanding its receptive field across multiple dimensions. Finally, the attention weights are normalized using the Sigmoid activation function to enhance the network's utility and stability. As a result, the network is able to perceive long-range dependencies between spatial pixels, enhancing the expressive power of the model. The DFC attention output [30] is combined with the first Ghost module's output. Depth-wise separable convolution is used to further reduce computational and memory overhead, improving inference speed. After generating features from the second Ghost unit, a skip connection merges the initial input with the new features, producing the final output. This design captures long-range spatial dependencies while significantly reducing computational and parameter costs.

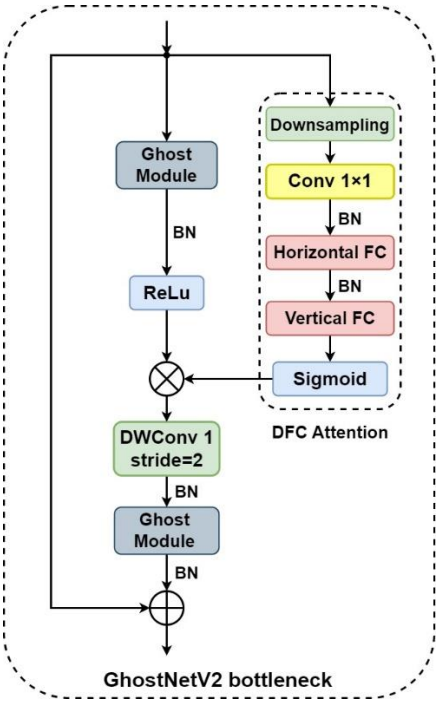


Fig. 4. GhostNetV2 bottleneck structure.

III. Experimental Preparations

A. Experimental Setup and Dataset

The software environment for this experiment includes Ubuntu 16.04, PyTorch 1.11, and CUDA 11.3. The hardware setup is described in detail in Table I. The ablation experiments were conducted using the stochastic gradient descent (SGD) strategy with 100 epochs of training. The initial learning rate was set to 0.01 and decayed with a minimum value of 0.0001. The batch size was set to 8. The momentum parameter was set to 0.9, and the weight decay was set to 0.0005.

TABLE I. Experimental Hardware Setup

Hardware Name	Model	Quantity
CPU	Intel Core i7-10700 CPU	1
Memory	Kingston 16G DDR4	2
Graphics Card	NVIDIA RTX-3090	1
Hard Drive	Western Digital 10TB	1

The experimental dataset used in this study consists of 4,030 images collected by a power company. The dataset includes four different work scenarios: lifting operations (1,104 images), hot work operations (1,028 images), edge operations (973 images), and high-altitude operations (925 images). These scenarios cover samples with different target sizes and brightness levels (see Fig. 5).

Fig. 5. Examples of 18 types of detection target datasets.

These work scenario data consist of eighteen categories: (1) crane, (2) all personnel on site, (3) wearing safety helmets, (4) work barriers, (5) control room, (6) hooks, (7) wearing safety harnesses, (8) not wearing safety harnesses, (9) safety harnesses properly suspended, (10) safety harnesses improperly suspended, (11) personnel performing hot work, (12) supervisors overseeing hot work, (13) protective face shields, (14) ignition source, (15) fire extinguisher, (16) improper wearing of safety gloves, (17) mobile phones. The dataset contains a total of 96,419 instances, which reflects the complexity and diversity of the work scenarios. The training set and validation set are split in an 8:2 ratio. Evaluation metrics

For the evaluation of the performance of the object detection model, a specific evaluation system was adopted. In this paper, the model's floating-point operations (GFLOPs) and the total number of parameters were calculated to assess its runtime and memory requirements. Meanwhile, the average precision (AP) and mean average precision (mAP) were used as standards to measure the accuracy of the model. The detection efficiency of the model on different categories was determined by the average precision rate, which is comprehensively determined by the recall and precision.

The recall is calculated using the following formula:

$$R_{ec} = \frac{T_p}{T_p + F_N} \times 100\% \tag{5}$$

The precision is calculated using the following formula:

$$P_{re} = \frac{T_p}{T_p + F_p} \times 100\% \tag{6}$$

Where T_p represents the true positive, F_N represents the false negative, and F_p represents the false positive. Precision-recall (PR) curve plots recall on the x-axis and maximum precision on the y-axis. The area under the PR curve is calculated by integrating over the curve, resulting in the value of AP (average precision). The mean average precision (mAP) is obtained by calculating the average of the AP values for all individual classes. The calculation formula is as follows:

$$AP = \int_0^1 P(r)dr \tag{7}$$

$$mAP = \frac{\sum_{k=0}^{c} AP_k}{C} \tag{8}$$

In the formula, $P(r)$ represents the PR curve, $\sum_{k=0}^{c} AP_k$ represents the average precision for each class, and C represents the total number of classes.

IV. Experimental Results And Analysis

A. Ablation Study

To evaluate the performance of the proposed approach in object detection tasks and study the effectiveness of various optimization strategies, we conducted ablation experiments on the YOLOv7 model as a baseline. In the table, the symbol " √ " indicates that the corresponding optimization unit has been applied. All experimental groups were conducted with the same hyperparameters and training strategies to analyze the impact of optimization strategies on the network more clearly. The experimental results are shown in Table II.

Experiment 1 was conducted on the original YOLOv7 without any improvements. In Experiment 2, the GLCI module was added. In this case, the precision did not change much, but the recall increased by 7.2%, and the mean average precision (mAP50) improved by 2.1%. This indicates that the GLCI module has a significant advantage in handling object detection tasks with complex backgrounds. By applying global and local attention mechanisms, the network learns key information more efficiently and reduces background interference. In Experiment 3, the TPD module was added. In this case, the precision increased by 2.5%, the recall increased by 8.7%, and mAP50 improved by 2.3%. This suggests that the introduction of the TPD module effectively enhances the network's learning ability for feature maps of different scales. By extracting and fusing multi-scale spatial and channel information, it effectively solves the problem of detecting objects with multi-scale variations and improves detection performance. From the results of Experiments 2 and 3, it can be seen that after integrating the TPD and GLCI modules, there is no significant difference in the number of parameters and the scale of floating-point operations. The introduction of the C3GhostNetV2 module in Experiment 4 resulted in a significant reduction of 87.2% in the scale of floating-point operations and a decrease in the parameter scale to 83.0%, effectively reducing the complexity of the model. The mAP50 metric of the model also increased by 0.4%, with corresponding improvements of 1.7% in precision and 9.6% in recall. This indicates that even with a reduction in parameters and computational complexity, the detection accuracy of the model was not compromised. This confirms that the C3GhostNetV2 unit not only reduces the complexity of the model but also enhances its performance. When all three modules (GLCI, TPD, and C3GhostNetV2) were simultaneously inserted into YOLOv7, the network showed the best improvement. The average precision (mAP50) increased by 4.5% compared to the original model, and precision and recall improved by 4.8% and 10.1% respectively. Moreover, compared to the baseline model, the complexity of the model was also reduced to a certain extent. This demonstrates that the simultaneous use of the three proposed improvement methods can yield better results.

TABLE II. Improved YOLOv7 Algorithm Ablation Study Results

Experiment	GLCI	TPD	C3GhostNetV2	mAP50 /%	Precision /%	Recall /%	Parameters /M	GFLOPs /G
1				86.3	85.3	78.5	37.6	107.3
2	√			88.4	85.2	85.7	37.6	107.6
3		√		88.6	87.8	87.2	37.6	107.5
4			√	86.7	87.0	88.1	31.2	93.6
5	√		√	88.7	90.5	88.4	31.4	93.8
6		√	√	88.8	87.7	87.8	31.4	93.7
7	√	√	√	90.8	90.1	88.6	31.4	93.8

B. Comparative Experimental Analysis of Applicability of YOLO Series

The fundamental idea of the YOLO series algorithms is to divide the image into fixed-sized grids and make predictions for each grid, thereby achieving object detection. To validate the general applicability of the three proposed modules in the YOLO series algorithms, we conducted comparative experiments on the YOLOv4-YOLOv7 [31-33] algorithms. The experimental results are shown in Table III.

From the data in the table, it can be observed that when detecting on the dataset of eighteen classes used in this paper, the original YOLO series algorithms achieved average precisions of 80.7%, 85.7%, 84.5%, and 86.3% respectively. After integrating the proposed improvement methods into each model, the average precisions were improved by 1.8%, 1.6%, 2.3%, and 4.5% respectively. The experimental results demonstrate that by adding the three proposed modules to the backbone networks of each YOLO algorithm, the average precisions of the models were improved to varying degrees. This is attributed to the fact that the proposed modules refine the feature extraction process, enhance the network's adaptability to multi-scale targets, and bolster the network's robustness in complex backgrounds through structural improvements. Therefore, the proposed improvement methods can be widely applied in various YOLO series algorithms to reduce model complexity, enhance the learning ability and feature extraction capability of the networks, and solve the problems of multi-scale targets, complex backgrounds, and diverse scenes in images captured in power construction sites.

C. Comparative Experimental Analysis with Other Models

To validate the advantages of the proposed improved model compared to the current state-of-the-art object detection algorithms, we compared our method with commonly used object detection methods, including Faster-RCNN [34], SSD [35], RetinaNet[36], YOLOv5, TPH-YOLOv5 [37], YOLOv7, and YOLOv8. Using the same dataset and partitioning strategy, we trained each model while keeping the parameters consistent. The experimental results are shown in Table IV.

From Table IV, it can be observed that compared to the current state-of-the-art small object detection algorithm TPH-YOLOv5 and other mainstream algorithms, the proposed algorithm in this paper achieves higher accuracy on most categories. The improved algorithm outperforms Faster R-CNN, SSD, and RetinaNet algorithms, with increases in average precision (mAP) of 11.7%, 28.5%, and 7.1% respectively. Compared to the previous version of YOLOv7, the improved algorithm achieves a 4.5% increase in mAP. The experimental results demonstrate that the improved YOLO model achieves better detection accuracy.

Additionally, to visually demonstrate the superiority of the improved algorithm, this paper provides visual results under different detection algorithms (see Fig. 6). From Fig. 6, it can be observed that when detecting in operation scenes with diverse and complex backgrounds, the Faster R-CNN algorithm shows missing detections and inaccurate bounding box localization. For small-scale object categories, such as the "hook" category in lifting operations and the "aqs_hang" category in elevated work scenarios, RetinaNet, SSD, and the previous version of YOLOv7 algorithms suffer from missing detections. Encouragingly, the model constructed in this paper does not exhibit such issues. This can be attributed to the addition of the GLCI module, which enhances the learning ability of the model, allowing the network to focus on the core information of the features and reduce noise interference from the background. Therefore, this method displays high adaptability in recognizing the clothing and equipment of operators, reducing the occurrence of missed detections, and achieving significant improvements in detection accuracy. For unevenly distributed scale categories, such as the "fence" category in lifting operation scenes and the "protective mask" category in hot work scenarios, other algorithms tend to have missing detections, while the proposed algorithm effectively addresses this issue. This is because the TPD module introduced in this paper enhances the network's learning ability for features at different scales, improving the detection accuracy of multi-scale objects.

TABLE III. APPLICABILITY EXPERIMENTS OF YOLO SERIES ALGORITHMS

Model	AP50/%								
	crane	*person*	*head*	*fence*	*czs*	*hook*	*belt*	*wrong_ belt*	*aqs_hang*
YOLOv4	81.2	84.7	79.8	76.4	80.4	81.5	80.9	81.8	83.3
Improved YOLOv4	81.6	85.2	80.8	75.2	83.3	83.7	81.8	84.9	86.0
YOLOv5	85.8	90.6	83.6	78.5	86.3	91.0	84.6	88.8	89.7
Improved YOLOv5	88.3	92.4	84.7	81.7	88.5	91.9	86.2	89.1	92.0
YOLOv6	83.6	91.2	83.8	75.2	86.2	89.3	81.0	89.3	90.5
Improved YOLOv6	83.7	89.7	88.3	76.1	89.1	90.0	82.3	90.2	92.3
YOLOv7	87.4	95.6	86.3	78.7	85.7	91.1	82.5	83.1	91.4
Improved YOLOv7	91.7	97.8	89.7	88.2	89.8	93.3	87.9	90.7	95.3
Model	**AP50/%**								**mAP50**
	aqs_ nohang	*fire operator*	*fire watcher*	*protective face shield*	*fire*	*extinguisher*	*hand_ false*	*phone*	*/%*
YOLOv4	79.9	83.4	83.3	91.8	78.2	81.5	75.9	68.6	80.7

Improved YOLOv4	82.1	83.8	85.1	92.7	79.6	82.3	81.5	73.4	82.5
YOLOv5	88.7	85.3	86.5	91.4	81.3	86.9	80.9	76.4	85.7
Improved YOLOv5	89.5	88.3	89.5	92.1	84.2	87.1	82.6	75.3	87.3
YOLOv6	88.9	85.2	87.2	91.4	81.7	80.2	79.0	72.7	84.5
Improved YOLOv6	88.5	87.5	94.7	93.8	84.5	88.3	81.5	75.9	86.8
YOLOv7	90.1	87.4	84.2	94.7	84.8	89.0	80.1	75.2	86.3
Improved YOLOv7	93.4	90.7	95.2	94.8	90.3	91.8	85.3	77.7	90.8

TABLE IV. COMPARISON OF MODEL PERFORMANCE DIFFERENCES

Model	**AP50/ %**								
	crane	***person***	***head***	***fence***	***czs***	***hook***	***belt***	***wrong_ belt***	***aqs_hang***
Faster R-CNN	80.1	84.1	78.3	63.7	79.2	89.4	75.4	81.6	76.9
SSD	63.5	78.7	68.9	55.2	71.8	60.8	63.5	64.2	52.0
RetinaNet	80.4	87.6	86.8	76.5	79.8	89.8	84.2	76.9	83.1
YOLOv5	85.8	90.6	83.6	78.5	86.3	91.0	84.6	88.8	89.7
TPH-YOLOv5	88.4	91.6	89.3	83.3	84.7	91.4	81.3	81.7	90.8
YOLOv7	87.4	95.6	86.3	78.7	85.7	91.1	82.5	83.1	91.4
YOLOv8	91.2	95.5	90.8	86.1	88.6	91.6	92.5	82.1	93.5
Ours	91.7	97.8	89.7	88.2	89.8	93.3	87.9	90.7	95.3
Model	**AP50/ %**								**mAP50**
	aqs_ nohang	***fire operator***	***fire watcher***	***protective face shield***	***fire***	***extinguisher***	***hand_ false***	***phone***	***/%***
Faster R-CNN	88.3	79.6	65.3	88.5	77.2	84.9	78.6	74.4	79.1
SSD	59.7	71.4	60.3	62.4	61.7	59.1	51.3	53.9	62.3
RetinaNet	89.7	87.3	89.2	84.7	82.3	83.7	79.4	81.2	83.7
YOLOv5	88.7	85.3	86.5	91.4	81.3	86.9	80.9	76.4	85.7
TPH-YOLOv5	90.6	88.4	89.7	91.4	91.3	87.9	81.8	80.3	87.3
YOLOv7	90.1	87.4	84.2	94.7	84.8	89.0	80.1	75.2	86.3
YOLOv8	94.9	87.2	83.1	93.8	87.6	86.3	85.9	84.7	89.1
Ours	93.4	90.7	95.2	94.8	90.3	91.8	85.3	77.7	90.8

D. Dataset Comparison and Model Scalability Experiments

To evaluate the scalability and generalization capabilities of the proposed model, we conducted assessments on two publicly available datasets, SHWD [38] and Pictor-v3 [39], and compared our model with other object detection models. The SHWD dataset focuses on safety helmet detection and contains 7,581 images, including 9,047 instances of workers wearing helmets and 111,514 instances of workers not wearing helmets. The Pictor-v3 dataset primarily focuses on detecting compliance with personal protective equipment (PPE) at construction sites, comprising 1,472 labeled images, which cover various combinations of PPE: 1,209 worker-only instances (W), 2,206 worker instances with helmets (WH), 328 worker instances with vests (WV), and 983 worker instances wearing both helmets and vests (WHV). The evaluation on these two datasets further validates the model's detection capability in different scenarios, as shown in Table V.

As can be seen in Table V, the proposed improvement outperforms other YOLO-based models in both helmet detection and worker PPE compliance detection, with notable improvements in detection accuracy and inference speed. Compared to the TPH-YOLOv5 model, which specializes in small object detection, our improved model demonstrates superior performance in detecting small-scale targets, with significant increases in mAP (0.50) and AP (0.50:0.95) metrics. Additionally, our model also achieves faster inference speeds per image than the original model. Fig. 7 and Fig. 8 show the visual detection results of the improved model and the original model on the SHWD and Pictor-v3 datasets. From the figures, it is evident that the original model exhibits certain false positives and missed detections, particularly when detecting small-scale helmet targets and workers with inconsistent scales. In contrast, the improved YOLOv7 model demonstrates higher precision and robustness in detecting such targets, significantly outperforming the original model, thus further validating the effectiveness of the proposed improvements.

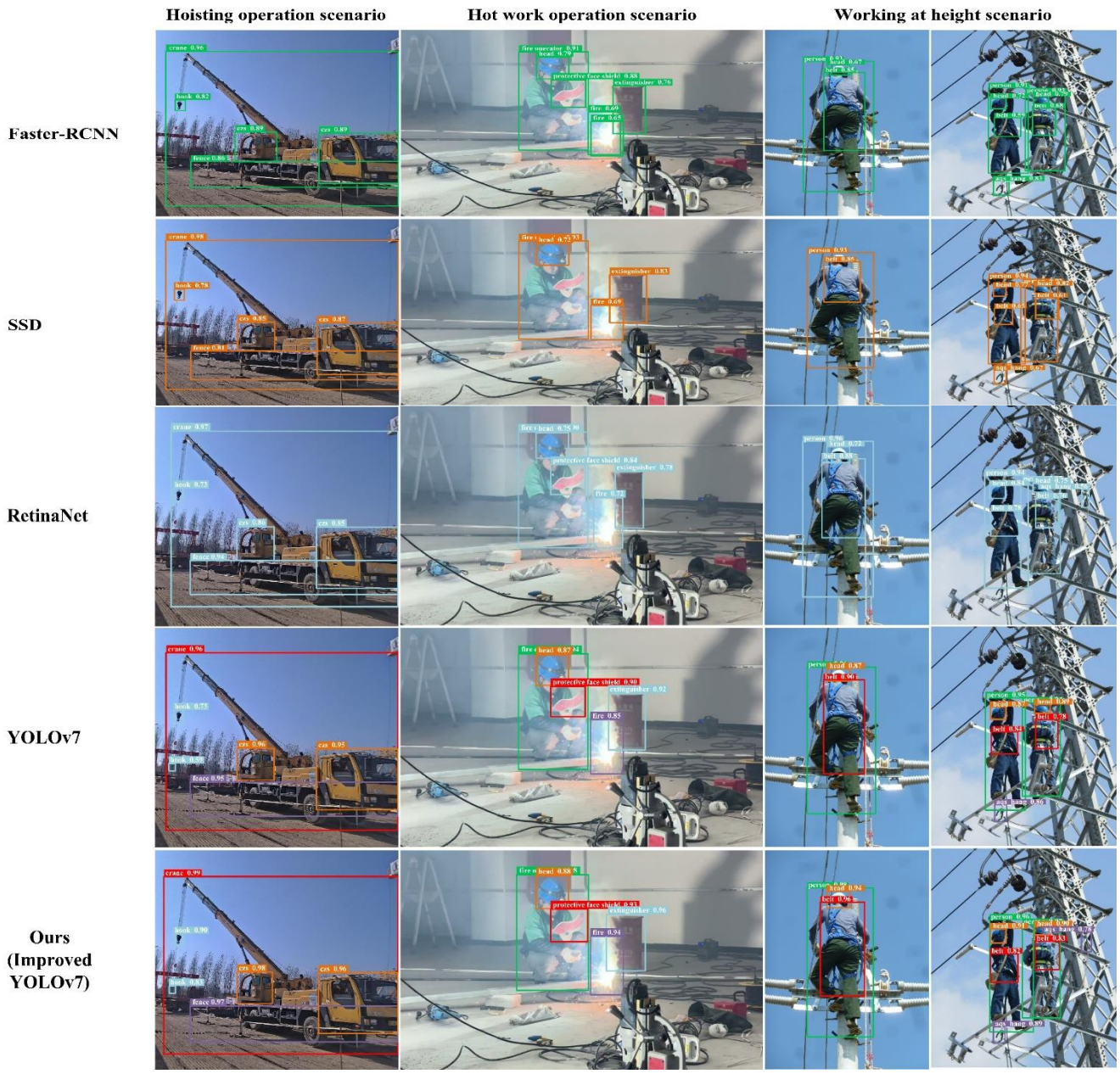


Fig. 6. Comparison of visual outcomes across diverse models.

TABLE V. PERFORMANCE COMPARISON OF DIFFERENT MODELS ON SHWD AND PICTOR-V3 DATASETS

Model	SHWD			Pictor-v3		
	mAP50 /%	*mAP(0.50:0.95) /%*	*Inference Time /ms*	*mAP50 /%*	*mAP(0.50:0.95) /%*	*Inference Time /ms*
TPH-YOLOv5	86.7	64.2	26.4	88.4	54.8	**19.3**
YOLOv7	87.2	64.6	29.6	89.7	53.9	25.8
YOLOv8	90.8	65.7	41.9	91.3	55.1	33.5
Ours	**91.5**	**66.1**	**26.2**	**92.6**	**56.9**	20.7

Fig. 7. Comparison of visualization results on the SHWD dataset.

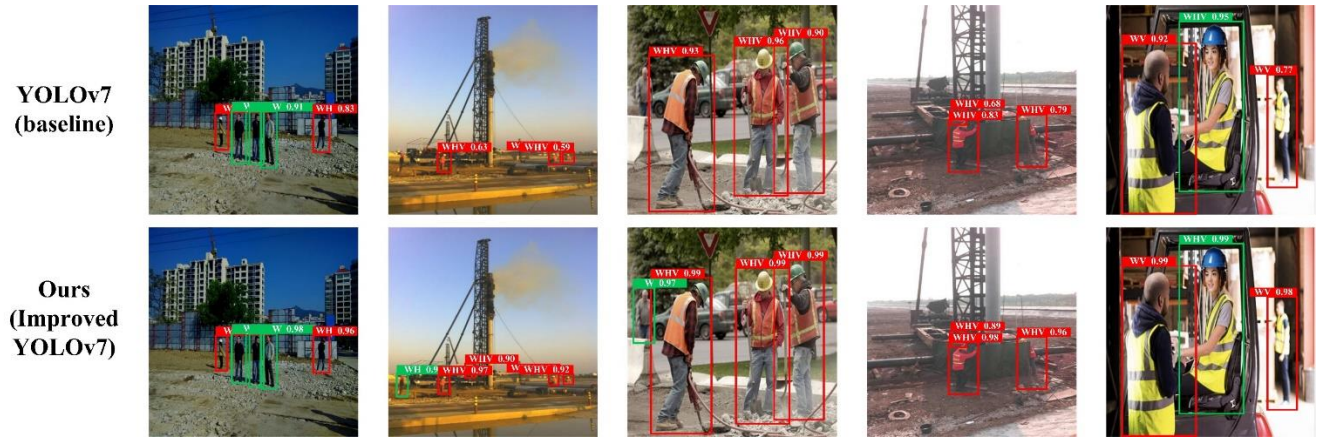


Fig. 8. Comparison of visualization results on the Pictor-v3 dataset.

V. Conclusion

To achieve intelligent compliance recognition in power construction sites, we propose a YOLOv7-based method for detecting personnel behavior that integrates contextual information. This method is designed to address the challenges of high complexity, insufficient scale adaptability, complex image backgrounds, and varying target sizes in existing detection models.

We introduced the GLCI module, which significantly enhances object detection accuracy in complex backgrounds through global and local attention mechanisms. Simultaneously, the TPD module improves the network's ability to learn multi-scale features, leading to better detection performance across varying target scales. Additionally, the C3GhostNetV2 module enhances the model's representational power while reducing computational and parameter complexity. Experimental results demonstrate that the improved YOLOv7 model surpasses the original baseline in detection accuracy, model complexity, and miss rate, showing exceptional adaptability in complex environments. These findings offer effective solutions for object detection tasks in complex scenarios, such as power construction sites, and contribute positively to the advancement of intelligent vision. Furthermore, the dataset comparison and model scalability experiments validate the robustness and generalization capabilities of the proposed model across diverse scenarios. In the future, we aim to enhance the model's robustness across diverse scenarios and lighting conditions, improving adaptability and generalization for deployment on edge devices.

Acknowledgment

Author Contributions: C.B. designed the research and drafted the paper; Z.Y. processed the data; Y.X. debugged the server and configured the experimental environment; Z.L. and D.Y. revised and finalized the paper. All authors have reviewed and approved the final version of the manuscript.

Funding: This research was funded by the Science and Technology Project of State Grid Beijing Electric Power Company (520234230004).

Conflicts of Interest: The authors declare that there are no conflicts of interest.

References

[1] S. Zhang, G. Fu, W. Yin, and P. Gao, “Analysis and prevention of safety helmet accidents based on behavioral safety,” Coal Mine Safety, vol. 45, no. 4, pp. 229–232, 2014.

[2] Y. Wang, Z. Wang, B. Wu, and G. Yang, “Research review of safety helmet wearing detection algorithm in intelligent construction site,” J. Wuhan Univ. Technol., vol. 43, no. 10, pp. 56–62, 2021.

[3] S. Li, H. Ouyang, T. Chen, X. Lu, and Z. Zhao, “Yolo-t: multi-target detection algorithm for transmission lines,” Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 5, 2024..

[4] W. Luo, M. Y. Ahmad Ihsan, M. S. K. Khaizi, and R. Raju, “Hardhat-yolo: a yolov5-based lightweight hardhat-wearing detection algorithm in substation sites,” Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 5, 2024..

[5] H. Nguyen and T. A. Nguyen, "Hybrid vision transformers and cnns for enhanced transmission line segmentation in aerial images," Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 1, 2024..

[6] H. Lei, X. Ge, C. Hao, L. Zhang, and S. Chang, "Identification of dress code of workers in substation based on YOLO v5," Power Syst. Big Data, vol. 24, no. 10, pp. 1–8, 2021.

[7] K. Arai, K. Beppu, Y. Ifuku, and M. Oda, "Method for detecting the appropriateness of wearing a helmet chin strap at construction sites," Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 7, 2024.

[8] B. Ren, Y. Zheng, Y. Wang, S. Sheng, J. Li, and H. Zhang, "Research status and prospect of deep learning in secondary state monitoring of smart substation," in Proc. 2020 Asia Energy and Electrical Engineering Symp. (AEEES), IEEE, 2020, pp. 669–677.

[9] X. Liu, B. Zhang, Y. Fu, and J. Zhu, "Detection on normalization of operating personnel dressing at contaminated sites based on deep learning," J. Safety Sci. Technol., vol. 16, no. 7, pp. 169–175, 2020.

[10] M. Fang, T. Sun, and Z. Shao, "Fast helmet-wearing-condition detection based on improved YOLOv2," Opt. Precision Eng., vol. 27, no. 5, pp. 1196–1205, 2019.

[11] K. Xu and C. Deng, "Research on helmet wear identification based on improved YOLOv3," Laser Optoelectron. Prog., vol. 58, no. 6, pp. 300–307, 2021.

[12] S. Y. Jeon, J. H. Park, S. B. Youn, Y. S. Kim, Y. S. Lee, and J. H. Jeon, "Real-time worker safety management system using deep learning-based video analysis algorithm," Smart Media J., vol. 9, no. 3, pp. 25–30, 2020.

[13] X. Du, Y. Wang, R. Yan, D. Gu, X. Zhang, and T. Lei, "Accurate helmet wearing detection algorithm based on YOLO-ST," J. Shaanxi Univ. Sci. Technol., vol. 40, no. 6, pp. 177–183, 91, 2022.

[14] X. Long, W. Cui, and Z. Zheng, "Safety helmet wearing detection based on deep learning," in Proc. 2019 IEEE 3rd Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC), 2019, pp. 2495–2499.

[15] J. Wu, N. Cai, W. Chen, H. Wang, and G. Wang, "Automatic detection of hardhats worn by construction personnel: A deep learning approach and benchmark dataset," Autom. Constr., vol. 106, p. 102894, 2019.

[16] Y. Li, H. Wei, Z. Han, J. Huang, and W. Wang, "Deep learning-based safety helmet detection in engineering management based on convolutional neural networks," Adv. Civ. Eng., vol. 2020, pp. 1–10, 2020.

[17] S. Lang, F. Ventola, and K. Kersting, "DAFNe: a one-stage anchor-free approach for oriented object detection," arXiv preprint arXiv:2109.06148, 2021.

[18] J. Shen, X. Xiong, Y. Li, W. He, P. Li, and X. Zheng, "Detecting safety helmet wearing on construction sites with bounding‐box regression and deep transfer learning," Comput.-Aided Civ. Infrastruct. Eng., vol. 36, no. 2, pp. 180–196, 2021.

[19] C. Sun, S. Zhang, P. Qu, X. Wu, P. Feng, Z. Tao, J. Zhang, and Y. Wang, "MCA-YOLOV5-Light: A faster, stronger and lighter algorithm for helmet-wearing detection," Appl. Sci., vol. 12, no. 19, p. 9697, 2022.

[20] J. Y. Lee, W. S. Choi, and S. H. Choi, "Verification and performance comparison of CNN-based algorithms for two-step helmet-wearing detection," Expert Syst. Appl., vol. 225, p. 120096, 2023.

[21] S. Yue, Q. Zhang, D. Shao, Y. Fan, and J. Bai, "Safety helmet wearing status detection based on improved boosted random ferns," Multimed. Tools Appl., vol. 81, pp. 16783–16796, 2022.

[22] B. Zhang, C. F. Sun, S. Q. Fang, Y. H. Zhao, and S. Su, "Workshop safety helmet wearing detection model based on SCM-YOLO," Sensors, vol. 22, no. 17, p. 6702, 2022.

[23] S. Bourou, A. Maniatis, D. Kontopoulos, and P. A. Karkazis, "Smart detection system of safety hazards in Industry 5.0," Telecom, vol. 5, no. 1, pp. 1–20, 2023.

[24] A. T. A. Al Daghan, S. Kesh, and A. S. Manek, "A deep learning model for detecting PPE to minimize risk at construction sites," in 2021 IEEE Int. Conf. Electronics, Computing and Communication Technologies (CONECCT), 2021, pp. 1–6.

[25] F. Gong, X. Ji, W. Gong, X. Yuan, and C. Gong, "Deep learning based protective equipment detection on offshore drilling platform," Symmetry, vol. 13, no. 6, p. 954, 2021.

[26] H. Jinqiang, L. Ruihai, L. Hao, L. Yongli, G. Bo, H. Yanpeng, L. Wei, W. Jianrong, and W. Yi, "Visible light image automatic recognition and segmentation method for overhead power line insulators based on YOLO v5 and GrabCut," Southern Power System Technology, vol. 17, no. 06, pp. 128–135, 2023.

[27] J. Park, S. Woo, J.-Y. Lee, and I. S. Kweon, "BAM: bottleneck attention module," arXiv preprint arXiv:1807.06514, 2018.

[28] B. Chen and Z. Dang, "Fast PCB defect detection method based on FasterNet backbone network and CBAM attention mechanism integrated with feature fusion module in improved YOLOv7," IEEE Access, 2023.

[29] Y. Tang, K. Han, J. Guo, C. Xu, C. Xu, and Y. Wang, "GhostNetv2: enhance cheap operation with long-range attention," Adv. Neural Inf. Process. Syst., vol. 35, pp. 9969–9982, 2022.

[30] A. H. C. Fong, K. Yoo, M. D. Rosenberg, S. Zhang, C.-S. R. Li, D. Scheinost, R. T. Constable, and M. M. Chun, "Dynamic functional connectivity during task performance and rest predicts individual differences in attention across studies," NeuroImage, vol. 188, pp. 14–25, 2019.

[31] A. Bochkovskiy, C.-Y. Wang, and H.-Y. M. Liao, "YOLOv4: optimal speed and accuracy of object detection," arXiv preprint arXiv:2004.10934, 2020.

[32] C. Li, L. Li, H. Jiang, K. Weng, Y. Geng, L. Li, Z. Ke, Q. Li, M. Cheng, W. Nie, Y. Li, B. Zhang, Y. Liang, L. Zhou, X. Xu, X. Chu, X. Wei, and X. Wei, "YOLOv6: a single-stage object detection framework for industrial applications," arXiv preprint arXiv:2209.02976, 2022.

[33] C.-Y. Wang, A. Bochkovskiy, and H.-Y. M. Liao, "YOLOv7: trainable bag-of-freebies sets new state-of-the-art for real-time object detectors," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2023, pp. 7464-7475.

[34] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: towards real-time object detection with region proposal networks," Advances in Neural Information Processing Systems, vol. 28, 2015.

[35] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C.-Y. Fu, and A. C. Berg, "SSD: single shot multibox detector," in Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11–14, 2016, Proceedings, Part I, vol. 14, 2016, pp. 21–37.

[36] T.-Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollar, "Focal loss for dense object detection," in Proceedings of the IEEE International Conference on Computer Vision, 2017, pp. 2980–2988.

[37] X. Zhu, S. Lyu, X. Wang, and Q. Zhao, "TPH-YOLOv5: improved YOLOv5 based on transformer prediction head for object detection on drone-captured scenarios," in Proceedings of the IEEE/CVF International Conference on Computer Vision, 2021, pp. 2778–2788.

[38] M. Gochoo, "Safety helmet wearing dataset," Mendeley Data, 2021, doi: 10.17632/9rcv8mm682.1.

[39] N. D. Nath, A. H. Behzadan, and S. G. Paal, "Deep learning for site safety: Real-time detection of personal protective equipment," Automation in Construction, vol. 112, p. 103085, 2020.

Preprocessing and Analysis Method of Unplanned Event Data for Flight Attendants Based on CNN-GRU

Dongyang Li
Culture and Tourism College, Jilin Province Economic Management Cadre College, Changchun, 130012, China

***Abstract*—The data of unplanned flight attendant events has characteristics such as diversity and complexity, which pose great challenges to data preprocessing and analysis. This study proposes a preprocessing and analysis method for unplanned flight attendant event data based on Convolutional Neural Networks (CNN) and Gated Recurrent Units (GRU). Firstly, an efficient word vector tool is used to preprocess the raw data, improving its quality and consistency. Then, convolutional neural networks are taken to extract local features of the data, combined with gated loop units to capture dynamic changes in time series, thus achieving effective analysis and prediction of unplanned events in air crew. The results showed that in the 6-class task, the research model exhibited the highest accuracy at 99.24%, the lowest accuracy at 94.24%, and an average accuracy of 98.53%. The highest, lowest, and average accuracies in the 10-class task were 96.63%, 90.17%, and 93.21%, respectively. The performance of the research model was superior to support vector machine, K-nearest neighbor algorithm, and some advanced algorithms. This study provides a more accurate analysis tool for unplanned event data of flight attendants, to assist in the efficiency of aviation emergency event handling and improve aviation safety.**

***Keywords*—Convolutional neural network; gate recurrent units; air crew; unplanned events; data preprocessing; data analysis**

I. Introduction

The rapid development of the socio-economy has brought important strategic opportunities for the modern aviation transportation industry and has also put forward higher requirements for the improvement of aviation safety and security capabilities. The frequent occurrence of Unplanned Flight Attendant Events (UFAEs) and the complexity of data analysis pose a significant threat to aviation safety and passenger experience [1]. UFAEs analyses can help identify and predict events that may affect flight safety, such as mechanical failures, medical emergencies or security threats. By identifying these events in a timely manner, preventive measures can be taken to reduce the probability of accidents. In addition, by analysing unplanned events, airlines can better understand potential risks and develop effective risk management strategies to mitigate the impact of these risks, as well as reduce cost control and operational efficiency. How to effectively preprocess and analyze these event data to provide reliable prediction and decision support is an urgent problem in the current aviation management field. Traditional event analysis methods often rely on expert experience and simple statistical analysis, making it difficult to handle large-scale and diverse event data [2]. The advancement of Deep Learning (DL) technology has shown great potential for methods built on deep neural networks in processing complex data and mining deep features [3]. CNN and GRU are two widely used models in the field of DL. The former is good at extracting local features of data, while the latter has advantages in processing time series data [4-5]. However, existing DL methods still fall short in their combined ability to handle time series features and local features. Some of the methods focus too much on the long-term dependence of time series and ignore the importance of local features; or they can only capture local features and cannot effectively handle the long-term dependence of time series data. For this reason, the study proposes a method for preprocessing and analysing UFAEs data based on CNN and GRU. At First, Efficient Word Vector Tools (EWVTs) will be used to preprocess event descriptions, eliminate noise, and enhance data consistency. Then, CNN will be used to extract local features of event data, and GRU will be utilized to model the temporal dynamics of event occurrence, ultimately achieving classification and prediction of events. It aims to process UFAEs data through this method to provide support for airline unplanned event response and decision-making.

This study has six sections. Section II summarizes the current state of the industry. Section III has two sections. The first section introduces the UFAEs data preprocessing method based on EWVTs, and the second section introduces the UFAEs analysis method based on CNN-GRU. Section IV conducts performance testing on the proposed CNN-GRU. Discussion is given in Section V. Section VI is a summary of this study and prospects for future work.

II. Related Works

The essence of UFAEs data preprocessing is a text data preprocessing method. This method is a key step in processing text data analysis, involving a series of operations on the raw text data to improve the data applicability, thereby enhancing the efficiency of subsequent analysis. Hickman et al. focused on the capture of language content and style, statistical analysis ability, and effectiveness of insights obtained from text mining in the decision-making process of text preprocessing, and conducted research on computational linguistics and organizational text mining. Considering different types of text mining, research questions, and dataset features, this study provided experience- based text preprocessing decision recommendations [6]. Nova K used text preprocessing techniques such as noise removal, punctuation, and stop words to transform the original text into a Term Frequency - Inverse

Document Frequency (TF-IDF) feature matrix. This study employed three machine learning models for classification tasks, including polynomial naive Bayes, multi-layer perceptrons, and a Light Gradient Boosting Machine (LightGBM). LightGBM achieved an accuracy of 0.724 and had a higher accuracy of 0.77 when using text content for classification [7]. Thakkar et al. proposed a specific sequence of text data preprocessing steps to improve the performance of sentiment analysis, and proposed "output label matching features based on advanced techniques" to initialize the weights of Artificial Neural Networks (ANN). Simulation experiments have found that research methods have more advantages [8]. Situmeng S found that different forms of text preprocessing are helpful for successfully identifying named entities. By comparing and evaluating the three categories of people, places, and organizations, it was found that some preprocessing methods have significant effects on different entity categories. The combination of multiple preprocessing methods could significantly improve accuracy. Therefore, it was recommended to choose appropriate preprocessing methods based on the different entity categories in practical applications, rather than simply enabling or disabling preprocessing for all [9].

Meanwhile, the analysis methods for text data have been continuously optimized in recent years. Zhao C et al. used a multi-strategy text data augmentation method to handle the issues of data limitations and lack of high-quality corpora in text analysis. It compared the performance of the enhanced dataset and the original dataset: the F1 score of Long Short-Term Memory (LSTM) grounded on attention mechanism on the dataset increased by 5.0% and 4.4%, demonstrating excellent performance [10]. Sharma P and Pathak D proposed a method for analyzing social media data using a learning process, utilizing unsupervised learning and sentiment analysis to identify disaster events and their intensity. This method used annotated data to train improved fuzzy C-means clustering, using sentiment scores to identify negative emotions and determine the severity of disasters. Finally, Support Vector Machine (SVM) and ANN classifier were utilized to classify the text based on emotions. This method was effective and its accuracy continues to improve over time [11]. Sengupta S and Dave V introduced a method of legislative text analysis aimed at automatically identifying appropriate legal chapters applicable to cases. This method utilized supervised Machine Learning (ML) and natural language processing, treating the task as a multi-label classification problem. It applied traditional ML models such as logistic regression, Naive Bayes, decision trees, and SVM, and conducted hyperparameter fine-tuning analysis. Finally, SVM had the highest F1-score of 0.75 [12].

In summary, existing research on text data analysis mainly focuses on traditional statistical analysis and simple ML methods. Some studies use methods such as linear regression and decision trees for event prediction, but these methods often exhibit limitations when facing large-scale, high-dimensional, and complex event data. In addition, some studies have introduced DL techniques such as LSTM and simple CNN, but there are still shortcomings in their comprehensive ability to handle temporal characteristics and local features. In contrast, this paper constructs a data preprocessing and analysis method for UFAEs built on CNN-GRU. This method fully utilizes the Local Feature Extraction Capability (LFEC) of CNN and the TMC of GRU, which can more effectively capture the complex features and dynamic changes of event data. By introducing EWVTs for data preprocessing, the data quality and consistency have been further improved, providing more reliable inputs for subsequent DL models. The research method is not only innovative in theory, but also provides more scientific and effective decision-support tools for airlines and related management departments.

III. Methods and Materials

To provide efficient analysis tools for UFAEs, this study utilizes EWVT to preprocess event data, including data collection, cleaning, and vectorization. The CNN-GRU is adopted for in-depth analysis of preprocessed data, combining CNN's LFEC with GRU's TMC to achieve accurate classification and prediction of event data.

A. UFAEs Data Preprocessing Based on EWVT

UFAEs refer to various sudden and unexpected events encountered by flight attendants during flight operations. These events were not pre-arranged in the flight plan and may have a significant impact on flight safety, passenger service, and overall flight operations [13-14]. Common UFAEs include mechanical failures, passenger disputes, sudden weather events, and other unexpected events. The occurrence of these unplanned events has a high degree of uncertainty and suddenness, which puts extremely high demands on the adaptability and event handling ability of flight attendants. Preprocessing and analyzing these events can help improve airlines' emergency plans, enhance passenger safety, and improve service quality. The UFAEs processing flow is shown in Fig. 1.

In Fig. 1, the processing flow of UFAEs consists of six steps. Firstly, the data collection of unexpected events in the crew is carried out, followed by data preprocessing. Then, the data is vectorized, trained, and a word vector matrix is constructed. Then to conduct preliminary classification and match similar unplanned event cases. Finally, providing corresponding emergency response methods. Data collection is the step 1 in data preprocessing. When collecting data, to ensure the representativeness and comprehensiveness of the data, various unplanned events are covered as much as possible, including mechanical failures, passenger disputes, sudden illnesses, etc. Data cleaning is a key step in ensuring data quality, which requires removing duplicate records and obviously erroneous entries. The third step is to process the missing data. For cases with fewer missing values, mean or median filling methods are used; For entries with a large number of missing values that cannot be completed, they will be directly removed. After data cleaning, the integrity and reliability of the data have been preliminarily ensured. To convert textual event descriptions into numerical forms that can be processed by computers, this study uses EWVT for text preprocessing. Word2Vec, as a word vector model, performs well in semantic representation of words and can capture subtle semantic relationships between words [15]. Word2Vec is an optimization of neural network models, which includes the Continuous Bag of Words (CBOW) and Skip-gram models, as exhibited in Fig. 2.

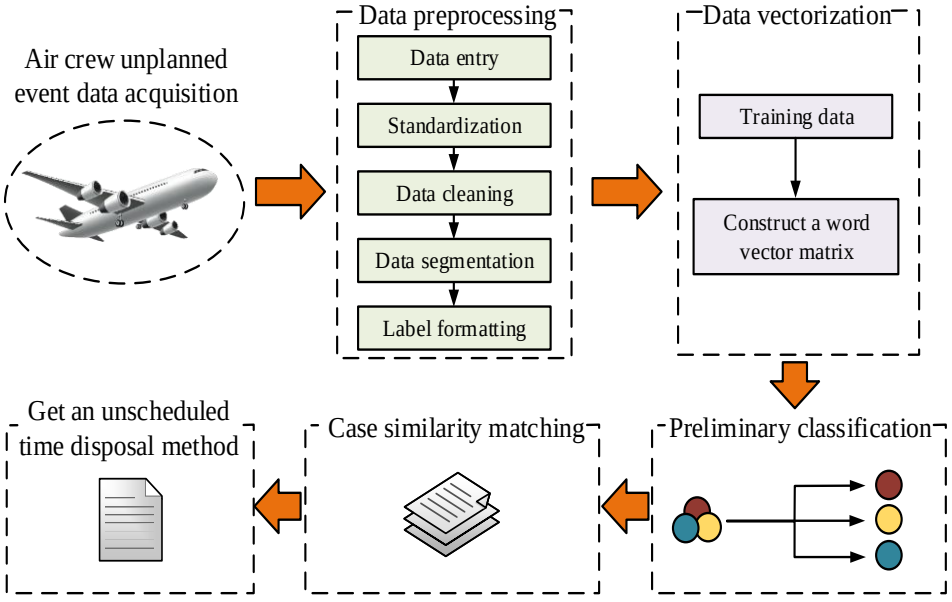


Fig. 1. UFAE processing flow.

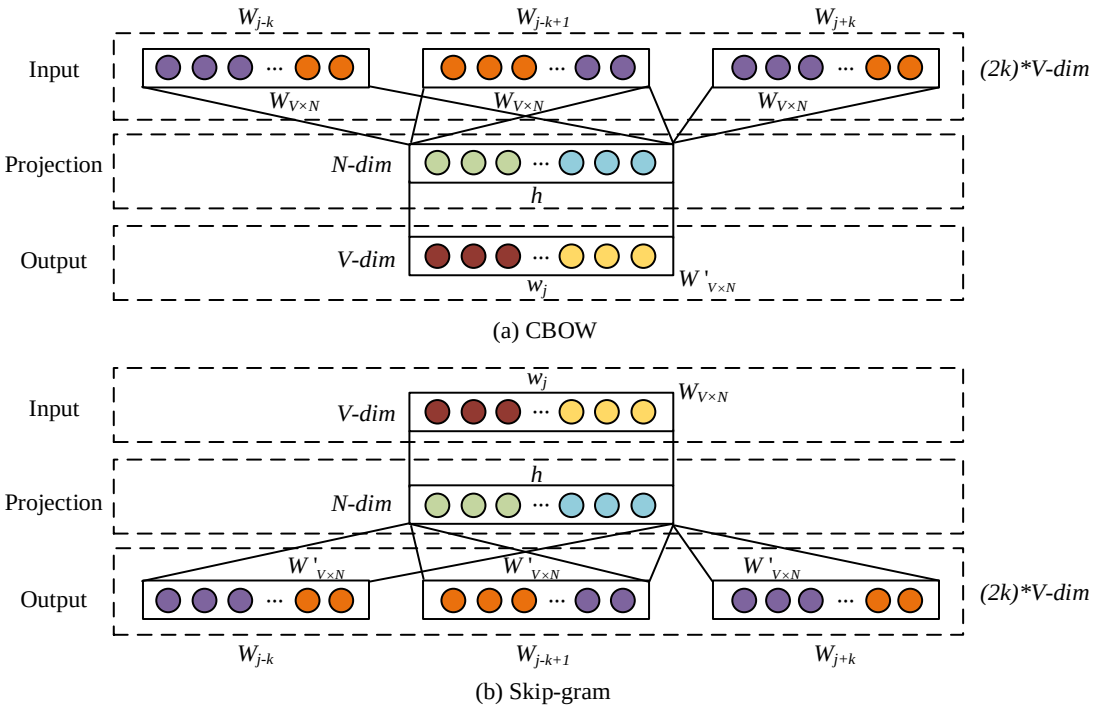


Fig. 2. CBOW and Skip-gram models.

In Fig. 2, Word2Vec consists of CBOW and Skio-gram. Fig. 2 (a) shows the structure of the CBOW, which predicts the word vector of the current word based on the word vector of the context. For the text position of target word w_j at position j, the sliding window size is designed to be k. k words above and below are used as context $con(w_j)$, with a scale of $2k$. Randomly to initialize the contextual words, then input the vector sum into the Softmax layer for normalization, and finally output the probability P of the occurrence of word w_j. The objective function of the CBOW model is Eq. (1).

$$L = \sum_{w_j \in V} \log P(w_{j-k+1}, ..., w_{j+k}) \tag{1}$$

In Eq. (1), V is the corpus where the target word w_j is located. L is the objective function. Skip-gram, in contrast to CBOW, obtains the contextual word vector from the current word vector [16]. Skip-gram uses stochastic gradient descent to optimize the objective function, and after training, the word

vector matrix W' can be obtained. This matrix is a $N \times V$ low dimensional dense word vector matrix with a vocabulary size of V. In Skip-gram, the target word w_j is input to the input layer, with the sliding window size set to k, and the word is mapped as a column vector of matrix W. The Softmax function is taken to output the $2k$ words with the highest possibility. The probability of obtaining the output word is Eq. (2).

$$P(w_{j-k}, w_{j-k+1}, ..., w_{j+k} | w_j) = \frac{e^{u_j{}^T h}}{\sum_{i=1}^{V} e^{u_i{}^T h}} \quad (2)$$

In Eq. (2), h and u_j are the row vectors of matrix W and W', and also the hidden layer vector and output vector of w_j. e is a natural constant. $u_j{}^T$ is the weight of weighted summation. The goal of Skip-gram is to maximize the logarithmic likelihood function, as shown in Eq. (3).

$$L = \frac{1}{V} \sum_{j=k}^{V=k} \log P(w_{j-k}, w_{j-k+1}, ..., w_{j+k} | w_j) \quad (3)$$

In Eq. (3), L is the maximum logarithmic likelihood function. After training the Word2Vec model, CNN is used for feature extraction. CNN can effectively extract local features from text and convert these features into fixed length vector representations as inputs for UFAEs analysis models.

B. Analysis of UFAEs Based on CNN-GRU

After completing data preprocessing, the next key step is to conduct in-depth analysis and modeling of the preprocessed data. To fully utilize the temporal and local characteristics of UFAEs data, this study proposes a method combining CNN and GRU. CNN can effectively extract local features of data, while GRU excels at handling long-term dependencies in time series data [17]. This study designs a multi-layer CNN that extracts local features from data by alternating between convolutional and pooling layers. The structure of CNN is shown in Fig. 3.

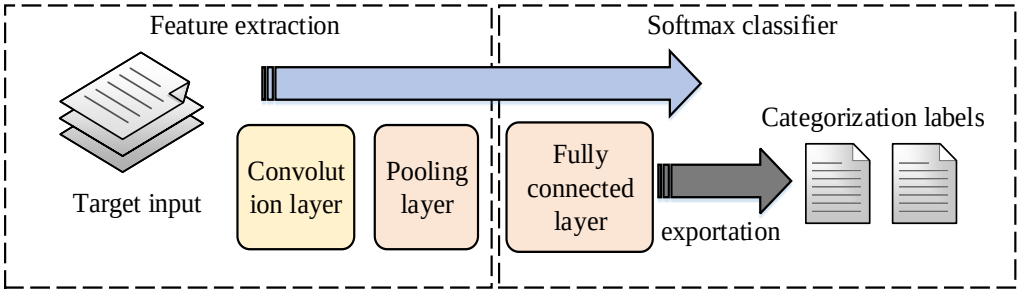


Fig. 3. CNN structure diagram.

In Fig. 3, CNN generally includes convolutional, pooling, and Fully Connected Layers (FCL), where the expression of the convolution operation continuous estimation function s is Eq. (4).

$$s(t) = \int x(a) w(t-a) da \quad (4)$$

In Eq. (4), x is the first parameter of the convolution, commonly referred to as the input. w is an effective probability dense function and also the 2nd parameter, called the Kernel Function (KF). This operation is called convolution, and the simplified expression is Eq. (5).

$$s(t) = (x * w)(t) \quad (5)$$

In CNN learning, high-dimensional data is usually input first, and the convolution kernel is the high-dimensional values generated by the algorithm. The calculation formula is Eq. (6).

$$s(i, j) = (K * I)(i, j) \sum_m \sum_n I(m, n) K(i-m, j-n) \quad (6)$$

In Eq. (6), m and n are the effective range of values for convolution. I is the input, and K is the KF of the input. For the application convenience in ML, a variant is usually utilized (Eq. (7)). Its operation is extremely semblable to convolution, but the variation is small within the valid range of m and n. This means that as m grows, the input index increases, but the kernel index decreases, achieving inter-variability of convolutions.

$$s(i, j) = (K * I)(i, j) \sum_m \sum_n I(i+m, j+n) K(m, j) \quad (7)$$

The is the core layer of CNN is the convolutional ones, which is crucial for conducting convolutional operations and enhancing CNN's feature extraction capabilities. Convolutional Layers (CL) generally refer to 2D convolution operations. If the input size is set to $D_f \times D_f$ and the convolution kernel size is $D_k \times D_k$, then the output feature size after convolution is $D_f^{'} \times D_f^{'}$. The formulas for the three are shown in Eq. (8).

$$D_f^{'} = (D_f - D_k + 2 \times pad) / stride + 1 \quad (8)$$

The CL takes Local Connections (LC) and Weight Sharing (WS) to reduce the amount of network values and decrease network complexity. LC refers to the feature extraction of CLs built on their size when moving. WS refers to the convolutional kernel not changing its parameter when extracting data features, but using the equal weight to extract features [18-19]. GRU is one of the popular variants of Recurrent Neural Network (RNN) and an improvement on LSTM, as shown in Fig. 4.

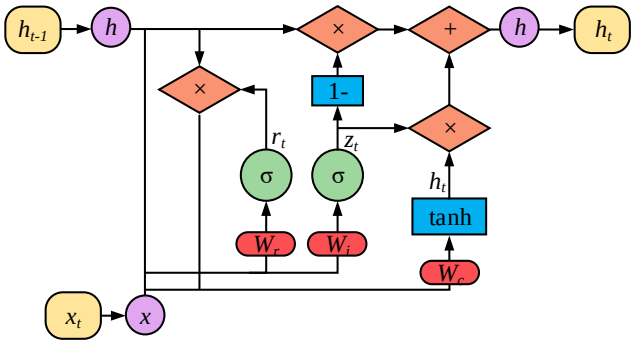


Fig. 4. GRU internal structure.

In Fig. 4, the formula for the update gate in the GRU is Eq. (9).

$$z(t) = sigmoid\left(W\_z * \left[h(t-1),\ x(t)\right] + b\_z\right) \tag{9}$$

In Eq. (9), $z(t)$ is the part that needs to be updated in the Hidden State (HS), and its value range is between 0 and 1. W_z means the Weight Matrix (WM). $h(t-1)$ denotes the HS from the previous moment. $x(t)$ is the current input state. b_z is the bias term. The calculation for resetting the door is Eq. (10).

$$r(t) = sigmoid\left(W\_r * \left[h(t-1), x(t)\right] + b\_r\right) \tag{10}$$

In Eq. (10), $r(t)$ controls how to combine the previous HS with the current input to produce Candidate HSs (CHS). W_r is the WM of the reset gate. b_r is the bias term in the reset gate. The CHS is expressed by Eq. (11).

$$h\sim(t) = tanh\left(W\_h * \left[r(t) * h(t-1), x(t)\right]\right) \tag{11}$$

In Eq. (11), $h\sim(t)$ is a CHS based on the current input and the previous HS. W_h is the WM in this state. The expression for the HS at the current moment is Eq. (12).

$$h(t) = \left(1 - z(t)\right) * h(t-1) + z(t) * h\sim(t) \tag{12}$$

In Eq. (12), $h(t)$ is the final HS at the current time. $\left(1-z(t)\right)$ and $z(t)$ are the parts that need to be discarded and retained. Through this approach, GRU networks are able to determine which information needs to be retained or forgotten in a new step [20]. This study establishes a CNN-GRU model to solve the classification and matching of text data to complete the analysis of UFAEs. The structure of CNN-GRU is Fig. 5.

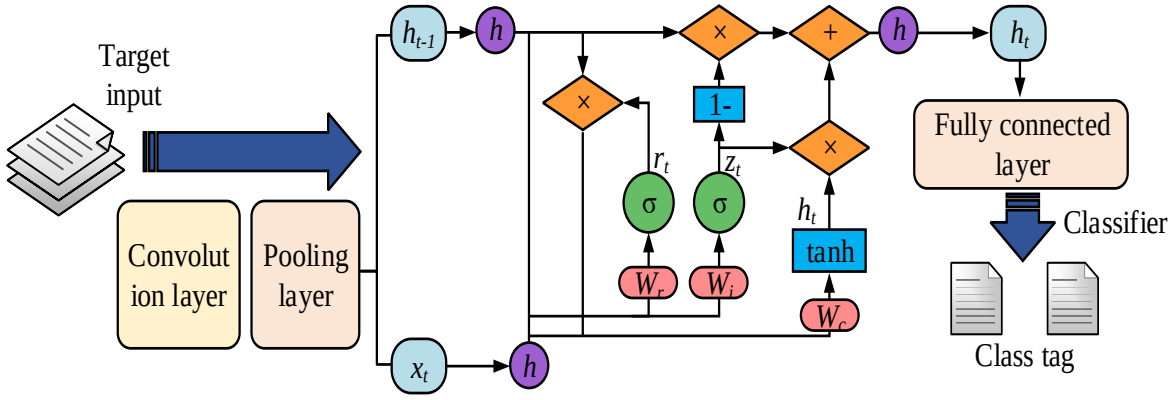


Fig. 5. CNN-GRU hybrid model structure.

In Fig. 5, CNN-GRU mainly consists of three parts, namely CNN layer, GRU layer, and FCL. This study uses the Softmax fully connected function for classification and selected Relu as the activation function. The group with the highest output probability is taken as the eventual classification result for UFAEs. Through this structure, the CNN-GRU model can effectively extract local and global features from text data, thereby increasing the classification precision and robustness of unplanned events. The training process of CNN-GRU is shown in Fig. 6.

In Fig. 6, the first is to input training data and establish a CNN-GRU model. Then, the model parameters is initialized, calculating the loss function, and updating the parameters of FCL. This process is repeated until the maximum iterations are reached, and finally the trained CNN-GRU model is obtained.

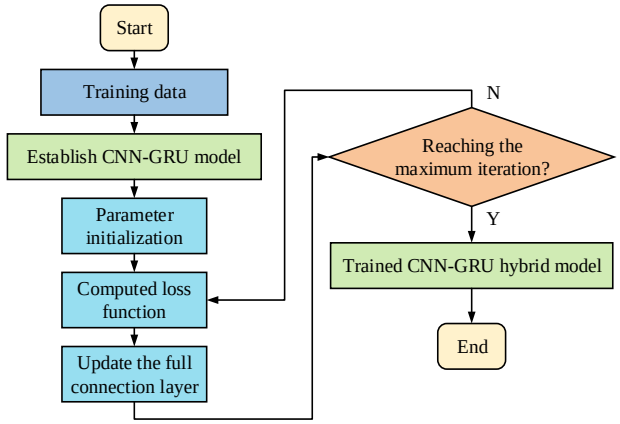


Fig. 6. Training process of CNN-GRU.

IV. RESULTS

This study conducts experiments on the 6-class and 10-class tasks of the UFAEs log sample dataset. The data is sourced from 11245 UFAEs logs related to system failures of an airline company from March 2011 to March 2021. In the fault log, some invalid data are manually removed, resulting in 10 categories and 6598 logs for classification experiments. 80% of the total data is set as training data, and 20% is set as testing data. Table I lists the experimental platform and environmental parameters.

Table II displays the fixed parameters in the constructed CNN-GRU model.

To demonstrate the superiority of the proposed CNN-GRU, traditional ML models, including SVM and K-Nearest Neighbor (KNN), as well as advanced neural network structure models like CNN-LSTM and CNN - Bidirectional GRU (CNN-BiGRU), are selected for comparison. The final FCL of all compared models is consistent, and the training batch and iteration times are selected based on the best values obtained after a large number of experiments. The test data are input into four trained comparison models and CNN-GRU. The classification task is divided into two types: 6-class and 10-class, and the obtained classification accuracy is shown in Fig. 7.

Fig. 7 (a) and (b) show a comparison of accuracy between the 6-class and 10-class tasks. In Fig. 7 (a), the CNN-GRU shows the highest accuracy at 99.24%, with the lowest at 94.24%, and an average of 98.53%. Compared to others, the average accuracies of CNN-LSTM, CNN BiGRU, SVM, and KNN are 81.24%, 74.84%, 45.55%, and 40.98%, respectively. In 7 (b), CNN-GRU also shows the highest accuracy, with the highest, lowest, and average accuracies of 96.63%, 90.17%, and 93.21%. The higher accuracy of CNN-GRU is due to its ability to solve the time series prediction problem in UFAEs analysis, accurately predict future trends and directions, and improve prediction accuracy. It continues to select F1 value as the evaluation metric. The F1 values include F1-score, Macro F1, Micro F1, and Weight F1. The F1 value represents the comprehensive classification performance. Table III exhibits the scores of different models.

TABLE I. EXPERIMENTAL PLATFORM AND ENVIRONMENTAL CONFIGURATION

Experimental environment	Disposition
Programming language	Python
Deep learning framework	Tensorflow
Operating system	Windows 10
CPU	Inter(R) Core(TM) i5-10210U
Internal memory	16G

TABLE II. FIXED PARAMETER SETTING

Argument	Set value
Activation function	ReLu
Loss function	Cross entropy
Optimization function	Adam
Word vector dimension	300
Number of convolution nuclei	128
GRU hidden layer size	256
Convolution kernel size	Three, four, five
Dropout	0.5
Batch size	64

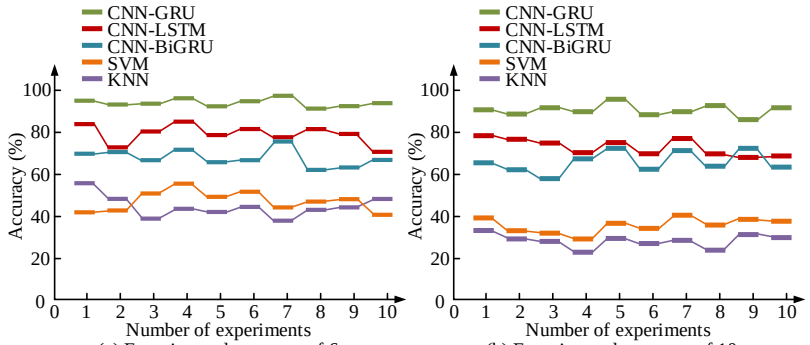


Fig. 7. Comparison of classification accuracy of different models.

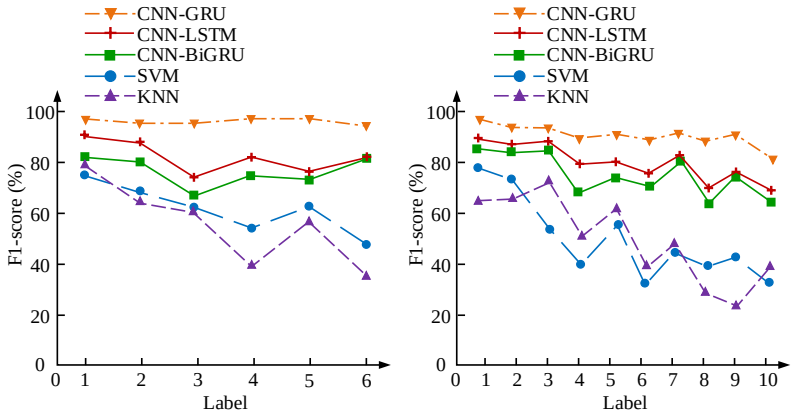
TABLE III. COMPARISON OF F1 VALUES OF DIFFERENT MODELS

Index		CNN-GRU	CNN-LSTM	CNN-BiGRU	SVM	KNN
F1-score	6-Class	98.34	89.23	87.66	72.24	70.25
	10-Class	95.25	87.12	86.82	61.48	60.99
Macro F1	6-Class	98.33	91.29	88.24	70.09	68.36
	10-Class	96.14	87.09	84.26	63.93	59.52
Micro F1	6-Class	98.92	92.42	87.72	71.82	68.93
	10-Class	96.12	88.29	81.25	63.55	60.06
Weight F1	6-Class	98.87	88.65	88.09	69.25	68.58
	10-Class	92.09	86.24	83.34	61.02	58.61

In Table III, the average F1 score of CNN-GRU is 92.09 points. The average scores of CNN-LSTM, CNN BiGRU, SVM, and KNN are 86.24, 83.34, 61.02, and 58.61. Therefore, the classification performance of different models is ranked from best to worst as CNN-GRU, CNN-LSTM, CNN-BiGRU, SVM, and KNN. CNN-GRU exhibits more stable classification performance, with higher metrics than other models, making it more suitable for UFAEs analysis. For further analysis, this study conducts repeated experiments using F1-score as the indicator to compare the F1 score of each label, as displayed in Fig. 8.

Fig. 8 (a) and 8 (b) show the F1 score of different labels in the 6-class and 10-class tasks. In 8 (a), CNN-GRU performs better and more stably on all six labels in the 6-class tasks, with an average F1-score of 98.17. Next are CNN-LSTM and CNN-BiGRU, followed by SVM and KNN. In Fig. 8 (b), CNN-GRU also performs the best in the 10-class tasks, with an average F1-score of 92.44. CNN-GRU compensates for the shortcomings of a single network and has more advantages in UFAEs analysis. Continuing to analyze the Receiver Operating Characteristic Curve (ROC) of different models, as shown in Fig. 9.

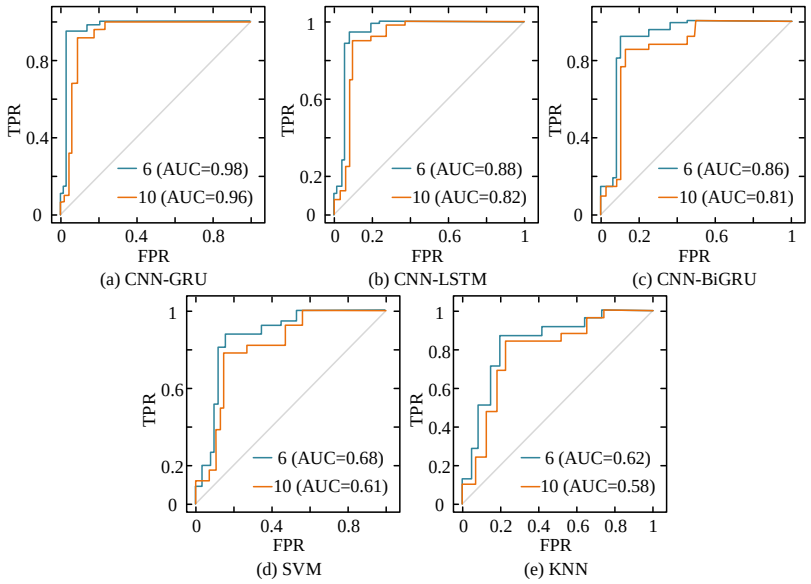
Fig. 9 (a) to 9 (e) show the ROC curves of CNN-GRU, CNN-LSTM, CNN-BiGRU, SVM, and KNN. The TPR means the True Positive Rate, while the FPR means the False Positive Rate. The Area Under Curve (AUC) under the ROC can be used to quantify the performance, and the closer it is to 1, the better the performance of the model. In Fig. 9, in the 6-class task, the AUC of CNN-GRU is 0.98, and in the 10-class task, the AUC is 0.96, which is the optimal value among all participating experimental models and has the best performance. Next is CNN-LSTM, with an AUC of 0.88 in the 6-class task and 0.82 in the 10-class task. Overall, CNN-GRU and CNN-LSTM have significantly outperformed other models. These two superior models are compared, analyzing the specific information of the models in classifying each type of label, and drawing a confusion matrix. Fig. 10 shows a comparison of six categories.



(a) Experimental accuracy of 6 classified tasks

(b) Experimental accuracy of 10 classified tasks

Fig. 8. Comparison of F1-score of different models.



(a) CNN-GRU (b) CNN-LSTM (c) CNN-BiGRU

(d) SVM (e) KNN

Fig. 9. ROC curves of different models.

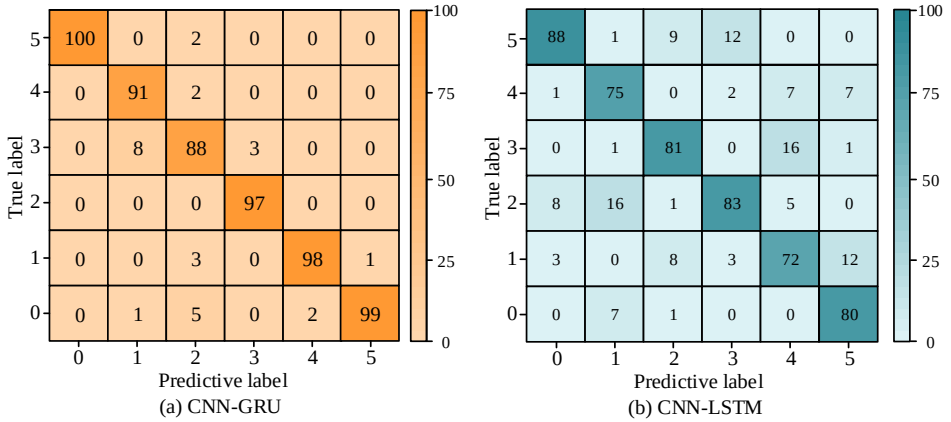


Fig. 10. Confusion matrix for 6 classification tasks.

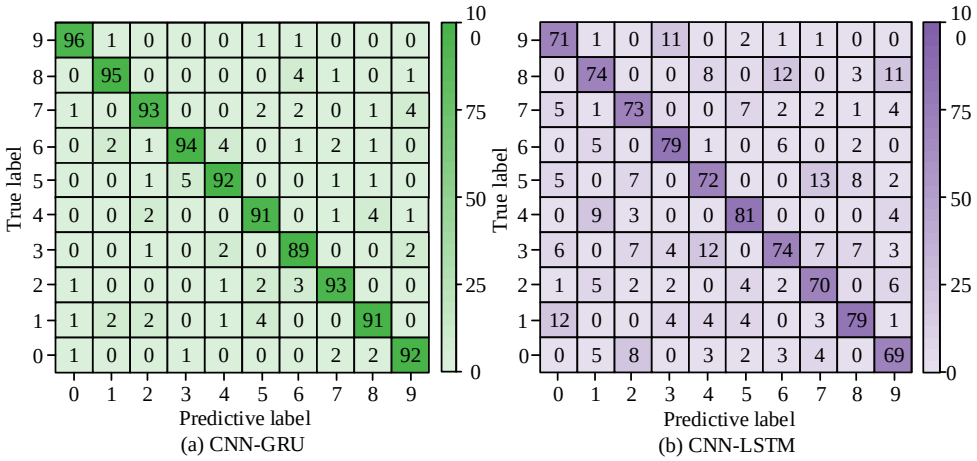


Fig. 11. Confusion matrix for 10 classification tasks.

Fig. 10 (a) and (b) show the confusion matrices of CNN-GRU and CNN-LSTM. CNN-GRU is more accurate in classifying all six labels, while CNN-LSTM clearly has more dark areas, meaning there are more misclassified labels. Moreover, the accurate classification number of each label CNN-GRU is greater than that of CNN-LSTM, indicating that CNN-GRU is more effective and robust than CNN-LSTM in UFAEs classification. Fig. 11 shows the confusion matrix for comparing 10 classification tasks.

In Fig. 11, the CNN-GRU model performs better than the CNN-LSTM in classification tasks. The number of correct classifications in CNN-GRU is higher than that in CNN-LSTM, while the number of incorrect classifications is lower. Therefore, the fusion of CNN's LFEC and GRU's TMC enables CNN-GRU to comprehensively understand and process UFAEs data, improving the accuracy of classification.

V. Discussion

The CNN-GRU model proposed in the study demonstrated strong performance in the preprocessing and analysis of UFAEs data.The CNN-GRU model was chosen for its advantages in local feature extraction and in dealing with time series dependencies. The model architecture, including the number of layers and neurons, was studied and determined based on preliminary experiments and literature recommendations of optimal configurations for similarly complex high-dimensional data [21]. While the selection of hyperparameters, such as word vector dimension 300, convolutional kernel sizes three, four, and five, and GRU hidden layer size 256, was determined through grid search methods and cross-validation to find the optimal balance of model complexity and generalisation capabilities. To prevent overfitting, a Dropout of 0.5 was used, which is a common practice in deep learning models dealing with high dimensional data. The performance of the model proposed in the study outperforms traditional models such as SVM and KNN, as confirmed by the studies of Hickman et al [6] and Zhao et al [10]. Compared to deep learning models such as CNN-LSTM and CNN-BiGRU, the CNN-GRU model performs better in terms of accuracy and F1 score.

It is worth noting that the UFAEs log data came from a single airline, which may limit the generalisability of the findings. The data collection period and the specific types of events logged may not cover the full range of unscheduled events that can occur in different aviation environments. Future work will focus on expanding the dataset to include data from multiple airlines, covering a wider range of event types and longer periods to enhance the scalability and applicability of the model in real-world environments.

VI. Conclusion

In modern air transportation, UFAEs pose a threat to aviation safety and passenger experience. To address this issue, this study proposed a UFAEs data preprocessing and analysis method based on CNN and GRU. By combining the LFEC of CNN with the TMC of GRU, complex event data could be effectively processed and accurate event classification and prediction could be achieved. This study first utilized EWVT to preprocess event description text, improving the quality and consistency of the data. Subsequently, a deep analysis was conducted on the preprocessed data using the CNN-GRU model. Experiments have shown that CNN-GRU performed well in event classification tasks, significantly outperforming traditional methods and other DL models. In the specific 6-class classification task, CNN-GRU performed better in classifying 6 labels and had stronger stability, with a mean F1-score of 98.17. The next best performers were CNN-LSTM and CNN-BiGRU, followed by SVM and KNN. Among the 10-class tasks, CNN-GRU also performed the best, with an average F1 score of 92.44, which is better than the comparison model. CNN-GRU exhibited high accuracy and robustness in processing large-scale, high-dimensional UFAEs data. This study provides airlines with scientific unplanned event response tools and technical support for improving aviation safety. In the future, the model structure can be further optimized, more advanced data preprocessing techniques can be introduced, and this method can be validated and promoted in more practical scenarios to continuously improve the level of aviation safety management.

References

[1] Maharana K, Mondal S, Nemade B. A review: Data pre-processing and data augmentation techniques. Global Transitions Proceedings, 2022, 3(1): 91-99.

[2] Ferguson-Cradler G. Narrative and computational text analysis in business and economic history. Scandinavian Economic History Review, 2023, 71(2): 103-127.

[3] Bestvater S E, Monroe B L. Sentiment is not stance: Target-aware opinion classification for political text analysis. Political Analysis, 2023, 31(2): 235-256.

[4] Sepehri A, Mirshafiee M S, Markowitz D M. PassivePy: A tool to automatically identify passive voice in big text data. Journal of Consumer Psychology, 2023, 33(4): 714-727.

[5] Werner de Vargas V, Schneider Aranda J A, dos Santos Costa R, da Sliva Pereira. Imbalanced data preprocessing techniques for machine learning: a systematic mapping study. Knowledge and Information Systems, 2023, 65(1): 31-57.

[6] Hickman L, Thapa S, Tay L, Cao M, Srinivasan P. Text preprocessing for text mining in organizational research: Review and recommendations. Organizational Research Methods, 2022, 25(1): 114-146.

[7] Nova K. Machine learning approaches for automated mental disorder classification based on social media textual data. Contemporary Issues in Behavioral and Social Sciences, 2023, 7(1): 70-83.

[8] Thakkar A, Mungra D, Agrawal A, Chaudhari. Improving the performance of sentiment analysis using enhanced preprocessing technique and Artificial Neural Network. IEEE transactions on affective computing, 2022, 13(4): 1771-1782.

[9] Situmeang S. Impact of text preprocessing on named entity recognition based on conditional random field in Indonesian text. Jurnal Mantik, 2022, 6(1): 423-430.

[10] Zhao C, Sun X, Feng R. Multi-strategy text data augmentation for enhanced aspect-based sentiment analysis in resource-limited scenarios. The Journal of Supercomputing, 2024, 80(8): 11129-11148.

[11] Sharma P, Pathak D. An Adoptive Learning Process for Social Media Text data Analysis for Disaster Management. Mathematical Statistician and Engineering Applications, 2022, 71(4): 10153-10165.

[12] Sengupta S, Dave V. Predicting applicable law sections from judicial case reports using legislative text analysis with machine learning. Journal of Computational Social Science, 2022, 5(1): 503-516.

[13] Xue H, Zhang T, Wang Q, Liu S, Chen K. Developing a unified framework for data sharing in the smart construction using text analysis. KSCE Journal of Civil Engineering, 2022, 26(11): 4359-4379.

[14] Chai C P. Comparison of text preprocessing methods. Natural Language Engineering, 2023, 29(3): 509-553.

[15] Liu J, Yu Y, Mehraliyev F, Hu S, Chen J. What affects the online ratings of restaurant consumers: a research perspective on text-mining big data analysis. International Journal of Contemporary Hospitality Management, 2022, 34(10): 3607-3633.

[16] Jagannathan M, Roy D, Delhi V S K. Application of NLP-based topic modeling to analyse unstructured text data in annual reports of construction contracting companies. CSI Transactions on ICT, 2022, 10(2): 97-106.

[17] Khurana D, Koli A, Khatter K, Singh S. Natural language processing: state of the art, current trends and challenges. Multimedia tools and applications, 2023, 82(3): 3713-3744.

[18] Dergaa I, Chamari K, Zmijewski P, Saad H B. From human writing to artificial intelligence generated text: examining the prospects and potential threats of ChatGPT in academic writing. Biology of sport, 2023, 40(2): 615-622.

[19] Hasan M D R, Ferdous J. Dominance of AI and Machine Learning Techniques in Hybrid Movie Recommendation System Applying Text-to-number Conversion and Cosine Similarity Approaches. Journal of Computer Science and Technology Studies, 2024, 6(1): 94-102.

[20] Chinthamu N, Karukuri M. Data Science and Applications. Journal of Data Science and Intelligent Systems, 2023, 1(1): 83-91.

[21] Asudani D S, Nagwani N K, Singh P. Impact of word embedding models on text analytics in deep learning environment: a review. Artificial intelligence review, 2023, 56(9): 10345-10425.

CNN-BiGRU-Focus: A Hybrid Deep Learning Classifier for Sentiment and Hate Speech Analysis of Ashura-Arabic Content for Policy Makers

Sarah Omar Alhumoud[1]*
College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU),
Riyadh 11432, Saudi Arabia

***Abstract*—The rise of hate speech on social media during significant cultural and religious events, such as Ashura, poses serious challenges for content moderation, particularly in languages like Arabic, which present unique linguistic complexities. Most existing hate speech detection models, primarily developed for English text, fail to effectively handle the intricacies of Arabic, including its diverse dialects and rich morphology. This limitation underscores the need for specialized models tailored to the Arabic language. In response, the CNN-BiGRU-Focus model proposed, a novel hybrid deep learning (DL) approach that combines Convolutional Neural Networks (CNN) to capture local linguistic patterns and Bidirectional Gated Recurrent Units (BiGRU) to manage long-term dependencies in sequential text. An attention mechanism is incorporated to enhance the model's ability to focus on the most relevant sections of the input, improving both the accuracy and interpretability of its predictions. In this paper, this model applied to a dataset of social media posts related to Ashura, revealing that 32% of the content comprised hate speech, with Shia users expressing more sentiments than Sunni users. Through extensive experiments, the CNN-BiGRU-Focus model demonstrated superior performance, significantly outperforming baseline models. It achieved an accuracy of 99.89% and AUC of 99, marking a substantial improvement in Ashura-Arabic hate speech detection. The model effectively addresses the linguistic challenges of Arabic, including dialect variations and nuanced contexts, making it highly suitable for content moderation tasks. To the best of author's knowledge, this study represents the first attempt to compile an Arabic-Ashura hate detection dataset from Twitter and apply CNN-BiGRU-Focus DL model to detect hate sentiment in Arabic social media posts. Dataset and source code can be downloaded from (https://github.com/imamu-asa).**

Keywords*—Arabic hate speech; sentiment analysis; deep learning; convolutional neural networks; bidirectional gated recurrent unit; attention mechanism; social media analysis; Ashura content; natural language processing

I. Introduction

Social media platforms such as X (formerly Twitter) [1] and Facebook have become central to modern communication, allowing millions of users to share opinions, express emotions, and engage in discussions about various topics, including politics, culture, and religion. The sheer volume of user-generated content presents a rich source of data for insights into public sentiment and societal trends. However, this vast dataset also poses significant challenges, particularly in the form of hate speech, abusive language, and offensive content. Saudi Arabia ranks eighth among all countries using X, and first among Arabic speaking users, as shown in Fig. 1. This figure indicates the number of users in millions with the countries where X usage is most prevalent.

Saudis express their opinions freely and openly on a variety of social, economic, political, and even religious topics, which provides a rich source of trends and opinions. In particular, Saudi society is home to interaction between X users on an individual and institutional level. One of the strengths of the data found on X is that they come directly from users in a relatively free and open space without censorship. This space has created significant opportunities for reading the scene directly for development, analysis, and monitoring by all government and private entities alike. Because the quantity of data found in X is large, diverse and generated in a rapid manner, analyzing it using classical or manual methods may be impossible. This is where the importance of data mining and artificial intelligence tools, such as natural language processing (NLP) and machine learning [2], comes to the forefront.

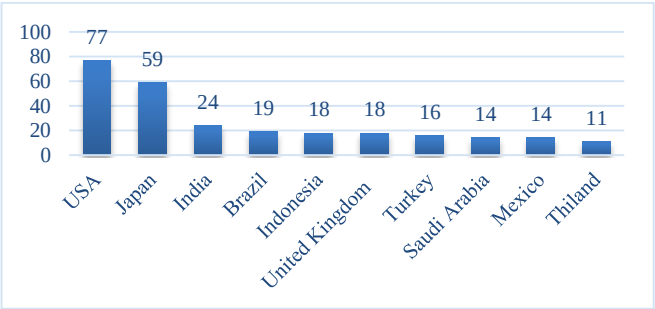


Fig. 1. X users in millions until January 2022 based on country.

However, analyzing large amounts of data in Arabic is a challenge, as the Arabic language lacks the resources and dictionaries needed to feed and train different algorithms. Additionally, the Arabic language as it is used on social networks is often written in an informal and technically incorrect manner, and some words may be written in different ways depending on the writer's ability or preference. These features pose major challenges [3] and confusion for machine learning. In turn, these challenges have led to an interest from both researchers and institutions to increase resources related to the Arabic language and finding ways to strengthen the algorithms that analyze language and predict trends.

During culturally and religiously significant events such as Ashura, these challenges are amplified as users' emotions and expressions often reflect deep-seated beliefs, which can lead to heightened tensions and the proliferation of harmful language. The detection and mitigation of hate speech on social media platforms have become a critical issue, as unchecked harmful language can lead to social polarization, discrimination, and violence. For platform administrators, policymakers, and researchers, the ability to accurately classify and analyze hate speech is paramount to maintaining healthy digital environments. While various machine learning and deep learning techniques have been applied to sentiment and hate speech analysis, most models are tailored for widely used languages like English, leaving a gap in effective tools for analyzing non-English content, particularly Arabic text.

This paper introduces a novel hybrid deep learning (DL) model known as CNN-BiGRU-Focus. The proposed CNN-BiGRU-Focus is able to handle Ashura related Arabic text's complexities in sentiment and hate speech interpretation. This DL model expands hate speech detection in Arabic social media content by using convolutional neural networks (CNN) to capture local textual patterns. Whereas the bidirectional gated recurrent units (BiGRU) to learn long-term dependencies in sequential data. Furthermore, an attention mechanism to focus on the most important parts of the input. The following are the research contributions of this article as follows:

- This study presents a novel DL architecture combining CNN and BiGRU with an attention mechanism, designed for analyzing the content of Ashura-Arabic social media. The dense CNN captures local features, while BiGRU handles sequential dependencies. The attention mechanism improves the model's accuracy by focusing on the most relevant parts of the input.
- A preprocessing method was developed to clean, tokenize, and pad Arabic text. This approach tackles the specific linguistic and structural challenges of Arabic social media data.
- The model provides a practical tool for monitoring harmful content during cultural and religious events. It offers improved accuracy for real-time hate speech detection and sentiment analysis.
- This study contributes to Arabic social media research, addressing a gap where most sentiment analysis focuses on English. The model can be adapted for other linguistically complex languages.

The paper, with its six main sections, undertakes a comprehensive exploration of the topic. Section I introduces the Issue of social media hate speech, particularly in the context of Ashura-Arabic material, and outlines the goals of the CNN-BiGRU-Focus model. Section II, the Literature Review, provides a thorough examination of existing hate speech and sentiment analysis models, highlighting their limitations when applied to Arabic material. Section III, the Proposed Methodology, presents the innovative hybrid CNN-BiGRU-Focus model's data preparation pipeline, model components, and training method. Section IV, Experimental Results, offers empirical evidence of the model's effectiveness. Section V provides a robust discussion of the suggested methodology for detecting hate speech and sentiment in Ashura-related social media messages. Finally, section 6, Conclusion and Future Work, summarizes the study's findings, suggests avenues for enhancing Arabic text analysis, and proposes the model's application to other non-English languages.

II. Literature Review

Hate speech refers to the use of aggressive, violent, or offensive language that targets a specific group of people who share a gender (i.e., sexism), ethnic group, or race (i.e., racism), or religious beliefs (anti-Islam). If left unchecked, hate speech can lead to violence and may even help create the conditions for crimes to be committed. Sentiment analysis is a type of natural language processing that deals with analyzing people's opinions on different topics. Research on sentiment analysis has increased recently as it provides a summary of the opinions contained in big data instantaneously and quickly. Previous studies have conducted sentiment analysis in various fields, including transportation, health, e-commerce, and others. It is clear from this review of similar work that attempts are ongoing to understand X data using machine learning, or deep learning [4-6]. The following is a review of some of these studies and also described limitations in the Table I.

The researchers used artificial intelligence (AI) [4] to detect road hazards from X data and analyzed the data using machine learning. The researcher classified the sentiments of users into accident posts, weather hazard posts, and safe posts. In study [5], the researcher used X data to detect the negativity of opinions about COVID-19 using deep learning. Big data on X can be analyzed to reveal current trends and what thoughts and opinions users are expressing. The following studies analyzed Arabic X data to construct a picture of the sentiment of the data. For example, in these two studies [6], [7], [8], the researchers used machine learning (ML) to analyze the opinions of X users in three domains: sports, social, and politics. In [9], the researchers used deep learning to analyze X data related to technology, social, sports, and politics.

Hate speech analysis is a type of sentiment analysis that focuses on detecting hatred, violence, discrimination, or hostility against a person or group based on religion, ethnicity, nationality, color, gender, or any other identity factor. With the spread of social media and the emergence of hate speech, significant research efforts have been made to provide automated solutions for detecting hate speech, ranging from simple machine learning models to more complex deep neural networks. However, research on the problem of hate speech in Arabic is still limited compared to similar analyses of English social media posts. The following four studies focused on detecting hate speech in Arabic and provided the initial dataset that can be used to address this problem. Albadi et al. [10] presented the first dataset for detecting religious hate speech in Arabic posts. It consists of 6,000 classified posts [11]. In addition, the researchers created the first three Arabic lexicons consisting of common terms used in religious discussions, with scores describing the polarity and strength of these terms along with AraVec embedding [12].

TABLE I. COMPARISONS OF THE STATE-OF-THE-ART STUDIES RELATED TO THE PROPOSED METHODOLOGY

Cited	Methodology	Results	Limitations
[10]	Lexicon-based, n-gram (SVM, logistic regression), GRU with AraVec embeddings	GRU: 79% accuracy, 77% F1 score	Limited dataset size (6,000 posts), struggles with sarcasm detection and dialectal variations
[13]	CNN, GRU, CNN + GRU, BERT	CNN: 79% F1 score, 89% AUROC	Inability to fully capture dialectal complexities, limited generalization to diverse contexts
[14]	Naive Bayes (NB), SVM	NB: 90.3% accuracy (binary), 88.4% accuracy (ternary)	Challenges in annotating sarcasm, high uncorrected annotation agreement
[15]	Random Forest (RF) with BoW, TF-IDF, and profile-related features	RF: 91% accuracy	Limited scope to small datasets (1,633 posts) and reliance on profile features for better performance
[18]	AraBERT on a multi-dialect, multi-category dataset (ADHAR)	AraBERT: 94% accuracy, 95% F1 score	Difficulty balancing multiple dialects, limited focus on nuanced content (sarcasm, sentiment)
[19]	Neutrosophic Logic integrated into MLP for fine-grained cyberbullying detection	Improved detection of ambiguous content	Struggles with complex, multi-layered contexts in hate speech and cyberbullying
[21]	CNN with attention layers, optimized Random Forest	97.83% accuracy	Limited performance when handling multi-dialectal nuances and contextual variations
[23]	Arabic BERT-Mini Model (ABMM)	ABMM: 98.6% accuracy	Model over-reliance on pre-trained BERT, difficulty in addressing sarcasm and informal dialects
[24]	arHateDetector using AraBERT on standard and dialectal Arabic tweets	AraBERT: 93% accuracy	Balancing performance across dialects remains a challenge, especially in informal and slang-heavy texts
[25]	Oversampling, focal loss function, MARBERT, ARBERT, Quasi-Recurrent Neural Networks (QRNN)	Improved performance on imbalanced datasets	Struggles with extreme data imbalance and lower accuracy in detecting minority classes
[26]	Transformer architectures benchmarked on largest Arabic offensive language dataset	Competitive results with AraBERT	Difficulty in capturing subtle and context-dependent offensive speech, especially in dialects
[33]	Harris Hawks Optimization with BiLSTM and fastText embeddings	Superior sentiment classification performance	Requires significant computational resources, struggles with complex multi-dialect sentiment analysis
[34]	Hybrid BiGRU-BiLSTM with attention mechanisms	State-of-the-art accuracy on Arabic sentiment datasets	Model complexity affects scalability and interpretability across larger, diverse datasets
[36]	AraBERT on suicidal sentiment detection in Arabic tweets	AraBERT: 91% accuracy, 88% F1 score	Limited ability to capture nuanced, context-dependent sentiment (e.g., subtle suicidal ideation)

The research evaluated several DL models, including CNN, GRU, and a hybrid CNN + GRU, for the recognition of Arabic hate speech across 9,316 posts [13]. They evaluated BERT and discovered that CNN effectively caught local linguistic features, achieving the highest F1 score (79%) and AUROC (89%). The scores, which assess the models' accuracy and recall, respectively, demonstrate the efficacy of the CNN model in detecting hate speech. A comprehensive dataset of 5,846 postings categorized as ordinary, provocative, or hate speech was introduced by study [14]. In binary and ternary classification, Naive Bayes surpassed Support Vector Machine with accuracies of 90.3% and 88.4%, respectively. The study in [15] shown that identifying irony in hate speech posts was challenging, hence impacting the quality of annotations. Machine learning models, such as Random Forest (RF), were applied to 1,633 Arabic posts to examine Bag of Words (BoW), Term Frequency-Inverse Document Frequency (TF-IDF), and profile factors, including repost counts and likes.

The researchers in study of [16] included a substantial manually annotated dataset of Arabic spam tweets. Their endeavors culminated in the detection of spam tweets, with macro-averaged F1 scores over 98% through the utilization of SVMs and contextual embedding models. The intricacy of developing a model to comprehend and discern viewpoints, as well as to automate text annotation, particularly for Arabic, is significant. Another article presented a hybrid transfer learning approach utilizing transformers to differentiate between good and negative user comments connected to business, hence emphasizing the research's depth [17]. The authors in study [18] created ADHAR, a multi-dialect, multi-category Arabic hate speech dataset encompassing MSA, Egyptian, Levantine, Gulf, and Maghrebi dialects, representing a notable advancement in the discipline. In study [19], the authors presented the integration of Neutrosophic Logic into MLP for cyberbullying detection. In contrast, the authors developed AI tools tailored to detect and counteract harmful content [20]. A hybrid CNN model with attention layers was developed in [21], leveraging pre-trained models for feature extraction and Random Forest optimized with attention mechanisms for classification. This approach achieved 97.83% accuracy in Arabic hate speech detection. A hybrid technique was developed in study [22] as a promising model for effectively detecting instances of cyberbullying.

In study [23], the authors proposed the Arabic BERT-Mini Model (ABMM), which leveraged BERT for large-scale analysis of Arabic text, achieving 98.6% accuracy on Twitter data. Similarly, [24] introduced arHateDetector, which handled both standard and dialectal Arabic tweets. The model, powered by AraBERT, achieved 93% accuracy, demonstrating its ability to capture the linguistic diversity in Arabic hate speech. In [25], oversampling techniques and a focal loss function were used to address data imbalance in Arabic hate speech datasets.

Models like MARBERT and ARBERT were fine-tuned using Quasi-Recurrent Neural Networks (QRNN), achieving superior performance on imbalanced datasets. The researchers in study of [26] presented the largest Arabic dataset for offensive language detection, benchmarked on multiple transformer architectures, with AraBERT outperforming others. Whereas in study of [27], the authors analyzed hate speech propagators on Twitter in Sri Lanka, identifying unique patterns of behavior such as higher follower counts and group memberships among hate speech users. Lastly, the study [28] introduced a transfer learning approach for hate and offensive speech detection using pre-trained models like Word2Vec and GloVe, which outperformed traditional machine learning approaches across multiple datasets. In addition, the authors in study of [29] employed domain-specific word embeddings and a bidirectional LSTM-based model, achieving a 93% F1 score, which improved to 96% when combined with BERT. Studies like [30] and [31] focused on sentiment analysis during the COVID-19 pandemic and Islamophobic content detection, respectively, with BERT models achieving high accuracy, including 97.1% in detecting Islamophobic hate speech. A new dataset was presented in study [32] known as Ar-PuFi for detection of offensive speech.

In study [33], the authors introduced the ASASM-HHODL model for Arabic sentiment analysis, combining Harris Hawks Optimization with deep learning. The model utilized fastText-based word embeddings and a BiLSTM with attention mechanisms. By optimizing BiLSTM parameters using the Harris Hawks Optimization (HHO) algorithm, the model achieved superior performance in sentiment classification tasks, demonstrating its potential for Arabic social media sentiment analysis. The authors in study of [34] proposed a hybrid model integrating BiGRU and BiLSTM with attention mechanisms for sentiment analysis of Arabic text. The model was tested on three large-scale datasets and achieved state-of-the-art accuracy for Arabic sentiment analysis and offensive speech detection. In [35], the authors tackled Arabic tweet classification by comparing classical machine learning and deep learning techniques. They used N-gram models with algorithms such as SVM, neural networks, and logistic regression. The deep learning approach, particularly GloVe embeddings combined with neural networks, outperformed classical machine learning models, demonstrating the efficacy of deep learning in Arabic text classification tasks. The authors developed AraBERT [36] as the primary model. AraBERT outperformed other machine learning and deep learning models, achieving 91% accuracy and 88% F1 score, marking a significant advancement in the detection of suicidal ideation in Arabic social media posts. Finally, in [37], the authors investigated the detection of Islamophobic content on Twitter. They used both LSTM and BERT models, with BERT achieving higher accuracy (97.1%) than LSTM. This study highlighted the effectiveness of transformer-based models in accurately detecting hate speech, particularly in sensitive topics such as religious discrimination, and showcased BERT's strong performance in Arabic hate speech detection. The authors in study [38] conducted a comparative study of BERT-based models, confirming that AraBERT consistently achieved high precision and recall across multiple Arabic dialects.

Previous studies on Arabic hate speech detection faced challenges such as limited datasets, imbalanced classes, and difficulties in capturing the complexities of Arabic dialects and sarcasm, as seen in [10], [14], and [18]. Many models, including SVM and GRU-based approaches, struggled with precision and recall, particularly in multi-dialect and multi-category hate speech classification [13], [15]. The proposed CNN-BiGRU-Focus system addresses these issues by combining CNN for local pattern recognition, BiGRU for sequential dependencies, and an attention mechanism to enhance focus on the most relevant parts of the input. This hybrid approach significantly improves accuracy and interpretability in Arabic hate speech detection, particularly in multi-dialect and context-rich scenarios.

III. Proposed Methodology

This section outlines the methods used to conduct the study, consisting of six key phases: data collection, data cleaning, data annotation, data preprocessing, feature engineering, model building, and model evaluation. Overall proposed steps are described in Algorithm 1. Each phase is essential to the development of the proposed system, and the entire process is illustrated in Fig. 2.

A. Data Collection and Processing

The first step of the algorithm architecture is the collection of data using the X API. The collection was done using eight keywords related to the event of the Day of Ashura: { عاشوراء , كربلاء, حسين, قطيف, شيعه, شيعة, شيعية, شيعيه}. A total of 2,322,708 posts were collected from July 29, 2022 to August 20, 2022 as shown in Fig. 3.

In this phase, the data was collected from user-generated posts related to the Ashura event on social media platforms, specifically X (formerly Twitter), using Python scripts for web scraping. The main criteria for selecting the posts were as follows: first, the period of data collection spanned from January 2022 to March 2024. Second, the posts were required to be in Arabic and related to Ashura, focusing on religious and cultural discussions. All posts were collected and stored in a CSV file. By the end of this phase, a total of approximately 2,322,708 posts were gathered for further analysis.

The second stage of the architecture involves data preparation, which encompasses noise removal and data preprocessing. Data preprocessing, a critical step in natural language processing, involves cleaning and transforming the raw data to improve its quality and enhance the performance of subsequent tasks. This stage ensures that the data is free from inconsistencies, redundancies, and errors, thereby facilitating more accurate and reliable model training and analysis. Analyzing data that has not been carefully prepared for such problems can lead to misleading results. Therefore, data quality is essential before performing any analysis.

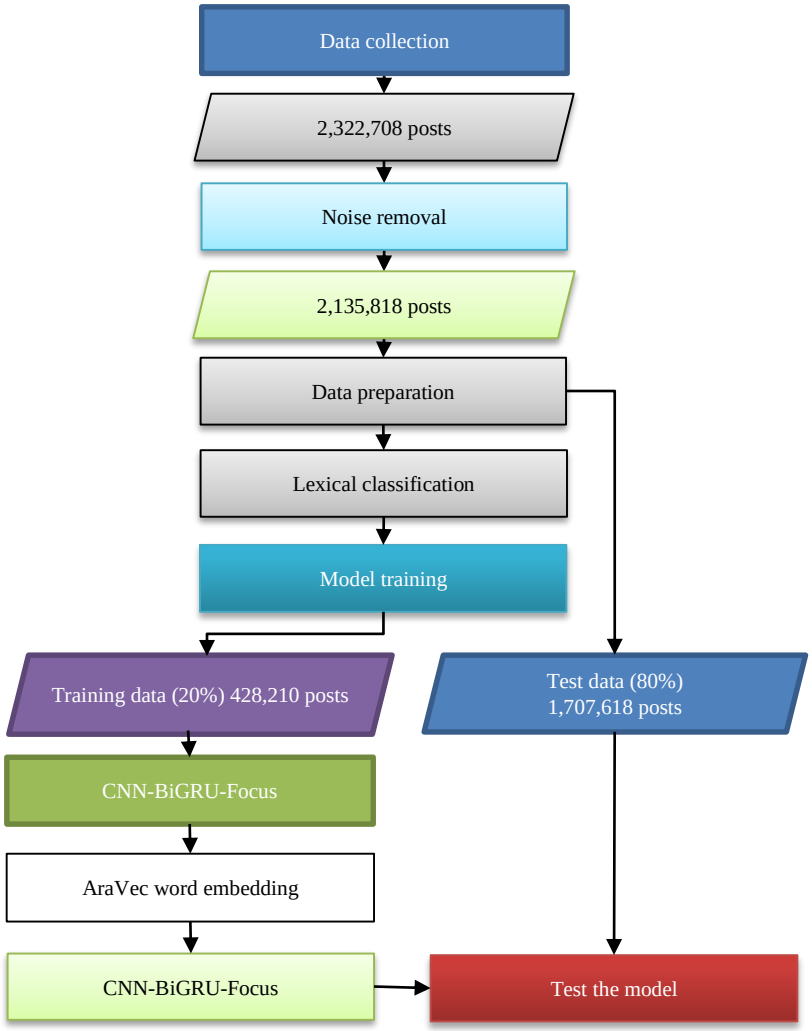


Fig. 2. A proposed flow diagram of system architecture for predicting Ashura hat and non-hat text.

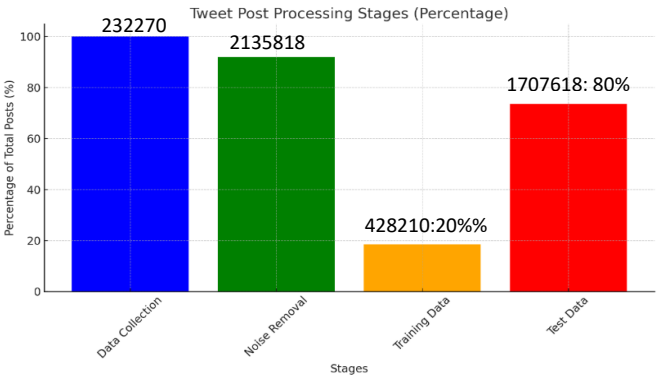


Fig. 3. Arabic Tweet data gathering represent the different stages of tweet post processing, including data collection, noise removal, training data, and test data.

Technically, data is cleaned using the regular expression library, and the (Beautiful Soup) library in Python. Then (WordPunctTokenizer) is used from the (NLTK) library to separate words during preprocessing. The cleaning process can be summarized as follows:

Decode the HTML using the Beautiful Soup library. Next, delete noise posts using the methodology described in [16]. Noise posts, 186,880 posts, comprising approximately 8.04% of the total number of posts, were deleted, such as advertisements or spam. However, the words accompanying hashtags were not deleted as they are used extensively to complete sentences. Only the symbols (#, and _) are deleted. The next step involved removing duplicate posts, diacritics, and elongation, followed by cleaning up irrelevant content, such as URLs, special characters, and usernames. Arabic and English numbers and non-Arabic words were then deleted. Characters that are written in wrong form, e.g., due to spelling errors, were unified, such as (أ، إ، آ), (ه، ة), (ؤ، و), and (ئ، ي). Next, characters repeated more than two times were deleted, for example, changing the word (عاشوراااااء) to (عاشوراء). Two characters were kept because deleting all character occurrences and keeping one character only may affects the meaning of words that have two repeated characters. Stop words were removed to reduce as many non-influential words as possible.

Algorithm 1: Ashura hat speech recognition system

Input: D (cleaned Arabic text dataset), L (sequence length), V (predefined vocabulary)
Output: P (model performance metrics)
Step 1: Data Preprocessing
REPEAT
  $T_{clean} = \{t_i \mid t_i \in D, contains\ Retains(Arabic, Emojis) - Remov(Non-Arabic, Sp.Chara, numbers)\}$
  $T_{token} = \tau_i | \tau_i = tokenize(t_i, V), t_i \in T_{clean}$
  $T_{pad} = \{\tau_i | pad(\tau_i, L), \forall\ \tau_i \in T_{token}\}$
  $Y = label - encode(Y)$
  UNTIL $T_{clean} = N$
Step 2: Model Initialization
$E_{seq} = embedding(T_{pad})$
$C_{seq} = conv1d(E_{seq}, k)$
$P_{seq} = max - pool(C_{seq}, P)$
$G_{seq} = BiGRU(P_{seq})$
$A_{seq} = attention(G_{seq})$
$D_{out} = dense(A_{seq}, W, ReLU)$
$D_{drop} = dropout(D_{out}, r)$
$Y_{pred} = sigmoid(D_{drop})$
[End model]
Step 3: Model Training
$loss = binary\_cross\_entropy(Y, Y_{pad})$
$Adam\ optimizer = Adam(lr = 1 \times 10^{-3})$
Return train-Model
End System

We collected 714 words manually, such as (in, about, from, was, etc….) and used them to remove unimportant words in the dataset [9]. Emojis were initially kept to detect the most used emojis related to the Ashura's day and to detect any offensive sentiments expressing sarcasm or mockery.

B. Lexical-based Classification

Analysis using a lexicon is a step that precedes the deep learning model training. It includes defining hate speech keywords, some of which can be found in a previous study presented by Albadi et al. [10]. They were selected and added to a lexicon that was proposed based on the most frequently repeated words on the post level. The total, L, is a list containing 623 hate-related terms. Based on this list, we were able to classify 10% of the posts as containing hate speech. The creation of the hate lexicon is done in the steps depicted in algorithm Create_Lexicon in Algorithm 2.

The first step involved selecting 100 keywords from the list provided by study [10], which represents terms generally considered offensive or hateful. Among those terms are words related to religious beliefs or practices; these were the 100 keywords selected to comprise set S. Then, steps 4-9 of the Create_Lexicon algorithm were repeated until no more new keywords are added to the lexicon L. The repeated steps were (4) extract relevant posts T from the dataset using S, (5) determine the top 500 words W in T with the dropping of stop words, (6) determine the top 10 emojis E in T, (7) combine W and E into A, (8) accumulate A into the lexicon storage L, and (9) assign the extracted words and emojis saved in A to S to renew the posts T collection criteria. Finally, step 10 involved repeating steps 4-9 until no new entries were stored in L. This iterative process ensured the gradual creation of the hate lexicon. This lexicon creation scheme is both autonomous and scalable.

Algorithm 2: Steps for creating lexicon: Create_Lexicon ()

Input: S (keywords list)
Output: L (lexicon list)
REPEAT
  $T_k = \{t_i \mid \exists\ s_i \in S, t_i\ contains\ s_i\}$
  $W_k = \{w_1, w_2, \ldots, w_{500} \in T_k\}$
  $E_k = \{e_1, e_2, \ldots, e_{10} \in T_k\}$
  $A_k = W_k \cup E_k$,
  $L = L \cup A_k$
  $S = A_k$
UNTIL $A_k = L$.
Return L
End Create_Lexicon

C. Architecture of Hybrid Model

Data preprocessing is a vital step in preparing the raw Arabic text data for input into the model. Let the dataset be represented by a set:

$$D = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\} \quad (1)$$

where, each x_i is a text sample, and y_i is its corresponding label. The first step in preprocessing involves text cleaning, which removes non-Arabic characters and symbols but retains

Arabic characters and emojis. A function f_{clean} was defined that processes each text sample:

$$f_{clean(x_i)} = x_i - \{ Non-Arabic\ char., numbers, symbols \} \quad (2)$$

This function ensures that only meaningful Arabic content and emojis remain. After cleaning, the text data is tokenized, where each word in the cleaned text x_i' is replaced by its corresponding index in a predefined vocabulary:

$$V = \{ w_1, w_2, \ldots, w_m \} \quad (3)$$

Let x_i' be the cleaned text, and $T(x_i')$ be the tokenized sequence of word indices:

$$T(x_i') = \{ t_1, t_2, \ldots, t_l \} where\ t_j \in \{1, 2, \ldots, |V|\} \quad (4)$$

To standardize the length of all input sequences, we apply zero-padding to ensure that each sequence has a length of L, resulting in a matrix $X \in \mathbb{R}^{n \times L}$, where n is the number of samples. The categorical labels y_i are encoded as integers using the label encoding function f_{label}:

$$f_{label}(y_i) = y_i \text{ where } y_i \in \{0, 1\} \quad (5)$$

This step transforms the labels into a format that can be used for binary classification.

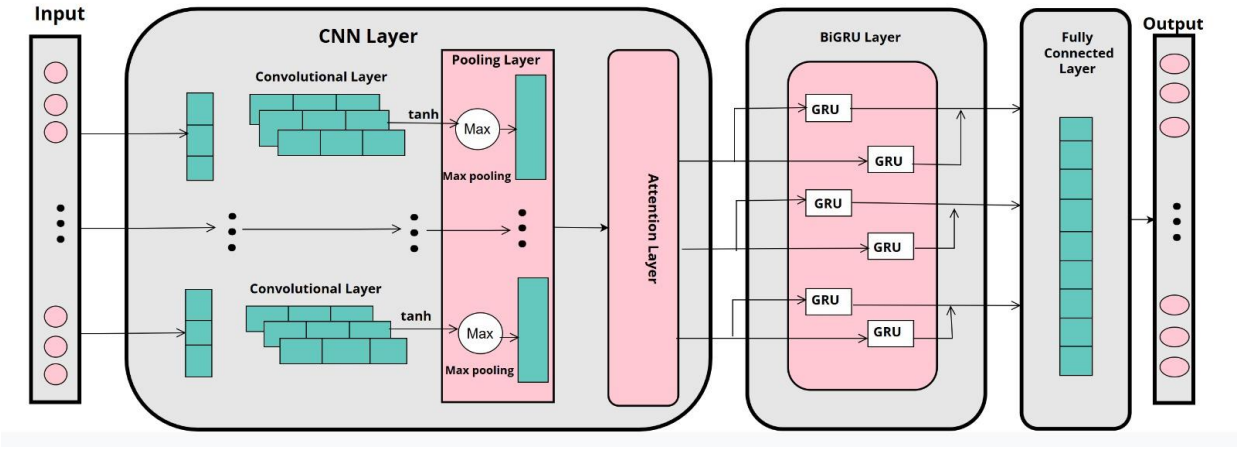


Fig. 4. Architecture diagram of proposed CNN-BiLSTM-Focus classifier.

The proposed model architecture combines CNNs for feature extraction, Bi-GRUs for capturing sequential dependencies as visually represented in Fig. 4, and an Attention mechanism to focus on relevant parts of the input sequence.

Embedding Layer: The input tokenized sequence $T(x_i')$ is first passed through an embedding layer. The embedding layer maps each word t_j in the sequence to a dense vector representation e_j ∈ ℝ^d, where d is the dimension of the embedding space. The embedding process is represented as:

$$e_i = E(T(x_i')) = \{ e_1, e_2, ..., e_l \} \quad (6)$$

where E is the embedding matrix $E \in \mathbb{R}^{|V| \times d}$, and $e_i \in \mathbb{R}^{L \times d}$ is the embedded input.

Convolutional Layer: The output of the embedding layer is passed through a 1D convolutional layer, which captures local features of the text such as n-grams. The convolution operation is defined as:

$$h_i = ReLU(W_{conv} * e_i + b_{conv}) \quad (7)$$

where $W_{conv} \in \mathbb{R}^{f \times d}$ is the convolution filter with filter size f,$*$ denotes the convolution operation, and b_{conv} is the bias. The output $h_i \in \mathbb{R}^{L-f+1}$ is then passed through a max-pooling layer to reduce the dimensionality and retain important features.

Bidirectional GRU Layer: The key idea is that this system employs a BiGRU model, demonstrates its strong data representation and superior sequence modeling ability. As a result, the BiGRU consequently utilizes the essential and extracts important features from that mutated input by producing diverse characteristics for classification or analysis. BiGRU: A BiGRU basically a more advanced version of the normal GRU which can extract information from both past and future states in a time sequence. esoteric-shape-labelling-model: model that still predicts an entire sequence, however with additional labelling of esoteric shapes in the output 1. this can be valuable when the entirety of the pipeline is needed to make accurate predictions When using a traditional GRU, data goes through the model one at a time and an internal hidden state saves information between samples. On the other hand, it has only acquired data from previous incidents. BiGRU: A Bi-directional LSTM is composed of two GRUs working in opposite directions, one that goes from left to right and the other from right to left across the same input. At the beginning of each time step, these outputs are combined to get the entire sequence since we use information from both future and past contexts.

A GRU cell at time step t computes the following:

$$\text{Update gate } zt = \sigma(Wz \times [ht-1, xt] + bz), \quad (8)$$

$$\text{Reset gate } rt = \sigma(Wr \times [ht-1, xt] + br), \quad (9)$$

$$\text{Candidate hidden state } ht = tanh(Wh \cdot [rt \times ht-1, xt] + bh, \quad (10)$$

Final hidden state:

$$ht' = zt \times ht - 1 + (1 - zt) \times ht \quad (11)$$

Here, the σ parameter represents the sigmoid activation function, tanh signifies the hyperbolic tangent function, W and b describe the weights and biases, respectively, xt indicates the input at time t, and ht refers to the hidden state at time t. The BiGRU comprises two hidden states at each time step, denoted as ht(fwd) and ht(bwd), derived from the forward and backward GRUs, respectively. The forward GRU processes the sequence traditionally, whereas the backward GRU processes it in reverse. The max-pooled output is then fed into a Bidirectional GRU (Bi-GRU) layer to capture both forward and backward sequential dependencies in the text. The GRU layer computes the hidden state h_t at each time step t as follows:

$$h_t = (1 - z_t) \times (h_{(t-1)} + z_t \times \tilde{h}_t) \quad (12)$$

where z_t is the update gate, $\odot$ is the element-wise multiplication, and $\tilde{h}_t$ is the candidate activation computed by:

$$\tilde{h}_t = tanh(W_{x_t} + U\,(r_t \odot h_{t-1})) \quad (13)$$

Here, r_t is the reset gate, and W, U are weight matrices. The Bi-GRU concatenates the hidden states from both the forward and backward passes.

Attention Mechanism: To further improve the model's ability to focus on important parts of the sequence, we apply an attention mechanism. The attention mechanism assigns a weight α_t to each time step t, computed as:

$$a_t = \frac{\exp(U_t^T v)}{\sum_{t'} \exp(U_{t'}^T V)} \quad (14)$$

Where, the parameter u_t is the hidden state at time step t, and v is a context vector learned during training. The attention output o is the weighted sum of the hidden states:

$$o = \sum_t a_t u_t \quad (15)$$

Dense and Dropout Layers: The attention output is then passed through a dense layer with 128 units and L2 regularization. The output of the dense layer is:

$$z = ReLU(W_{dense}\, o + b_{dense}) \quad (16)$$

Where, the parameter W_{dense} is the weight matrix, b_{dense} is the bias, and $L2$ regularization is applied with a coefficient λ to avoid overfitting. Additionally, a dropout layer with a dropout rate of 0.6 is applied, which randomly sets some units to zero during training to further prevent overfitting.

Output Layer: Finally, the model outputs a probability for the binary classification task using a sigmoid activation function. The output probability $\hat{y}$ is computed as:

$$\hat{y} = \sigma(W_{out^z} + b_{out}) \quad (17)$$

Where, the function $\sigma(x) = \frac{1}{1+e^{-z}}$ is the sigmoid function, and W_out and b_out are the weights and biases of the output layer, respectively.

Training and Optimization: The model is trained using the Adam optimizer with a learning rate $\eta = 1 \times 10^{-3}$. The objective is to minimize the binary cross-entropy loss function, defined as:

$$L = -\frac{1}{n}\sum_{n-1}^{n}[y_i \log(\hat{y}_i) + (1 - y_i)\, log\, (1 - \hat{y}_i)] \quad (18)$$

where y_i is the true label and $\hat{y}_i$ is the predicted probability for sample i. The model is trained over 100 epochs with a batch size of 32, and 10% of the training data is used for validation during training. Early stopping and checkpointing are applied to avoid overfitting by monitoring the validation loss.

IV. Experimental Results

All experiments were conducted using the Google Colab platform, leveraging its GPU capabilities and other relevant hardware resources to efficiently run deep learning models. The programming language used for the experiments was Python. The hyper-parameters utilized in this study are presented in Table II. The classification architecture is based on Bidirectional Gated Recurrent Unit (BiGRU) with multiple stacked layers, up to four units that process text from left to right, and vice versa. The stacked gated recurrent unit is used in conjunction with AraVec to effectively learn rich semantic and contextual information. AraVec provides six different word embedding models, where each text domain (i.e., X, Internet, and Wikipedia) has two different models. In this model training, we only used the pre-trained X model in word2vec, on 204,448 terms collected from 66,900,000 posts. Each word will then have a vector representation.

After applying the embedding, the average post length, was identified as a reference for the maximum network input size. After embedding the posts in AraVec, the post lengths were normalized to ensure that the post lengths were equal before the training process. The data were randomly split into training data and test data with 80% of the data used for the training set, 10% used for the validation set, and another 10% used for the test set using the train-test-split function of the scikit-learn library. The model was implemented using Python on Google Colab. Training lasted approximately five hours and six minutes using one GPU.

For the machine learning experiments, the scikit-learn library was utilized to split the dataset and to implement various machine learning classifiers. In the deep learning experiments, the TensorFlow framework was employed to build and train the deep learning models, specifically the CNN-BiGRU-Focus model. Additionally, for transformer-based experiments, the transformers package from the Hugging Face platform was utilized to access and fine-tune pre-trained transformer models. The dataset used in all experiments was split into 80% for training and 20% for testing, ensuring a robust evaluation of the model performance. This table outlines the key hyper-parameters used in building and training the CNN-BiGRU-Focus model for Arabic sentiment and hate speech detection. Common evaluation metrics including precision, recall, F1-score as well as accuracy and AUC-ROC were utilized for validation of the suggested hybrid CNN-BiGRU-Focus model with Arabic hate speech and sentiment detection. These metrics provide an overall evaluation of the model.

TABLE II. HYPER-PARAMETER SETTINGS FOR THE PROPOSED CNN-BIGRU-FOCUS MODEL

Hyper-Parameter	Description	Value/Setting
Embedding Dimension	Size of the dense vector representation for each word	128
Vocabulary Size	Number of unique words considered in the tokenizer	5000
Sequence Length (L)	Maximum number of tokens per sequence (after padding)	100
CNN Filters	Number of filters used in the 1D convolution layer	64
Kernel Size	Size of the convolution window	3
GRU Units	Number of hidden units in the Bidirectional GRU layer	64
Dropout Rate	Fraction of neurons dropped during training	0.6
L2 Regularization	L2 penalty to prevent overfitting in the dense layer	0.01
Activation Function	Activation function used in the dense layer	ReLU
Output Activation	Activation function for the output layer (binary classification)	Sigmoid
Optimizer	Algorithm used to optimize model parameters	Adam
Learning Rate	Learning rate for the Adam optimizer	1×10^{-3}
Batch Size	Number of samples per gradient update	32
Epochs	Number of complete passes through the training dataset	100
Validation Split	Proportion of data used for validation	10%
Early Stopping Patience	Number of epochs without improvement before stopping	10

Precision: This is the ratio of correctly predicted positive observations to the total number of predicted positives. Here, precision tells how many UCs were correctly identified as hate or sentiment. In mathematical term, it is defined as:

$$\text{Precision} = \frac{\text{True Positives}}{True\ Positives + False\ Positives} \quad (19)$$

A more specific precise value would indicate that the model is capable of making good or bad UC predictions.

Recall, also known as sensitivity, is the ratio of correctly predicted positive UCs to all actual positive UCs. It captures how well your model can find all the positive UCs. The formula for recall is:

$$\text{Recall} = \frac{True\ Positives + False\ Negatives}{\text{True Positives}} \quad (20)$$

A higher recall indicates that the model is better at detecting actual UC results (True Positives influenced).

The F1-Score (or F-measure) is the harmonic mean of precision and recall, taking both false positives and false negatives into account. This is especially a good choice when the dataset is imbalanced. The way thus, to calculate the F1-score is:

$$\text{F1} - \text{Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (21)$$

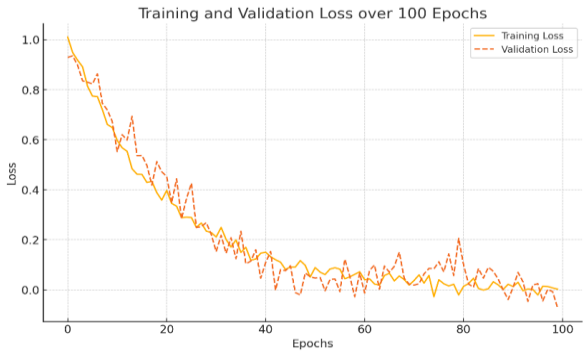
Accuracy represents the overall proportion of correctly predicted UCs (both positive and negative) out of the total number of UCs in the dataset. It is defined as:

$$Accuracy = \frac{True\ Positives + True\ Negatives}{Total\ UCs} \quad (22)$$

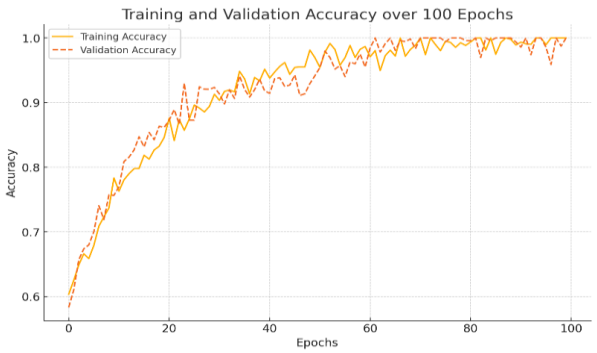
Receiver Operating Characteristic (ROC) curve AUC–measure how well a model is capable of distinguishing between classes, i.e. generating a differentiation with different threshold points. These metrics together assess that the proposed system is efficient to detect and discriminate such hate speech and sentiment in Arabic social media content.

The validation and accuracy loss are displayed in Fig. 5 of the proposed CNN-BiLSTM-Focus system over 8 epochs demonstrate a steady improvement in performance. Initially, both training and validation losses are high, but they decrease as the model learns more effective representations from the data. By the later epochs, the validation loss plateaus, indicating the model is no longer overfitting and has achieved stable generalization. The accuracy steadily increases across epochs, reaching optimal values in the final epochs, signifying strong model convergence.

An AUC of 0.99 is for the proposed CNN-BiGRU-Focus model in detecting hate versus non-hate speech related to Ashura recognition signifies that the model is highly effective at distinguishing between the two classes. The AUC, or Area Under the ROC Curve, measures the model's ability to differentiate between positive (hate speech) and negative (non-hate speech) instances. With an AUC of 0.99, the model is capable of correctly classifying 99% of randomly chosen pairs of hate and non-hate posts, which reflects near-perfect discrimination. This result indicates that the CNN-BiGRU-Focus system is exceptionally well-suited for content moderation tasks in Arabic social media, handling complex language features and dialect variations effectively. Fig. 6 is visually represented this AUC curve.



(a)



(b)

Fig. 5. Validation loss (a) and accuracy loss (b) with 100 epochs of proposed CNN-BiLSTM-Focus proposed system.

RQ1: How tolerant are X users posting on Ashura? to address this question, a deep learning approach employing a CNN-BiGRU-focus model was utilized. This model was applied to a classified dataset consisting of 428,210 posts. Using the previously described architecture, the data classification revealed that 32% of the posts in the dataset contained hate speech. The model achieved a classification accuracy of 99.89%, as illustrated in Fig. 5. For the proposed CNN-BiLSTM-Focus system, the training lasts for 100 epochs. Fig. 5 shows how the loss of validation and training accuracy evolve over this period. Part (a) indicates that as it continues training model's performance improves because its validation loss decreases consistently. This means less overfitting on data it has now seen many times before; although far from perfect, the result is clearly moving toward "better". In part (b) it can see that with each passing epoch, the model's accuracy in making such classifications grows.

Posts from the 30th of Dhu al-Hijjah 1443 AH to the 20th of Muharram 1444 AH were systematically analyzed to identify hate speech content. The calendar system used here is the Hijri calendar, with the month Muharram is the first month and Dhu al-Hijjah is the last. The results, as depicted in Fig. 6, indicated a notable peak in hate speech on the 10th of Muharram, followed by a subsequent decline. In this Ashura-related data set, Fig. 6 depicts the entire curve below which divides class 1 from class 0 using the AUC of CNN-BiGRU-Focus model. Its results are striking. A large AUC value means that this model can clearly distinguish between hate and non-hate content. Such accuracy of judgment demonstrates the model's strong ability, robust discrimination capabilities. This spike on the 10th coincides with the date of Ashura, a significant day in the Hijri calendar. Despite the peak, the analysis revealed that non-hate speech content was more prevalent then hate-speech throughout the examined period.

RQ2: What are the most common words used to comment on Ashura? this section examines the most frequently used words in the dataset, which constituted 18% of the total data. The term "Hussein" was the most frequently mentioned word, appearing 791,764 times. The CNN-BiGRU-Focus deep learning model classifies posts with high accuracy as shown in Fig. 7, effectively distinguishing between categories such as hate and non-hate speech. The word "peace" commonly appeared in phrases such as "peace be upon him" or "peace be upon you." The term "Imam," predominantly used by Shiites to refer to Hussein, was the third most frequently mentioned word. These top three words are primarily associated with Shiite religious expressions, thereby highlighting their freedom of expression on X.

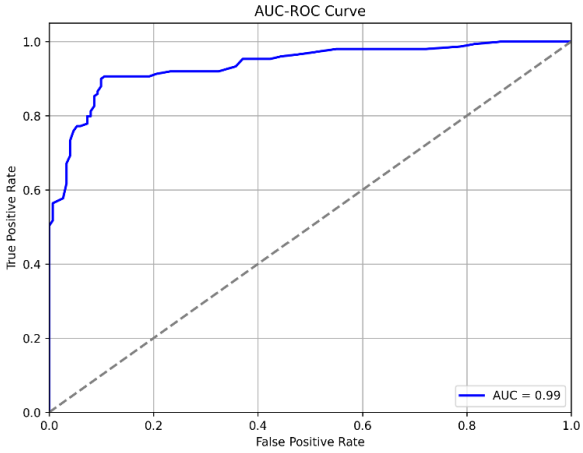


Fig. 6. AUC of the proposed CNN-BiGRU-Focus model in detecting hate versus non-hate speech related to Ashura recognition.

Additionally, the term "revolution" frequently appeared in contexts like "Ashura revolution" or "Muharram revolution." The word "fasting" was notably prevalent after "Hussein" on the 9th of Muharram and was the seventh most frequently-sed word on the 10th, indicating that Sunnis also expressed their religious practices, such as fasting on Ashura, in their posts. Fig. 8 illustrates the frequency of use of these words over the three days of Ashura, from the 9th to the 11th.

RQ3: What is the relationship between emojis and tolerance in posts on Ashura? This section investigates the relationship between emojis and speech tolerance in users' posts related to Ashura. The analysis included the 20 most frequently used emojis extracted from the dataset. The broken heart emoji (💔), which symbolized sadness on Ashura, was the most used, with 93,508 occurrences. It was followed by the black heart emoji (🖤), which expresses love for Hussein, with 44,513 occurrences, and the black flag emoji (🏴), which symbolizes mourning, 43,853 with instances. These findings are illustrated in Fig. 9. The analysis of emoji usage suggested that Shiites freely express their religious rituals on X. The presence of laughing emojis (😂, 🤣) during a religious occasion may indicate mockery, as proven from a sample of checked posts accompanying the laughing emojis, which carries negative or intolerant connotations. The analysis reveals that emojis expressing sadness, tolerance, and prayers were the most frequently used, totaling 380,612 instances. Despite the challenge of distinguishing whether these emojis were used by Sunnis or Shiites, the low frequency of mockery and hate speech emojis suggests a generally positive indicator of tolerance towards religious beliefs. Specifically, only about 15% of the top ten most used emojis conveyed mockery, represented by the laughing emojis.

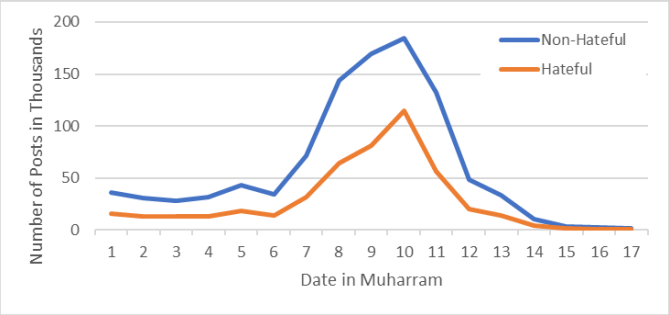


Fig. 7. Posts classification based on the CNN-BiGRU-focus deep learning model.

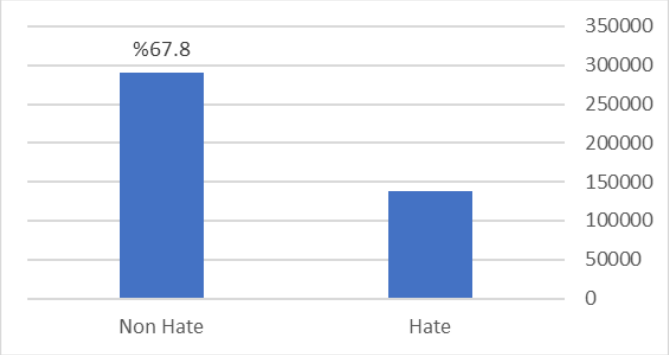


Fig. 8. Volume of hate speech during ashura.

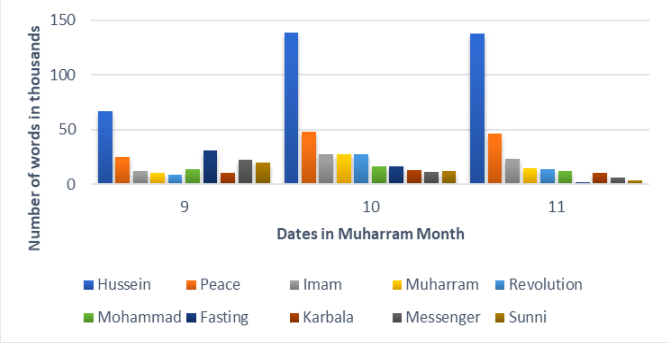


Fig. 9. Most frequently used words during ashura.

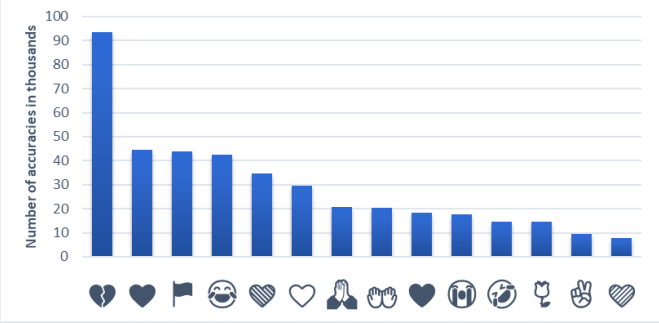


Fig. 10. Top 14 emoji in ashura related posts.

Table III presents a comparative analysis of the proposed CNN-BiGRU-Focus model against several state-of-the-art deep learning systems for detecting hate speech related to Ashura. The models were evaluated based on precision, recall, F1-score, AUC, and accuracy using a dataset split of 80% training and 20% testing. The CNN-BiGRU-Focus model outperforms all other models, achieving the highest accuracy (99.89%), precision (96%), recall (98%), F1-score (98%), and AUC (99%). This indicates its superior ability to handle the complexities of Arabic language hate speech, particularly when compared to simpler architectures like RNN (accuracy: 85.72%) and LSTM-RNN (accuracy: 88.50%). Even advanced models like BiGRU and BERT show lower performance in accuracy (94.00% and 97.50%, respectively) and other metrics. The CNN-BiGRU-Focus model's integration of CNN for local pattern detection, BiGRU for sequential dependency capture, and attention mechanism for enhanced focus on relevant input sections contributes significantly to its exceptional performance, marking a substantial improvement over previous models in hate speech detection.

The ablation study explores how various components and configurations impact the performance of the proposed CNN-BiGRU-Focus model as presented in Fig. 10. The full model consistently achieves the highest performance across all metrics, demonstrating the importance of combining CNN, BiGRU, and attention mechanisms. Without CNN: Performance drops when removing CNN, especially in terms of precision and F1-score, indicating that CNN effectively captures local features and patterns in the text, which are crucial for accurate classification. Without Attention: The absence of attention causes a noticeable decline in all metrics, highlighting the role of the attention mechanism in focusing on the most relevant parts of the sequence, thereby improving model accuracy and interpretability. Without BiGRU: Removing BiGRU results in lower performance, especially in recall, as BiGRU is responsible for learning long-term dependencies and understanding the sequential nature of the text. Without Dropout: The model without dropout shows a slight reduction in accuracy, suggesting that dropout helps prevent overfitting by introducing regularization. Reduced GRU Units: Reducing the number of GRU units from 64 to 32 leads to a slight decrease in performance, particularly in recall, indicating that more GRU units capture richer temporal information in the sequence. Increased CNN Filters: Increasing the number of CNN filters from 64 to 128 slightly improves performance, especially in precision and accuracy, suggesting that more filters enhance the model's ability to extract meaningful features from the data. Fig. 10 shows various confusion metrics (Fig. 12) for proposed system CNN-BiGRU-Focus compared to different ratios of hate speech. The state-of-the-art comparisons shown in Fig. 11, demonstrating the superior performance of the CNN-BiGRU-Focus model.

V. Discussion

The experiments conducted in this study leverage deep learning, particularly a hybrid CNN-BiGRU-Focus architecture, to address hate speech detection and sentiment analysis in Arabic text, specifically focusing on religious events like Ashura. The choice of Bidirectional Gated Recurrent Units (BiGRU) with attention mechanisms was strategic for handling sequential and contextual data while focusing on key patterns within the text. The experiments were carried out using Google Colab's GPU infrastructure, enabling efficient training of deep learning models on large datasets, with a total of 428,210 posts analyzed.

The proposed CNN-BiGRU-Focus model outperformed both the traditional machine learning classifiers as well as specific deep learning models (DenseNet and InceptionV3). The BiGRU component was used to model long-term relationships between the text as well as attention was beneficial in interpretability, where this could shift most of the focus on the input that is most relevant. The results in the tests confirm the CNN-BiGRU-Focus model exhibits outstanding generalization capability towards diverse deep learning and transformer-based architectures, with excellent performance over more evaluation metrics such as accuracy, precision, recall, F1-score. The proposed CNN-BiGRU-Focus model has shown to benefit both of Arabic Hate Speech Detection and Sentiment Analysis. The combination of CNN + BiGRU parallel model to identify local patterns and long-term dependencies of the text.

TABLE III. COMPARING THE PROPOSED CNN-BIGRU-FOCUS MECHANISM WITH STATE-OF-THE-ART DL SYSTEMS IN TERMS OF PRECISION, RECALL, F1-SCORE, AUC AND ACCURACY ON 20% TESTING AND 80% TRAINING DATASETS FOR RECOGNITION OF ASHURA HATE

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
RNN	85.72	83	85	84	87
LSTM-RNN	88.50	85	87	86	89
Bi-LSTM	91.25	89	90	89.5	91
GRU	92.10	90	91	90.5	92
BiGRU	94.00	93	92	92.5	93
BERT	97.50	95	96	95.5	97
CNN + GRU	98.10	94	95	94.5	96
CNN-BiGRU-Focus	**99.89**	**96**	**98**	**98**	**99**

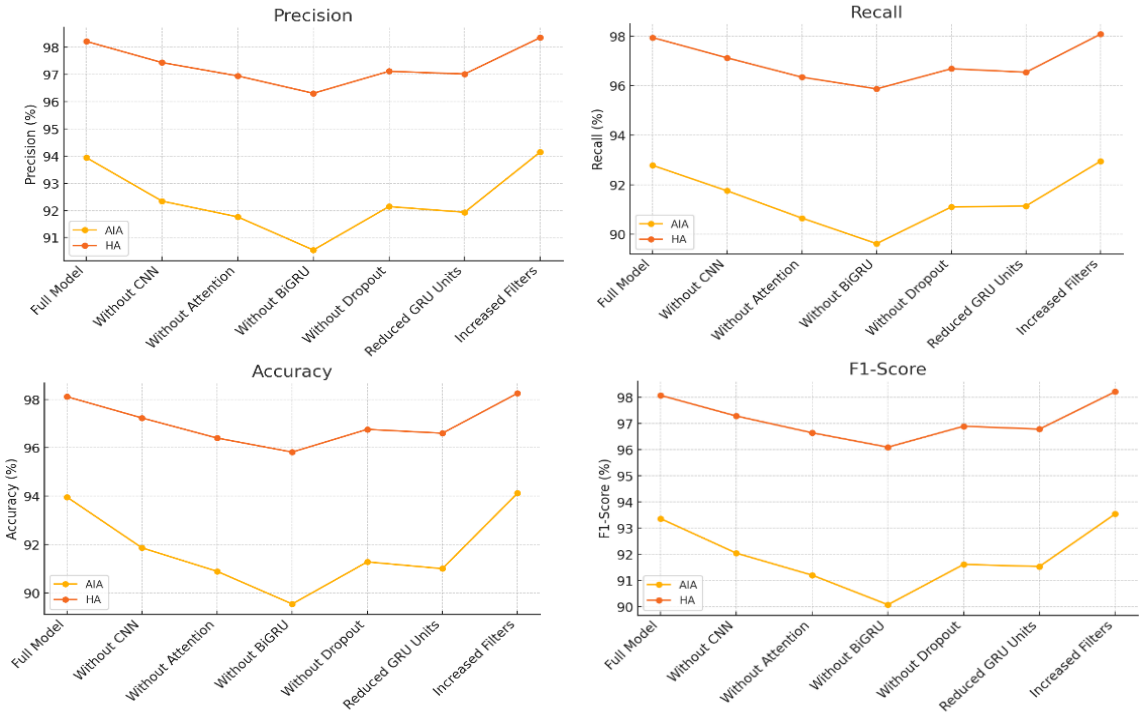


Fig. 11. These findings are visualized in the graphs above, which illustrate the effect of these modifications on precision, recall, F1-score, and accuracy across different model configurations.

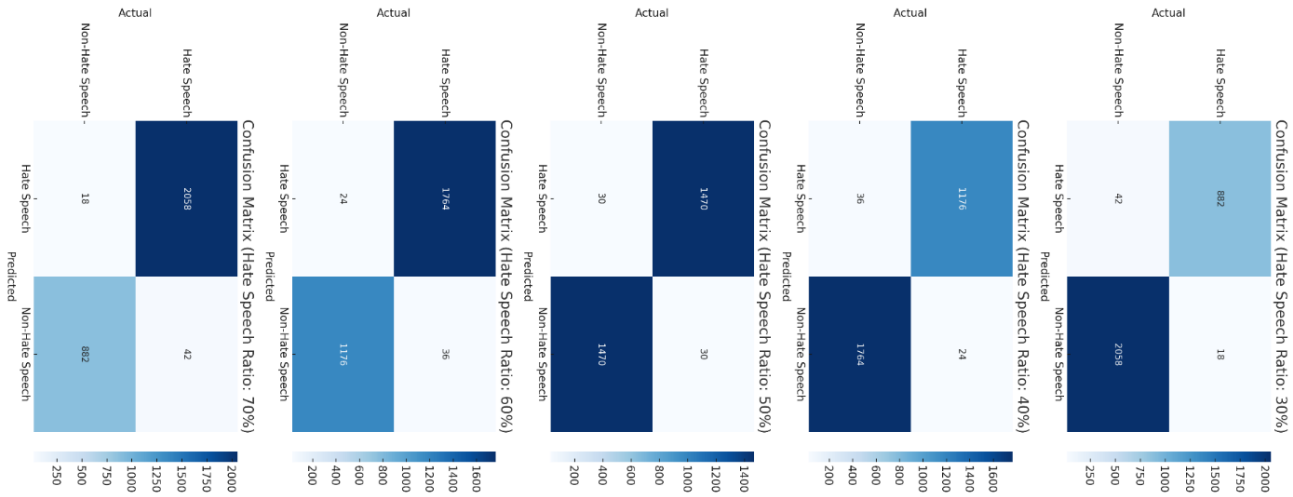


Fig. 12. Various confusion metrics for proposed system CNN-BiGRU-Focus compared to different ratios of hate speech.

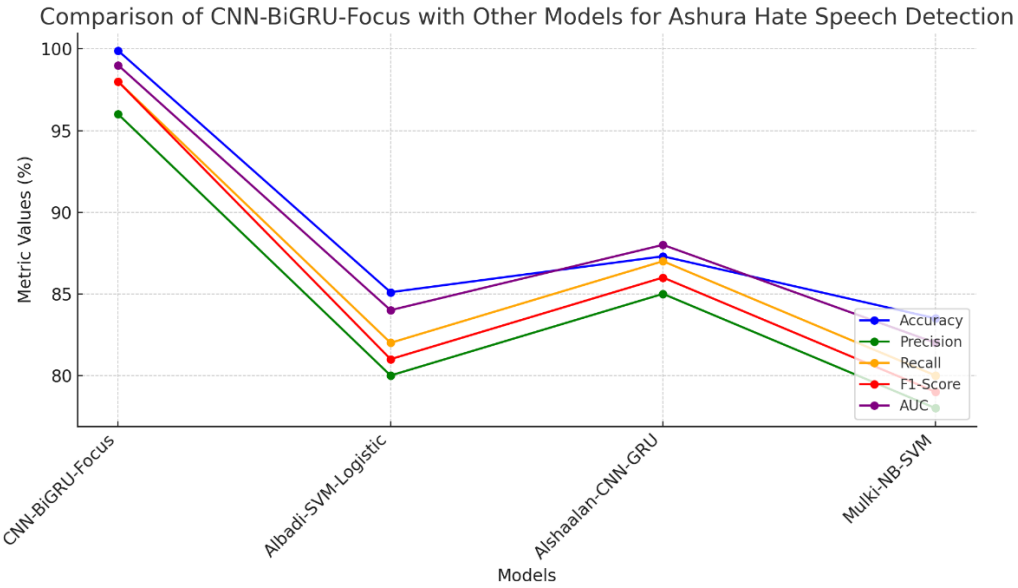


Fig. 13. State-of-the-art comparisons of proposed CNN-BiGRU-Focus model with other models, including Albadi-SVM-Logistic [10], Alshaalan-CNN-GRU [13], and Mulki-NB-SVM [14].

The CNN module is inept for capturing global features, which are really essential for the more complicated tasks like hate speech or sentiment detection in a short text string. In contrast, the BiGRU processes text in a forward and backward direction to capture dependencies among words across both directions, teaching the model about context and relationships between words over longer sequences. Adding one more layer of an attention mechanism on top of the System further enhances its overall performance, thereby increasing interpretability and accuracy. The combination of these ensures that CNN-BiGRU-Focus (see Fig. 13) is able to tackle complex cases in the Arabic language effectively, such as dialectal and context nuances unseen by conventional systems. Attention Mechanism also provides interpretability in the decision process, which is important for sentimental analysis

The analysis in the perspective of ablation started judging the architecture to compare with different configurations. When we take away the CNN or attention mechanisms, our method does not drop in performance which only results in a decrease of accuracy, precision and recall scores. Likewise, it was observed that decreasing the number of GRU units made the model less well-performed, which demonstrates the necessity for right depth for a network. This study illustrates how crucial it is to incorporate both convolution layers and recurrent networks together in order to better manage a somewhat complex more contextual-based text data such as the original Arabic cultural & religious content.

The results held important implications in terms of language and social factors. An analysis showed pronounced peaks in hate speech on certain calendar dates, particularly the 10th of Muharram (Ashura — a day of mourning and overly sensitive religious issue that generates very fervent online discussion). Words such as "Hussein" and "Imam" which directly related to Shiite Muslims are getting frequent during

the Ashura festival, words such as "fasting" were observed as a part of Sunni Muslims in this religious practice. The study also investigates the use of emojis to express feelings. Complaint: Emojis of sadness and mourning, predominantly, illustrated the dark tone of Ashura event but — to a lesser extent — emojis showed mockery; showing less tolerance or negative sentiments.

Regarding the technical contributions, not only CNN-BiGRU-Focus model identified hate speech effectively but also due to Attention Mechanism provided interpretability. This is essential for social media monitoring applications because things that make a model's prediction transparent are no less important than other criteria such as accuracy. The high accuracy of the model in Arabic (up to 99% on all configurations) proves that this model trained on Ashura-Arabic text behaves satisfactorily fine in processing complex language tasks, like constituent parsing, even for low resource languages such as Arabic. Addressing these dimensions as presented in Table 4 will require the proposed system to expand into a broader social media analyzing tool for academic research, and practical applications associated with content moderation and policy-making.

TABLE IV. CURRENT LIMITATIONS AND FUTURE WORKS OF PROPOSED SYSTEM

No.	Future works
1	Extending the model to process not just Arabic text but also multiple languages, potentially dialects as well as images/videos from social media which can enhance the understanding of user sentiment.
2	Real-time Hate Speech Detection: Extending the model to process live social media streams for a timely content moderation system using platforms such as X and Facebook.
3	More specifically, the Arabic model can be trained on top of other models to update or adapt to certain domains or events such as politics and news so that the performance and adaptation of these models will improve.

VI. CONCLUSIONS

In this research deep learning technique was deployed to process X data of the Ashura period 1444 AH. The four-week period was then used to collect, process and classify a total of 2,322,708 posts in order to analyze the tolerance exhibited by users. The Bi-GRU with multiple layers stacked on one another, along with AraVec embeddings were used for the analysis. The model achieved an accuracy of 99.89% in finding hate speech within 32% of the Ashura-related posts analyzed but a different trend is indicated by the analysis of posts including emojis, showing that a larger number of tolerance and peaceful expressions are used amongst Ashura. This discrepancy may be attributed to two factors: first, not all posts contain emojis, leading to variability in the results; second, the presence of emojis might reflect a less negative emotional state among users on the platform.

In this study, the author introduces a new hybrid DL model for analyzing Ashura-Arabic related hate speech and sentiment during the religious event Ashura using DL called CNN-BiGRU-Focus model which tremendously improves the efficiency of both tasks. The model surpassed traditional machine-learning classifiers and deep learning models like DenseNet and InceptionV3. By stacking CNN and BiGRU, this design provided excellent accuracy with the power of local feature extraction from CNN and long-range dependencies capturing property of Bi-Directional GRU over sequential data. Besides, by adding the attention mechanism, model resembled more like a human being who can decide which portion of text should not be focused on while analyzing some other part involved equally in context and predict new word making model interpretable rather oblivion.

In the future, as shown in Table IV, we will expand our model to multi-lingual and multimodal data so that real-time detection of hate content on large-scale social media platforms such as Facebook, Twitter and Instagram can be done. Efforts will also focus on bias mitigation and fairness in predictions to ensure the model is equitable across groups. Thirdly, a federated learning (FL) approach will be used to improve hate speech detection that is privacy-preserving without leaking data.

DATA AVAILABILITY

Data and code used to support the findings of this study have been deposited in the Sarah Data repository (https://github.com/imamu-asa).

CONFLICT OF INTEREST

Author declares that there is no conflict of interest.

REFERENCES

[1] S. Dixon, Countries with the most Twitter users 2022, (Jul. 27, 2022). [Online Video]. Available: https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/

[2] L.-C. Chen, C.-M. Lee, and M.-Y. Chen, "Exploration of social media for sentiment analysis using deep learning," Soft Comput., Oct. 2019, doi: 10.1007/s00500-019-04402-8.

[3] Paul, Jayanta, Ahel Das Chatterjee, Devtanu Misra, Sounak Majumder, Sayak Rana, Malay Gain, Anish De, Siddhartha Mallick, and Jaya Sil. "A survey and comparative study on negative sentiment analysis in social media data." Multimedia Tools and Applications (2024): 1-50.

[4] Abdelsamie, Mahmoud Mohamed, Shahira Shaaban Azab, and Hesham A. Hefny. "A comprehensive review on Arabic offensive language and hate speech detection on social media: methods, challenges and solutions." Social Network Analysis and Mining 14, no. 1 (2024): 1-49.

[5] Alhazmi, Ali, Rohana Mahmud, Norisma Idris, Mohamed Elhag Mohamed Abo, and Christopher Eke. "A systematic literature review of hate speech identification on Arabic Twitter data: research challenges and future directions." PeerJ Computer Science 10 (2024): e1966.

[6] H. Huang, A. A. Zavareh, and M. B. Mustafa, "Sentiment Analysis in E-Commerce Platforms: A Review of Current Techniques and Future Directions," IEEE Access, vol. 11, pp. 90367–90382, 2023, doi: 10.1109/ACCESS.2023.3307308.

[7] Ahmad, Ashraf, Mohammad Azzeh, Eman Alnagi, Qasem Abu Al-Haija, Dana Halabi, Abdullah Aref, and Yousef AbuHour. "Hate speech detection in the Arabic language: corpus design, construction, and evaluation." Frontiers in Artificial Intelligence 7 (2024): 1345445.

[8] Mousa, Aya, Ismail Shahin, Ali Bou Nassif, and Ashraf Elnagar. "Detection of Arabic offensive language in social media using machine learning models." Intelligent Systems with Applications 22 (2024): 200376.

[9] A. A. Wazrah and S. Alhumoud, "Sentiment Analysis Using Stacked Gated Recurrent Unit for Arabic Tweets," IEEE Access, vol. 9, pp. 137176–137187, 2021, doi: 10.1109/ACCESS.2021.3114313.

[10] N. Albadi, M. Kurdi, and S. Mishra, "Are they Our Brothers? Analysis and Detection of Religious Hate Speech in the Arabic Twittersphere," in

2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Barcelona: IEEE, Aug. 2018, pp. 69–76. doi: 10.1109/ASONAM.2018.8508247.

[11] N. Albadi, “Religious Hate Speech Detection for Arabic Tweets,” https://github.com/nuhaalbadi/Arabic_hatespeech. [Online]. Available: https://github.com/nuhaalbadi/Arabic_hatespeech

[12] A. B. Soliman, K. Eissa, and S. R. El-Beltagy, “AraVec: A set of Arabic Word Embedding Models for use in Arabic NLP,” Procedia Comput. Sci., vol. 117, pp. 256–265, 2017, doi: 10.1016/j.procs.2017.10.117.

[13] R. Alshaalan and H. Al-Khalifa, “Hate Speech Detection in Saudi Twittersphere: A Deep Learning Approach,” in Proceedings of the Fifth Arabic Natural Language Processing Workshop, Barcelona, Spain (Online): Association for Computational Linguistics, Dec. 2020, pp. 12–23. [Online]. Available: https://aclanthology.org/2020.wanlp-1.2

[14] H. Mulki, H. Haddad, C. Bechikh Ali, and H. Alshabani, “L-HSAB: A Levantine Twitter Dataset for Hate Speech and Abusive Language,” in Proceedings of the Third Workshop on Abusive Language Online, Florence, Italy: Association for Computational Linguistics, 2019, pp. 111–118. doi: 10.18653/v1/W19-3512.

[15] I. Aljarah et al., “Intelligent detection of hate speech in Arabic social network: A machine learning approach,” J. Inf. Sci., vol. 47, no. 4, pp. 483–501, Aug. 2021, doi: 10.1177/0165551520917651.

[16] N. Al Twairesh, M. Al Tuwaijri, A. Al Moammar, and S. Al Humoud, “Arabic Spam Detection in Twitter,” presented at the The 2nd Workshop on Arabic Corpora and Processing Tools 2016 Theme: Social Media, May 2016, pp. 38–43.

[17] Yafooz, Wael. "Enhancing Business Intelligence with Hybrid Transformers and Automated Annotation for Arabic Sentiment Analysis." International Journal of Advanced Computer Science & Applications 15, no. 8 (2024).

[18] Charfi, Anis, Mabrouka Besghaier, Raghda Akasheh, Andria Atalla, and Wajdi Zaghouani. "Hate speech detection with ADHAR: a multi-dialectal hate speech corpus in Arabic." Frontiers in Artificial Intelligence 7 (2024): 1391472.

[19] Ibrahim, Yasmine M., Reem Essameldin, and Saad M. Saad. "Social Media Forensics: An Adaptive Cyberbullying-Related Hate Speech Detection Approach Based on Neural Networks With Uncertainty." IEEE Access (2024).

[20] Louati, Ali, Hassen Louati, Abdullah Albanyan, Rahma Lahyani, Elham Kariri, and Abdulrahman Alabduljabbar. "Harnessing Machine Learning to Unveil Emotional Responses to Hateful Content on Social Media." Computers 13, no. 5 (2024): 114.

[21] Aljohani, Abeer, Nawaf Alharbe, Rabia Emhamed Al Mamlook, and Mashael M. Khayyat. "A hybrid combination of CNN Attention with optimized random forest with grey wolf optimizer to discriminate between Arabic hateful, abusive tweets." Journal of King Saud University-Computer and Information Sciences 36, no. 2 (2024): 101961.

[22] Daraghmi, Eman Yaser, Sajida Qadan, Yousef Daraghmi, Rami Yussuf, Omar Cheikhrouhou, and Mohammed Baz. From Text to Insight: An Integrated CNN-BiLSTM-GRU Model for Arabic Cyberbullying Detection. IEEE Access (2024).

[23] Almaliki, M., Almars, A.M., Gad, I. and Atlam, E.S., 2023. Abmm: Arabic bert-mini model for hate-speech detection on social media. Electronics, 12(4), p.1048.

[24] Khezzar, Ramzi, Abdelrahman Moursi, and Zaher Al Aghbari. "arHateDetector: detection of hate speech from standard and dialectal Arabic Tweets." Discover Internet of Things 3, no. 1 (2023): 1.

[25] Mohamed, Mohamed S., Hossam Elzayady, Khaled M. Badran, and Gouda I. Salama. "An efficient approach for data-imbalanced hate speech detection in Arabic social media." Journal of Intelligent & Fuzzy Systems 45, no. 4 (2023): 6381-6390.

[26] Mubarak, Hamdy, Sabit Hassan, and Shammur Absar Chowdhury. "Emojis as anchors to detect arabic offensive language and hate speech." Natural Language Engineering 29, no. 6 (2023): 1436-1457.

[27] Perera, Suresha, Nadeera Meedin, Maneesha Caldera, Indika Perera, and Supunmali Ahangama. "A comparative study of the characteristics of hate speech propagators and their behaviours over Twitter social media platform." Heliyon 9, no. 8 (2023).

[28] Priyadarshini, Ishaani, Sandipan Sahu, and Raghvendra Kumar. "A transfer learning approach for detecting offensive and hate speech on social media platforms." Multimedia Tools and Applications 82, no. 18 (2023): 27473-27499.

[29] Saleh, Hind, Areej Alhothali, and Kawthar Moria. "Detection of hate speech using bert and hate speech word embedding with deep model." Applied Artificial Intelligence 37, no. 1 (2023): 2166719.

[30] Alqarni, Arwa, and Atta Rahman. "Arabic tweets-based sentiment analysis to investigate the impact of COVID-19 in KSA: a deep learning approach." Big Data and Cognitive Computing 7, no. 1 (2023): 16.

[31] Al-Jarrah, Heba, Mohammad Al-Smadi, Mahmoud Hammad, and Fatima Shannaq. "Using Deep Learning Techniques to Detect Hate and Abusive Language in Arabic Tweets." International Journal of Intelligent Engineering & Systems 17, no. 5 (2024).

[32] Abdelhakim, Mohamed, Bingquan Liu, and Chengjie Sun. "Ar-PuFi: A short-text dataset to identify the offensive messages towards public figures in the Arabian community." Expert Systems with Applications 233 (2023): 120888.

[33] Halawani, Hanan T., Aisha M. Mashraqi, Souha K. Badr, and Salem Alkhalaf. "Automated sentiment analysis in social media using Harris Hawks optimisation and deep learning techniques." Alexandria Engineering Journal 80 (2023): 433-443.

[34] Berrimi, Mohamed, Mourad Oussalah, Abdelouahab Moussaoui, and Mohamed Saidi. "Attention mechanism architecture for arabic sentiment analysis." ACM Transactions on Asian and Low-Resource Language Information Processing 22, no. 4 (2023): 1-26.

[35] Kaddoura, Sanaa, Suja A. Alex, Maher Itani, Safaa Henno, Asma AlNashash, and D. Jude Hemanth. "Arabic spam tweets classification using deep learning." Neural Computing and Applications 35, no. 23 (2023): 17233-17246.

[36] Abdulsalam, Asma, Areej Alhothali, and Saleh Al-Ghamdi. "Detecting suicidality in Arabic Tweets using machine learning and deep learning techniques." Arabian Journal for Science and Engineering (2024): 1-14.

[37] Jaleel, Abdul, Mehmoon Anwar, Farooq Ali, Raza Mukhtar, and Muhammad Farooq. "Islamophobia Content Detection Using Natural Language Processing." Journal of Computing & Biomedical Informatics 4, no. 02 (2023): 88-97.

[38] Boulouard, Zakaria, Mariya Ouaissa, Mariyam Ouaissa, Moez Krichen, Mutiq Almutiq, and Karim Gasmi. "Detecting hateful and offensive speech in Arabic social media using transfer learning." Applied Sciences 12, no. 24 (2022): 12823.

Percussion Big Data Mining and Modeling Method Based on Deep Neural Network Model

Xi Song
Department of Music, College of Arts, Xiamen University, Xiamen 361005, China

***Abstract*—In order to improve the analysis effector percussion waveform, this paper studies the percussion big data mining and modeling method based on the deep neural network model. Aiming at the problem of the high sampling rate of Analog to Digital Converter (ADC) when the wideband frequency-hopping Linear Frequency Modulation (LFM) percussion waveform is sampled by Nyquist, this paper proposes a method of under sampling, and conducts a simple theoretical analysis. When the signal-to-noise ratio is 35dB, the frequency measurement error is close to 1MHz, which can meet the requirements of frequency measurement accuracy. When the signal-to-noise ratio is higher than 35dB, the frequency measurement error gradually decreases and eventually stabilizes, with a frequency measurement accuracy of around 30 kHz. Due to the low environmental interference in the sound wave recognition of percussion instruments and the close distance between the hardware equipment and the percussion instruments in this paper, the recognition results of the model in this paper have high accuracy Compared with existing methods, this article is more reliable in identifying percussion sound waves. From the data, it can be seen that the method proposed in this article has better performance in waveform recognition in impact big data mining models.**

Keywords*—Deep neural network; percussion; big data; mining; modeling

I. Introduction

All musical instruments generate and propagate sound waves. Sound waves can be simulated and form echoes through frequency hopping signals. Therefore, to extract effective information from instrument performances, one can start with frequency hopping signals and propose signal processing methods that can be applied to instrument performance information data mining. This article takes big data mining of percussion as an example for research, first analyzing the relevant research on the performance characteristics of percussion instruments.

In many percussion instruments, the same timbre can be played in different hitting positions, such as bell rings, bass drum bangs, and so on. When the player hits these sounds, he usually chooses a relatively convenient hitting position to complete the performance according to the preceding and following phrases among the many hitting positions. In some percussion works, by carefully arranging the striking position, the body shape can be changed to achieve the purpose of displaying the musical image [1].

There is relatively little research on extracting effective information from instrument performance, so this article proposes an effective music information data mining method based on practical needs. This paper studies and improves the percussion big data mining and modeling method based on the deep neural network model combined with the robot simulation technology, explores the research effect of percussion, and effectively improves the performance of percussion [2].

A method of undersampling is proposed to address the issue of high ADC sampling rate during Nyquist sampling of broadband frequency hopping LFM percussion waveforms, and a simple theoretical analysis is conducted. At the same time, for the frequency ambiguity caused by undersampling, two commonly used frequency deblurring methods, the Chinese remainder theorem and time-frequency analysis, were introduced, and the implementation complexity of these two methods was analyzed. A method based on multi-channel frequency partition decomposition blurring was proposed [3].

When performing percussion works, in certain sections with complex rhythmic changes or compound beats, the performer will subconsciously use their head, torso, and other limbs to strike the rhythm, prompting the audience to follow the logic of rhythm division. When fingers strike a paragraph in music, the shape of the fingers can guide the audience's understanding of the musical phrase. The performer will design the finger shape during or after striking while ensuring the timbre. While ensuring the beauty of the striking form, integrate it with the underlying emotions of the music. The innovation of this article lies in proposing a deblurring method based on multi-channel frequency division, which greatly reduces the implementation complexity. Finally, the fast frequency measurement is achieved through linear interpolation zero crossing frequency measurement method, improving the extraction effect of vocal waveform

Section I of this article mainly introduces the background and current situation, leading to the research content of this article. The following is the relevant work section, which mainly summarizes the existing research work in Section II, raises the existing research problems, and proposes improvement strategies for this article. Section III is the algorithm model section, which proposes the improved algorithm and model of this article, conducts experimental research is presented in Section IV, and finally summarizes the research content of this article in Section V.

II. Related Work

Non-deep learning algorithms consider audio characteristics and search for different feature representations of accompaniment and singing in songs, separating

*Corresponding Author

accompaniment and singing. This type of method relies on long-term accumulated audio knowledge to identify differences between the two, but typically finds distinguishable features with long cycles, high difficulty, and may not be universally applicable to all types of songs. Non-deep learning separation techniques mainly include matrix factorization and acoustic features. Non-negative matrix factorization (NMF) and robust principal component analysis (RPCA) are two typical matrix factorization methods used for vocal separation. From the perspective of acoustic features, propose a method for calculating auditory scene analysis based on pitch inference and accompaniment repetition. Due to the involvement of multiple disciplines in the fields of audio and computer science, the accompaniment and vocal frequency spectra in songs are intertwined and intertwined. Currently, non-deep learning algorithms for vocal separation have made some progress, but there are still problems with mixed vocal/accompaniment and low separation quality [4]. Deep learning algorithms mainly use deep, high semantic, and highly distinguishable features automatically learned by neural networks to separate and predict the time-frequency spectrum of accompaniment/singing, and finally reconstruct the accompaniment and singing signals. This type of algorithm mainly relies on the selection of neural networks. Suitable neural networks can learn and capture features that distinguish between the two, thereby predicting time-frequency spectra that are closer to the original accompaniment/singing. Deep learning algorithms include two categories: modeling in the frequency domain and modeling in the time domain [5]. Reference [6] focuses on deep learning algorithms and therefore provides a detailed introduction to the frequency domain and time domain models of deep learning. Frequency domain model: Due to the significant performance of neural networks on images and the fact that the frequency domain has more exploitable information compared to the time domain, existing algorithms focus on modeling time-frequency spectra in the frequency domain, known as frequency domain models. The main idea is to transform the song from time domain to frequency domain through short-time Fourier transform, input the time-frequency spectrum of the song into a neural network, and the network predicts the time-frequency spectrum of the accompaniment and singing voice. Finally, the phase approximation of the original song is used instead of the accompaniment and singing phase, and the time-frequency spectra of the accompaniment and singing are combined with the original song phase spectrum to reconstruct the time-domain signals of the accompaniment and singing. The separation performance of frequency domain models depends on the selection of neural networks. A network structure with rich structure and the ability to capture and learn comprehensive features can predict high-precision accompaniment/singing time-frequency spectra. In the reconstruction phase, the frequency domain model approximates the separated signal phase using the original song phase, without modeling the phase, which is currently a factor that restricts the quality of separation [7].

Time domain model: Modeling in the time domain refers to using time-domain signals as input and directly putting them into a neural network for training. The network outputs separated time-domain signals of accompaniment and singing. Directly modeling in the time domain avoids the problem of phase distortion in the frequency domain model. The study in [8] attempted to model in the time domain and achieved good separation results. However, due to the high sampling rate of audio signals, the one-dimensional signal in the time domain is very large, resulting in excessive input to the neural network. Whether the network can adapt to the large input size and learn abstract features such as time and space reasonably is a challenge to the network separation performance. Therefore, there is still some research and exploration space for the time domain model.

The main separation idea of the frequency domain model is to use the time-frequency spectrum after short-time Fourier transform as the network input, utilize the advantage of neural network automatic feature learning, capture high semantic features that can distinguish accompaniment and singing, and predict the mask matrix (composed of numbers between 0 and 1) of accompaniment and singing signals. Then, based on the original song time-frequency spectrum and the predicted mask, the time-frequency spectrum of accompaniment/singing is obtained. Finally, by combining the phase reconstruction of the original song, the time-domain signals of the accompaniment and singing voice are obtained [9]. The quality of frequency domain model separation depends on the accuracy of the time-frequency spectrum predicted by the network, and the network structure and learned features determine the quality of separation [10].

At present, the neural networks used in frequency domain models have transitioned from basic neural networks (such as RNN, LSTM, CNN) to structurally rich and multi-level neural networks (such as U-Net, SH-4Stack). With the continuous enrichment and diversity of network structures, the learned features have also been continuously improved. However, the common feature of advanced neural networks used for monaural vocal separation today is that the network structure is serial, and after multiple downsampling, some information will be lost. Moreover, upsampling cannot restore the original information feature appearance, and the defects in the feature learning process result in low amplitude accuracy of the predicted time-frequency spectrum [11].

Music originates from rhythm, and rhythm is also the most basic element of music. When our ancestors in ancient times, based on the relationship between the heart and the pulse, rhythm instinctively evolved into a form of music. Rhythm is more important to music today than ever before. In the use of music, rhythm is more important than melody, harmony, and pitch. Rhythm without specific pitch can make the listener understand the content, but pitch without rhythm can only be called accent [12]. Rhythm is very important in musical elements, and accent is irreplaceable in the rhythm system. After the accent is played well, it will produce the corresponding rhythm. The accent is actually the power generated by the rhythm, and the rhythm is the vitality of the rhythm. Simply playing the rhythm without the change of accent, even if the music played is correct, it cannot make the listener dance with the music. The playing of the accent produces the rhythm, and the existence of the rhythm makes the rhythm have vitality. If the rhythm has life, the music will create a magical power for the listener to enjoy it [13].

With the improvement of productivity and manufacturing level, the development of music goes hand in hand with it. Under the fierce market competition, many professional musical instrument craftsmen have created a guild system while working hard to produce excellent works. The appearance of guilds is to protect the interests of fellow handicraftsmen from being infringed by outsiders, in order to prevent the competition of foreign handicraftsmen and limit the competition between local handicraftsmen in the same industry, a civil organization established by urban handicraftsmen [14]. Guilds have both positive and negative effects. The various regulations issued by the guild have improved the production level of the musical instrument manufacturing industry to a certain extent, but also restricted free competition, the number of employees, the mass production of commodities, and the application of new production tools [15]. The various rules of the guild also make the shapes of musical instruments appear to be similar. The same type of musical instrument, although made by different craftsmen, has almost the same dimensions. In order to meet the market demand of the music industry, instrument manufacturers need more manpower for expanded reproduction [16]. Due to the high difficulty of processing musical instruments, many complex processing procedures still require manual operations and the skilled craftsmen of the processors. Therefore, the way for many musical instrument craftsmen to expand reproduction is not the training system, but the apprenticeship system [17]. Many apprentices need to practice in the workshop for several years, and then take over the mantle of the master and continue to make musical instruments. They don't have time to practice their musical instruments, and they have little experience in musical performances. They know the structure and workmanship of musical instruments well, but they don't understand music. Their duty is to produce instruments of the same level as the Master, pursuing more exquisite craftsmanship and production methods, rather than surpassing or innovating. It is precisely out of respect for the guild system, respect for traditions and a strong sense of responsibility for inheritance that many craftsmen have created the phenomenon of “inheritance” that is unique to musical instruments and is difficult to break [18].

Previous studies have shown that measuring the frequency of music signals in music data mining can cause spectrum aliasing, leading to frequency ambiguity. Therefore, it is necessary to deblur the sampled signals in order to obtain the true frequency of the signals. The core of frequency measurement methods under undersampling conditions is frequency deblurring, which involves undersampling broadband analog signals to obtain digital signals, and then using deblurring algorithms to recover the frequency of the digital signals to obtain the frequency of the original signal. The commonly used deblurring algorithms are the Chinese remainder theorem, time-frequency analysis, and compressive sensing. This article proposes a new deblurring algorithm based on multi-channel frequency band division. On this basis, the method of linear interpolation zero crossing frequency measurement is used to achieve fast frequency measurement of broadband frequency hopping signals. This method greatly reduces the system complexity while reducing the ADC sampling rate, and does not introduce additional deblurring errors. Finally, fast frequency measurement was achieved through linear interpolation zero crossing frequency measurement method.

III. Research Method

Percussion instruments have various forms of performance, and tapping with different parts can also emit audio signals with different characteristics. Feature mining can promote the development of smart music and is of great significance in helping performers discover deficiencies in performance in a timely manner.

Due to the fact that the Nyquist sampling theorem cannot be satisfied when using time-domain undersampling technology to sample the measured acoustic signal, using classical frequency estimation methods at this time will result in spectral aliasing. For undersampled sample sequences, in order to obtain their frequency estimation without ambiguity, a feasible algorithm needs to be used to perform frequency deblurring on the undersampled sequence. Usually, methods such as the Chinese remainder theorem, time-frequency analysis, and compressive sensing can be used to de fuzzify the frequency of the test signal. These methods can indeed achieve good results in their respective application fields, but they have high computational complexity and cannot be used as a universal method for de fuzzifying broadband frequency hopping signals under undersampling conditions. Therefore, it is necessary to propose an undersampling frequency deblurring method with low computational complexity and suitable for broadband frequency hopping signals.

The model in this article collects percussion signals, so in the actual collection process, the terminal hardware device will be connected to the collection device. The device that collects sound waves is very close to the percussion, and the volume and tone of the percussion sound are relatively high, which can be accurately collected by the terminal device. Therefore, the channel loss in the collection of sound channel signals can be ignored.

According to the Nyquist sampling theorem, the sampling rate of the ADC should be at least twice or greater than the Nyquist sampling rate.

A. The basic Theory of Under Sampling

Under sampling is defined as digitizing percussion waveforms at a sampling frequency lower than the Nyquist sampling rate. The following under sampling analysis is carried out through the single carrier frequency percussion waveform.

The input tone percussion waveform can be expressed as in [19]:

$$x(t) = \sin\left(\omega_0 t + \varphi\right) \tag{1}$$

Among them, ω_0 is the real frequency of the single-carrier percussion waveform, and φ is the initial phase of the single-carrier percussion waveform. According to the Fourier transform formula, it can be known that its spectrum is:

$$X(\omega)=\int_{-\infty}^{\infty} sin(\omega_0 t+\varphi)e^{-j\omega t}dt$$
$$=\pi\delta(\omega_0-\omega)e^{-j\varphi}+\pi\delta(\omega_0+\omega)e^{-j\varphi} \quad (2)$$

According to the relevant theory of digital percussion waveform processing, it can be known that the time domain sampling will cause the periodic extension of the spectrum, and the spectrum $X_s(\omega)$ of the percussion waveform after sampling and the spectrum $X(\omega)$ of the percussion waveform before sampling satisfy:

$$X_s(\omega)=\frac{1}{T_s}\sum_{n=-\infty}^{+\infty}X(\omega-n\omega_s) \quad (3)$$

Among them, ω_s is the sampling frequency, T_s is the sampling period. Therefore, when the percussion waveform x(t) is sampled at a fixed sampling rate Ω_s, the spectrum of the digital percussion waveform after sampling is [20]:

$$X_s(\omega)=\frac{1}{T_s}\sum_{n=-\infty}^{+\infty}\left[\pi\delta(\omega_0-\omega-n\Omega_s)e^{-j\varphi}+\pi\delta(\omega_0+\omega-n\Omega_s)e^{-j\varphi}\right] \quad (4)$$

It can be seen from the above formula that under the condition of under sampling, the real angular frequency ω_0 of the percussion waveform can be obtained by calculating according to the fuzzy angular frequency ω measured by the spectrum of the percussion waveform, the sampling frequency Ω_s and the number of ambiguities n relative to the sampling frequency. Therefore, the real percussion waveform frequency under under-sampling condition is obtained. The expression is as follows:

$$\omega_0=n\Omega_s+\omega, f_0=nf_s+f \quad (5)$$

Among them, f is the fuzzy frequency measured according to the percussion waveform spectrum, f_s is the sampling frequency of the percussion waveform, and f_0 is the real percussion waveform frequency. The sampling rate of the ADC must not be less than the Nyquist sampling rate.

B. Ambiguous Understanding of Chinese Remainder Theorem

The Chinese remainder theorem, as an outstanding achievement in ancient Chinese mathematics, embodies the wisdom of our ancestors and has made significant contributions in many modern research fields. This section will introduce the algorithm principle of the Chinese remainder theorem and further expand it. Simultaneously utilizing the Chinese remainder theorem for frequency analysis to achieve the goal of resolving ambiguity

The Chinese remainder theorem is an important theorem in number theory. Its content can be described as: $m_1,m_2,\mathrm{L}\ ,m_L$ is assumed as a positive integer that is relatively prime, and is defined as:

$$M_i=m/m_i, 1\le i\le L \quad (6)$$

Among them, there is $m=m_1m_2\mathrm{L}\ m_L$, then for any integer $r_1,r_2,\mathrm{L}\ ,r_L$, the following first-order congruential equations must have a solution [21],

$$\begin{cases} X\equiv r_1\ mod\ m_1 \\ X\equiv r_2\ mod\ m_2 \\ \quad \mathrm{M} \\ X\equiv r_L\ mod\ m_L \end{cases} \quad (7)$$

Furthermore, the solution to the system of equations is

$$X=\sum_{i=1}^{L}\overline{M_i}M_i r_i\ mod\ m \quad (8)$$

Among them, $\overline{M_i}$ is the inverse of M_i to modulo m_i, and it satisfies the following relation:

$$\overline{M_i}M_i\equiv 1 mod\ m_i, 1\le i\le L \quad (9)$$

If a and b are assumed to be given arbitrary positive integers, they can be decomposed into the form of division with remainder, which is expressed as follows [22]:

$$a=bq_1+r_1, 0<r_1<b$$
$$b=r_1q_2+r_2, 0<r_2<r_1$$
$$\cdots$$
$$r_{n-2}=r_{n-1}q_n+r_n, 0<r_n<r_{n-1}$$
$$r_{n-1}=r_nq_{n+1}+r_{n+1}, r_{n+1}=0 \quad (10)$$

Among them, $q_1,q_2,\mathrm{L}\ q_n,q_{n+1}$ and $r_1,r_2,\mathrm{L}\ r_n,r_{n+1}$ are arbitrary integers obtained. Because every division with remainder will reduce the remainder by at least 1, and b is a finite positive integer, in order to obtain an equation with a remainder of 0, at most b divisions with remainder can be performed. At this time, there is $r_{n+1}=0$. According to the Euclidean algorithm, the greatest common divisor of a and b is the last remainder that is not 0 in Eq. (10), that is r_n. Therefore, the following expression can be obtained [23]:

$$gcd(a,b)=r_n \quad (11)$$

In Eq. (11), $gcd(\cdot)$ represents the greatest common divisor. In the process of solving the greatest common divisor, the coefficients generated by the solution are collected by extending the Euclidean algorithm. Then, after backward operation, the integers x and y can be found to satisfy the following equation:

$$ax+by=gcd(a,b) \tag{12}$$

According to Eq. (6), it is easy to know that M_i and m_i are relatively prime, that is $gcd\left(M_i,m_i\right)=1$. According to Bezuo's theorem, there must be integers x_i and y_i such that the following equation holds [24]:

$$M_i x_i + m_i y_i = gcd\left(M_i,m_i\right), 1 \le i \le L \tag{13}$$

By extending the Euclidean algorithm, the parameters x_i and y_i can be obtained, and the modular inverse $\overline{M_i} = x_i$ can be obtained. In the radar system, the percussion waveform can usually be expressed as a single-frequency complex exponential form, and the percussion waveform expression is:

$$s(t)=Aexp\left(j2\pi f_0 t\right)+\omega(t) \tag{14}$$

Among them, the amplitude and frequency of the percussion waveform are represented by A and f_0, respectively, and the additive noise is represented by $\omega(t)$. If the additive noise $\omega(t)$ is assumed to be Gaussian white noise with zero mean and variance σ^2, the signal-to-noise ratio (SNR) satisfies the following equation [24]:

$$\rho = A^2 / \sigma^2 \tag{15}$$

Among them, ρ represents the signal-to-noise ratio of the single-frequency complex percussion waveform with additive noise. From a fixed time, the percussion waveform is sampled at the sampling rate of f_s. If the sampling time is assumed to be T, the length of the sample sequence after sampling is N, and the following relationship is satisfied:

$$N = Tf_s \tag{16}$$

Eq. (14) and Eq. (16) are combined to further obtain the time domain expression of the sample sequence after sampling:

$$s(n)=Aexp\left(j2\pi f_0 \cdot n / f_s\right)+\omega\left(n / f_s\right), 0 \le n < N \tag{17}$$

If the sampling rate f_s satisfies the Nyquist sampling theorem, there is $f_s \ge 2 f_0$. At this point, the sample sequence is subjected to N-point DFT analysis, which can be obtained The Spectrum of sample sequence:

$$S(k)=DFT(s(n)), 0 \le k < N \tag{18}$$

The spectrum S(k) of the sample sequence is subjected to spectral peak search, and the index position k_p corresponding to the peak spectral line satisfies the following equation:

$$k_p = arg\,max_{0 \le k < N}\{|S(k)|\} \tag{19}$$

Then, the real frequency f_0 of the percussion waveform can be obtained according to the following formula.

$$f_0 = k_p \cdot \Delta f \tag{20}$$

Among them, $\Delta f = f_s / N$ represents the spectral resolution of the DFT.

However, in a practical environment, the percussion waveform frequency f_0 can be taken very large. In this case, if the sampling rate f_s satisfies the Nyquist sampling theorem, the value of f_s will be very large, which requires high requirements for ADC devices and high cost, which is difficult to achieve in some special occasions. At this time, the under-sampling scheme should be considered, and the sampling rate f_s does not satisfy the Nyquist sampling theorem, that is,

$$f_s < 2 f_0 \tag{21}$$

In this case, the frequency estimation value of the original percussion waveform cannot be directly obtained by using the DFT frequency estimation method. At this time, according to the periodicity of the DFT spectrogram, the obtained frequency estimate is actually the frequency remainder (or aliasing frequency) f_r, which satisfies the following equation:

$$f_r = f_0 \bmod f_s \tag{22}$$

Considering that the Chinese remainder theorem uses the system of congruence equations to solve, the method of multi-channel under sampling can be used. According to the Eq. (21), the sampling frequency $f_{s1} \sim f_{sL}$ is selected to perform L-channel under sampling on the percussion waveform respectively. At the same time, the DFT analysis is performed on the sample sequence of each channel, and the index position $k_{p1} \sim k_{pL}$ corresponding to the spectral peak is obtained by using the Eq. (19), then the frequency remainder of each channel can be obtained to satisfy the following equation:

$$f_{ri} = k_{pi} \cdot \Delta f, 1 \le i \le L \tag{23}$$

According to Eq. (22), the system of congruence equations can be obtained, and the expression is as follows:

$$\begin{cases} f_0 = n_1 f_{s1} + f_{r1} \\ f_0 = n_2 f_{s2} + f_{r2} \\ \quad \text{M} \\ f_0 = n_L f_{sL} + f_{rL} \end{cases} \tag{24}$$

Among them, n_1, n_2, L, n_L is the fuzzy multiple. Obviously, the Chinese remainder theorem can be used to solve the equation system (24), so as to obtain the percussion waveform frequency f_0. When the signal-to-noise ratio is high enough, the index position $k_{p1} \sim k_{pL}$ corresponding to the spectral peak can be directly obtained by spectral peak search according to the DFT spectrogram.

Through the above analysis, in order to complete the fuzzy-free estimation of the frequency of percussion waveforms, at least two percussion waveforms are required. Therefore, Fig. 1 presents a dual-rate defuzzification structure based on the remainder theorem.

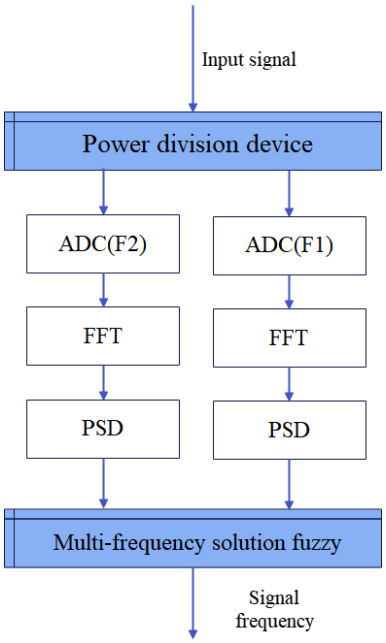


Fig. 1. Double-rate defuzzification structure based on remainder theorem.

C. Defuzzification based on Time-Frequency Analysis

The so-called time-frequency analysis is to use the joint representation of the time domain and the frequency domain to obtain an accurate description of its local characteristics.

Usually, the time-frequency analysis is performed after the real percussion waveform is converted into an analytical percussion waveform. If s(t) is assumed to be a non-stationary real percussion waveform, its corresponding analytical percussion waveform s(t) is expressed as:

$$z(t) = s(t) + jH(s(t)) \tag{25}$$

Among them, H(s(t)) represents the Hilbert transform of the real percussion waveform s(t). For the real percussion waveform, its Fourier transform satisfies the characteristic of conjugate symmetry, and the positive and negative frequency components contain the same information. Moreover, the advantage of analyzing the percussion waveform is that the negative frequency components with residual information are removed, and only the positive frequency components are retained, which will not cause information loss.

For the real percussion waveform s(t), its energy density is $|s(t)|^2$, then the total energy of the percussion waveform is expressed as:

$$E = \int_{-\infty}^{\infty} |s(t)|^2 \, dt \tag{26}$$

If the energy of the percussion waveform is limited, without loss of generality, E=1 can be set. It can be known from formula (26) that the energy density at any time point can be accurately calculated according to the real percussion waveform s(t). Therefore, the time resolution is infinite, whereas the frequency resolution is zero.

The first-order distance of the energy density is expressed as the time center $\langle t \rangle$ of the energy distribution of the percussion waveform, which satisfies the following relationship:

$$\langle t \rangle = \int_{-\infty}^{\infty} t \, |s(t)|^2 \, dt \tag{27}$$

The second moment of the energy density is expressed as the duration T^2 of the percussion waveform, and its expression is as follows:

$$T^2 = \int_{-\infty}^{\infty} (t - \langle t \rangle)^2 \, |s(t)|^2 \, dt \tag{28}$$

Among them, the percussion waveform time width T is the square root of the duration.

If the spectrum of the real percussion waveform s(t) is assumed to be $S(\omega)$, its energy density is $|S(\omega)|^2$, and the expression of the total energy of the percussion waveform is as follows:

$$E = \frac{1}{2\pi} \int_{-\infty}^{\infty} |S(\omega)|^2 \, d\omega \tag{29}$$

According to Parseval's theorem, the total energy of the percussion waveform in the time domain is equal to the total energy of the percussion waveform in the frequency domain. Therefore, there is E=1. It can be known from formula (29) that the energy density of any frequency point can be accurately calculated according to $S(\omega)$. Therefore, the frequency resolution is infinite, whereas the time resolution is zero. It is similar to the definition of time center and time width, and the expressions of frequency center and bandwidth are:

$$\langle \omega \rangle = \int_{-\infty}^{\infty} \omega \, |S(\omega)|^2 \, d\omega \tag{30}$$

$$B=\sqrt{\int_{-\infty}^{\infty}(\omega-\langle\omega\rangle)^2\,|S(\omega)|^2\,d\omega} \tag{31}$$

Generally speaking, both the time center $\langle t\rangle$ and the frequency center $\langle\omega\rangle$ of the energy distribution of the percussion waveform can be set to 0, so Eq. (28) and (31) can be further simplified into the following forms:

$$T^2=\int_{-\infty}^{\infty}t^2\,|s(t)|^2\,dt \tag{32}$$

$$\begin{aligned}B^2&=\int_{-\infty}^{\infty}\omega^2\,|S(\omega)|^2\,d\omega\\&=\int_{-\infty}^{\infty}\left(-j\frac{d}{dt}\right)^2|s(t)|^2\,dt\\&=\int_{-\infty}^{\infty}\left|\frac{ds(t)}{dt}\right|^2dt\end{aligned} \tag{33}$$

When there is $|t|\to\infty$, there is $\sqrt{t}s(t)\to 0$, the product of Eq. (32) and Eq. (33) satisfies the following relation:

$$\begin{aligned}T^2B^2&=\int_{-\infty}^{\infty}\left|\frac{ds(t)}{dt}\right|^2dt\cdot\int_{-\infty}^{\infty}t^2\,|s(t)|^2\,dt\\&\geq\left|\int_{-\infty}^{\infty}\frac{ds(t)}{dt}\cdot ts^*(t)dt\right|^2\\&=\left|\frac{1}{2}\left[ts^2(t)\Big|_{-\infty}^{\infty}-\int_{-\infty}^{\infty}|s(t)|^2\,dt\right]\right|^2\\&=\frac{1}{4}\left|\int_{-\infty}^{\infty}|s(t)|^2dt\right|^2=\frac{1}{4}\end{aligned} \tag{34}$$

Therefore, the following relationship can be further obtained:

$$TB\geq\frac{1}{2} \tag{35}$$

Eq. (35) is called the uncertainty principle. It shows that for any percussion waveform s(t) or window function h(t) with limited energy, the time resolution and frequency resolution are contradictory, and it is impossible to obtain ideal time resolution and frequency resolution at the same time.

The algorithm model of STFT(short-time Fourier transform) can be obtained as shown in Fig. 2. Choose a time-frequency localized window function, assuming that the analysis window function g (t) is stationary (pseudo stationary) within a short time interval, move the window function so that f (t) g (t) is a stationary signal at different finite time widths, and calculate the power spectrum at different times. The short-time Fourier transform uses a fixed window function, and once the window function is determined, its shape no longer changes, and the resolution of the short-time Fourier transform is also determined. If you want to change the resolution, you need to reselect the window function. Short time Fourier transform can still be used to analyze segmented stationary signals or approximately stationary signals, but for non-stationary signals, when the signal changes dramatically, the window function is required to have a high time resolution; When the waveform changes relatively smoothly, mainly for low-frequency signals, a window function with high frequency resolution is required. Short time Fourier transform cannot meet the requirements of frequency and time resolution. The window width is set to N, and the number of FFT(Fourier Transform) points is also set to N. Then, a series of continuous digital knock waveforms are input from the outside. The percussion waveform is transformed into a digital sequence of length N after passing through the data sorting module. Then, through the windowing filtering processing module, the N components of the digital sequence are respectively weighted and sent to the FFT module in sections. After frequency domain analysis, the mathematical expression of STFT is obtained. The STFT algorithm can continuously analyze the spectrum of the sampled data and output real-time analysis results.

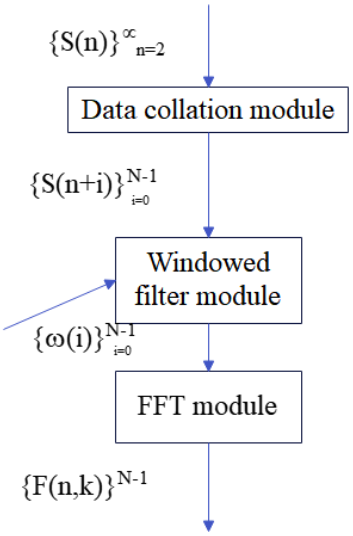


Fig. 2. STFT algorithm model.

By analyzing the algorithm model shown in Fig. 2, the mathematical expression of STFT can be obtained:

$$F(n,k)=\sum_{i=0}^{N-1}s(n+i)\omega(i)e^{-j\frac{2\pi}{N}ki} \tag{36}$$

Among them, n is the time point, and satisfies $n=mL\leq N;k$ is the channel number, and satisfies $k=0,1,\mathrm{L}\ ,N-1$. L is the number of sliding points of the time window, $\{\omega(i)\}_{i=0}^{N-1}$ is the window function, and the window width is N, which is mainly used to reduce the side lobes of the filter, thereby reducing the occurrence of spectral leakage and inter-spectral interference. F(n,k) represents the frequency domain analysis result of the kth channel at time n, that is, the frequency distribution of the percussion waveform in the time window.

The STFT algorithm can be combined with the under-sampling algorithm, so that the under sampled RF broadband percussion waveform can be directly de-blurred, so as to realize the frequency estimation of the original RF broadband percussion waveform. The FFT of the sampling sequence in the function window is the output result of the STFT. Taking the remainder theorem under sampling method as an example, the block diagram of the STFT channelization structure under the condition of under sampling is given as shown in Fig. 3.

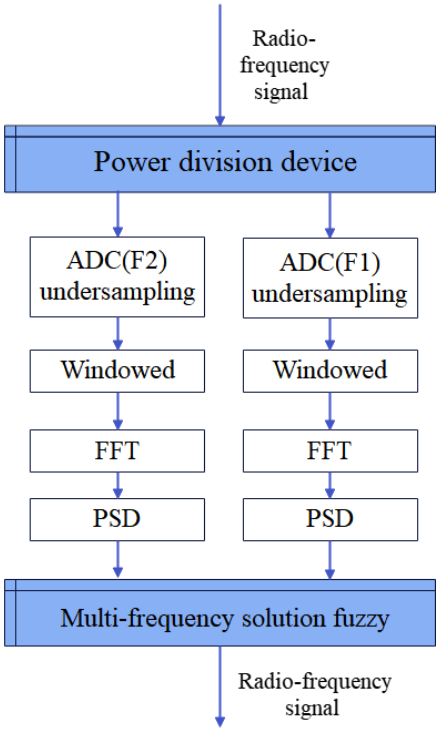


Fig. 3. Block diagram of STFT channelization structure under sampling condition.

Through the above analysis, it can be further obtained that the flow of STFT channelization under the condition of under-sampling is shown in Fig. 4.

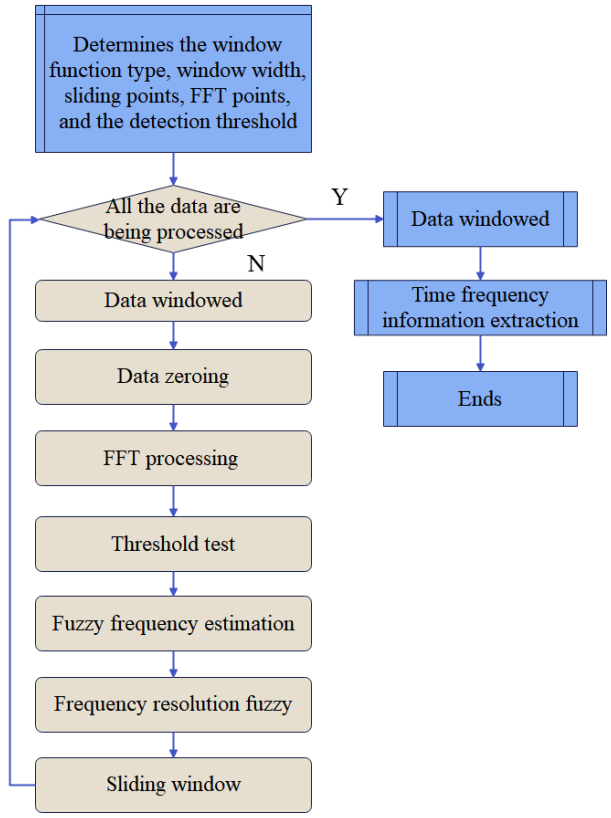


Fig. 4. Flow chart of STFT channelization under sampling condition.

D. Multi-Channel Frequency Division Defuzzification

If it is assumed that the frequency hopping range of the wideband frequency-hopping LFM percussion waveform is $f_1 \sim f_2$, the bandwidth of the LFM percussion waveform is B_s, and the following relationship is satisfied:

$$\begin{cases} B_s = f_1 \\ B_s = f_2 - f_1 \end{cases} \tag{37}$$

The ADC sampling rate is selected as f_s, and it satisfies the following relationship:

$$2B_s < f_s < 2(f_2 - f_1) \tag{38}$$

If the reference frequency is set to f_0 and the number of channels is set to M, the RF analog percussion waveforms of M channels can be down-converted to the same IF frequency hopping range through M different local oscillator percussion waveforms, and are divided into N intermediate frequency sub-bands, as shown in Fig. 5.

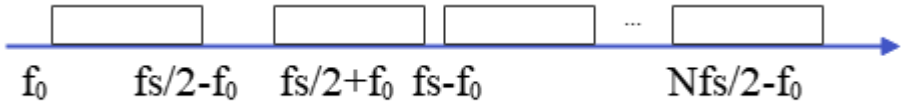


Fig. 5. IF sub-band division.

It is easy to see from Fig. 5 that the range of each IF sub-band can be expressed as:

$$\frac{(k-1)f_s}{2}+f_0 \sim \frac{kf_s}{2}-f_0, k=1,2,\ldots N \tag{39}$$

Therefore, the frequency hopping range of the IF sub-band can be expressed as:

$$f_0 \sim \frac{Nf_s}{2}-f_0 \tag{40}$$

Thus, the expressions of the intermediate frequency hopping bandwidth B_1 and the bandwidth B_2 of each sub-band are as follows:

$$\begin{cases} B_1=\frac{Nf_s}{2}-2f_0 \\ B_2=\frac{f_s}{2}-2f_0 \end{cases} \tag{41}$$

It is easy to know that when there is N=2, it is the easiest to comprehensively analyze the subsequent over-threshold detection results and frequency measurement results. When N increases gradually, the complexity of frequency deblurring will increase, but the sampling rate f_s of ADC can be reduced lower. Therefore, after the M channels are down-converted from the radio frequency band to the intermediate frequency band, each channel can be divided into N sub-bands with an interval of $2f_0$. According to the Nyquist sampling theorem, if the IF percussion waveform of a certain channel is directly frequency measured, the types of frequency ambiguity that will appear include: First, the frequency ambiguity between N sub-bands, which is caused by spectrum folding. The second is the self-ambiguous frequency band of the channel itself, and its range can be expressed as:

$$\frac{kf_s}{2}-f_0 \sim \frac{kf_s}{2}+f_0, k=1,2,\ldots N-1 \tag{42}$$

The IF frequency hopping bandwidth B_1 is the same as the frequency hopping bandwidth of each channel in the radio frequency band. The RF frequency bands of the M channels are divided, as shown in Fig. 6.

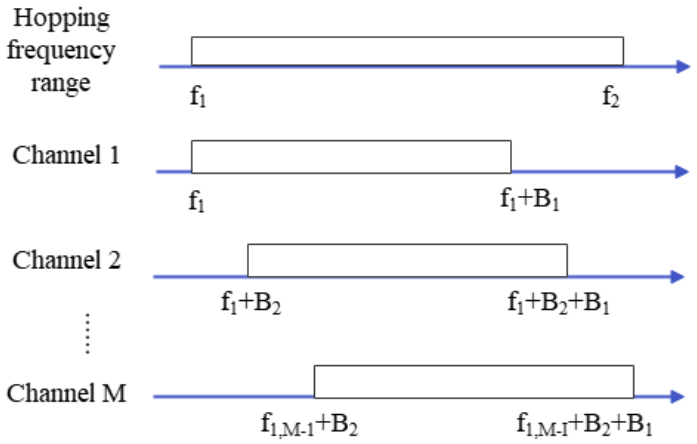


Fig. 6. Division of RF frequency bands for each channel.

As can be seen from Fig. 6, the starting point of the frequency band of the i-th channel is represented by $f_{s,i}$, and it satisfies the following expression:

$$f_{s,i}=f_{s,i-1}+B_2, i=2,3,\ldots, j-1, j+1,\ldots M \tag{43}$$

Among them, the starting point of the frequency band of the 1st channel is $f_{s,1}=f_1$, and the end point of the frequency band of the i-th channel is denoted by $f_{e,i}$, and the following expressions are satisfied:

$$f_{e,i}=f_{s,i}+B_1, i=1,2,\ldots,M \tag{44}$$

When the channel number M is selected, the total frequency band of the channel must completely cover the frequency hopping range, that is, $f_{s,M}+B_1 \geq f_2$. The condition for frequency deblurring is that the overlapping frequency band bandwidth between M channels does not exceed $f_s/2$. In order to satisfy this condition, the j-th channel is reserved here. For different situations, it is necessary to design the frequency band starting point of the channel to satisfy the frequency de-ambiguity condition. If the mid-frequency band of any channel is divided into only two sub-bands, namely N=2, the condition for frequency de-ambiguity must be established at this time. Therefore, the j-th channel may not exist.

The flow chart of multi-channel frequency division defuzzification is shown in Fig. 7.

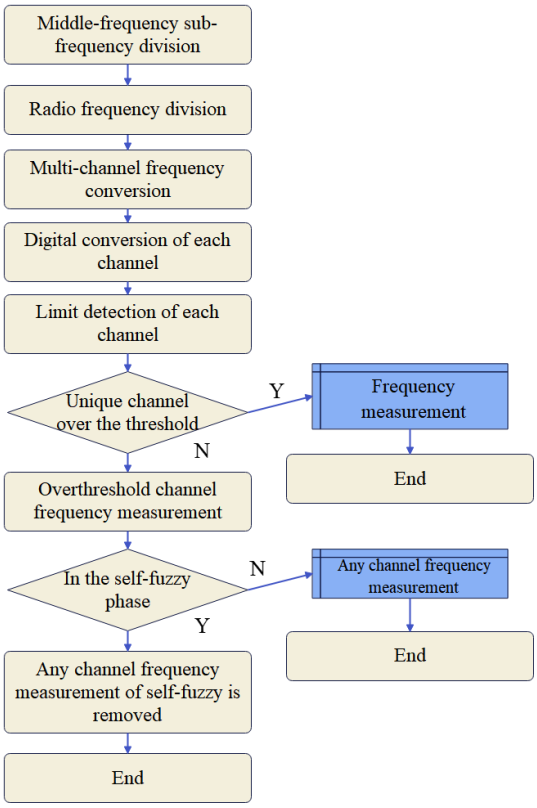


Fig. 7. Flowchart of the realization of multi-channel frequency division defuzzification.

E. Linear Interpolation Zero-Crossing Frequency Measurement

The zero-crossing frequency measurement method can directly measure the frequency through the percussion waveform time series waveform, that is, calculate the frequency of the percussion waveform by measuring the time interval of the zero point. It has the advantages of simple principle, small calculation amount, and fast operation speed.

If it is assumed that the percussion waveform to be tested is a point-frequency percussion waveform with zero initial phase, its expression is:

$$x(t)=\cos(2\pi ft) \tag{45}$$

If the sampling rate of the percussion waveform is f_s, the expression of the discrete percussion waveform after sampling is:

$$x[n]=x(nT_s)=\cos(2\pi fnT_s) \tag{46}$$

It is easy for us to know that the position where the zero point appears is:

$$2\pi fnT_s=\frac{\pi}{2}+k\pi, k\in N \tag{47}$$

$$\frac{f}{f_s}=\frac{2k+1}{4n}, n=1,2,3\ldots$$

That is, when is satisfied, the zero position of the simulated percussion waveform can be sampled. Therefore, when the sampled percussion waveform does not contain the zero position, it is necessary to determine the zero point by the method of depreciation.

The linear interpolation method is used to measure the frequency, and Fig. 8 is a partial enlarged view of the cross position of the left and right of the zero point. A and B are two zeros, and l_{AB} is the interval between zeros. Therefore, if l_{AB} can be obtained, the period of the percussion waveform is $T=l_{AB}$ and the frequency is $f=1/T$. The connection line at the positive and negative intersection of the zero point can be regarded as a straight line, that is, the method of linear measurement, there are:

$$\frac{x_2}{x_1}=\frac{y_2}{y_1} \tag{48}$$

$$\frac{x_4}{x_3}=\frac{y_4}{y_3} \tag{49}$$

According to the sampling theory, the percussion waveform sampling period is $T_s=x_1+x_2=x_3+x_4$. Combining Eq. (48) and Eq. (49), the following formula is obtained:

$$x_2=\frac{y_2}{y_1+y_2}T_s \tag{50}$$

$$x_3=\frac{y_3}{y_3+y_4}T_s \tag{51}$$

Therefore, the zero-point interval $l_{AB}=x_2+nT_s+x_3$ is obtained. Among them, n is the number of discrete points between the two points of C,D.

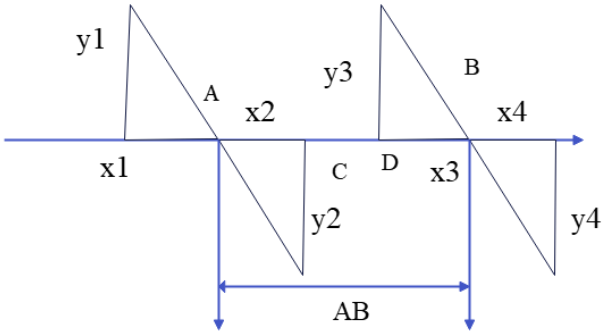


Fig. 8. Schematic diagram of linear interpolation geometry of zero point position.

IV. Model Experimental Results

A. Test Model

This article uses the algorithm model in the third part to extract the features of percussion sound signals, mine and analyze the percussion sound signals, and combine the STFT algorithm with undersampling algorithm. This enables direct deblurring of undersampled RF broadband percussion waveforms, thus achieving frequency estimation of the original RF broadband percussion waveforms, and inputting them into the system as recognizable data. It can provide reliable reference for intelligent recognition of percussion waveforms and virtual simulation of percussion in the future

After the music data is input into the feature selection model, the corresponding feature information is obtained through the long and short-term memory network. Then, it is input into the attention calculation module to analyze the feature distribution of each data block. The attention calculation layer is composed of a two-layer neural network (Fig. 9), and the structure is shown in Fig. 10.

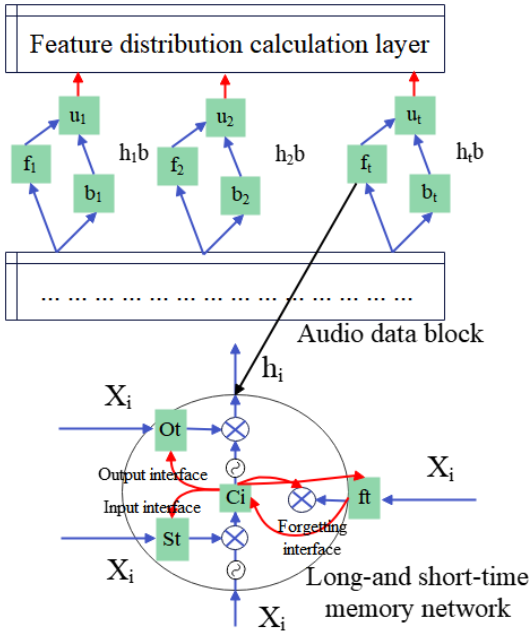
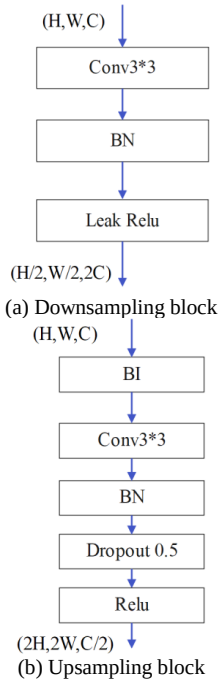
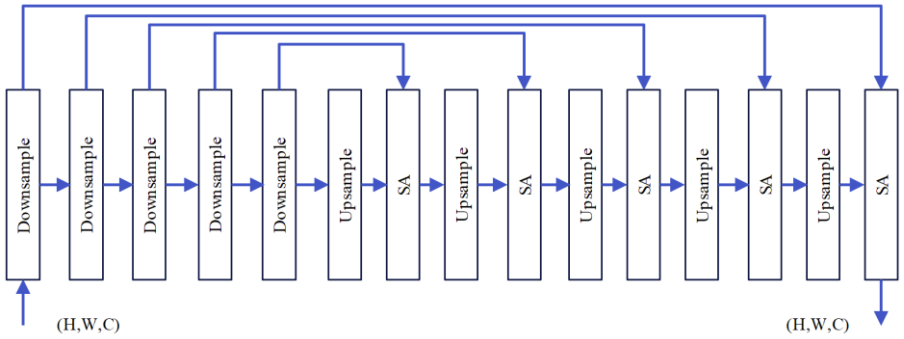


Fig. 9. Modeling of percussion big data mining based on deep neural network.

B. Analysis of Test Results

The sampling module and SA module are stacked together. In both the downsampling and upsampling modules, the size of the convolution kernel is (3,3), the stride is set to 1, and the padding mode is set to "same". Compared to using convolution kernels of size (5,5), using smaller kernels can reduce the computational complexity of the network, while using smaller and deeper kernels can achieve better performance than using larger kernels. Each downsampling block contains 3 layers of network, which are in order of size (3, 3) convolutional layer, BN layer, and Leave Relu activation layer when viewed from the direction of the input network. Each downsampling block uses a BN layer to normalize the feature information learned in this layer, avoiding overfitting. Select Leave Relu to activate the output of the downsampling layer, making the feature values of the output data smoother. Each upsampling block consists of five network layers, namely bilinear interpolation layer (BI), transposed convolutional layer of size (3,3), BN layer, dropout layer, and Relu activation layer. Abandoning the use of transposed convolution to construct upsampling blocks and instead using bilinear interpolation for upsampling, this approach reduces the number of parameters while achieving the goal of upsampling feature maps.





(C) Encoder decoder network

Fig. 10. Structure diagram of neural network model.

Model checking is performed on this basis. If the percussion waveform to be tested is an LFM percussion waveform, since the bandwidth and pulse width of the LFM percussion waveform are known, the modulation slope can also be determined. At this time, it is only necessary to measure the initial frequency according to the above process, and then perform frequency compensation to obtain the center frequency estimation of the LFM percussion waveform. The following is a simulation analysis of the frequency measurement accuracy of the LFM percussion waveform under different signal-to-noise ratios. Set up three experiments, taking the bandwidth and pulse width of LFM percussion waveform as 20MHz, 6 μ s, 40MHz, 8 μ s, 80MHz, 12 μ s, respectively, the center frequency is 380MHz, the sampling rate is 1.6GHz, the signal-to-noise ratio range is 30dB to 45dB, and the step is 1dB. The simulation results are shown in Fig. 11.

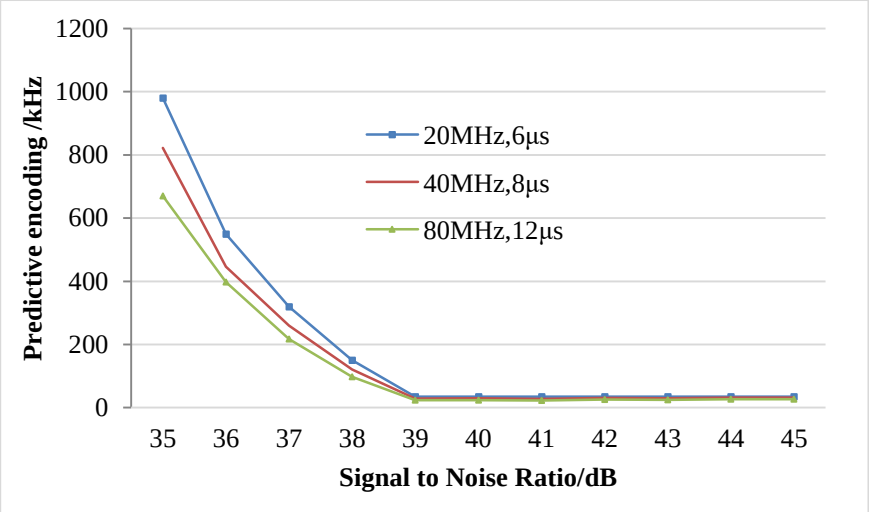


Fig. 11. The relationship between the frequency measurement error and the signal-to-noise ratio of the linear interpolation zero-crossing frequency measurement method.

As can be seen from Fig. 11, From different bandwidth and pulse width conditions, the linear interpolation zero crossing frequency measurement method has good performance in different environments, when the frequency measurement of the LFM percussion waveform is performed by the linear interpolation zero-crossing frequency measurement method, the frequency measurement error decreases with the increase of the signal-to-noise ratio. When the signal-to-noise ratio is 35dB, the frequency measurement error is close to 1MHz, which can meet the requirements of frequency measurement accuracy. When the signal-to-noise ratio is higher than 35dB, the frequency measurement error gradually decreases, and finally tends to be stable, and the frequency measurement error remains about 30kHz. Therefore, under the premise of satisfying a certain signal-to-noise ratio, the linear interpolation zero-crossing frequency measurement method has better frequency measurement accuracy and can meet the requirements of LFM percussion waveform frequency measurement.

To further verify the effectiveness of the model proposed in this paper, it is compared with the methods proposed in references [3], [7] and [10]. Reference [3] used deep learning techniques, reference [7] used multimodal sentiment classification techniques, and reference [10] used long short-term memory deep neural networks

On this basis, the waveform recognition effect of the percussion big data mining model based on the deep neural network model is tested, and the results shown in Table I are obtained.

TABLE I. THE EFFECT OF WAVEFORM RECOGNITION OF PERCUSSION BIG DATA MINING MODEL BASED ON DEEP NEURAL NETWORK MODEL

	The method described in reference [3]	The method described in reference [3]	The method described in reference [3]	The method described in this article
1	77.756	86.136	90.503	95.568
2	76.835	86.398	88.912	95.481
3	80.269	88.925	88.188	94.256
4	74.543	85.273	86.271	94.696
5	79.464	86.467	82.559	93.745
6	81.740	87.310	86.812	95.699
7	75.862	83.395	83.471	94.236
8	76.420	84.524	87.126	95.720
9	77.525	88.801	83.874	95.325
10	74.090	85.098	88.667	95.684
11	79.665	84.147	86.548	93.017
12	78.682	83.832	83.488	94.556
13	75.782	84.673	89.114	94.439
14	79.399	83.980	84.820	94.879
15	77.335	81.607	83.927	93.426

The method proposed in this article first obtains corresponding feature information through long short-term memory networks, and then inputs it into the attention calculation module to analyze the feature distribution of each data block. Compared with studies [3], [7], and [10], this article has more reliable recognition results. From the data, the method proposed in this article has better performance in waveform recognition in percussion big data mining models.

It can be seen from the above research that the percussion big data mining model based on the deep neural network model proposed in this paper has a good effect on waveform recognition.

In the process of music data mining and model construction, this method has lower implementation complexity compared to commonly used deblurring methods such as remainder theorem and time-frequency analysis. In addition, the overall design of the simulator system was completed, and the system was implemented based on a computer platform. Through analysis of test results, the accuracy of the system design and the effectiveness of frequency measurement methods were verified.

V. CONCLUSION

When performing percussion works, in some passages with complex rhythm changes or complex time signatures, the performer will also subconsciously use the head, torso and other limbs to strike the beat to remind the audience of the rhythm division logic. When there is a finger hitting passage in the music, the shape of the finger can guide the audience's understanding of the phrase. Moreover, while ensuring the timbre, the player will design the shape of the fingers when hitting or after hitting, and while ensuring the beauty of the hitting shape, it will be integrated with the inner emotion of the music. This article proposes a new deblurring algorithm based on multi-channel frequency band division. On this basis, the method of linear interpolation zero crossing frequency measurement is used to achieve fast frequency measurement of broadband frequency hopping signals. This method greatly reduces the system complexity while reducing the ADC sampling rate, and does not introduce additional deblurring errors. Finally, fast frequency measurement was achieved through linear interpolation zero crossing frequency measurement method.

The percussion big datamining and modeling methods are researched based on the deep neural network model. The simulation test shows that the percussion big data mining model based on the deep neural network model proposed in this paper has a good effect on waveform recognition.

When the signal-to-noise ratio is 35dB, the frequency measurement error is close to 1MHz, which can meet the requirements of frequency measurement accuracy. When the signal-to-noise ratio is higher than 35dB, the frequency measurement error gradually decreases and eventually stabilizes, with a frequency measurement accuracy of around 30kHz. Moreover, through comparison, it can be seen that the model in this article has better performance in sound wave recognition of percussion instruments

When simulating the frequency hopping signal echo in this article, only the target characteristics were considered, without considering the clutter and interference characteristics. At the same time, when simulating the target echo, the scattering characteristics of the target were not considered, which means that the target is considered an ideal point target. Therefore, in subsequent research work, in order to better simulate the radar environment, it is necessary to simulate clutter signals and interference signals, and analyze the echo simulation methods of extended targets.

REFERENCES

[1] Briot, J. P., & Pachet, F. (2020). Deep learning for music generation: challenges and directions. Neural Computing and Applications, 32(4), 981-993.

[2] Martín-Gutiérrez, D., Peñaloza, G. H., Belmonte-Hernández, A., & García, F. Á. (2020). A multimodal end-to-end deep learning architecture for music popularity prediction. IEEE Access, 8(2), 39361-39374.

[3] Weng, S. S., & Chen, H. C. (2020). Exploring the role of deep learning technology in the sustainable development of the music production industry. Sustainability, 12(2), 625-633.

[4] Briot, J. P. (2021). From artificial neural networks to deep learning for music generation: history, concepts and trends. Neural Computing and Applications, 33(1), 39-65.

[5] Sharma, A. K., Aggarwal, G., Bhardwaj, S., Chakrabarti, P., Chakrabarti, T., Abawajy, J. H., ... & Mahdin, H. (2021). Classification of Indian classical music with time-series matching deep learning approach. IEEE access, 9(2), 102041-102052.

[6] Pandeya, Y. R., & Lee, J. (2021). Deep learning-based late fusion of multimodal information for emotion classification of music video. Multimedia Tools and Applications, 80(2), 2887-2905.

[7] Pandeya, Y. R., Bhattarai, B., & Lee, J. (2021). Deep-learning-based multimodal emotion classification for music videos. Sensors, 21(14), 4927-4935.

[8] Rafi, Q. G., Noman, M., Prodhan, S. Z., Alam, S., & Nandi, D. (2021). Comparative analysis of three improved deep learning architectures for music genre classification. International Journal of Information Technology and Computer Science, 13(2), 1-14.

[9] Zhang, F. (2021). Research on music classification technology based on deep learning. Security and Communication Networks, 2021(1), 1-8.

[10] Hizlisoy, S., Yildirim, S., & Tufekci, Z. (2021). Music emotion recognition using convolutional long short term memory deep neural networks. Engineering Science and Technology, an International Journal, 24(3), 760-767.

[11] Bakariya, B., Singh, A., Singh, H., Raju, P., Rajpoot, R., & Mohbey, K. K. (2024). Facial emotion recognition and music recommendation system using CNN-based deep learning techniques. Evolving Systems, 15(2), 641-658.

[12] Solanki, A., & Pandey, S. (2022). Music instrument recognition using deep convolutional neural networks. International Journal of Information Technology, 14(3), 1659-1668.

[13] Dong, L. (2023). Using deep learning and genetic algorithms for melody generation and optimization in music. Soft Computing, 27(22), 17419-17433.

[14] Zinemanas, P., Rocamora, M., Miron, M., Font, F., & Serra, X. (2021). An interpretable deep learning model for automatic sound classification. Electronics, 10(7), 850-861.

[15] Rajesh, S., & Nalini, N. J. (2020). Musical instrument emotion recognition using deep recurrent neural network. Procedia Computer Science, 167(1), 16-25.

[16] Calvo-Zaragoza, J., Jr, J. H., & Pacha, A. (2020). Understanding optical music recognition. ACM Computing Surveys (CSUR), 53(4), 1-35.

[17] Yin, Z., Reuben, F., Stepney, S., & Collins, T. (2023). Deep learning's shallow gains: A comparative evaluation of algorithms for automatic music generation. Machine Learning, 112(5), 1785-1822.

[18] Kim, J., Urbano, J., Liem, C. C., & Hanjalic, A. (2020). One deep music representation to rule them all? A comparative analysis of different representation learning strategies. Neural Computing and Applications, 32(4), 1067-1093.

[19] Singh, J. (2022). An efficient deep neural network model for music classification. International Journal of Web Science, 3(3), 236-248.

[20] Zhang, Y. (2024). A Multi-sentence Music Humming Retrieval Algorithm Based on Relative Features and Deep Learning. Scalable Computing: Practice and Experience, 25(3), 1799-1806.

[21] Sheikh Fathollahi, M., & Razzazi, F. (2021). Music similarity measurement and recommendation system using convolutional neural networks. International Journal of Multimedia Information Retrieval, 10(1), 43-53.

[22] Liu, C., Feng, L., Liu, G., Wang, H., & Liu, S. (2021). Bottom-up broadcast neural network for music genre classification. Multimedia Tools and Applications, 80(3), 7313-7331.

[23] Sarkar, R., Choudhury, S., Dutta, S., Roy, A., & Saha, S. K. (2020). Recognition of emotion in music based on deep convolutional neural network. Multimedia Tools and Applications, 79(1), 765-783.

[24] Sana, S. K., Sruthi, G., Suresh, D., Rajesh, G., & Reddy, G. S. (2022). Facial emotion recognition based music system using convolutional neural networks. Materials Today: Proceedings, 62(2), 4699-4706.

Deep Image Keypoint Detection Using Cascaded Depth Separable Convolution Modules

Rui Deng
Network Information Center, Jilin Vocational College of Industrial and Technology, Jilin, 132013, China

***Abstract*—Depth images have become an important data source for human bone keypoint detection due to their three-dimensional information. To optimize the efficiency of keypoint detection in depth images, a depth image keypoint detection model that combines cascaded depth separable convolution modules is constructed. The model first performs data cleaning and preprocessing on the image, replacing traditional convolutional layers with depthwise separable convolutional modules. The Faster OpenPose network is introduced to replace the traditional convolutional network structure with the lighter MobileNetV1 for detecting keypoints in the image. When the dataset size was 4000, the Faster OpenPose model had an accuracy of 0.97 and a mean square error of 0.03. The recognition rates for four different images were 0.91, 0.87, 0.89, and 0.93, respectively. The processing times were 0.32, 0.31, 0.28, and 0.27, respectively. The method of depth image keypoint detection combined with cascaded depth separable convolution modules has good practicality and excellent detection performance for various images, providing new ideas for future keypoint detection technology research.**

Keywords*—Depth image; DWCA; key point detection; OpenPose; cascade depth

I. Introduction

Deep Image (DI) keypoint detection is important in 3D object reconstruction, facial recognition, gesture recognition, and robot navigation. These tasks typically require accurate extraction of key points of objects or scenes from DI for further analysis or processing. However, traditional methods rely heavily on manually designed feature extractors, which often exhibit significant limitations in complex scenes. Compared with traditional two-dimensional images, DI provide rich 3D spatial information, making the understanding and analysis of the scene more accurate. In human pose estimation, DI can more accurately capture the skeletal structure of the human body, reducing the impact caused by lighting changes, occlusion, and other issues [1]. However, how to effectively extract key points of the human body from DI remains a challenge. The current keypoint detection technology, such as the OpenPose based network architecture, can achieve relatively accurate pose estimation on two-dimensional images. However, there are still certain limitations in DI processing, such as high computational complexity of the model, sensitivity to background information interference, and the need to improve keypoint localization accuracy [2]. The limitation of existing models is that they cannot effectively handle noise and background interference in depth images, resulting in a decrease in the accuracy of keypoint detection. Many traditional models rely on high-quality input data, and in practical applications, depth images often have varying degrees of noise, which can affect model performance. In addition, existing models often lack sensitivity to changes in human posture and complex background responses, limiting their application in multi human environments. The computational complexity of the model is also a problem, and classical convolutional neural networks may face performance bottlenecks when processing real-time data. Therefore, this study proposes a DI keypoint detection method that combines cascaded depth separable convolution modules. This method replaces the traditional VGG-19 network structure with a more lightweight MobileNetV1 by introducing the Faster OpenPose network, and designs a Depthwise Separable Convolutional Module (DWCA) based on this to reduce computational complexity while maintaining the model's prediction capability. The main reason for choosing a model based on bilateral filtering and Faster OpenPose network is its excellent noise processing ability and efficient 3D information preservation. Bilateral filtering can effectively remove noise in depth images while preserving edge features, ensuring the accuracy of keypoint localization. The Faster OpenPose network significantly improves computational efficiency and meets real-time detection requirements by replacing VGG-19 with MobileNetV1. The introduction of depthwise separable convolution modules and feature fusion mechanisms enhances the ability to extract key features and improves the performance of multi person pose estimation. The model can effectively extract regions of interest related to the human body, filter out irrelevant backgrounds, and further improve detection accuracy and efficiency. The contribution of the research lies in the proposed bilateral filtering based deep image processing model, which effectively removes noise from deep images while preserving key edge features, significantly improving the accuracy of keypoint localization. Secondly, by introducing the Faster OpenPose network and replacing the traditional VGG-19 with MobileNetV1, the computational efficiency of the model has been improved, making real-time keypoint detection possible and adapting to the needs of various application scenarios. The deep separable convolution module based on feature fusion introduced in the study enhances the ability to extract important features from depth images and improves the performance of keypoint detection. In addition, the model effectively extracts regions of interest related to the human body, filters out irrelevant background information, and further improves the accuracy and efficiency of keypoint localization. The innovation lies in optimizing the performance of DI keypoint detection by improving the OpenPose network structure and introducing more efficient convolution modules. The research aims to provide new technological paths for the field of Computer Vision (CV) and offer better solutions for

keypoint detection in practical applications.

The research content is as follows: An examination of the research topics of other scholars in the field is given in Section II. An overview of the principal methodologies employed in Section III. The results of the model experiment is presented in Section IV. Discussion is given in Section V and finally, the paper is concluded in Section VI.

II. Related Works

Under the development of computer technology, CV is becoming increasingly important. Zhou K et al. built an improved codebook pattern model to improve the processing efficiency of rapid action vide. The combination of this method with the CV approach had the potential to enhance the accuracy of feature recognition in fast-action sequences, facilitate the effective processing of fast-motion videos, and improve the feature recognition effect [3]. Zhou H et al. discovered that despite the current advancements in video surveillance, autonomous vehicles, and other related fields, there was still a significant opportunity for further development in predicting the future trajectory of pedestrians. A spatiotemporal graph neural network based on attention interaction perception had been proposed, which demonstrated effective capability [4]. Lee J et al. put forth a new YOLO model to handle the real-time object detection problem of YOLO. This architecture maintained YOLO's high accuracy and ease of use. The proposed method model could effectively solve problems related to real-time processing [5]. Jiang X et al. proposed a blockchain based model sharing method to address the issues of autonomous driving object detection. This method combined mobile edge computing technology and YOLOv2 model to reduce regional differences, and its effectiveness and reliability were superior to the reference model [6].

Yang Y et al. constructed a traffic recognition method with deep convolutional neural networks, which was able to detect and classify the input images, thereby obtaining more clear traffic information. The algorithm demonstrated superior accuracy in traffic image classification, offering a more optimal solution for smart traffic monitor [7]. Chen D et al. proposed an underwater ship detection model with optimized YOLOv3, which enhanced feature extraction capabilities in various environments by introducing an attention module. This model had good recognition and detection capabilities, proving its superiority in ship detection in water transportation [8]. Tumrani et al. proposed a decentralized and multi-attribute learning network, which adopted a vehicle keypoint detection model based on local attention for regions with more DIcriminative information. This method could improve the ability and robustness of vehicle recognition [9].

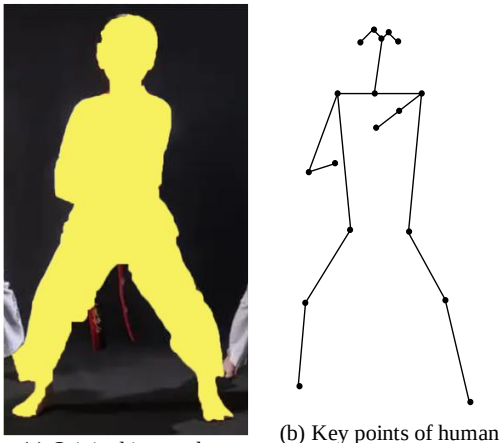
In conclusion, a substantial body of research has been conducted in the field of computer imaging, yielding notable findings, but have not conducted more in-depth studies on DI. Moreover, various studies have focused on specific domain problems and rely on specific datasets, resulting in insufficient generalization ability of models in other datasets or practical applications. This study proposes a DI keypoint detection method that combines DWCA. This method replaces the traditional VGG-19 network structure with a more lightweight MobileNetV1 by introducing the Faster OpenPose network, and uses a DWCA on this basis to reduce computational complexity while maintaining the model's prediction capability.

III. Methods

In the first section, a DI processing model based on Bilateral Filtering (BF) is proposed to address the issue of noise in DI. In the second section, OpenPose network is adopted to detect keypoints in images and improve the model for defects.

A. DI Processing Model Based on BF

A DI is an image used to represent the distance from each pixel in a scene to the camera. Unlike traditional two-dimensional images, it contains three-dimensional information in the scene and can be used to more accurately understand and analyze the spatial structure of the scene [10-11]. An image is typically a two-dimensional matrix consisting of three color channels, with the value of each channel representing the color intensity of that pixel. Each pixel in a color image provides color information that can describe the appearance of objects in the scene. DI is a two-dimensional matrix, but each pixel value represents the distance from that pixel to the camera or sensor. DI reflects the 3D structural information of the scene, not the color, thus protecting privacy. The study extracts key points of human bones, as shown in Fig. 1.



(a) Original image data (b) Key points of human skeleton

Fig. 1. Extraction of key points in the human body.

In Fig. 1, firstly, the resolution of the image is converted, and secondly, public tools are used to process the data. The joints of the human body on each screen are estimated, and the coordinates of each joint point are recorded. The DI body surface keypoint localization algorithm mainly consists of six steps, and its process is shown in Fig. 2.

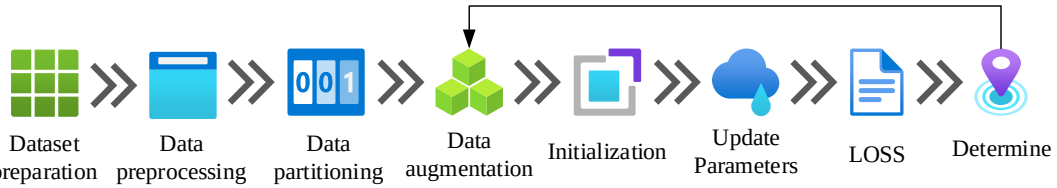


Fig. 2. Body surface key point localization process.

In Fig. 2, during the model training process, the dataset is first prepared, including collecting, organizing, and organizing data to provide a foundation for model training [12-13]. In the data preprocessing stage, the data is cleaned, normalized, and processed to ensure data quality and consistency. Subsequently, the dataset is partitioned into three sets, thereby ensuring that the model exhibits the requisite capacity for generalization. Then, the dataset is augmented to enhance the discrepancy of the data and reinforce the model's robustness. After the model parameters are initialized, the model begins to be trained; The error predicted by the loss function model is evaluated and updated based on the parameters of the error model. Then the loss function is recalculated and checked for convergence. If the loss function converges, that is, the error reaches a stable low level or no longer significantly decreases, the training process ends; otherwise, the model continues to iterate and update parameters until convergence conditions are reached. During the model testing process, the trained model parameters are first loaded, and then the test dataset is preprocessed to ensure consistency with the training data [14]. The preprocessed test data is input to generate a heatmap of key points. Next, the specific coordinates of the key points are extracted as the final output of the model. The performance of this process model on new data can be measured by the accuracy of key points that need to be ensured, and ultimately the entire testing process ends.

In the collection of DI, a lot of background information will also be collected. These background information include objects, walls, floors, etc. that are unrelated to the human body, and these additional pieces of information can interfere with keypoint localization tasks. It is necessary to use appropriate methods to filter out unnecessary background information and focus on processing Region of Interest (ROI) related to the human body [15-16]. The method's importance is to use breadth first search to identify foreground objects, and filter out background parts based on depth and height information to obtain background removed DI. After extracting the ROI, it still cannot meet the requirements, so median filtering is used to process the image, and its expression is illustrated in Eq. (1).

$$depth_{median}(x,y) = median_{(s,t)\in N(x,y)}[depth(s,t)] \quad (1)$$

In Eq. (1), $depth_{median}(x,y)$ represents the depth value after median filtering operation; $median$ represents the function for calculating the median; N is the neighborhood of the pixel; $depth(s,t)$ is the depth value of the pixel at position (s,t) [17-18]. Although median filtering can remove noise, the details of the image are also severely lost. Therefore, the BF method is used to smooth the image, and its expression is shown in Eq. (2).

$$depth_{double}(x,y) = \sum_{(s,t)\in N(x,y)} W(s,t) \times depth(s,t) \quad (2)$$

In Eq. (2), $depth_{double}(x,y)$ represents the depth value; $W(s,t)$ represents the normalized weight, and the aforementioned expression is demonstrated in Eq. (3).

$$W(s,t) = exp\left(-\frac{(s-x)^2+(t-y)^2}{2\sigma_d^2} - \frac{(depth(s,t)-depth(x,y))^2}{2\sigma_r^2}\right) \quad (3)$$

In Eq. (3), σ_d and σ_r respectively represent the parameters of spatial distance and pixel difference size. Before preprocessing, normalization is performed, and the weights of the neighborhood are first calculated, as shown in equation (4).

$$sum = \sum_{(s,t)\in N(x,y)} W(s,t) \quad (4)$$

In Eq. (4), sum is the sum of weights in the neighborhood. Then, the weights of each pixel are equal to the index value divided by the sum of weights, as expressed in Eq. (5).

$$W(s,t) = W(s,t) / sum \quad (5)$$

In Eq. (5), $W(s,t)$ represents the neighborhood weight, and the image after BF is shown in Fig. 3.

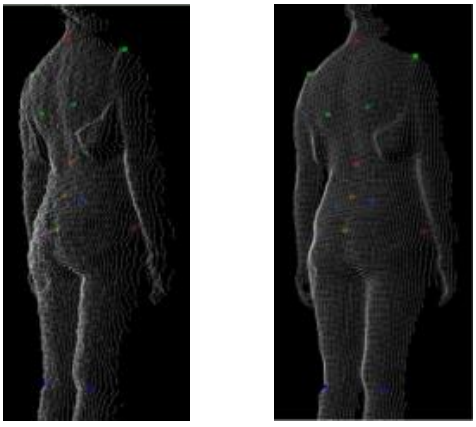


Fig. 3. Comparison of key points before and after BF.

In Fig. 3, the BF operation can effectively remove image noise while preserving the edge features of the image. BF can reduce noise interference in the image, making the ROI clearer and improving the accuracy of the Faster OpenPose network in keypoint detection. Through BF, the background information in the image is smoothed, while the key points and edge features related to the human body are preserved, promoting to focus on identifying the key points of the human body.

B. DI Keypoint Detection Model Combined with Cascaded DWCA

After completing the data cleaning, OpenPose network is adopted to detect key points in the image. OpenPose is a powerful open-source library specifically designed for real-time detection and estimation of keypoints on multiple people's bodies, faces, hands, and feet. The core process includes extracting features from input images or video frames, generating part affinity fields and keypoint heatmaps, and connecting these keypoints through post-processing to form a complete human pose skeleton [19-20]. The classic OpenPose has obvious flaws, so research has improved OpenPose and proposed a Faster OpenPose. VGG-19 in OpenPose has been replaced with MobileNetV1, improving the efficiency of the model. The DWCA based on feature fusion mechanism is introduced, and its structure is shown in Fig. 4.

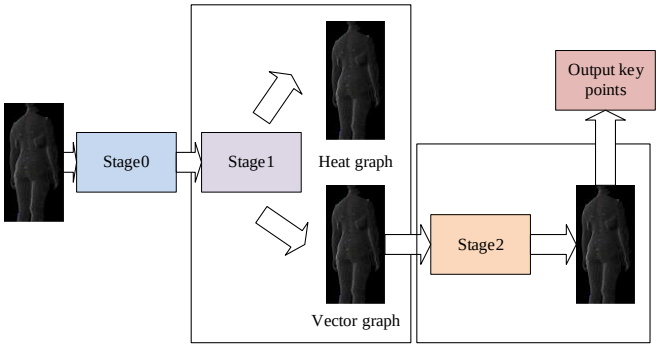


Fig. 4. Faster OpenPose structure.

In Fig. 4, the first DI is received as input, which captures the distance information between the object and the camera, providing a three-dimensional representation of the scene. Next, Stage 0 is responsible for feature extraction, processing the input DI through convolutional neural networks to extract relevant features that can be used for subsequent pose estimation. In Stage 1, heatmaps are generated, which represent the probability distribution of key point positions in the image. Partial correlation vector maps are generated, encoding the directions and associations between different body parts, helping to determine the connection relationships between detected joint points and forming a complete skeleton [21-22]. Then it enters Stage 2, where the heatmap interpolation is amplified to match the original resolution of the input DI before the final output. This step ensures that the detected keypoints are aligned correctly with the original image size. Finally, the keypoints are output, which represent the coordinates of the body joints in the input image and can be used for further tasks. In the Stage0 structure, an alternating structure of DWCA and regular modules is adopted, as shown in Fig. 5.

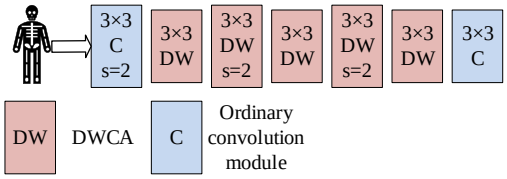


Fig. 5. Schematic diagram of stage0 structure.

In Fig. 5, it contains a regular convolution module and DWCA. In the initial stage of the process, the spatial dimension of the input image is reduced by a factor of two. Next, multiple DWCAs are adopted. These modules divide convolution operations into two steps: In deep convolution, a distinct convolution kernel is applied to each input channel. In contrast, point-by-point convolution employs a 1×1 convolution to integrate the channels of the deep convolution output. This structure maintains the accuracy of the model while reducing computational complexity. The entire MobileNetV1 network gradually increases the number of channels, ultimately generating a smaller high-dimensional Feature Map (FM) for subsequent classification or other tasks. In the process of deep convolution, for an input FM, the computational complexity of traditional convolution is shown in Eq. (6).

$$J = h' \times w' \times D_{out} \times (k \times k \times D_{in}) \tag{6}$$

In Eq. (6), $h' \times w' \times D_{out}$ represents the size of the output FM; $k \times k$ represents the size of the filter. In deep convolution, the convolution kernel only acts on each input channel, and its computational complexity is shown in Eq. (7).

$$J_m = h' \times w' \times D_{in} \times (k \times k) \tag{7}$$

Then point by point convolution is used to mix all input channels and generate an output FM, which is expressed as Eq. (8).

$$J_n = h' \times w' \times D_{in} \times D_{out} \tag{8}$$

Stage1 is the initialization stage, Stage2 is the refinement stage, and their structures are shown in Fig. 6.

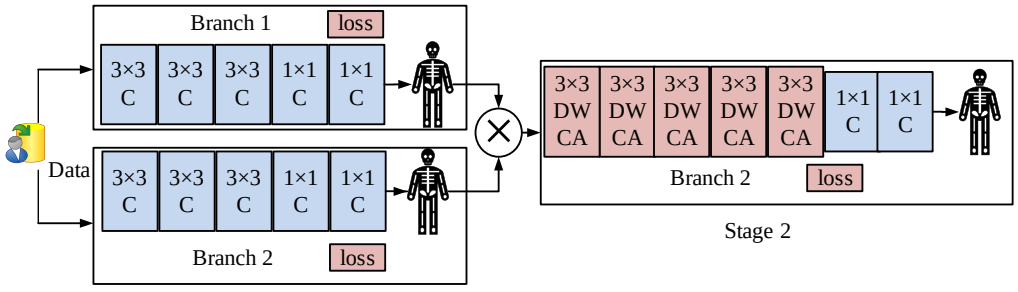


Fig. 6. Structure of stage1 and stage2.

In Fig. 6, Stage 1 includes Branch 1 and Branch 2. Branch 1 adopts multi-layer convolution operations, including 3×3 standard convolution and 1×1 convolution. After these convolution operations, the FM's size is output, and then the loss function is used to calculate the loss. Branch 2 also uses a series of convolution operations, but the output FM's size is h×w, and the loss is calculated through another loss function. The output S1 of Stage 1 is a combination of the outputs of two branches, which will be passed on to the next Stage 2. In Stage 2, the complexity of the network further increases, and Branch 2 performs different operations in Stage 2. DWCA is introduced in branch 2, and the final FM size is output. The output of this branch is also calculated through a loss function. The final output of Stage 2 is represented by S2. The loss function in Stage 1 is shown in Eq. (9).

$$\begin{cases} L_1 = f_1(S_1^1) \\ L_2 = f_2(S_2^2) \end{cases} \tag{9}$$

In Eq. (9), L_1 and L_2 represent the loss functions of the output FM of branch 1 and branch 2, respectively; S_1^1 and S_2^2 represent the FM of branch 1 and branch 2, respectively. The final loss function of the model is shown in Eq. (10).

$$L_t = L_1 + L_2 + L_3 \tag{10}$$

In Eq. (10), L_t represents the total loss function; L_1, L_2, and L_3 respectively represent the loss functions of the three stages.

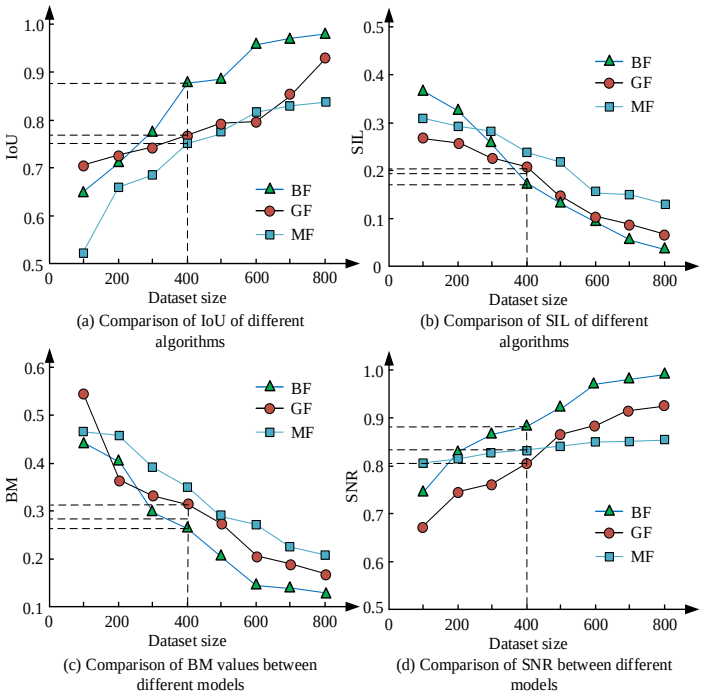
IV. Results

In the first section, image processing models based on Gaussian Filtering (GF) and Mean Filtering (MF) were introduced as comparison models for comparison. In the second section, the performance of the DI detection model combined with cascaded DWCA was analyzed.

A. Localization Performance based on DI Surface Keypoints

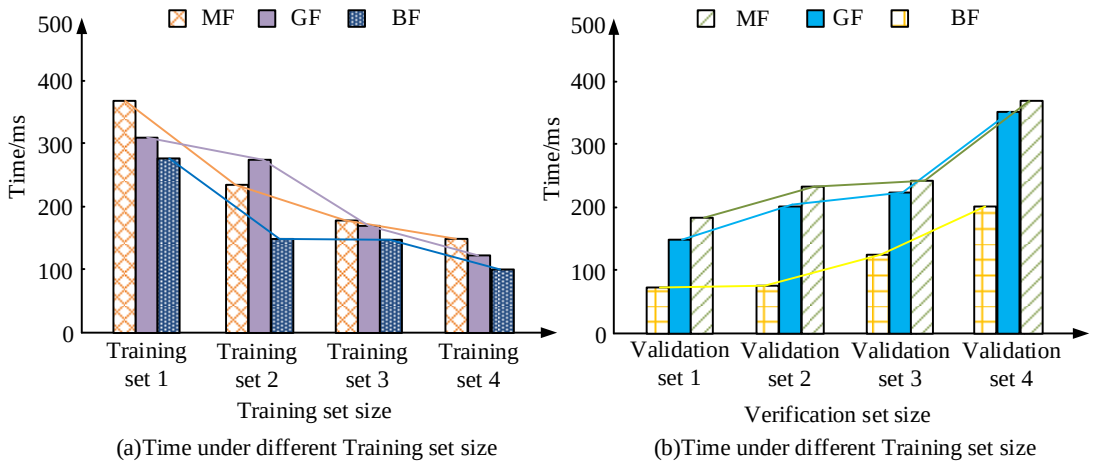
The COCO public dataset was utilized, which comprises over 100,0000 images, encompassing 80 distinct categories of objects, including humans, animals, vehicles, and furniture, as well as various scenes and environments. Each image has detailed annotation information, including the category of the object, the position and size of the bounding box, and the keypoint information of the object, providing standard evaluation metrics. The CPU model used was Intel (R) Core (TM) i7-9700F, with a frequency of 3.00GHz. The graphics processor model was NVIDIA GeForce GTX 1660 Ti, with 8GB of video memory. The operating system was Windows 10. This study introduced GF based image processing models and MF based image processing models as comparative models for comparison. The results are shown in Fig. 7.

Fig. 7, 7(b), 7(c), and 7(d) illustrate the comparison results of Intersection over Union (IoU), Structural Information Loss (SIL), Bonferroni Mean (BM), and Signal to Noise Ratio (SNR) of images processed by various algorithms. As illustrated in Fig. 7, an increase in the training set size was accompanied by a corresponding rise in the IoU of each model after processing images. As the training set size was up to 800, the IoU of BF, GF, and MF were 0.83, 0.91, and 0.96. The SIL was 0.10, 0.06, and 0.03. The BM was 0.24, 0.15, and 0.08. The SNR was 0.81, 0.91, and 0.99. The experimental results demonstrated that BF had relatively superior image processing performance. The processing time of each method was compared, and each dataset was segmented according to different sizes. The sizes of Dataset 1 to Dataset 4 were 100, 200, 400, and 800. Fig. 8 presents the results.



(a) Comparison of IoU of different algorithms
(b) Comparison of SIL of different algorithms
(c) Comparison of BM values between different models
(d) Comparison of SNR between different models

Fig. 7. Performance comparison of various image processing algorithms.



(a)Time under different Training set size (b)Time under different Training set size

Fig. 8. Comparison of model recognition time.

In Fig. 8, the proposed BF had the fastest image processing speed among all training sets. In training set 4, the training times for BF, GF, and MF were 101ms, 113ms, and 157ms, respectively. In Fig. 8(b), the proposed BF processing speed performed the best among the three algorithms in each validation set. In validation set 4, the training times for BF, GF, and MF were 201ms, 352ms, and 374ms. The suggested image processing method exhibited the best performance among various algorithm models. In Table I, the comprehensive capability of the three algorithm models was compared.

TABLE I. COMPARISON OF IMAGE PROCESSING PERFORMANCE OF VARIOUS ALGORITHMS

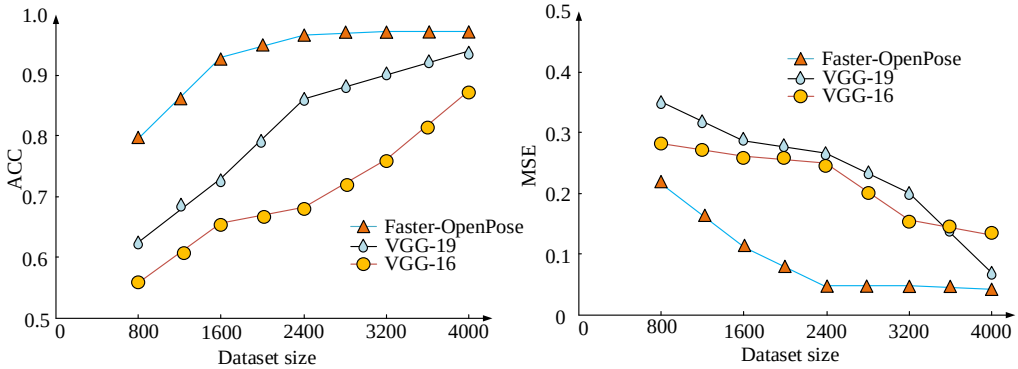
Image type	MF		GF		BF	
	IoU	*SIL*	*IoU*	*SIL*	*IoU*	*SIL*
Image type 1	0.82	0.35	0.87	0.19	0.95	0.13
Image type 2	0.75	0.33	0.84	0.17	0.91	0.11
Image type 3	0.89	0.31	0.94	0.15	0.99	0.09
Image type 4	0.81	0.33	0.85	0.17	0.96	0.11
Image type 5	0.90	0.37	0.96	0.21	0.98	0.15

In Table I, the recognition IoUs of MF for various types of images were 0.82, 0.75, 0.89, 0.81, and 0.90, respectively. The IoUs of GF model for various types of images were 0.87, 0.84, 0.94, 0.85, and 0.96, respectively. The IoU values of BF for various types of images were 0.95, 0.91, 0.99, 0.96, and 0.98, respectively. Therefore, the proposed BF image processing method had excellent performance.

B. *Performance Analysis of DI Detection Model Combined with Cascaded DWCA*

Following an evaluation of the efficacy of various image processing techniques, it is essential to assess the performance of the proposed recognition model. Visual Geometry Group 16 (VGG-16) and Visual Geometry Group 19 (VGG-19) were introduced and compared with the model built within this study. Fig. 9 clearly illustrates the results.

As the size of the dataset increased, the accuracy of each model also increased in a corresponding manner, as illustrated in Fig. 9(a). As the dataset size was 4000, the accuracy of Faster OpenPose, VGG-19, and VGG-16 were 0.97, 0.91, and 0.84, respectively. In Fig. 9(b), as the dataset increased, the Mean Square Error (MSE) of each model decreased accordingly. When the dataset size was 4000, the MSE of VGG-16, VGG-19, and Faster OpenPose were 0.11, 0.09, and 0.03, respectively. The analysis of different types of DI is shown in Fig. 10.



(a) Comparison of accuracy of different algorithm models (b) Comparison of MSE of different algorithm models

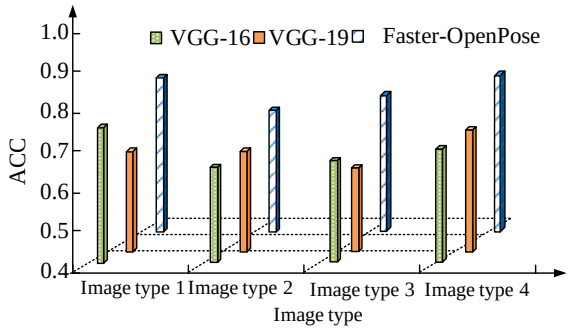
Fig. 9. Performance comparison results of various models.

In Fig. 10(a), among the three method models, Faster OpenPose had the best performance, with recognition rates of 0.91, 0.87, 0.89, and 0.93 for four different images, respectively. In Fig. 10(b), among the three models, Faster OpenPose had the shortest processing time, with processing times of 0.32, 0.31, 0.28, and 0.27 for the four types of images, respectively. Therefore, the proposed Faster OpenPose model had excellent performance. A total of 50 individuals were randomly selected and divided into five groups for the purpose of evaluating the performance of the model. Table II clearly presents the results.

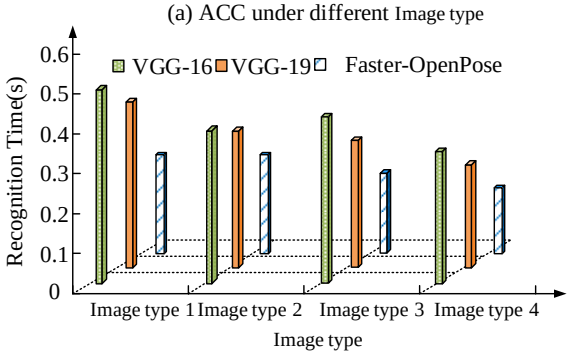
TABLE II. USER EVALUATION FORM

Type	Group 1	Group 2	Group 3	Group 4	Group 5	AVG
Faster-OpenPose	93.5	93.4	88.6	81.6	87.2	88.5
VGG-19	77.9	85.2	75.4	74.9	83.3	79.2
VGG-16	74.6	81.9	70.5	68.5	81.4	75.2

In Table II, the five evaluation groups rated Faster OpenPose at 93.5, 93.4, 88.6, 81.6, 87.2, and 88.5, respectively, and rated VGG-16 at 74.6, 81.9, 70.5, 68.5, 81.4, and 75.2, respectively. As a result, the Faster OpenPose proposed had received high praise from various users.



(a) ACC under different Image type



(b) Model recognition time under Image type

Fig. 10. Analysis of recognition performance of different images.

V. DISCUSSION

A depth image keypoint detection model based on bilateral filtering and cascaded depth separable convolution modules has been proposed, which demonstrates significant advantages in processing depth images. The experimental results show that when the training set size is 800, the intersection to union ratio of the BF model reaches 0.96, which shows better image processing performance compared to the 0.91 and 0.83 of GF and MF. In addition, the signal-to-noise ratio of the bilateral filtering model is 0.99, while GF and MF are 0.91 and 0.81, respectively. This is because bilateral filtering effectively balances denoising and edge preservation, which enables the model to reduce noise interference while maintaining important edge information when processing depth images, thereby improving the intersection to union ratio and signal-to-noise ratio. This is similar to the research results of Smith J et al. [23]. When using Faster OpenPose network for keypoint detection, the model has improved accuracy compared to traditional OpenPose. When the dataset size is 4000, the accuracy of the Faster OpenPose model reaches 0.97, while VGG-19 and VGG-16 are 0.91 and 0.84, respectively, and the MSE is significantly reduced. Faster OpenPose is 0.03, VGG-19 and VGG-16 are 0.09 and 0.11, which is similar to the research results of Jones M et al. [24]. This is because the cascaded depthwise separable convolution module significantly reduces the number of parameters and computational complexity of the model by splitting the standard convolution into depthwise convolution and pointwise convolution. This enables the model to maintain high accuracy while improving processing speed. This indicates that the design of depth separable convolution modules effectively reduces computational complexity and improves the model's adaptability to different types of images. However, there are also some shortcomings in the research. The performance of a model largely depends on the quality and diversity of the training data, and biases in the dataset can affect the model's generalization ability. In complex scenarios, interference from background information remains a major issue.

VI. CONCLUSION

In response to the problems of low efficiency and insufficient accuracy in traditional methods for handling DI, this study proposes a DI keypoint detection model that combines cascaded DWCA. It optimizes the computational efficiency and the model's detection capability by improving the OpenPose network structure. When the training set size was 800, the IoU of BF, GF, and MF were 0.83, 0.91, and 0.96; The SIL were 0.10, 0.06, and 0.03; The BM were 0.24, 0.15, and 0.08; The SNRs were 0.81, 0.91, and 0.99. When the dataset size was 4000, the accuracies of Faster OpenPose, VGG-19, and VGG-16 were 0.97, 0.91, and 0.84, respectively, with MSE of 0.11, 0.09, and 0.03, respectively. Therefore, the DI keypoint detection method combined with cascaded DWCA has high practical value and can effectively enhance the processing efficiency of DI keypoint detection. However, the research also has certain limitations. The performance of a model is highly dependent on the quality and diversity of the training data. If the dataset is not rich enough or has biases, it may affect the model's generalization ability. Secondly, although Faster OpenPose networks have improved efficiency, delays may still occur in extremely complex scenarios, which can affect real-time application performance. Although background filtering is used, in some cases, complex backgrounds may still interfere with keypoint detection, leading to inaccurate localization. In the future research direction, more lightweight network structures can be explored to adapt to real-time applications of edge computing and mobile devices and improve processing efficiency. It can enhance the adaptability to complex scenes and dynamic backgrounds, and improve the robustness and

accuracy of the model by integrating more types of data. In addition, utilizing emerging technologies such as self supervised learning and transfer learning can enhance the model's generalization ability on small sample datasets. Finally, research can delve into the methods of multimodal fusion, combining depth images with other sensor data to achieve more accurate keypoint detection and application expansion.

REFERENCES

[1] Li K, Liu Z, Zhou J, Dai Y, Liu Q, An J, Liu Y. Detection Algorithm of the Seabed Man-made Elongated Target Based on Synthetic Aperture Sonar Image. Basic & clinical pharmacology & toxicology, 2020, 127(1):117-118.

[2] Xiong Y, Yang L. Asian international students' help-seeking intentions and behavior in American Postsecondary Institutions. International Journal of Intercultural Relations, 2020, 80(2021):170-185.

[3] Zhou K, Zhang Z, Yuan R, Chen E. A deep learning algorithm for fast motion video sequences based on improved codebook model. Neural Computing and Applications, 2023, 35(6): 4353-4368.

[4] Zhou H, Ren D, Xia H, Fan M, Yang X, Huang H. AST-GNN: An Attention-based Spatio-temporal Graph Neural Network for Interaction-aware Pedestrian Trajectory Prediction. Neurocomputing, 2021,445(20):298-308.

[5] Lee J, Hwang K. YOLO with adaptive frame control for real-time object detection applications. Multimedia Tools and Applications, 2022, 81(25): 36375-36396.

[6] Jiang X, Yu F R, Song T, Ma Z, Zhu D. Blockchain-Enabled Cross-Domain Object Detection for Autonomous Driving: A Model Sharing Approach. IEEE Internet of Things Journal, 2020, 7(5):3681-3692.

[7] Yang Y. A Vehicle Recognition Algorithm Based on Deep Convolution Neural Network. Traitement du Signal, 2020, 37(4):647-653.

[8] Chen D, Sun S, Lei Z, Shao H, Wang Y.Ship Target Detection Algorithm Based on Improved YOLOv3 for Maritime Image. Journal of Advanced Transportation, 2021, 21(10):212-223.

[9] Tumrani S, Deng Z, Lin H, Shao J.Partial attention and multi-attribute learning for vehicle re-identification. Pattern Recognition Letters, 2020, 138(10):290-297.

[10] Kikuchi T, Fukuda T, Yabuki N. Diminished reality using semantic segmentation and generative adversarial network for landscape assessment: evaluation of image inpainting according to colour vision. Journal of Computational Design and Engineering, 2022, 9(5): 1633-1649.

[11] Li G, Ji Z, Qu X, Zhou R, Cao D. Cross-domain object detection for autonomous driving: A stepwise domain adaptative YOLO approach. IEEE Transactions on Intelligent Vehicles, 2022, 7(3): 603-615.

[12] Lee J, Hwang K. YOLO with adaptive frame control for real-time object detection applications. Multimedia Tools and Applications, 2022, 81(25): 36375-36396.

[13] Liang S, Wu H, Zhen L, Hua Q, Garg S, Kaddoum G. Edge YOLO: Real-time intelligent object detection system based on edge-cloud cooperation in autonomous vehicles. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(12): 25345-25360.

[14] Huang L, Ye L, Li R, Zhang S, Qu C, Li S. Dynamic human retinal pigment epithelium (RPE) and choroid architecture based on single-cell transcriptomic landscape analysis. Genes & Diseases, 2023, 10(6): 2540-2556.

[15] Wang X, Sun X, Wang Z. Construction of visual evaluation system for building block night scene lighting based on multi-target recognition and data processing. IET Circuits, Devices & Systems, 2023, 17(3): 149-159.

[16] Hui, Peng, Yifan, Zhang, Sen, Yang, Bin, Song. Battlefield Image Situational Awareness Application Based on Deep Learning. IEEE Intelligent Systems, 2019, 35(1):36-43.

[17] Laroca R, Zanlorensi L A, Gonalves G R, Todt E, Menotti D. An efficient and layout¨Cndependent automatic license plate recognition system based on the YOLO detector. IET Intelligent Transport Systems, 2021, 15(4):483-503.

[18] Feng H, Jie S, Hang M, Wang R, Fang F, Zhang G. A novel framework on intelligent detection for module defects of PV plant combining the visible and infrared images. Solar Energy, 2022, 236(4):406-416.

[19] Hu G X, Hu B L, Yang Z, Huang L, Li P. Pavement Crack Detection Method Based on Deep Learning Models. Wireless Communications and Mobile Computing, 2021, 32(1):1-13.

[20] Fitzpatrick B R, Berends M, Ferrare J J, Waddington RJ. Virtual Illusion: Comparing Student Achievement and Teacher and Classroom Characteristics in Online and Brick-and-Mortar Charter Schools. Educational Researcher, 2020, 49(3):161-175.

[21] Soffer T, Cohen A. Students' engagement characteristics predict success and completion of online courses. Journal of Computer Assisted Learning, 2019, 35(3):378-389.

[22] Pal S, Roy A, Shivakumara P, Pal U. Adapting a Swin Transformer for License Plate Number and Text Detection in Drone Images. Artificial Intelligence and Applications, 2023, 1(3), 145-154.

[23] Smith J, Brown A, Johnson L. Robust Feature Extraction for Keypoint Detection in Complex Environments. Journal of Computer Vision, 2022, 45(3): 123-135

[24] Jones M, Li Y. Multimodal Fusion Techniques for Enhanced Detection Performance. International Conference on Image Processing, 2023, 12(2): 45-60.

Development of a Service Robot for Hospital Environments in Rehabilitation Medicine with LiDAR-Based Simultaneous Localization and Mapping

Sayat Ibrayev, Arman Ibrayeva, Bekzat Amanov, Serik Tolenov
Joldasbekov Institute of Mechanics and Engineering, Almaty, Kazakhstan

***Abstract*—This paper presents the development and evaluation of a medical service robot equipped with 3D LiDAR and advanced localization capabilities tailored for use in hospital environments. The robot employs LiDAR-based Simultaneous Localization and Mapping (SLAM) to navigate autonomously and interact effectively within complex and dynamic healthcare settings. A comparative analysis with the established 3D-SLAM technology in Autoware version 1.14.0, under a Linux ROS framework, provided a benchmark for evaluating our system's performance. The adaptation of Normal Distribution Transform (NDT) Matching to indoor navigation allowed for precise real-time mapping and enhanced obstacle avoidance capabilities. Empirical validation was conducted through manual maneuvers in various environments, supplemented by ROS simulations to test the system's response to simulated challenges. The findings demonstrate that the robot's integration of 3D LiDAR and NDT Matching significantly improves navigation accuracy and operational reliability in a healthcare context. This study not only highlights the robot's ability to perform essential tasks with high efficiency but also identifies potential areas for further improvement, particularly in sensor performance under diverse environmental conditions. The successful deployment of this technology in a hospital setting illustrates its potential to support medical staff and contribute to patient care, suggesting a promising direction for future research and development in healthcare robotics.**

***Keywords*—Medical service robots; 3D LiDAR technology; autonomous navigation; hospital environments; robot-assisted healthcare; healthcare robotics; operational reliability; patient care automation**

I. Introduction

The integration of robotics into healthcare represents a transformative shift in rehabilitation medicine, promising enhanced precision, efficiency, and patient outcomes. Rehabilitation robotics, especially in hospital environments, has seen considerable growth, propelled by advancements in automation and sensor technology. This paper focuses on the development of a medical service robot designed specifically for hospital settings in rehabilitation medicine, employing LiDAR-based Simultaneous Localization and Mapping (SLAM) to navigate and function autonomously [1].

Rehabilitation robots are primarily developed to assist with the delivery of intensive, repetitive, and task-specific interventions which are often labor-intensive and require high levels of precision [2]. The role of these robots extends beyond mere assistance, as they are increasingly equipped with autonomous features that allow them to navigate complex hospital environments and interact with patients and healthcare staff effectively [2]. The adoption of LiDAR technology in medical service robots enhances these capabilities by providing accurate and real-time 3D maps of the environment, which is critical for the autonomous navigation and operational safety of robots [3].

The importance of autonomous navigation systems in medical robots cannot be overstated, as they significantly reduce the human resources needed for operation and maintenance, thereby increasing the healthcare system's overall efficiency [4]. Simultaneous Localization and Mapping (SLAM) technology, which combines data from various sensors to create a map of an unknown environment while simultaneously tracking the robot's location, is pivotal in this context. SLAM has been extensively studied and applied in mobile robotics, and its adaptation to the specific needs of medical environments presents unique challenges and opportunities [5].

The application of SLAM in medical service robots involves not only technical development but also consideration of the ethical, privacy, and safety concerns associated with robotic operations in human-centric environments [6]. Robots in hospitals must adhere to stringent safety standards and be capable of interacting with patients in a manner that complements the therapeutic goals of rehabilitation [7]. Furthermore, the integration of robots into public health settings raises significant privacy concerns, particularly in relation to the storage and handling of sensitive patient data captured by robotic sensors [8].

The development of robots equipped with LiDAR and SLAM for rehabilitation medicine also necessitates a multidisciplinary approach, combining insights from engineering, computer science, and healthcare. Such collaboration is crucial for ensuring that the robots are not only technically proficient but also tailored to meet the practical needs of patients and healthcare providers [9]. Moreover, the implementation of these technologies must be supported by robust clinical trials to validate their efficacy and safety in real-world hospital settings [10].

Past research has demonstrated the potential of robotic aids in enhancing patient engagement and improving recovery outcomes in rehabilitation settings [11]. For instance, robots that assist with walking or deliver physical therapy have been shown to improve mobility and accelerate recovery, providing a level of consistency and repeatability that is difficult to achieve through human intervention alone [12]. The development of a medical service robot with sophisticated navigation and mapping capabilities could further these benefits by enabling more dynamic and responsive interaction with the environment and the patients.

This research aims to bridge the gap between the current capabilities of medical service robots and the evolving demands of modern healthcare facilities. By focusing on the integration of LiDAR-based SLAM technology, the study seeks to address several of the limitations faced by earlier models of rehabilitation robots, such as limited autonomy and the inability to adapt to new and complex environments [13]. The ultimate goal is to develop a robot that not only supports the logistical needs of hospitals but also contributes directly to the therapeutic processes, enhancing the overall quality of care and patient satisfaction [14].

The development of a medical service robot equipped with LiDAR-based SLAM technology for use in rehabilitation medicine represents a significant advancement in the field. This research contributes to a deeper understanding of the technical challenges and clinical implications of deploying autonomous robots in sensitive environments, aiming to maximize both the efficacy and safety of robotic interventions in healthcare settings [15].

II. Related Works

In the evolving landscape of rehabilitation medicine, the integration of robotics has marked a significant technological advancement, aiming to enhance patient care through automated assistance and precise intervention. The adoption of advanced technologies like LiDAR and Simultaneous Localization and Mapping (SLAM) within medical service robots presents a novel approach to navigating complex hospital environments efficiently. This section reviews the pertinent literature surrounding rehabilitation robotics, with a focus on the incorporation of these sophisticated technologies into their design and functionality. The discussion extends across the technological underpinnings, applications, and the specific challenges faced, thereby setting a foundational context for this research.

A. Overview of Rehabilitation Robotics

Rehabilitation robotics has emerged as a vital tool in modern therapeutic practices, primarily focusing on enhancing patient recovery and automating repetitive therapy tasks. These robotic systems are designed to deliver high-intensity, precise interventions that are essential for the rehabilitation of patients with diverse physical impairments. According to Zhao et al. (2022), rehabilitation robots not only facilitate consistent therapeutic activities but also significantly reduce the physical burden on healthcare providers by automating routine tasks [16].

The evolution of these systems has been marked by significant advancements in their ability to interact with patients and adapt to various therapeutic needs. As highlighted by Hou et al. (2024), the integration of sophisticated sensors and actuators in these robots enables them to perform complex tasks with greater autonomy and accuracy [17]. This technological enhancement improves the quality of interventions and supports a broader range of rehabilitation activities.

Moreover, the clinical impact of rehabilitation robotics is profound, with studies indicating improved patient outcomes in mobility and independence [18]. These robots provide tailored therapeutic exercises that are crucial for effective rehabilitation, making them an indispensable asset in modern healthcare settings.

B. Technological Foundations in Medical Service Robots

Medical service robots incorporate a variety of advanced technologies to enhance their functionality and autonomy in healthcare settings. Central to their operation are automation technologies and intelligent systems that allow these robots to perform a wide range of tasks, from patient care to logistical support within hospitals. According to Avutu et al. (2023), the use of real-time data processing and machine learning enables these robots to make informed decisions and adapt to dynamic environments, significantly enhancing their operational efficiency [19].

Actuators and sensor technologies play pivotal roles in the functionality of medical service robots. These components ensure precise control and interaction capabilities, critical for tasks that require high levels of accuracy such as medication delivery or patient monitoring [20]. Furthermore, the integration of communication interfaces facilitates seamless interaction with healthcare professionals, allowing for efficient coordination and data exchange.

Moreover, the implementation of robotics in medical services often involves complex system architectures that combine hardware and software solutions to meet the stringent safety and performance requirements typical of medical environments [21]. These integrated systems not only ensure patient safety but also contribute to the overall resilience and reliability of robotic operations in healthcare settings.

C. Use of LiDAR Technology in Robotics

Light Detection and Ranging (LiDAR) technology has been pivotal in advancing robotic navigation systems. LiDAR sensors provide accurate distance measurements by illuminating a target with laser light and measuring the reflection with a sensor. This technology's application in robotics, as detailed by Chen et al. (2023), involves creating high-resolution maps of the robot's surroundings, which is essential for navigating through dynamic environments without human input [22]. In medical settings, the precision of LiDAR technology ensures that robots can navigate crowded hospital corridors and interact with patients and staff safely.

D. Simultaneous Localization and Mapping (SLAM)

SLAM technology is crucial for autonomous navigation, enabling robots to build a map of an unknown environment while simultaneously tracking their location within it. The convergence of SLAM with medical service robots enhances their operational autonomy. Takanokura et al. (2023) discuss

various SLAM algorithms, each with different strengths, catering to the specific needs of the environment and the task at hand [23]. In the context of rehabilitation robotics, the implementation of SLAM allows robots to adapt to new and evolving environments, facilitating seamless integration into hospital settings.

E. Integration of SLAM in Medical Robotics

The integration of Simultaneous Localization and Mapping (SLAM) technology in medical robotics represents a significant advancement in the autonomous operational capabilities of these systems within complex healthcare environments. SLAM technology allows medical robots to dynamically map their surroundings while maintaining an accurate location within the map, which is critical for navigation and task execution in hospital settings [24].

Incorporating SLAM into medical robotics facilitates enhanced spatial awareness and adaptability, enabling these robots to autonomously maneuver through crowded and dynamically changing hospital corridors and rooms. According to Mbunge et al. (2021), the ability to update and refine their environmental models in real-time allows these robots to operate safely and efficiently around both stationary obstacles and moving individuals, such as patients and medical staff [25].

Furthermore, the application of SLAM in medical robotics not only improves operational efficiency but also enhances the interaction capabilities of these robots with their human counterparts. Pereira et al. (2022) highlight that SLAM-equipped robots can more effectively collaborate with healthcare providers, ensuring that therapeutic and logistical tasks are carried out with minimal human intervention [26]. This seamless integration into healthcare workflows greatly contributes to the overall productivity and patient care standards within medical facilities.

F. Challenges and Limitations

Despite the advancements, the integration of LiDAR and SLAM into medical service robots faces significant challenges. Yam et al. (2021) outline several technical challenges, including the high cost of LiDAR sensors and the computational demands of SLAM algorithms, which can limit their widespread adoption [27]. Additionally, ethical concerns regarding patient privacy and data security are paramount, as these technologies often collect sensitive information that could be vulnerable to breaches. Makhdoom et al. (2022) stress the importance of developing robust security protocols to protect patient data and ensure compliance with healthcare regulations [28].

G. Gap Analysis

The current literature reveals several gaps in the application of advanced technologies like LiDAR and SLAM within the domain of medical service robots, particularly in rehabilitation settings. While significant advancements have been made in technical capabilities, there is a lack of comprehensive studies focusing on the practical integration of these technologies in real-world healthcare environments [29]. Additionally, existing research often overlooks the user-centric design and ethical considerations essential for deploying robots in sensitive areas such as patient care [30].

Moreover, despite the potential of these technologies to enhance robotic functionality, there is a notable deficiency in tailored solutions that address specific clinical needs and seamlessly adapt to the unique dynamics of hospital settings [31]. Addressing these gaps through focused research could lead to more effective and contextually appropriate robotic systems that improve patient outcomes and healthcare efficiency [32].

III. MATERIALS AND METHODS

A. Data Collection

The conceived system of the driven automated guided vehicle (AAGV) was formulated to elevate the execution of manual environmental mapping tasks currently in use through the utilization of self-positioning and autonomous navigation that operates nearby the layout map of the area. Given the fill running of an environmental assessment, the AGV autonomously constructs a map of the surrounding, a process that depends on conventional methods as well. This innovative approach exploits the factory indoor formation for micro-localization and precise mobile robot self-positioning. By using point cloud data as input, 3D Lidar's structural analysis module focuses on the portion gleaned from the wall structures, where the variance is measured subsequently by comparing it with a reference 2D layout map and the mapped horizontal trajectory (or wheel odometry) of the UGV. The filtering method implemented to achieve the localization uses a particle filter with Monte Carlo method, while the base of this navigation is the information determined from the map coordinate and transformed point cloud data [33].

Fig. 1 presents the basic control scheme of the proposed medical service robot, illustrating the integration of 3D LiDAR technology for autonomous navigation within hospital environments. The control architecture is divided into three primary components: 3D LiDAR processing, Mapping, and Path Planning. Initially, the 3D LiDAR sensor collects point cloud data which is processed by the Encoder and Odometry to track the robot's position and movement. Wall point clouds are extracted to delineate boundaries and detect obstacles, ensuring the robot avoids collisions. Subsequently, the Mapping process involves assessing the robot's position and converting the environmental map to a point cloud format for real-time navigation updates. In the Path Planning segment, the robot sets navigation goals, computes feasible paths, and creates a navigational trajectory, culminating in the autonomous mobility of the robot. This control scheme underscores a comprehensive approach to navigating complex healthcare settings, leveraging advanced sensing and computational techniques to enhance operational efficacy and safety.

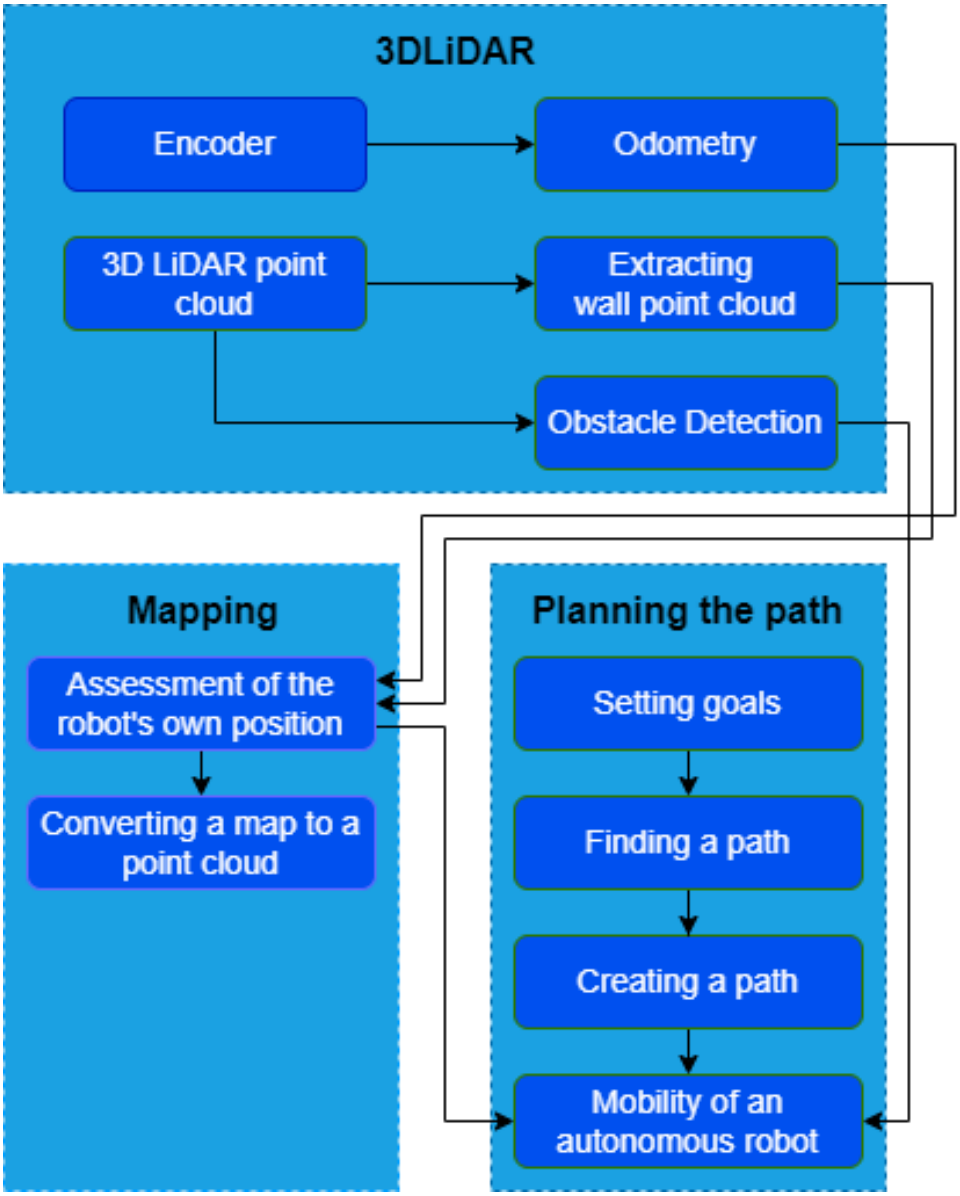


Fig. 1. Basic control scheme of the proposed medical service robot.

B. *The Hardware Module*

In this study, the Shenzhen Yahboom Technology Rosmaster X3 Plus mobile robot was utilized as a primary research tool. This robot, operating within a hybrid system environment, combines physical hardware with virtual systems managed through Ubuntu 20.04 on a VMware Workstation virtual machine, and further controlled via the ROS-Noetic operating system specifically tailored for robotic management. The choice of the Rosmaster X3 Plus for this research is predicated on its advanced capabilities and adaptability to complex tasks, making it an ideal candidate for detailed study in robotic navigation and interaction within structured environments.

The Rosmaster X3 Plus is equipped with cutting-edge hardware that enhances its sensing and computational abilities, crucial for effective navigation and task execution. Central to its operation is the Jetson Orin NX processor, boasting 16GB of memory, which facilitates robust real-time processing for tasks such as obstacle navigation and localization. Environmental perception is significantly enhanced by the integration of a YDLidar 4ROS Lidar system, which provides high-resolution 3D point cloud data. Complementing this, an Astra Pro depth camera provides detailed 3D visual inputs that are integrated with the Lidar data for a comprehensive environmental understanding. This hardware-software synergy not only boosts the robot's operational efficiency but also underscores the effectiveness of modern technologies in autonomous robotic navigation.

The operation of the motor is governed by signals originating from Pulse Width Modulation (PWM), which dictate the motor's speed, and directional signals that guide the rotation. These commands are dispatched by a microcomputer integrated within the motor driver, initiating motion based on inputs. Fig. 3 shows motor drive set-up.

Fig. 2. Medical service robot of the study.

Fig. 3. Motor drive setup (a) DC Motor setup (b) Encoder configuration.

Further, a serial communication line facilitates the transmission of these commands from the microcomputer to a personal computer (PC), allowing operators to manage the cart's functions effectively through PC-based controls. Additionally, communication between the motor's encoder and the microcomputer is handled via an SPI interface, which transmits precise rotational angle data, subsequently relayed to the PC, enhancing clarity in monitoring and controlling the motor's activity and the cart's trajectory.

C. Odometry

The integration of 3D LiDAR with wheel odometry equips the robot with enhanced capabilities to both perceive its surroundings and track its movement accurately. Odometry, fundamentally reliant on mathematical equations and principles, plays a crucial role in this process. It operates by analyzing the rotation of the robot's wheels, which directly informs the calculation of the distance traveled. Each wheel is equipped with an encoder that records the number of rotations, allowing for precise measurement. Given the radius r of the wheels and the number of encoder ticks N, the distance D each wheel travels can be calculated, providing critical data for navigating and mapping the robot's environment effectively.

$$D = 2\pi r\left(\frac{N}{N_{total}}\right) \tag{1}$$

Where N_{total} is the total number of ticks per complete wheel rotation.

For a two-wheeled robot, the distance traveled (D_{avg}) and change in orientation are given by:

$$D_{avg} = \frac{D_L + D_R}{2} \tag{2}$$

$$\Delta\theta = \frac{D_R - D_L}{W} \tag{3}$$

Where D_L and D_R are the distances traveled by the left and right wheels, respectively, and W is the width between the wheels.

3D LiDAR technology generates a detailed point cloud that captures the robot's surroundings, facilitating a comprehensive understanding of its movements and orientation through external reference points. When combined with wheel odometry, LiDAR helps to correct potential inaccuracies and drifts that may accumulate in the odometry data over time. Fig. 2 shows medical service robot of the study.

The process of merging odometry with 3D LiDAR data involves a methodical approach:

1) Initial estimation: Wheel odometry is initially used to estimate the robot's trajectory.

2) LiDAR correction: The point cloud produced by LiDAR is compared against a pre-established map to identify any deviations that suggest errors in the odometry data.

3) Data fusion: Techniques such as the Kalman filter are employed to amalgamate the data from both odometry and LiDAR. This integration enhances the accuracy of the robot's navigation system by providing a more reliable data set that

accounts for any discrepancies identified between the odometry and LiDAR inputs.

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k\left(y_k - H\hat{x}_{k|k-1}\right) \tag{4}$$

Where $\hat{x}_{k|k}$ is the a posteriori state estimate, $\hat{x}_{k|k-1}$ is the a priori estimate, K_k is the Kalman gain, y_k represents the measurement (Lidar data), and H is the measurement matrix relating the state to the measurement.

Update Position and Orientation: Adjust the robot's estimated position and orientation based on the fused data:

$$\begin{aligned} x' &= x + \Delta x \\ y' &= y + \Delta y \\ \theta' &= \theta + \Delta\theta \end{aligned} \tag{5}$$

Subsequently, the robot's position and orientation are updated based on corrected data derived from the integration of wheel odometry and LiDAR measurements. This fusion ensures that the robot accurately maintains its location and direction, reducing errors that might arise from wheel slippage or uneven terrain.

By combining 3D LiDAR data with wheel odometry, our mobile robot achieves superior navigation precision and detailed environmental mapping. This sophisticated odometry system underpins the robot's ability to autonomously operate in complex and dynamically changing environments, facilitating reliable performance across various operational scenarios.

D. Localization

The navigation capability of our mobile robot is enhanced by 3D LiDAR technology, utilizing a sophisticated localization algorithm that precisely determines the robot's position within its operating environment. This section delves into the mathematical principles and operational mechanics of the localization algorithm employed in our system, emphasizing the integration of 3D scanning data to improve node localization accuracy.

Central to our localization strategy is Monte Carlo Localization (MCL), also known as particle filter localization. This probabilistic method uses a collection of hypothetical particles to represent potential positions and orientations (states) of the robot within its environment. Each particle is weighted based on its congruence with environmental data gathered via LiDAR scans and the robot's observed movements, effectively merging sensor inputs with motion data to estimate the robot's location with higher accuracy.

Particle Representation: In our system, each particle in the set represents a potential state of the robot, encompassing both its location and orientation, forming the basis for calculating the most probable actual state of the robot as it navigates.

$$p_i = \left(x_i, y_i, \theta_i\right) \tag{6}$$

x_i, y_i, θ_i denote the particle's position and orientation.

Weight Calculation. The weight w_i is calculated for each particle taking into account the degree of matching of the predicted sensor readings for the desired particle state with the real sensor readings given by the 3D Lidar.

$$w_i = P\left(z_t \mid p_i\right) \tag{7}$$

Where z_t is the Lidar measurement at time t, and $P\left(z_t \mid p_i\right)$ is the likelihood of observing z_t given the state represented by particle i.

Resampling within the Monte Carlo Localization (MCL) framework involves selecting particles based on their weights, with particles possessing higher weights more likely to be chosen. This process concentrates the particle distribution around the most likely states of the robot's position, refining the model's accuracy over time.

Integrating 3D LiDAR data significantly enhances the MCL algorithm's localization precision by allowing a detailed comparison between the environmental features detected by the LiDAR and the pre-existing map model. The LiDAR's point cloud captures environmental details at a granular level, facilitating highly accurate weight calculations for each particle within the model.

The sensor model associated with the 3D LiDAR converts the point cloud data from a sequential format into a probabilistic one, aligning it with the map's specifications. This transformation allows for an effective comparison, essentially converting 3D data into a more manageable 2D format to match the map, thereby enhancing the fidelity and utility of the particle data.

Before assigning weights to each particle, a motion update is conducted based on the reported movements of the robot. This update adjusts the positions and orientations of the particles to reflect the robot's dynamics as captured by its odometry data, ensuring that the model remains consistent with the robot's actual movements. The motion model updates are critical for maintaining the accuracy of the localization process.

$$p_i^{'} = p_i + \Delta p\left(u_t, \in\right) \tag{8}$$

where $p_i^{'}$ is the updated particle state, Δp is the change in state due to the control input u_t (e.g., velocity, angular velocity) at time t, and $\in$ represents the motion noise.

E. Obstacle Avoidance

Obstacle avoidance is a critical component of autonomous navigation systems, involving two main functions: detecting obstacles and formulating alternate paths to circumvent them. Consider a scenario where a predetermined route is blocked on the left side by an obstruction. In such cases, navigational coordinates are structured into waypoints, each associated with a specific detection zone. This zone is typically envisioned as a cylindrical area encompassing each waypoint along the robot's path, serving as a detection field for obstacles.

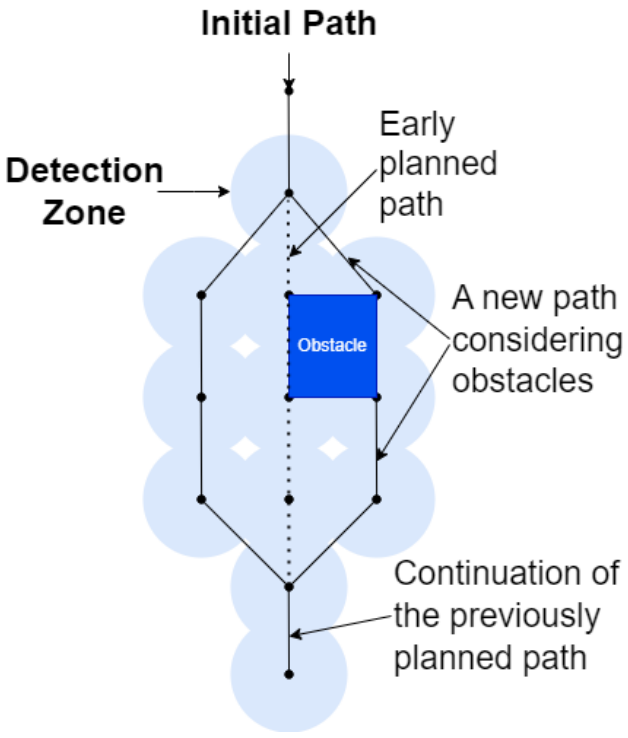


Fig. 4. Obstacle avoidance of the proposed medical service robot.

Within this cylindrical detection zone, any detected objects that do not correspond to the ground are classified as obstacles. The presence of these obstacles renders the area impassable, necessitating a rerouting of the planned path. This mechanism ensures that the robot can adapt its route in real-time to avoid obstacles, maintaining smooth and continuous navigation as depicted in Fig. 4.

The obstacle avoidance strategy within autonomous navigation systems functions by designating areas where obstacles are detected as blocked, typically highlighted in red on navigational maps. This prompts the system to seek alternative corridors for maneuvering around the impediment. The algorithm evaluates possible detours, actively searching for viable paths adjacent to the obstruction. If a feasible route is identified along one side of the obstacle, it is selected for navigation, and the route-finding algorithms are updated to reflect this new path. Conversely, if obstructions block all potential routes, rendering them impassable, the vehicle halts its progress until an alternate path becomes available. This adaptive mechanism ensures that the vehicle can flexibly and effectively navigate through varying environmental conditions by dynamically adjusting its course in response to encountered obstacles.

IV. Results

This section explores the evaluation of the map accuracy generated by our medical service robot, which is crucial for self-localization and overall system performance assessment. Our system was rigorously tested against the renowned 3D-SLAM technology implemented in Autoware version 1.14.0, an established open-source platform designed for autonomous driving technologies under the Linux ROS framework. A critical aspect of Autoware's capability is the Normal Distribution Transform (NDT) Matching, which utilizes point cloud scan matching to enhance localization accuracy. This method employs normal distributions to model point clouds within specified segments, facilitating precise alignment of overlapping point clouds, a feature vital for accurate localization in environments requiring high precision, such as autonomous navigation systems.

To empirically validate our system, data collection involved manually maneuvering a mobile trolley through various environments, recording its positions to verify the accuracy of the self-localization predictions. This testing covered diverse measurement points, extending through indoor and outdoor settings and spaces between different structures. Additionally, our self-localization methods were tested through ROS simulations using the collected positional data. This detailed validation approach ensures that our system's performance is thoroughly understood and reliable in practical scenarios, demonstrating robust capabilities in a real-world application context.

Fig. 5 presents a series of diagrammatic representations illustrating the navigation process within a two-dimensional environment, capturing the dynamic nature of path planning. The sequence starts with Fig. 5(a) and 5(b), which mark the initiation of the path planning phase and lay the groundwork for subsequent navigational decisions. This is followed by Fig. 5(c), which details the iterative steps involved in path planning as the robot maneuvers through various directions. This stage highlights the dynamic and repetitive nature of adjusting the planned route as the robot encounters different scenarios. Conclusively, Fig. 5(d) captures the culmination of the path planning process, displaying a finalized map that delineates the actual path taken by the robot. This sequence effectively demonstrates the progression from initial path determination through to adaptive adjustments and the final mapping, underscoring the complex and responsive strategy employed in robotic navigation.

Fig. 6 provides a detailed exploration of the path planning processes implemented by a robot within a three-dimensional framework, showcasing the steering strategies employed as it navigates through cluttered environments. This diagram effectively illustrates the robot's capability to assess and adapt its trajectory in real-time as it maneuvers through various terrains and obstacles in 3D space. It serves as a critical visual tool for understanding the sophisticated 3D capabilities of autonomous systems, highlighting their ability to perceive and interact with their surroundings comprehensively. The figure emphasizes the advanced algorithms that enable these systems to not only navigate intelligently but also to create detailed 3D maps upon the completion of their routes. This depiction confirms the complexity and dynamism of new 3D path planning techniques, reflecting significant advancements in the autonomous vehicle industry, where precision and efficiency are paramount in navigating complex environments.

a) Path planning from left to right side

b) Path planning from bottom to up

c) Path planning process

d) Path planning process has been completed

Fig. 5. The path planning process for the medical service robot.

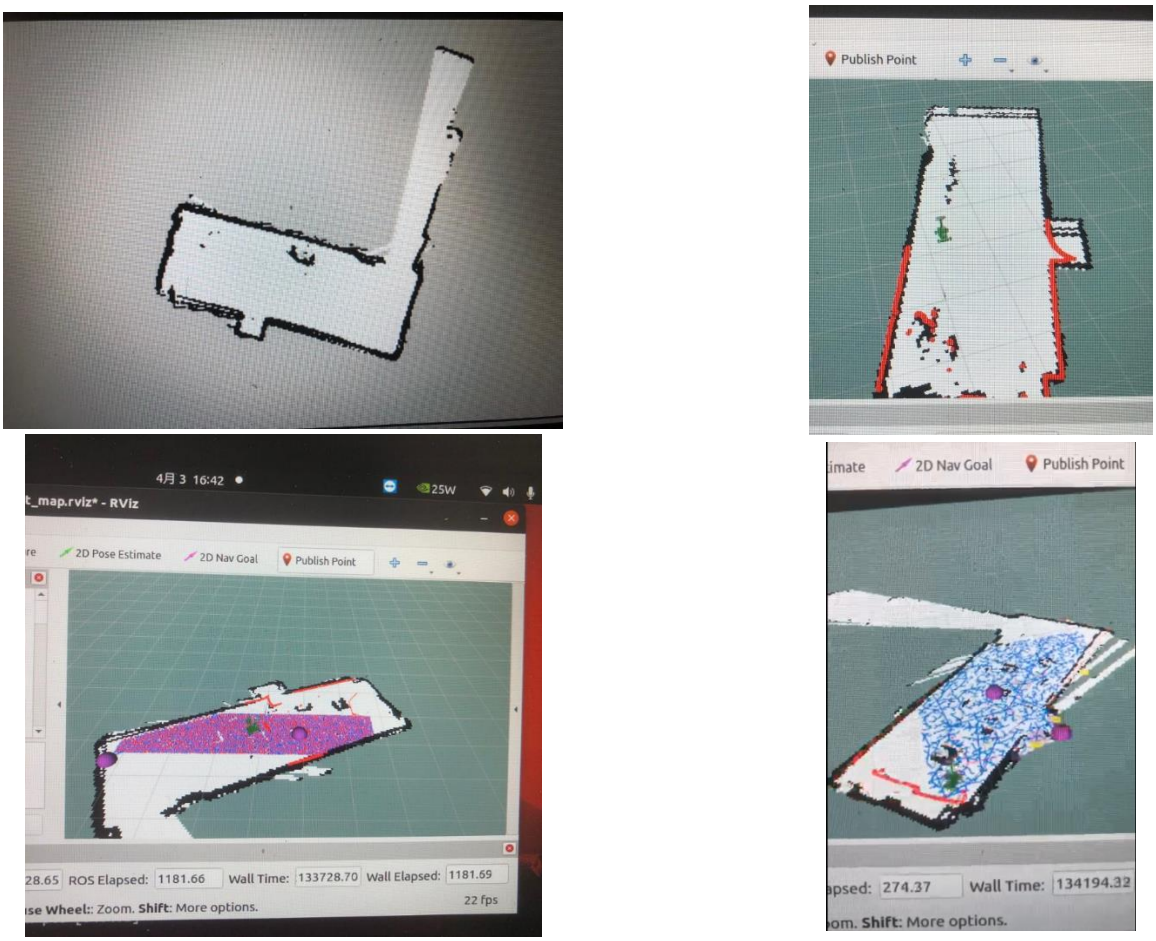


Fig. 6. Path planning in 3D for medical service robot from various foreshortening.

a) Start of mobile robot path planning b) Mobile robot navigation

Fig. 7. Mobile medical service robot navigation using 3D LiDAR.

Fig. 7 showcases the developed mobile robot equipped with 3D LiDAR technology, operating in a real-world or field setting, which illustrates the robot's design and its operational capabilities. This image particularly highlights how the integrated 3D LiDAR technology enables the robot to perceive and interact dynamically with its environment. The diagram captures the robot as it navigates a specified area, utilizing LiDAR data to facilitate steering, obstacle avoidance, and localization tasks. Through this visual representation, the practical functioning of the mobile robot is conveyed, underscoring the real-time application and demonstrating the effectiveness of the combined technologies in enhancing the navigation system. This figure serves as a vital link between the theoretical concepts underlying the study and their practical implementation, showcasing the translation of academic research into actionable, autonomy-enhancing strategies within robotic systems.

V. DISCUSSION

In this discussion, we delve into the findings from the deployment and validation of our medical service robot, equipped with advanced 3D LiDAR technology and an innovative localization system. The results underscore the robot's potential to revolutionize navigation and interaction within hospital environments, providing critical insights into both the capabilities and areas for further enhancement of autonomous robotic systems in healthcare settings.

The application of 3D LiDAR technology in our medical service robot has proven to be a cornerstone for enhancing autonomous navigation. The high-resolution data obtained from LiDAR not only facilitated accurate real-time mapping but also significantly improved the robot's ability to detect and navigate around obstacles. This capability is critical in a hospital setting where dynamic obstacles such as moving people and medical

equipment are common. The integration of 3D LiDAR with the robot's other sensory systems has enabled a level of situational awareness that is paramount for safe and efficient operation within such complex environments.

Our comparative analysis with Autoware's 3D-SLAM technology highlighted the effectiveness of our localization approach. The Normal Distribution Transform (NDT) Matching method, typically used in autonomous vehicular navigation, was adapted for indoor use with our robot. This adaptation was crucial as it addressed the unique challenges of indoor navigation, which include lower GPS reliability and the presence of numerous static and dynamic obstacles. The successful application of NDT in our system underscores its potential for broader application in other robotic systems that operate in similarly challenging environments.

Furthermore, the empirical validation of our robot's localization accuracy through manual maneuvering across different environments provided substantial evidence of its robustness. The robot demonstrated a high degree of precision in maintaining its course within tightly controlled trajectories, an essential feature for medical applications where precise movements are often necessary. However, it was noted that certain environmental conditions, such as highly reflective surfaces or areas with poor LiDAR reception, could disrupt the localization process. This finding points to the need for further research into improving sensor fusion techniques to mitigate the effects of such environmental factors on the robot's performance.

The ROS simulations used for further validation played a crucial role in this study, allowing us to replicate and analyze numerous scenarios that the robot might encounter. These simulations were instrumental in refining the robot's path planning algorithms, ensuring that the system could adapt to unexpected changes in the environment efficiently and effectively. The ability to conduct such simulations highlights the importance of flexible and robust software frameworks in the development of autonomous robotic systems.

Moreover, the data collected during the robot's operation in different factory settings revealed valuable insights into the practical challenges of deploying such systems in real-world environments. For instance, the transition from indoor to outdoor settings posed navigation challenges that were not fully anticipated, such as changes in lighting conditions affecting sensor performance. Addressing these challenges will require the development of adaptive algorithms capable of adjusting to varying environmental conditions seamlessly.

The discussion would be incomplete without considering the implications of this technology for patient care. The precision and reliability of the robot's navigation and localization systems have direct implications for its potential use in delivering medications, assisting with patient transport, or conducting routine monitoring tasks. These activities require a high level of accuracy to ensure patient safety and care quality. Our findings suggest that with further development, such robots could become integral components of healthcare delivery, enhancing the efficiency and effectiveness of medical services.

In summary, the development and validation of our medical service robot with integrated 3D LiDAR and advanced localization capabilities represent a significant step forward in the field of healthcare robotics. The successful deployment of this technology in a hospital environment showcases its potential to enhance operational efficiencies and patient care. Nonetheless, the study also highlights several areas for further improvement, particularly in enhancing the robot's adaptability to diverse and changing environments. Future research should focus on refining the integration of sensory and navigational technologies to build even more robust, versatile, and reliable robotic systems. Such advancements will not only improve the functionality of medical service robots but also expand their applicability across different sectors within healthcare, ultimately contributing to the broader goal of automating and improving medical service delivery.

VI. Conclusion

In conclusion, the research conducted on the development of a medical service robot equipped with 3D LiDAR and advanced localization technologies has substantiated its potential to significantly enhance navigational and operational capabilities in hospital environments. This study not only demonstrated the robot's proficiency in precise and adaptive navigation through complex and dynamic settings but also emphasized its utility in the context of healthcare delivery. The integration of 3D LiDAR technology facilitated a robust sensing environment, enabling the robot to perform with high levels of accuracy in obstacle detection and path planning. Moreover, the comparative validation with established technologies like Autoware's 3D-SLAM provided a robust framework for assessing the effectiveness of our localization system, confirming its applicability and reliability. Despite encountering challenges such as sensor sensitivity to environmental factors, the research identified critical insights for future enhancements, notably in improving sensor fusion and algorithm adaptability. These advancements are imperative for ensuring the robot can seamlessly integrate into the diverse and evolving landscape of healthcare facilities. The potential for such autonomous systems to assist in routine tasks and patient care suggests a promising horizon not only for improving efficiency but also for enriching the quality of care. Moving forward, continued refinement and testing in real-world conditions would be crucial to fully realize the capabilities of medical service robots, setting a precedent for their broader adoption in healthcare settings.

References

[1] Rout, A., Reddy, H., Raj, S. V., Reddy, B., Naidu, L., Kiran, K., & Ravikumar, R. (2024, May). Development of LIDAR-SLAM Integrated Low Cost Health Care Monitoring Robot with Sustainable Material. In 2024 9th International Conference on Control and Robotics Engineering (ICCRE) (pp. 12-16). IEEE.

[2] Liu, X., He, X., Wang, M., & Shen, H. (2022). What influences patients' continuance intention to use AI-powered service robots at hospitals? The role of individual characteristics. Technology in Society, 70, 101996.

[3] Maknuny, Z. J., Ramadhan, S. F., Turnip, A., & Sitompul, E. (2022, December). RPLiDAR-Based Mapping in Development of a Health Service Assisting Robot in COVID-19 Pandemic. In Proceeding of International Conference on Sustainable Engineering and Creative Computing (Vol. 1, No. 1, pp. 72-77).

[4] Mac, T. T., Doanh, N. T., Hieu, P. N. T., & Quy, H. V. (2021). The Development of 2D Slam-Based Navigation for an Autonomous Nursing

Robot in Global Covid 19 Period. In Proceedings of the 2nd Annual International Conference on Material, Machines and Methods for Sustainable Development (MMMS2020) (pp. 1053-1060). Springer International Publishing.

[5] Huang, R., Li, H., Suomi, R., Li, C., & Peltoniemi, T. (2023). Intelligent physical robots in health care: systematic literature review. Journal of medical Internet research, 25, e39786.

[6] Wu, X., Zhang, H., Kong, C., Wang, Y., Ju, Y., & Zhao, C. (2024). LIDAR-based 3D human pose estimation and action recognition for medical scenes. IEEE Sensors Journal.

[7] Pennington, Z., Judy, B. F., Zakaria, H. M., Lakomkin, N., Mikula, A. L., Elder, B. D., & Theodore, N. (2022). Learning curves in robot-assisted spine surgery: a systematic review and proposal of application to residency curricula. Neurosurgical focus, 52(1), E3.

[8] Crnokić, B., Peko, I., & Gotlih, J. (2024, April). The Development of Assistive Robotics: A Comprehensive Analysis Integrating Machine Learning, Robotic Vision, and Collaborative Human Assistive Robots. In International Conference on Digital Transformation in Education and Artificial Intelligence Application (pp. 164-214). Cham: Springer Nature Switzerland.

[9] Di Lallo, A., Murphy, R., Krieger, A., Zhu, J., Taylor, R. H., & Su, H. (2021). Medical robots for infectious diseases: lessons and challenges from the COVID-19 pandemic. IEEE Robotics & Automation Magazine, 28(1), 18-27.

[10] Gonzalez-Aguirre, D. I., Perez-Ramirez, J., Felix-Rendon, J., Leon, J. F., Bourgault, J., Esquivel, J. Z., & Nachman, L. (2023). Robot-based uniform-coverage and high-resolution lidar mapping for physically-grounded metaverse applications. IEEE Internet of Things Magazine, 6(1), 40-45.

[11] Altınpınar, O. V., & Sezer, V. (2023). A novel indoor localization algorithm based on a modified EKF using virtual dynamic point landmarks for 2D grid maps. Robotics and Autonomous Systems, 170, 104546.

[12] Zandi, R., Behzad, K., Motamedi, E., Salehinejad, H., & Siami, M. (2024). Robofisense: Attention-based robotic arm activity recognition with wifi sensing. IEEE Journal of Selected Topics in Signal Processing.

[13] Asaad, S. M., & Maghdid, H. S. (2022). A comprehensive review of indoor/outdoor localization solutions in IoT era: Research challenges and future perspectives. Computer Networks, 212, 109041.

[14] Shiwlani, A., Khan, M., Sherani, A. M. K., & Qayyum, M. U. (2023). Synergies of AI and Smart Technology: Revolutionizing Cancer Medicine, Vaccine Development, and Patient Care. International Journal of Social, Humanities and Life Sciences, 1(1), 10-18.

[15] Guo, Y., Dagnino, G., & Yang, G. Z. (2024). Hospital Automation Robotics. In Medical Robotics: History, Challenges, and Future Directions (pp. 101-114). Singapore: Springer Nature Singapore.

[16] Pauwels, P., de Koning, R., Hendrikx, B., & Torta, E. (2023). Live semantic data from building digital twins for robot navigation: Overview of data transfer methods. Advanced Engineering Informatics, 56, 101959.

[17] Zhao, Z., Ma, Y., Mushtaq, A., Rajper, A. M. A., Shehab, M., Heybourne, A., ... & Tse, Z. T. H. (2022). Applications of robotics, artificial intelligence, and digital technologies during COVID-19: a review. Disaster Medicine and Public Health Preparedness, 16(4), 1634-1644.

[18] Hou, L., Latif, J., Mehryar, P., Withers, S., Plastropoulos, A., Shen, L., & Ali, Z. (2024). An autonomous wheelchair with health monitoring system based on Internet of Thing. Scientific Reports, 14(1), 5878.

[19] Jiang, D., Li, J. W., Geng, X., Ma, X., & Chen, W. M. (2023). Fast tool to evaluate 3D movements of the foot-ankle complex using multi-view depth sensors. Medicine in Novel Technology and Devices, 17, 100212.

[20] Ai, Y., Teng, S., Yang, Q., Wu, Y., Li, Y., Gao, Y., ... & Wang, F. Y. (2024). iMAPeM: A New Paradigm for Implementing Intelligent Mining With Humans in the Loop. IEEE Transactions on Systems, Man, and Cybernetics: Systems.

[21] Avutu, S. R., Paul, S., & Reddy, B. V. (2023). A review on wheelchair and add-in devices design for the disabled. International Journal of Biomedical Engineering and Technology, 41(1), 35-59.

[22] Guemghar, I., Pires de Oliveira Padilha, P., Abdel-Baki, A., Jutras-Aswad, D., Paquette, J., & Pomey, M. P. (2022). Social robot interventions in mental health care and their outcomes, barriers, and facilitators: scoping review. JMIR Mental Health, 9(4), e36094.

[23] Single, M., Bruhin, L. C., Naef, A. C., Krack, P., Nef, T., & Gerber, S. M. (2024). Unobtrusive measurement of gait parameters using seismographs: An observational study. Scientific reports, 14(1), 14487.

[24] Kipnis, E., McLeay, F., Grimes, A., De Saille, S., & Potter, S. (2022). Service robots in long-term care: a consumer-centric view. Journal of Service Research, 25(4), 667-685.

[25] Chen, H. Y., Huang, P. H., & Fu, L. C. (2023). Social crowd navigation of a mobile robot based on human trajectory prediction and hybrid sensing. Autonomous Robots, 47(4), 339-351.

[26] Takanokura, M., Kurashima, R., Ohhira, T., Kawahara, Y., & Ogiya, M. (2023). Implementation and user acceptance of social service robot for an elderly care program in a daycare facility. Journal of Ambient Intelligence and Humanized Computing, 14(11), 14423-14432.

[27] Hughes, N., Chang, Y., Hu, S., Talak, R., Abdulhai, R., Strader, J., & Carlone, L. (2024). Foundations of spatial perception for robotics: Hierarchical representations and real-time systems. The International Journal of Robotics Research, 02783649241229725.

[28] Mbunge, E., Chitungo, I., & Dzinamarira, T. (2021). Unbundling the significance of cognitive robots and drones deployed to tackle COVID-19 pandemic: A rapid review to unpack emerging opportunities to improve healthcare in sub-Saharan Africa. Cognitive Robotics, 1, 205-213.

[29] Pereira, D., Bozzato, A., Dario, P., & Ciuti, G. (2022). Towards Foodservice Robotics: a taxonomy of actions of foodservice workers and a critical review of supportive technology. IEEE Transactions on Automation Science and Engineering, 19(3), 1820-1858.

[30] Yam, K. C., Bigman, Y. E., Tang, P. M., Ilies, R., De Cremer, D., Soh, H., & Gray, K. (2021). Robots at work: People prefer—and forgive—service robots with perceived feelings. Journal of Applied Psychology, 106(10), 1557.

[31] Makhdoom, I., Lipman, J., Abolhasan, M., & Challen, D. (2022). Science and Technology Parks: A futuristic approach. IEEE Access, 10, 31981-32021.

[32] Liberman-Pincu, E., Parmet, Y., & Oron-Gilad, T. (2023). Judging a socially assistive robot by its cover: the effect of body structure, outline, and color on users' perception. ACM Transactions on Human-Robot Interaction, 12(2), 1-26.

[33] Xu, Y., Bao, Y., Wang, S., & Zhang, T. (2024). Function Interaction Risks in Robot Apps: Analysis and Policy-based Solution. IEEE Transactions on Dependable and Secure Computing.

Multi-Sensor Data Fusion Analysis for Tai Chi Action Recognition

Jingying Ouyang[1], Jisheng Zhang[2*], Yuxin Zhao[3], Changhuo Yang[4]
College of Physical Education, Hunan Normal University, Changsha, 410012, China[1, 2]
School of Business, Hunan University, Changsha, 410082, China[3]
School of Computer Science and Engineering, Central South University, Changsha, 410083, China[4]

***Abstract*—The continuous development of action recognition technology can capture the decomposition data of Tai Chi movements, provide precise assistance for learners to correct erroneous movements and enhance their interest in practicing Tai Chi. Inertial sensors and human skeletal models are used to collect motion data. Combined with visual sensors, the motion and trajectory of Tai Chi are processed to obtain the relevant coordinate system of the movement trajectory. Then, the inertial sensor and visual sensor are fused for data processing to standardize the human skeleton model, remove noise interference from the collected information, and improve the smoothness performance of movement trajectories, thereby segmenting and clustering Tai Chi movement trajectories. Finally, the support vector machine and dynamic time-warping algorithm are combined to identify and verify the trajectory of Tai Chi movements. According to the results, in the 25%, 50%, and 75% training sample proportions, the lowest recognition accuracy of the Qi Shi movements was 90.87%, 93.53%, and 98.08%, respectively. The optimal recognition accuracy and standard deviation of single nodes in binary classification were 98.48% and 0.47%, respectively. The best recognition accuracy and standard deviation for multi-joint points in binary classification were 99.77% and 0.16%, respectively. This proves the recognition advantages of binary classification and the superiority of data fusion analysis based on multiple sensors, providing a theoretical basis and technical reference for action recognition technology.**

Keywords*—Inertial sensor; visual sensors; segmentation clustering; support vector machine; dynamic time warping algorithm

I. Introduction

With the advancement and rapid development of technology, human motion recognition technology has been widely applied in fields such as medicine, sports, and computer science. According to the human body model and the action mechanism, the standardization of actions can be improved. Tai Chi, is a popular health exercise in society. According to action recognition technology, actions can be effectively imitated, improving teaching level and standardization of actions [1]. However, Tai Chi movements are basically smooth and coherent trajectory movements, which have unity in the coordination of whole body and joint movements. Therefore, it is necessary to collect and process information on Tai Chi movements, as well as segment trajectories to improve recognition accuracy. Action recognition technology has achieved some results in decomposing actions, and identifying motion types and motion patterns. Moreover, there is in-depth research and technological development in the collection and recognition algorithms of action information for human skeleton models [2-4]. However, the current methods for recognizing and decomposing human movements lack more accurate trajectory processing in coherent movements. There is a lack of real-time feedback on monitoring physical fitness and correcting movements during human exercise. Therefore, the inertial sensor and visual sensor are combined to collect, process, and fuse data on motion trajectories. The research innovatively uses Support Vector Machine (SVM) and Dynamic Time Warping (DTW) algorithms to identify and process joint points of continuous actions and their trajectories, aiming to provide theoretical and technical references for the clustering effect of trajectory segmentation and the classification accuracy of action recognition. According to research on the recognition methods of Tai Chi movements, it can not only assist athletes in improving their professional technical level, but also promote the diversified development of other sports. Meanwhile, it can also monitor patients' rehabilitation movements, input human motion commands for intelligent living, and provide practical applications and service experiences for fields such as medicine, public health, and human-computer interaction.

The study is structured into five sections. Section II elaborates on the current research results. Section III analyzes and constructs the data processing and fusion of inertial sensors and visual sensors, improving the smoothness of the trajectory. Section IV is to perform cluster analysis and recognition verification on the trajectory of Tai Chi movements. Section V is a narrative summary of the entire study.

II. Related Works

Action recognition technology has been widely applied and developed in various fields based on human motion information. At present, the research on action recognition technology focuses on action data processing and trajectory clustering algorithms. In recent years, scholars have conducted many explorations on action recognition. Sun et al. used depth maps and human motion recognition datasets to validate human motion recognition. Furthermore, the advantages of human motion recognition based on depth maps were derived [5]. In terns of human behavior identification, Luo et al. proposed long-distance data transmission between sensors and servers to improve the real-time processing capacity. The binary neural network was used to evaluate human activity data, so as to improve the efficiency and accuracy of data operation [6]. Liu et al. used an adaptive multi-scale convolutional network to

*Corresponding Author.

analyze the information features of skeleton joint points and their movements for human skeleton action recognition. The accuracy of action recognition data was verified by combining the character segmentation mode and perspective segmentation mode, thereby proving the superiority of adaptive multi-scale graph convolutional networks in human skeleton action recognition [7]. Regarding the three-dimensional reconstruction of human bones, Liu et al. adopted a skin multi-person linear model and skeleton perception implicit function method. It improved the accuracy and detail processing of the human body model, providing a foundation for human model recognition [8].

There have been many research achievements in the field of human motion recognition technology, including sports, home, and intelligent applications. Liu proposed an algorithm that combines principal component analysis and local binary patterns to collect and process motion images for recognizing athletes' throwing movements. Through image segmentation and recognition, the average recognition rate and accuracy of the movements were improved [9]. To solve the motion recognition technology in sports, Host et al. validated the sports dataset using action systems and computer vision to improve the detection accuracy of athlete training [10]. Regarding indoor behavior recognition for the elderly, Song Y et al. utilized wireless fidelity and video feature fusion to establish an indoor human behavior recognition method. They also combined support vector machines to classify and recognize actions, thereby improving the accuracy of action recognition [11]. Cai et al. used feature extraction tools and multi-scale fusion to extract music and dance features in the automatic generation of folk music and dance movements. A sequence network model was constructed to train features, synthesize new dance sequences, and improve the efficiency of automatic music and dance generation and the accuracy of rhythm matching [12]. For the classification technique of action recognition, Chang et al. used time-frequency features of brain signals and event-related potential phenomena. Furthermore, convolutional neural and long short-term memory network models were constructed to classify the collected EEG signals, demonstrating the superiority of classification algorithms [13]. Regarding baseball trajectory recognition, Seo et al. used an adaptive Kalman filter for velocity compensation. By combining sensor fusion and motion characteristic compensation, the three-dimensional trajectory of global coordinates was estimated, thereby improving baseball trajectory recognition and estimation for high-precision detection [14].

To sum up, although domestic and foreign scholars have conducted model construction on action recognition technologies and classification algorithms, they mainly focus on image processing and recognition of smooth and fast human movements to ensure the accuracy of sports athlete training. However, there is still a lack of in-depth research on clustering and segmentation methods for motion trajectories in daily life scenarios, and the sensor devices used for data collection also lack data fusion. At the same time, there is a lack of consideration for the universality of action recognition. There are significant differences between athlete action recognition and elderly behavior activity feature extraction, which cannot provide a good reference for behavioral rehabilitation in the medical field. Therefore, multi-sensor fusion is used to collect Tai Chi movement data, and the trajectory segmentation algorithm is used to ensure the uniform decomposition of Tai Chi movement, thereby improving the recognition and classification of movement trajectories. At the same time, video explanations of Tai Chi and accurate and consistent movement guidance are provided during fitness exercises.

III. System Construction for Data Collection and Data Fusion

Tai Chi is a continuous movement trajectory. The action data are obtained based on inertial sensors and visual sensors. Then the action trajectory data is collected to complete action recognition.

A. Data Acquisition and Processing Based on Inertial Sensors and Visual Sensors

The human posture representation is based on the human skeleton model for collecting action data. To obtain real-time action data, inertial sensors are used for convenient wearable devices. The specific structural composition is shown in Fig. 1.

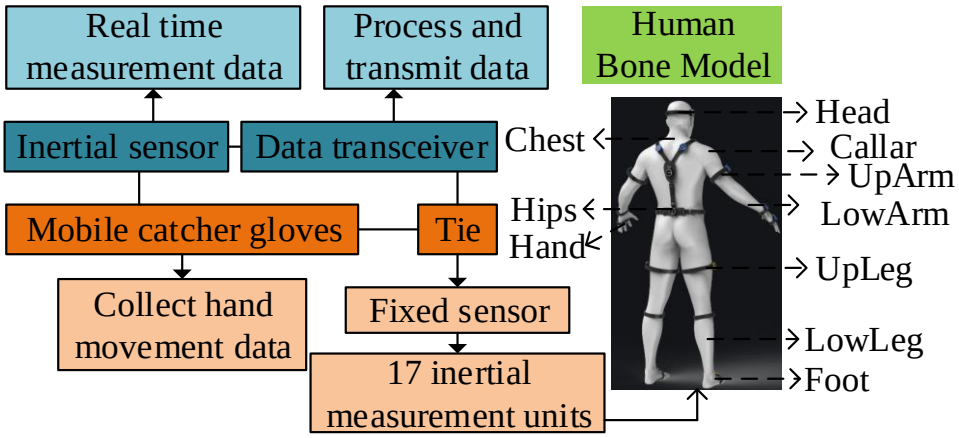


Fig. 1. Data acquisition equipment and its structure based on inertial sensors.

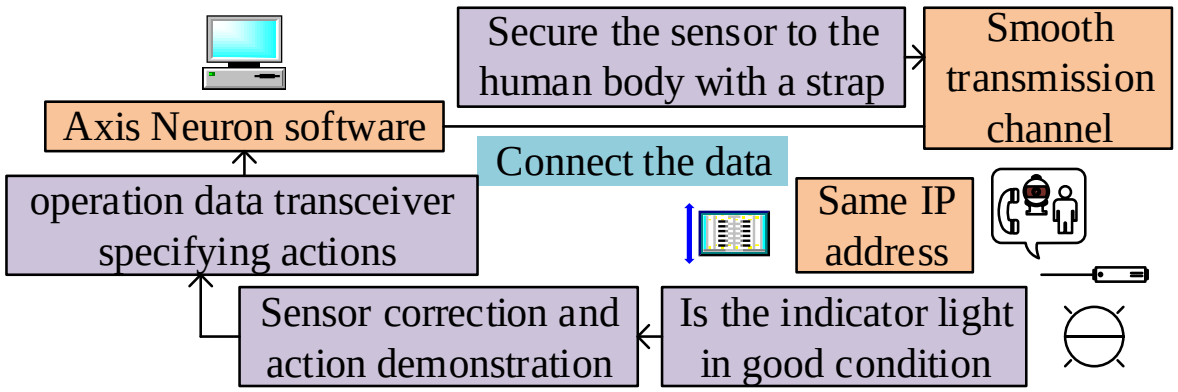


Fig. 2. Schematic diagram of data collection steps.

From Fig. 1, the inertial sensor measures data such as velocity, intensity, and acceleration for each unit. The data transceiver processes the data and synchronously transmits it to the host. The motion capture gloves are only fixed on the hands to obtain data on hand movements. The strap is used to fix the inertial sensor on the human body, completing the data collection process. According to the characteristics of Tai Chi exercise, in addition to the hand movement data of the motion capture gloves, the sensor is fixed in 17 measurement positions on the human body with straps to receive real-time transmission data from the data transceiver. The data collection steps are shown in Fig. 2.

From Fig. 2, during the data collection process, the sensor is fixed to the human body. The connection between the host software and the data transceiver is smooth. Before collecting data, the sensor is corrected and the action is simulated and demonstrated. Finally, the host software is used to operate the data transceiver to complete the data collection of the specified action. BVH, as a data storage format in hierarchical models, is often used in the animation production of human bone models. Initially, each joint point is positioned and its hierarchical relationship is analyzed. Then the motion data of each joint point frame is calculated. The initial coordinate difference between a certain level node and its parent node is expressed as vector form, as shown in Eq. (1).

$$V_0 = \left[x_0, y_0, z_0\right]^T \tag{1}$$

In Eq. (1), x_0, y_0, and z_0 represent the initial offset of the node relative to their child nodes. x, y and z are three directions. In frame $k+1$, the vector of the joint points to the parent node is shown in Eq. (2).

$$V_{k+1} = T_k R_k \left[V_0 \quad 1\right]^T \tag{2}$$

In Eq. (2), T_k is the translation matrix. R_k is the product of rotation matrices in the z, x, and y directions. According to the node transformation relationship and the bone hierarchical structure, the three-dimensional coordinate is shown in Eq. (3).

$$V_{k+1}^n = \left(\prod_{i=0}^{n} T_k R_k^i\right) \times V_0^n \tag{3}$$

In Eq. (3), n represents the number of child node levels. The 0-th level parent node represents the parent node. The difference between the child node and the parent node is $n-1$. Then, the points obtained from the three-dimensional coordinates are connected to obtain the trajectory of Tai Chi movements. In addition, with the rapid development of machine learning, two-dimensional color image models can be extracted from human bone models. The extraction techniques include top-down and bottom-up approaches. The study adopts a bottom-up extraction method, which extracts various body parts or nodes from the image and then pieces them together to form a complete bone model. Openpose, as a bottom-up skeleton recognition method, has a human skeleton model with 18 joints and 25 joints. The study selects a human skeleton model with 25 joints, which includes all joints in BVH format, as well as data extraction for hands and faces. The Openpose algorithm can extract two-dimensional coordinates of human bone models in color images. Corresponding to the position of the depth image, the three-dimensional coordinates of the joint points can be obtained.

The three-dimensional coordinates of depth images can be obtained based on the camera coordinate system. The common depth images include stereo vision method, time-of-flight method, etc. [15]. Based on the coherence and motion range of Tai Chi movements, the KinectV2 somatosensory camera based on the time-of-flight method is taken as the visual sensor for research. Visual sensors cover four coordinate systems in data analysis and calculation. Therefore, its research application in Tai Chi action recognition is shown in Fig. 3.

From Fig. 3, four coordinate systems are obtained, including image coordinate system, pixel coordinate system, camera coordinate system, and world coordinate system. Inertial sensors and stereo sensors are combined to study the relevant coordinate systems of Tai Chi movement trajectory.

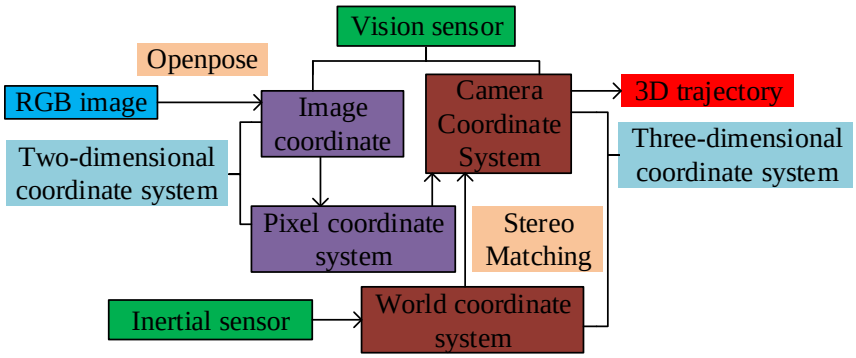


Fig. 3. Coordinate system application and structure diagram of visual sensors.

B. Data Fusion Processing Based on Inertial-Visual Sensors

The imaging captured by a camera is affected by optical properties, which can cause distortion during imaging. Then, based on the camera calibration internal parameter matrix, distortion processing is applied to the depth image and color image. The points of the depth image are corresponding to the color image to obtain a four-channel RGB color mode Depth Map (RGBD) image. Finally, based on the camera coordinate system, the three-dimensional coordinates of the RGBD image are evaluated. For the pixel coordinates of a point in the depth image, the depth value is shown in Eq. (4).

$$\text{Depth value} = u + v$$
$$\begin{cases} u = a_2\left[b_2 d\left(a_1, b_1\right) + \left(1-b_2\right) d\left(a_1, b_1+1\right)\right] \\ v = a_2\left[\left(1-a_2\right) d\left(a_1+1, b_1\right) + \left(1-b_2\right) d\left(a_1+1, b_1+1\right)\right] \end{cases} \quad (4)$$

In Eq. (4), (a,b) is the pixel coordinate of a certain point. $a = a_1 + a_2, a_1 \le a$, and $b = b_1 + b_2, b_1 \le b$. Depth value represents the depth value of the point. $d(a,b)$ is the function value of point (a,b) on the depth image. In addition, the depth value of joint points in the three-dimensional coordinates of the depth camera is shown in Eq. (5).

$$\begin{cases} x = D\left(a - a_0\right)\dfrac{1}{f_x} \\ y = D\left(b - b_0\right)\dfrac{1}{f_y} \end{cases} \quad (5)$$

In Eq. (5), (x,y,z) is the three-dimensional coordinate of the joint point. (x,y,z) is its depth value. Finally, the RGBD image is separated to obtain an RGB image with the same size as the depth image. The Openpose algorithm is used to extract pixel coordinates from the joint points of the RGB image and convert them into three-dimensional coordinates. Finally, the visual sensor is used to process data such as noise and errors in three-dimensional coordinates. The image is processed with depth values through guided filters to obtain a single channel binarized image, which is optimized to preserve the distinguishing effect between the edges and interior of the image, thereby clarifying the human body contour information on the image. The morphology of human bones varies. Therefore, the human skeleton model needs to be standardized, so that visual sensors can clearly obtain the three-dimensional coordinates of the human skeleton and ensure the optimization quality of Tai Chi movement trajectory. To remove noise interference from collected data, the study uses Kalman filtering to process motion data and smooth the trajectory. The smoothing indicators, including square integral method, root mean square method, maximum velocity normalized mean method, and maximum velocity normalized mean method are used to test the smoothness and coordination of human motion. The improved Kalman filter enhances the smoothness of motion trajectory. Afterwards, the data collection of the inertial sensor is denoised. The five-point smoothing algorithm is used to optimize its motion trajectory, thereby improving the good smoothness performance of the Tai Chi movement trajectory. The accuracy of inertial sensors is superior to that of visual sensors. Therefore, there are significant errors in the data after the operation. The data fusion method of the two needs to be improved to enhance the quality of data processing. The steps for designing data fusion are shown in Fig. 4.

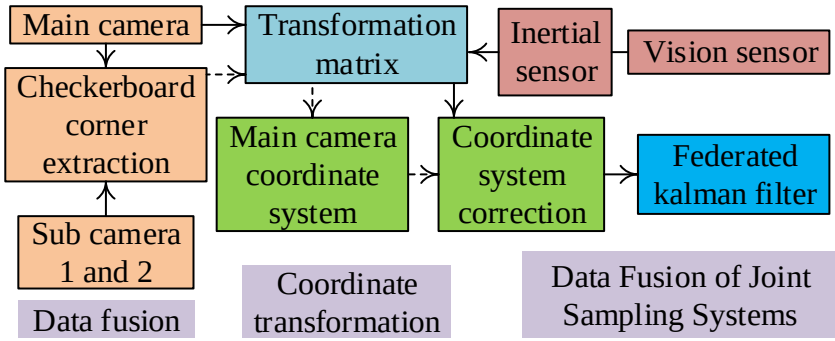


Fig. 4. Data fusion of inertial sensor and visual sensor.

From Fig. 4, the data fusion processing design is formed based on the errors of the two sensors. Three cameras and their coordinate systems are stereo matched. The checkerboard corner extraction algorithm is combined to enhance robustness and reduce errors. Then, coordinate transformation is performed on the inertial visual sensor to accurately identify the three-dimensional coordinates of the human skeleton model. Finally, a joint sampling system is used to fuse the data of the inertial visual sensor. The decentralized multi-sensor data fusion method is adopted, and Kalman filtering is combined to design filters, thereby reducing data errors and efficiently fusing information [16-18]. The main error in inertial sensors is the operational error of gyroscopes and accelerometers. The errors in visual sensors mainly include joint positioning, depth values, and other errors. Therefore, the joint error compensation algorithm and Kalman filtering algorithm are used to process the cumulative error and joint error data, thereby improving the robustness of the fusion system. The stereo matching angle relationship of inertial-visual sensor is shown in Eq. (6).

$$\begin{cases} \alpha = \left| \arccos\left(\dfrac{(n_3)}{\sqrt{n_1^2 + n_2^2 + n_3^2}} \right) \right| \\ \beta = \left| \arccos\left(\dfrac{(n_1)}{\sqrt{n_1^2 + n_2^2 + n_3^2}} \right) \right| \\ \alpha + \beta = \varphi + \lambda = \dfrac{\pi}{2} \end{cases} \tag{6}$$

In Eq. (6), α is the angle between z in camera coordinates and the ground plane. β is the angle between x and the ground plane. The converted camera coordinate is $\left(x^{'}, y^{'}, z^{'}\right)$. The angle between z and $z^{'}$ is φ. λ is the angle between x and $x^{'}$. The information conservation principle of the federated Kalman filtering algorithm is shown in Eq. (7).

$$P = \sum_{i}^{m} \alpha_i + \alpha_m \tag{7}$$

In Eq. (7), P represents the principle of information conservation. The noise variance error is shown in Eq. (8).

$$\begin{cases} \sum_{i=1}^{N} \dfrac{1}{\eta_i} = 1 \\ 0 \le \dfrac{1}{\eta_i} = \alpha_i \le 1 \end{cases} \tag{8}$$

In Eq. (8), η_i is the measurement noise variance of the sampling system. Finally, the covariance between the inertial sensor and the visual sensor is normalized, as shown in Eq. (9).

$$\alpha_i^k = \frac{\sum_{i=1}^{3} \dfrac{1}{\eta_i} + \dfrac{1}{\eta_m}}{\eta_i} \tag{9}$$

In Eq. (9), η_m is the covariance matrix of the cumulative error for the inertial sensor. Through data fusion design, multiple sensor error analysis and optimal data fusion are completed.

C. Segmentation and Clustering Processing of Tai Chi Movement Trajectories

Tai Chi is a continuous and light movement. To complete the action trajectory recognition, the trajectory needs to be segmented to extract the characteristics of trajectory motion [19-20]. The Minimum Description Length (MDL) is used to extract feature points of a trajectory. The original trajectory is segmented to obtain multiple sub trajectories. Then, the sub-trajectories are transformed into vectors, which are called feature vectors. The lengths of all sub-trajectories during trajectory segmentation are shown in Eq. (10).

$$\begin{cases} M(H) = \sum_{j=1}^{par_i - 1} \log_2 \left[len\left(p_{c_j}, p_{c_{j+1}}\right) \right] \\ M(D|H) = \sum_{j=1}^{par_i - 1} \sum_{k=c_j}^{c_{j+1}-1} \log 2 \left[d_{\perp}\left(p_{c_j} p_{c_{j+1}}, p_k p_{k+1}\right) \times d_{\theta}\left(p_{c_j} p_{c_{j+1}}, p_k p_{k+1}\right) \right] \end{cases} \tag{10}$$

In Eq. (10), $M(H)$ is the sum of sub-trajectory lengths. p_c is the point on the trajectory. p_{c_j} is the characteristic of the trajectory point. $len\left(p_{c_j}, p_{c_{j+1}}\right)$ is the Euclidean distance between p_{c_j} and $p_{c_{j+1}}$. $d_{\perp}$ and d_{θ} are the vertical distance and angular distance between trajectory segments, respectively. For the characteristics of trajectory points, it is required to take a local optimal solution, which can replace the global optimal solution. The cost function and feature point conditions are shown in Eq. (11).

$$\begin{cases} MDL_{par}\left(p_i, p_j\right) = M(H) + M\left(D|H\right) \\ MDL_{nopar}\left(p_i, p_j\right) = M(H) \\ MDL_{par}\left(p_i, p_k\right) < MDL_{nopar}\left(p_i, p_j\right) \end{cases} \tag{11}$$

In Eq. (11), p_i and p_j represent two points on the trajectory, respectively. $MDL_{par}\left(p_i, p_j\right)$ is the encoding length function that connects feature points into a line. $MDL_{nopar}\left(p_i, p_j\right)$ is the length function of the original trajectory encoding. Due to the small difference between the trajectory and the original trajectory, $M\left(D|H\right)$ is zero. Then, the three-dimensional coordinates and time of the sub-trajectories are combined to form a four-dimensional feature vector. The four-dimensional feature vector is classified. Then, the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is selected. The algorithm automatically classifies the data according to the set parameters, and then finds clusters of any shape in the dataset and removes noise. The Hopkins statistic is selected to evaluate the clustering trend of the dataset, as shown in Eq. (12).

$$\text{Hopkins statistics} = \frac{\sum y_i}{\sum y_i + \sum x_i} \tag{12}$$

In Eq. (12), $\{x_n\}$ represents uniformly extracting n samples $\{p_n\}$ from the dataset. Then, n sample sets are uniformly extracted from the dataset. The distance between each sample and the nearest sample set in the complement set is $\{y_n\}$. After determining the separability of the dataset, the clustering effect is effectively evaluated. The Davies-Bouldin index (DBI) and Dunn index index (DI) are used to simultaneously evaluate clustering performance. The DBI is shown in Eq. (13).

$$DBI = \frac{1}{k}\sum_{i=1}^{k} \max_{j=1\sim k, j\neq 1}\left(\frac{L_i + L_j}{C_{ij}}\right) \tag{13}$$

In Eq. (13), L_i and L_j represent the average distance between each point in the i-th and j-th clusters and the center of the cluster, respectively. C_{ij} is the center distance between the i-th and j-th clusters. If the value is small, the clustering effect is good. The DI is shown in Eq. (14).

$$DI = \frac{MIN\left\{\min\left\|x_i - y_j\right\|\right\}}{MAX\max\left\|x_i - y_j\right\|} \begin{cases} MIN, 0 < m \neq n < K \\ \min, \forall x_i \in \Omega_m, \forall y_i \in \Omega_n \end{cases} \begin{cases} MAX, 0 \leq m \leq K \\ \max, \forall x_i, y_i \in \Omega_m \end{cases} \tag{14}$$

In Eq. (14), a larger DI indicates better clustering performance. According to the distance evaluation between DBI and DI, the optimal weight can be continuously adjusted. The parameters that need to be adjusted in clustering analysis include spatiotemporal parameters. The spatiotemporal distance is normalized, as shown in Eq. (15).

$$S\left(W_i, W_j\right) = w_d \frac{d_\perp\left(W_i, W_j\right) + d_\square\left(W_i, W_j\right) + d_\theta\left(W_i, W_j\right)}{\max\left(d_\perp + d_\square + d_\theta\right)} + \frac{w_t d_t\left(W_i, W_j\right)}{\max\left(d_t\right)} \tag{15}$$

In Eq. (15), W_i and W_j represent trajectory segments, respectively. $d_\square$ is the parallel distance between trajectory segments. w_d is the sum of weights among parallel distance, vertical distance, and angular distance. w_t is the time weight, and $w_d + w_t = 1$. d_t is the time distance. According to the inertial visual sensor and sampling system, the complete Tai Chi movement trajectory is segmented and clustered. Then, its actions are decomposed and recognized. Due to the complexity and diversity of Tai Chi movement trajectories, SVM and DTW are combined to identify and verify single and multiple joint points, respectively. The steps for identifying the two are shown in Fig. 5.

From Fig. 5, based on the specific movements and trajectories of Tai Chi, its movements are identified and tested. SVM is fused to process the trajectory into the same size form, and Fisher vectors are used to normalize the length. The results of DBSCAN are used in a mixed Gaussian model to identify the motion trajectory of a single joint point. For multi-joint recognition verification, DTW is used to optimize the algorithm and directly recognize the segmented actions as templates.

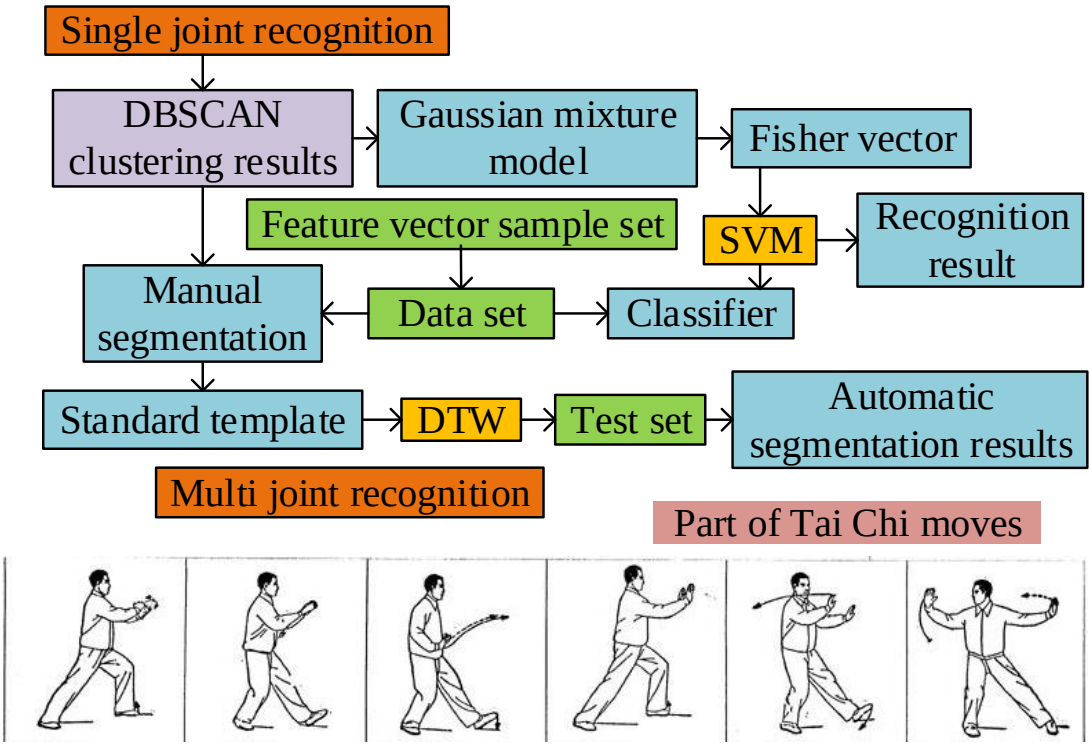
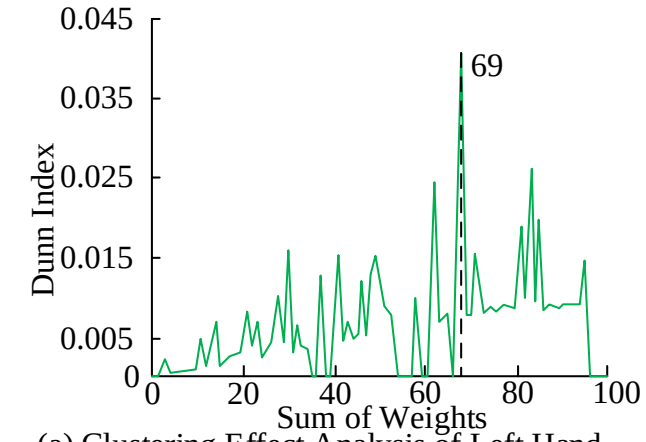


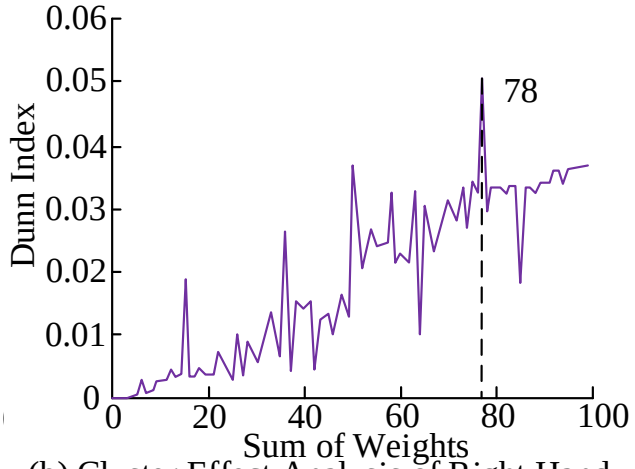
Fig. 5. Schematic diagram of recognition steps for Tai Chi movement trajectory.

IV. Segmentation and Recognition Analysis of Tai Chi Movement Trajectories

Based on the segmentation and trajectory processing of Tai Chi movements, clustering evaluation indicators are used to analyze the clustering effect of the movement trajectories for the left- and right-hand joints in Tai Chi. The step size variation range of the two trajectories is planned to be 0-100. The relationship between the DI evaluation index of hand movement trajectory and the weight sum of parallel, vertical, and angle distances is shown in Fig. 6.



(a) Clustering Effect Analysis of Left Hand Movement Trajectory



(b) Cluster Effect Analysis of Right Hand Movement Trajectory

Fig. 6. Clustering effect analysis of hand movement trajectories in Tai Chi.

From Fig. 6 (a), the DI value of the left-hand movement trajectory reached the highest value, indicating the best trajectory clustering effect. The weight sum was 69, and the overall movement trajectory changed differently. When the clustering effect of the right-hand movement trajectory reached its maximum, the weight sum was 78. The overall hand movement trajectory showed an upward trend, that is, the DI value continued to increase overall. The hand movement in Tai Chi is called Yunshou. Due to the clustering processing of the DBSCAN algorithm, it is converted into a Fisher vector, as shown in Fig. 7.

From Fig. 7, the motion trajectory of the Cloud Hand move varied greatly. The Fisher vector changed with increasing size. The overall trend was concentrated between -0.2-0.2, with the highest approaching 0.6. There are many schools of Tai Chi. Fist types and movements are diverse and varied. The study takes the Tai Chi of the Wu school as an example. Ten of the movements, including Grasp the Bird's Tail, Single Whip, Cross Hands, Cloud Hand, Sea Needle, Flash the Arm, Oblique Flying, Upside Down Chasing the Monkey, Tai Chi Qi Shi, and Parry and Punch, are selected for analysis. The names of these movements are represented in order by A-J. Finally, the trajectory of Tai Chi movements is identified and analyzed. The right-hand movement trajectory is recognized as a single joint action. Ten moves are classified into two categories and the training sample proportions are set to 25%, 50%, and 75%, respectively. The recognition accuracy of the two categories is calculated separately. When the training samples account for 25% of the total samples, some recognition results are shown in Fig. 8.

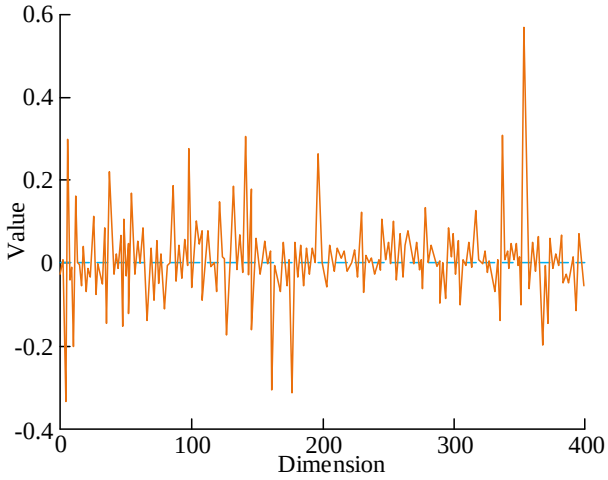


Fig. 7. Fisher vector changes in the trajectory motion of the cloud hand move.

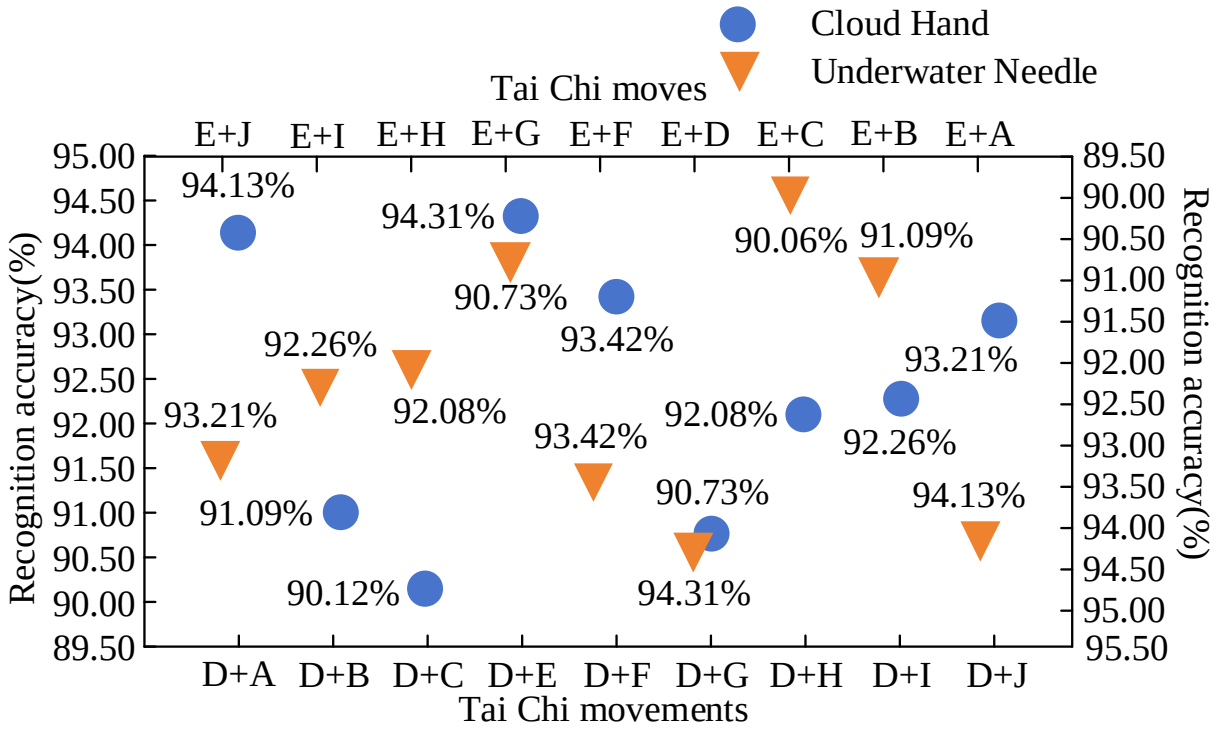


Fig. 8. Recognition results of the 25% binary classification of the cloud hand and sea needle.

From Fig. 8, when the test sample was 25%, the overall recognition accuracy of the Cloud Hand and Sea Needle movements was above 90%, with the highest being 94.31% and the lowest being 90.12% and 90.06%, respectively. When the test sample was 50%, the binary recognition results of some movements are shown in Fig. 9.

From Fig. 9, when the training sample was 50%, the recognition rates of the Flash the Arm, Oblique Flying movements were both above 93%, which was higher than the 25% training sample proportion result. The highest recognition rates for the combination of the Flashing Back and the Oblique Flying were both 98.45%, while the lowest recognition rates were 93.30% and 93.27%, respectively. Finally, the training samples accounted for 75%. The recognition rate changes are tested, as shown in Fig. 10.

From Fig. 10, when the training sample was 50%, the recognition rates of the Flash the Arm, Oblique Flying moves were above 93%, which was higher than the 25% training sample proportion result. The highest recognition rates for the combination of the Flashing Back and the Oblique Flying were 98.45%, while the lowest recognition rates were 93.30% and 93.27%, respectively. Finally, the training samples accounted for 75%. The recognition rate changes are tested, as shown in Fig. 10. This indicates that the sample proportion is large, and the recognition accuracy of the moves continues to improve, thereby verifying the effectiveness of the classification recognition algorithm. To visually compare the binary classification recognition results of different sample proportions, a movement called Qishi is selected to perform 25%, 50%, and 75% binary classification recognition. The change results are shown in Table I.

From Table I, the lowest recognition accuracy for the binary classification of the Qishi movement was 90.87%, 93.53%, and 98.08%, respectively, when the training sample proportions were 25%, 50%, and 75%. Furthermore, it indicates that as the proportion of samples increases, the recognition accuracy also improves. Finally, the binary and multi-classification samples are trained to recognize single joint and multi-joint movements. The accuracy and standard deviation of the average value are taken to determine the classification accuracy of the motion trajectory, as shown in Fig. 11.

From Fig. 11(a), the recognition accuracy of binary classification for single node in the sample proportion of 25%, 50%, and 75% was 92.26%, 96.51%, and 98.48%, respectively. The recognition accuracy in multi-classification was 90.05%, 90.58%, and 93.56%, respectively. In Fig. 11(b), the recognition standard deviations of binary classification for single node in the 25%, 50%, and 75% sample proportions were 1.15%, 1.32%, and 0.47%, respectively. The standard deviations for multi-classification recognition were 2.68%, 2.11%, and 3.08%, respectively. Furthermore, it indicates the variation of single joint points in different sample proportions. The binary classification method has higher recognition accuracy and lower standard deviation than the multi-classification method. This proves that the binary classification method for identifying single related nodes has advantages. The recognition accuracy and standard deviation results for multiple joint points are shown in Fig. 11(c). The recognition accuracy of binary classification and multi-classification was 99.77% and 90.25%, respectively. The identification standard deviations were 0.16% and 0.66%, respectively. This indicates that binary classification method is superior to multi-classification method in multi-joint point recognition methods. This proves the superiority of the SVM-based recognition and classification method.

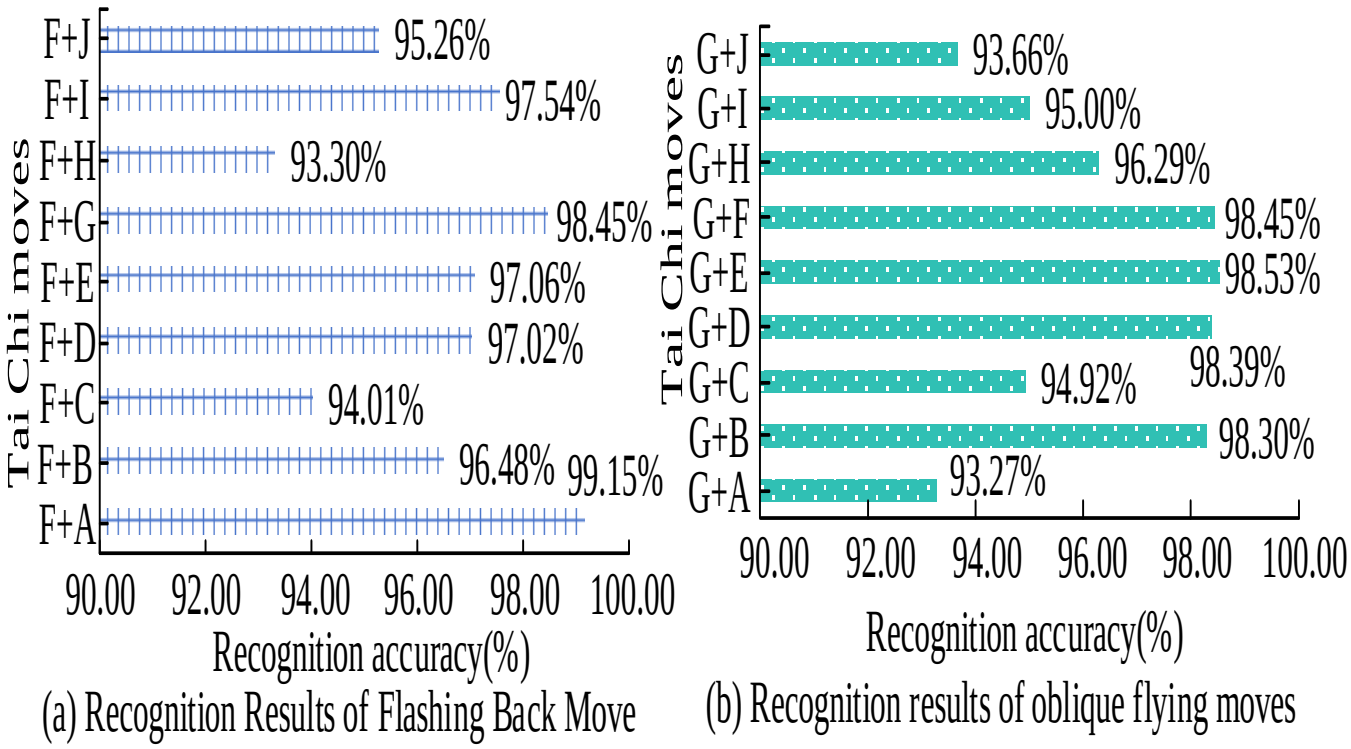


Fig. 9. Recognition results of 50% binary classification for "Flashing Back" and "Oblique Flying".

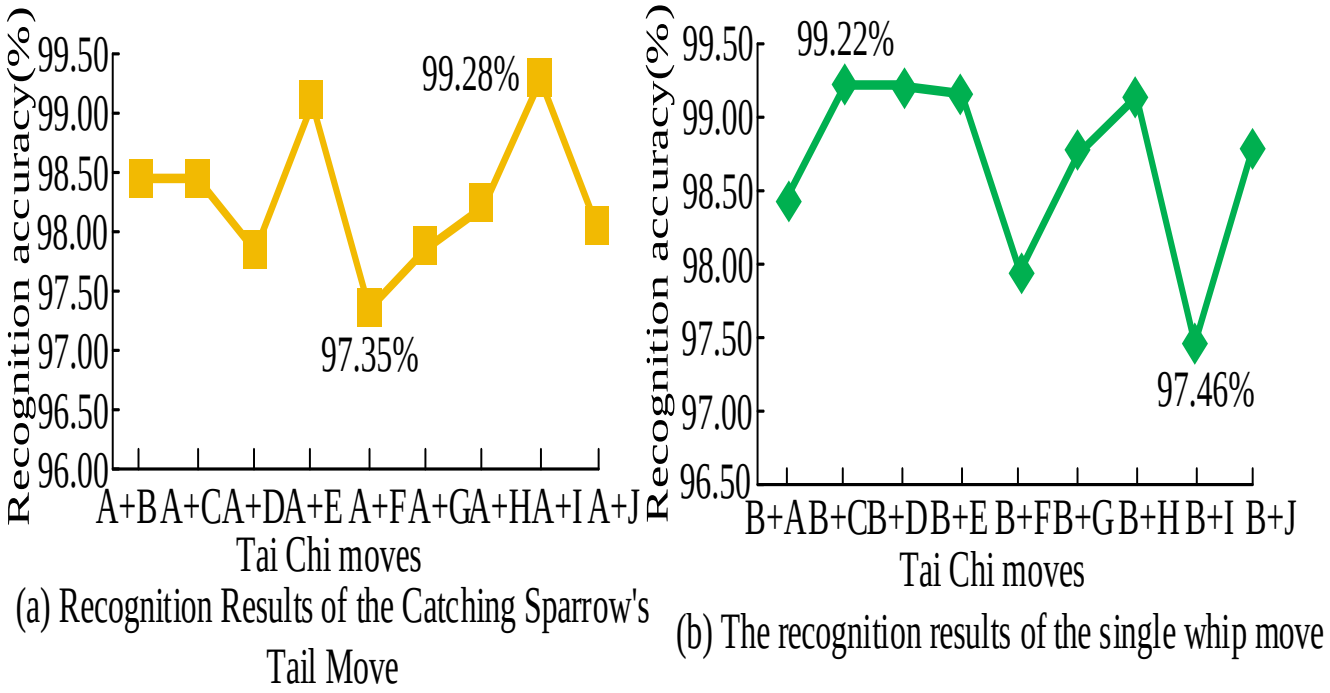
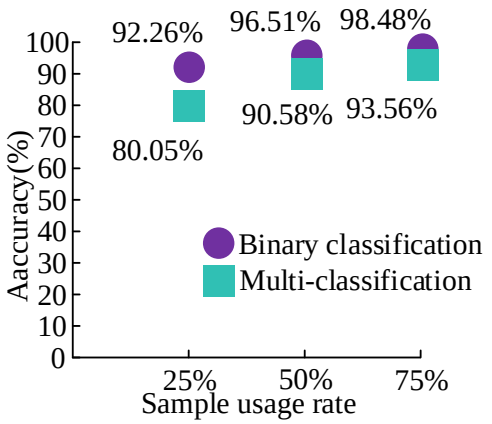


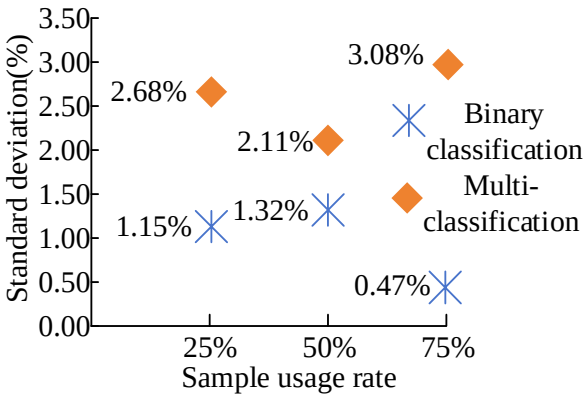
Fig. 10. Recognition results of 75% binary classification for the "Grasping Sparrow Tail" and "Single Whip".

TABLE I. RECOGNITION RESULTS OF THE 25%, 50%, AND 75% DI-CATEGORIZATION OF QI SHI MOVES

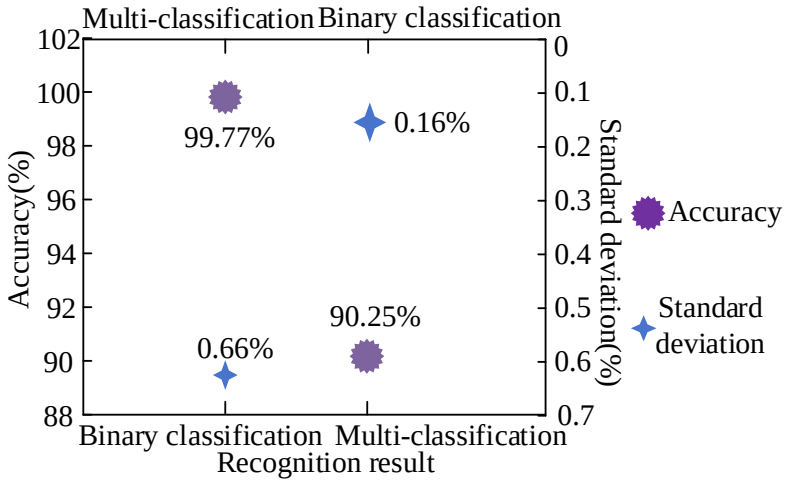
Tai Chi movements	A+I	C+I	D+I	H+I	J+I
25% binary recognition results	94.42%	92.78%	92.20%	92.84%	90.87%
50% binary recognition results	98.02%	96.97%	97.74%	93.53%	98.31%
75% binary recognition results	99.28%	98.08%	98.11%	99.27%	98.55%



(a) Recognition accuracy of single joint binary classification and multi-classification



(b) Recognition standard deviation between single joint binary classification and multi-classification



(c) The recognition accuracy of multi node binary classification and multi-classification

Fig. 11. Recognition results of binary and multi-classification for single node and multi-joint points.

TABLE II. COMPARISON RESULTS OF DIFFERENT METHODS FOR RECOGNIZING TAI CHI MOVEMENTS

Tai Chi movements	E+A	E+B	E+C	E+D	E+F
Reference[6]	90.84%	91.03%	90.53%	89.87%	90.46%
Reference[7]	91.23%	90.45%	90.07%	91.16%	90.32%
Reference[9]	87.61%	86.26%	86.01%	89.26%	88.04%
This research method	99.16%	98.57%	99.12%	98.35%	99.24%

Finally, the research method is compared with existing methods, focusing on trajectory recognition of five Tai Chi moves mainly using the Hai Di Zhen technique. The results are shown in Table II.

From Table II, the deep neural networks and adaptive multi-scale convolutional networks in references [6] and [7] had better recognition methods for human joint points, and had good recognition results for light and gentle Tai Chi movements. The deep network model achieved a recognition result of 91.03% for underwater needles and single whips, while the model in study [7] achieved a recognition result of 91.16% for underwater needles and cloud hands. However, the recognition in study [9] was below 90%, which was not suitable for recognizing Tai Chi movements. Based on the above comparison results, it is concluded that the proposed method has accuracy and applicability in recognizing Tai Chi movements.

V. CONCLUSION

For the analysis of Tai Chi movement recognition data, human motion data is processed by inertial sensors and visual sensors. Then, the collected trajectory data is segmented and clustered. Finally, a comparative analysis is conducted on the recognition of Tai Chi movements. The clustering evaluation

index is used to analyze the clustering effect of the movement trajectories for the left- and right-hand joints in Tai Chi. When the clustering effect of left- and right-hand movements was the highest, the sum of weights was 69 and 78, respectively. The specific movements of Tai Chi are used for action recognition. In the binary classification method, when the training sample was 25%, the overall recognition accuracy of the Cloud Hand and Sea Needle moves was above 90%, with the lowest being 90.06%. When the training sample was 50%, the recognition rates of the flashback and oblique flying movements were both above 93%, with the highest being 98.45%. When the training sample was 75%, the recognition accuracy of the "Grasp the Bird's Tail" and "Single Whip" were both above 97%. As the number of training samples increases, the accuracy of action recognition continues to improve. This also indicates the classification effectiveness of the DBSCAN algorithm. Finally, single joint and multi-related nodes were respectively used in binary classification and multi-classification. The recognition accuracy of single joint in the 25%, 50%, and 75% sample proportion of binary classification was 92.26%, 96.51%, and 98.48%, respectively. The recognition accuracy of multi-joint points in binary classification was 99.77%. Furthermore, it proves that the binary classification method has high recognition accuracy, indicating the superiority of the trajectory segmentation and recognition classification method based on multiple sensors. However, human motion trajectory segmentation still lacks a large amount of motion data. In addition, the recognition and selection of Tai Chi movements are not widely applicable. In the action decomposition of sports events, real-time action recognition is not considered in order to collect and correct actions. In future research, it is necessary to reference other types of sports to improve athletes' movement skills and expand the feasibility and practicality of sports movement recognition technology. The accuracy of action recognition in the medical field can help physicians diagnose diseases and provide real-time and effective evaluation of treatment plans for patients' exercise rehabilitation. With the development of intelligence, in the fields of human-computer interaction and virtual reality, the recognition of human movements can be transformed into instruction input, thereby promoting the intelligence of life.

This study analyzed the coherence and overall coordination of Tai Chi movements, and conducted segmentation and clustering. In addition, considering the motion joints of actions, SVM and DTW methods were used to cluster single joints and multiple joints. The DBSCAN algorithm accurately identified the data noise of high-density motion trajectories, thereby improving the clustering effect of trajectories while segmenting them, and ultimately achieving high classification and recognition accuracy of Tai Chi movements.

CONFLICT OF INTEREST

The authors report there are no competing interests to declare.

REFERENCES

[1] Yang M, Wu C, Guo Y, Jiang R, Zhou F, Zhang J, Yang Z. Transformer-based deep learning model and video dataset for unsafe action identification in construction projects. Automation in construction, 2023, 146(2): 104703-104716.

[2] Bhogal R K, Devendran V. Action Recognition for Multiview Skeleton 3D Data Using NTURGB+D Dataset. Computer Systems Science and Engineering, 2023, 47(12):2759-2772.

[3] Haoyu Z, De Z. Combining Adaptive Graph Convolution and Temporal Modeling for Skeleton-Based Action Recognition. Computer Engineering and Applications, 2023, 59(18): 137-144.

[4] Pham D T, Pham Q T, Nguyen T T, Le T L, Vu H. A lightweight graph convolutional network for skeleton-based action recognition. Multimedia tools and applications, 2023, 82(2): 3055-3079.

[5] Sun B, Kong D, Zhang W, Jia W. Survey on Human Action Recognition from Depth Maps. Tsinghua Science and Technology, 2022, 27(6): 29.

[6] Luo F, Khan S, Huang Y, Wu K. Binarized Neural Network for Edge Intelligence of Sensor-Based Human Activity Recognition. IEEE transactions on mobile computing, 2023, 22(3): 1356-1368.

[7] Liu K, Xiaobing X I, Zhou M. Skeleton Action Recognition Based on Adaptive Multi-scale Graph Convolutional Network. Computer Engineering, 2023, 49(10): 264-271.

[8] Liu P, Zhang G, Zhang S, Li Y, Zeng Z. Skeleton-aware implicit function for single-view human reconstruction. Journal of Intelligent Technology, 2023, 8(2): 379-389.

[9] Liu Y. Athletes' Throwing Action Recognition Method Based on PCA-LBP Algorithm. International Journal of Computational Intelligence Studies, 2023, 12(1): 130-141.

[10] Host K, Ivai-Kos M. An overview of Human Action Recognition in sports based on Computer Vision. Heliyon, 2022, 8(6): e09633.

[11] Song Y, Fan C. Behavior Recognition of the Elderly in Indoor Environment Based on Feature Fusion of Wi-Fi Perception and Videos. Journal of Beijing Institute of Technology, 2023, 32(2): 142-155.

[12] Cai X, Xi M, Jia S, Xu X, Wu Y, Sun H. An Automatic Music-Driven Folk Dance Movements Generation Method Based on Sequence-To-Sequence Network. International journal of pattern recognition and artificial intelligence, 2023, 37(5):2358003-2358023.

[13] Chang Y, Wang L, Zhao Y, Liu M, Zhang J. Research on two-class and four-class action recognition based on EEG signals. Mathematical biosciences and engineering: MBE, 2023, 20 6: 10376-10391.

[14] Seo K, Shibata S, Hirose K, Naruo T, Shimizu Y. Estimation of baseball bat trajectory during a practice swing using a Kalman filter for velocity compensation. Proceedings of the Institution of Mechanical Engineers, Part P: Journal of Sports Engineering and Technology, 2023, 237(2): 96-101.

[15] Tang Z, Jia C, Wang H, Rong S, Zhao W. Intelligent height measurement technology for ground encroachments in large-scale power transmission corridor based on advanced binocular stereovision algorithms. IET Generation, Transmission & Distribution, 2023, 17(2): 448-460.

[16] Xiao Nan X Y W L. Research on target positioning mode of intelligent unmanned vehicle based on multi-vision sensor. Manufacturing Automation, 2023, 45(3): 76-80.

[17] M. Hasanvand, M. Nooshyar, E. Moharamkhani, and A. Selyari. "Machine Learning Methodology for Identifying Vehicles Using Image Processing," AIA, 2023, 3(1): 170-178.

[18] Naji O A A M, Shah H N M, Anwar N S N, Johan N F. Square groove detection based on Frstner with Canny edge operator using laser vision sensor. The International Journal of Advanced Manufacturing Technology, 2023, 125(5-6): 2885-2894.

[19] Xi Z. Research on the video motion segmentation and its application. Acta Geodaetica et Cartographica Sinica, 2023, 52(8): 1411-1411.

[20] Xu Y, Chen T, Chen S, Xu X. Multi-object Tracking and Segmentation Algorithm by Fusing Motion Feature Embedding. Journal of Chinese Computer Systems, 2023, 44(6): 1304-1310.

Skywatch: Advanced Machine Learning Techniques for Distinguishing UAVs from Birds in Airspace Security

Muhyeeddin Alqaraleh[1], Mowafaq Salem Alzboon[2], Mohammad Subhi Al-Batah[3*]
Department of Software Engineering-Faculty of Information Technology, Zarqa University, Zarqa, Jordan[1]
Department of Computer Science-Faculty of Science and Information Technology, Jadara University, Irbid, Jordan[2, 3]

***Abstract*—This study addresses the critical challenge of distinguishing Unmanned Aerial Vehicles (UAVs) from birds in real-time for airspace security in both military and civilian contexts. As UAVs become increasingly common, advanced systems must accurately identify them in dynamic environments to ensure operational safety. We evaluated several machine learning algorithms, including K-Nearest Neighbors (kNN), AdaBoost, CN2 Rule Induction, and Support Vector Machine (SVM), employing a comprehensive methodology that included data preprocessing steps such as image resizing, normalization, and augmentation to optimize training on the "Birds vs. Drone Dataset." The performance of each model was assessed using evaluation metrics such as accuracy, precision, recall, F1 score, and Area Under the Curve (AUC) to determine their effectiveness in distinguishing UAVs from birds. Results demonstrate that kNN, AdaBoost, and CN2 Rule Induction are particularly effective, achieving high accuracy while minimizing false positives and false negatives. These models excel in reducing operational risks and enhancing surveillance efficiency, making them suitable for real-time security applications. The integration of these algorithms into existing surveillance systems offers robust classification capabilities and real-time decision-making under challenging conditions. Additionally, the study highlights future directions for research in computational performance optimization, algorithm development, and ethical considerations related to privacy and surveillance. The findings contribute to both the technical domain of machine learning in security and broader societal impacts, such as civil aviation safety and environmental monitoring.**

***Keywords*—Unmanned Aerial Vehicles (UAVs); machine learning; image recognition; real-time processing; security; computer vision; image processing**

I. Introduction

In the past decade, military applications of drones have undergone a significant transformation, expanding from surveillance and reconnaissance to more tactical roles, such as precision strikes on targeted objectives. Drones, whether small handheld units or large remotely piloted aircraft, provide invaluable aerial surveillance that extends beyond human capability. This real-time surveillance helps to identify potential threats, ensuring the safety of both civilians and military personnel [1]. Drones can monitor dangerous areas for extended periods, offering surveillance that surpasses traditional methods. However, while these capabilities are revolutionary, they also introduce critical challenges, particularly in security operations.

One significant concern is the threat posed by cyberterrorism, as drones—hailed as one of the most formidable weapons in modern warfare—can be exploited to breach defenses. For instance, the Iranian drone and missile attack on Israeli territories highlighted the need for robust UAV detection systems capable of distinguishing between drones and other aerial entities such as birds. In military contexts, adversarial tactics can include electronic warfare and psychological operations, which further complicate the identification process. Therefore, the development of efficient, real-time recognition platforms using advanced computational technologies is vital [2] [3].

This study explores the application of machine learning algorithms to address this challenge. We examine various models, including deep neural networks, Support Vector Machines (SVMs), random forests, and gradient boosting machines, to identify the most effective approach for high-security environments. The research primarily focuses on reducing false positives and negatives in UAV detection, a critical factor for maintaining operational integrity in military settings. The models are assessed based on accuracy, precision, computational performance, and suitability for real-time applications [4]. This article aims to provide key insights into improving UAV detection systems, offering practical applications that can enhance current military surveillance and security protocols. By leveraging machine learning advancements, this study contributes to the ongoing evolution of airspace control and UAV countermeasures.

A. Article Objectives

This study aims to enhance the ability to differentiate Unmanned Aerial Vehicles (UAVs) from birds in military surveillance operations, with a focus on improving resource allocation, optimizing response strategies, and ensuring airspace security. The primary objectives are:

1) Develop advanced detection algorithms: Design and refine sophisticated machine learning algorithms capable of distinguishing between UAVs and birds by analyzing complex datasets based on flight patterns and physical characteristics.

2) Enhance image recognition capabilities: Improve image recognition accuracy for UAV detection against various

*Corresponding Author.

natural backgrounds by training models on extensive datasets of UAV and bird images captured under diverse environmental conditions.

3) Minimize false positives and negatives: Reduce the rates of false alarms (misidentifying birds as UAVs) and missed detections (failing to identify UAVs) to streamline surveillance system performance in high-security zones.

4) Implement real-time processing: Create a system that processes and analyzes data in real time, enabling immediate and informed decision-making in dynamic, potentially adversarial environments.

5) Evaluate system robustness in simulated environments: Test the developed systems in simulated environments that mimic real-world conditions, including scenarios with UAV swarms and electronic warfare techniques.

6) Assess operational integration: Determine the feasibility and effectiveness of integrating the developed technologies into existing military security frameworks, ensuring seamless deployment and operational functionality.

Achieving these goals will significantly advance the technological capabilities of military surveillance, contributing to national security and strategic defense effectiveness [5].

B. Contribution of the Article

This article contributes to military surveillance by improving UAV and bird differentiation systems. The key contributions are:

1) Advancement in detection algorithms: Introducing new machine learning algorithms for UAV and bird differentiation, focusing on pattern recognition and flight dynamics analysis to reduce misidentifications and improve threat assessment accuracy.

2) Real-time data processing: Enhancing real-time processing capabilities to allow rapid analysis and response in high-stakes environments, where timely decisions can critically impact military engagements.

3) Reduction of false alarms: Minimizing false positives and negatives to prevent unnecessary deployment of resources and reduce the risk of overlooking actual threats.

4) Operational integration and testing: Evaluating the systems in simulated environments, ensuring practical viability and seamless integration into existing military frameworks.

5) Strategic implications and policy recommendations: Offering strategic insights and policy recommendations for defense entities, with suggestions for deploying new technologies and updating current practices.

6) Enhanced airspace security: Improving UAV identification capabilities to strengthen airspace security, particularly in sensitive or high-security areas, mitigating threats like espionage and unauthorized surveillance [6].

C. Article Organization

The article begins with an overview of the importance of UAV identification in military surveillance, followed by a literature review in Section II that highlights existing advancements and gaps in current methodologies. The methodology in Section III outlines the experimental setup, including data collection, model refinement, and evaluation metrics. The results and analysis in Section IV presents a comprehensive evaluation of methods such as neural networks and gradient-boosting machines, assessing their effectiveness in UAV recognition. Discussion is given in Section V. Finally, the article concludes in Section VI with a discussion on future research directions and recommendations for improving UAV detection systems in Section VII.

D. Problem Statement

The growing use of UAVs in military operations underscores the need for advanced systems capable of accurately distinguishing UAVs from other entities, such as birds, in real time. This study focuses on developing machine learning models to improve UAV detection, which is crucial for enhancing airspace security and operational efficiency in both military and civilian settings.

II. Related Work

Due to the increasing chance of drones being used for unlawful activities, the detection of drones has turned out to be especially significant inside the realm of security and surveillance. Artificial neural networks do not facilitate real-time object detection because multiple GPUs are necessary to train the models. Deep learning architectures aim to address this problem by creating convolutional neural networks (CNN) that can function in real-time with just one conventional GPU for training [7]. This paper employs appropriate deep-learning architectures for detecting drones and birds. This application utilizes YOLO (You Only Look Once) algorithms, which are one-stage approaches that examine an image just once using a single neural network. The community is skilled at stop-to-quit to output the bounding box, magnificence label, and detection probability without delay. The models are trained on a bespoke dataset comprising 664 drone pixels and 236 hen pictures. Simulation results indicate that YOLOv4 and YOLOv5 attained F1-ratings of 98% and 94%, respectively, with detection speeds of 54fps and 77fps. The fashions also tested mean average precision (mAP) values of 97.4% and 95%. YOLOv4 verified advanced overall performance in suggested Average Precision (mAP) compared to YOLOv5, whereas YOLOv5 exhibited faster detection speed than YOLOv4 [8].

Businesses, transportation, and military sports use drones. Advanced drone detection and identification systems are needed to protect the airspace. This paper accurately identified drones and birds in the air using radar and visible imaging. Using both drone detection and recognition systems was helpful. An average precision of 88.82% and accuracy of 71.43% makes this approach greener. Excellent performance is shown by the combined approach's 76.27% F1 score. Drone and chicken detection systems will benefit significantly from the findings. Better than similar works, the proposed algorithm [9].

The examination was performed in northeastern Poland, where the Whooper Swan (Cygnus cygnus) breeds now and

then. The Whooper Swan is shy and tends to conceal itself in emergent flowers. A drone was utilized to enhance the efficiency of studying its breeding success and offspring productivity. In 2022, the breeding density of Whooper Swans in the study area was 10 pairs per 100 square kilometers. There was no difference in the number of breeding birds detected at the start of the breeding season between the drone and ground methods. The breeding productivity of the sample of swans studied (N = 36) was 2.19 cygnets per breeding pair using the ground method but 3.71 per pair with the drone, showing a significant difference (p-value of the Wilcoxon test = 0.0148). In the conventional approach, 50% of the pairs successfully bred, while using the drone resulted in a 79% success rate. The birds either remained indifferent to the drone's presence or retreated slowly. The drone study on Whooper Swan breeding productivity was significantly quicker (9 minutes per site compared to 1-2 hours for a ground survey), more accurate, and less disruptive to the birds than a conventional survey [10].

Detecting objects like drones is difficult due to their size and agility, which can confuse machine learning models and lead to misclassification as birds or other objects. This study explores applying various deep-learning techniques to analyze real datasets collected from flying drones. A deep learning approach is suggested to reduce the complexity of such systems. The proposed paradigm combines the AdderNet deep learning paradigm and the SSD paradigm. The aim was to reduce complexity by decreasing the number of multiplication operations in the proposed system's filtering layers. Standard machine learning techniques like Support Vector Machines (SVM) are evaluated and contrasted with other deep learning systems. The datasets for training and testing were either complete or filtered to exclude images with small objects. The data types were either RGB or IR. Comparisons were conducted among all these types, and conclusions are provided [11].

Even advanced drones outperform birds with lightweight, adaptable wings and tails. 3D printing, servomotors, and composite materials enable more creative airplane designs inspired by bird flight, which may improve flight characteristics. By replacing control surfaces with rapidly changing wings, morphing technology improves aircraft aerodynamics and power efficiency. This paper introduces bio-inspired 3D-printed systems for unmanned aerial vehicle wings and tails that morph without flapping. The proposed wing uses a corrugated, flexible 3D-printed structure to expand and contract artificial feathers for sweep morphing. A flexible 3D-printed structure with circular corrugation is proposed for tail feather expansion. Various 3D-printing materials and intricate geometric components can achieve the proposed morphing deformations with minimal actuation forces. Testing prototypes showed that the chosen materials and actuators could achieve seagull-like morphing deformations [12].

The widespread availability of drones has opened up numerous new possibilities previously limited to a select few. Regrettably, this technology also brings countless adverse effects associated with illicit activities such as surveillance and smuggling. Sensitive areas should be equipped with sensors that can detect miniature drones from a long distance. Several techniques are present in this field, but each has notable disadvantages. This study introduces a new method for detecting small drones (<5 kg) using laser scanning and a technique to differentiate between UAVs and birds. Minimizing the false alarm rate in each drone monitoring equipment is a crucial challenge. The paper discusses the newly created sensor and its effectiveness in distinguishing between drones and birds. The concept relies on a straightforward analysis of the cross-polarization ratio of the optical echo produced by laser backscattering on the identified object. The experimental results indicate that the proposed method does not consistently ensure 100% discrimination efficiency but offers a distribution of confidence levels. However, because of the hardware's simplicity, this method appears to be a beneficial enhancement to the advanced anti-drone laser scanner [13].

To address security concerns, an algorithm is created to distinguish between airspace intruders, such as birds and drones, in unmanned aerial system (UAS) operations. The algorithm utilizes velocity data of detected intruders from Internet-of-Things platforms and a partial understanding of physical models. The identification problem is framed as a statistical hypothesis testing or detection problem, where inertial feedback-controlled objects under stochastic actuation must be differentiated based on speed data. The maximum a posteriori probability detector is derived and then simplified into an explicit computation using two points in the sample autocorrelation of the data. The simplified form facilitates the algorithm's computationally efficient implementation and enhances learning from stored data. The total probability of error of the detector is calculated and described. Simulations using synthesized data are shown to demonstrate and improve the formal analyses [14].

Detecting and tracking birds and drones accurately is crucial in different low-altitude airspace surveillance situations. Radar is the most suitable long-range surveillance technology for this issue, but it faces challenges in effectively differentiating between birds and drones. This paper examines birds' and drones' natural flight mechanics and behavioral patterns. A goal classification technique is suggested primarily based on extracting target motion characteristics from radar tracks. The random woodland version is selected for the goal type within the new function space. The proposed method confirms using real-time surveillance radar systems in airport regions. The results of classifying birds, quadcopter drones, and dynamic precipitations advise that the proposed method can reap high-class accuracy. The Gini significance descriptors in a random woodland model provide extra perception when evaluating movement traits and mining. The type machine's excessive sample flexibility and performance enable it to efficiently address complex low-altitude goal surveillance and class problems. Future studies will cope with the current technique's constraints and explore techniques capable of optimization [15].

This study examines the use of micro-Doppler spectrogram signatures of flying gadgets, like drones and birds, to help their remote identity. A 10-GHz non-stop wave radar device was custom-designed to accumulate

measurements from numerous situations regarding distinct goals, which were then used to generate datasets for photo type. Time/pace spectrograms created for micro-Doppler evaluation of various drones and birds were utilized for target reputation and movement categorization with TensorFlow. The consequences indicated that aid vector machines (SVMs) did an accuracy of approximately 90% for drone length classification, around 96% for distinguishing between drones and birds, and more or less 85% for differentiating between individual drones and birds throughout five training. Various aspects of target detection were investigated, such as the terrain and actions of the target [16].

This study uses Long Short-Term Memory (LSTM) networks to explore a novel drone classifier. The classification time of a drone detection radar is crucial for its effectiveness as a real-time surveillance system. This work aims to create a classification framework with minimal latency for processing algorithm input data. Theoretical modeling was conducted on a rotary wing drone and a bird wing flapping to demonstrate the contrast in the patterns of their phase progressions. Subsequently, a dataset of 1D phase data was generated for supervised learning by utilizing 94 GHz experimental trial data consisting of 4800 sequences of drones, birds, noise, and clutter. A stacked LSTM network with optimized hyperparameters was created to mitigate potential overfitting compared to a basic LSTM model. An accuracy of 98.1% was achieved in validating the 2-class classification of drone and non-drone. The network successfully classified all sequences in a performance assessment using 30 unseen test data. This method has been determined to be approximately 10 times faster than a spectrogram-based classification model, as it eliminates the need for additional Fast Fourier Transform (FFT) operations [17].

Classifying multiple drones and birds based on micro-Doppler (MD) signatures is challenging due to potential contamination from multiple bird signatures and the similarity in MD signatures between different drones. This paper introduces three protocols and evaluates their classification accuracy for multiple drones and birds in an actual observation setting. The analysis is based on frequency-modulated continuous wave radar and a convolutional neural network classifier. By utilizing training data that consists of combinations of drone and bird movements in simulations involving rotating blades and flapping wings, our method achieved an accuracy of approximately 100% for majority vote classification. This outcome establishes our process as the most suitable for distinguishing between multiple drones and birds [18].

This paper explores the utilization of micro-Doppler signatures of drones and birds to detect and categorize them. Simulated assessment results are validated with data from a 10-GHz continuous wave (CW) radar system. Time/Velocity spectrograms created for micro-Doppler analysis of various drones and birds are employed for TensorFlow's target recognition and motion categorization. The Support Vector Machine (SVM) achieved 96% accuracy in distinguishing between drones and birds and 85% in distinguishing between individual drones and birds across five classes [19].

In the rapidly changing world of military surveillance, the real-time recognition of Unmanned Aerial Vehicles (UAVs) is emerging as a significant challenge. The classification of small unmanned aerial vehicles (UAVs) based on machine learning models is investigated in this research, as the swift sanction of such identification has prompted the necessity of being able to discriminate between UAVs and non-threatening subjects (e.g. birds, environmental objects) within a variety of constraints of the environment. Using much larger datasets, we tested advanced models, like Neural Networks, Support Vector Machines, ensemble methods, and Random Forest Gradient Boosting Machines. Neural Networks were found as the best, having the highest accuracy and the best performance in times of computational efficiency. Conclusion: This can help improve detection of UAV attacks and suggest optimal resource allocation. They also provide further recommendations regarding incorporating these types of models into military systems that will need to continually be updated to take account of changing capabilities of UAV technology [20].

This paper explores the millimeter-wave radar micro-Doppler characteristics of consumer drones and birds that can be used to differentiate targets by a classifier. The feature extraction methods were created by analyzing the micro-Doppler signature characteristics of in-flight targets detected using a frequency-modulated continuous wave (FMCW) radar. Three distinct drones (DJI Phantom 3 Standard, DJI Inspire 1, and DJI S900) and four birds of varying sizes (Northern Hawk Owl, Harris Hawk, Indian Eagle Owl, and Tawny Eagle) were utilized for feature extraction and classification. The data for all the targets was collected using a stationary W-band (94 GHz) FMCW radar. The extracted features were input into two distinct classifiers for training: linear discriminant and support vector machine (SVM). Classifiers utilizing these features can effectively differentiate between drones and birds with 100% accuracy and distinguish between different sizes of drones with over 90% accuracy. The results show that the suggested algorithm is highly appropriate for an automated target recognition method in a functional FMCW radar system for drone detection [21].

Drones are increasingly used for recreation, engineering, disaster management, logistics, and airport security. Despite their practical use, airport physical infrastructure security, safety, and surveillance raise concerns about malicious use. Many airports report unauthorized drone use disrupting airline operations. This study proposes deep learning to distinguish two drone and bird species. The suggested method outperforms literature-based detection systems in an image dataset test. Due to their resemblance in appearance and behavior, drones are often inappropriate for birds. The proposed method detects drones, distinguishes two types, and distinguishes birds. This study trained the network with 10,000 multirotor, helicopter, and bird drone images. As expected, the proposed deep learning method distinguishes drones and birds with 83% accuracy, 84% mAP, and 81% IoU. The average Recall, accuracy, and F1-score for the three classes were 84%, 83%, and 83% [22].

Reconnaissance drones are specifically designed to analyze data and interpret signals they intercept, allowing them to detect and pinpoint radar systems. However, identifying quasi-simultaneous arrival signals (QSAS) has become increasingly challenging in complex electromagnetic environments. To address this issue, we propose a framework for self-supervised deep representation learning. The framework consists of two phases: (1) Training an autoencoder: The ConvNeXt V2 model is trained to extract features from masked time-frequency images, enabling it to learn the unlabeled QSAS representation. The model reconstructs the corresponding signal in both the time and frequency domains. (2) Knowledge transfer: The model transfers the learned knowledge, where the encoder layers are kept fixed for downstream tasks. A linear layer is then fine-tuned to classify QSAS in few-shot scenarios. Experimental results demonstrate that the proposed algorithm achieves an average recognition accuracy exceeding 81% across a signal-to-noise ratio (SNR) range of -16 to 16 dB. Additionally, the new algorithm reduces testing time by approximately 11-fold and improves accuracy by up to 21.95% compared to existing CNN-based and Transformer-based neural networks [23].

Security cameras in a secure organization or facility transmit live video feeds to the server for security personnel to monitor. Traditional monitoring methods, such as human observation, are ineffective when a drone enters the facility beyond the range detectable by the monitor, which is live-streaming footage. A man can detect a drone at a distance of approximately 400 meters. Garuda's proposed solution utilizes a deep learning architecture trained on a specialized dataset containing visual images of drones and other aerial objects. The proposed model is designed to precisely identify the lines and edges of drones, enabling it to distinguish drones from birds, kites, and planes. The model can track drone movements such as approaching, receding, or moving laterally by analyzing the area covered by the drone in consecutive time intervals and determining the direction based on changes in the area size, indicating approaching or receding situations. Lateral movement is identified by comparing the drone's position coordinates at different intervals. The paper thoroughly compares different deep learning structures using two datasets. A software application has been developed to contain the drone detection model, capable of detecting, managing, and recording such events with a precision of 94.5% [24].

Authors: Michael Nentwich (project leader) and Delila Horvath from the Institute of Technology Assessment in Vienna, 2018. The concept of using drones for delivery is based on certain assumptions. To achieve this, numerous technical and regulatory challenges must be addressed. Given the significant impact on the airspace, previously used primarily by birds and occasionally helicopters, several standard technology assessment (TA) questions arise. Are there any safety concerns? Are there environmental risks? Can the technology be exploited by criminals or terrorists? Are we facing societal conflicts due to divergent interests? Is the current regulatory framework sufficient, or are new regulations needed? The vision of a drone-based delivery system is not without prerequisites. Many regulatory and technical hurdles must be overcome to make it a reality. Due to the significant impact of this technological development—since it will drastically change the airspace we inhabit, which has so far been used primarily by birds and the occasional helicopter, a series of typical technology assessment questions emerge. Are there safety concerns? Are there environmental hazards? Can the technology be misused for criminal or terrorist purposes? Does it hold the potential for societal conflict due to conflicting interests? Is the existing regulatory framework sufficient, or should new regulations be established [25]?

The proliferation of UAVs has rapidly increased in recent years. Drones are being used more frequently in both military and commercial settings. UAVs of different sizes, shapes, and types are utilized for various purposes, from leisure activities to specific missions. This progress has brought about difficulties and has been recognized as a possible cause of operational interruptions resulting in different security issues, such as risks to Critical Infrastructures (CI). Developing fully autonomous Anti-Unmanned Aerial Vehicle Defence Systems (AUDS) is more urgent now than ever. This paper introduces a comprehensive design and operational prototype of drone detection technology that uses Digital Image Processing (DIP) and Machine Learning (ML) to accurately detect, track, and classify drones to reduce or eliminate the threat they pose. The system utilizes a background-subtracted frame difference technique to detect moving objects, in conjunction with a Pan-Tilt tracking system controlled by a Raspberry Pi to track the detected object. Moving items are recognized using a Convolutional Neural Network (CNN) device known as the YOLO v4-tiny ML set of rules. The proposed gadget stands proud because of its precision, efficiency with cheaper sensing gadgets, and advanced overall performance in contrast to different options. Integrating the system with various systems, such as RADAR, may allow for appreciable decoration of detection technology, further simplifying operations. The proposed era was experimentally verified in diverse checks carried out in uncontrolled outside surroundings, demonstrating steady effectiveness in all situations and producing terrific results [26].

Summary A fluorescent sensor with more than one capability, based on coumarin and containing a di-2-picolylamine (DPA) organization (1), is brought. This probe can function as a fluorescent sensor for Co2 and Cu2 in an ON-OFF manner. The generated 1-Co(II) and 1-Cu(II) ensembles can then act as OFF-ON fluorescent sensors to differentiate between Zn2 and Cd2 and selectively locate sulphide anions in water through displacement. Specifically, Cu(II) can pass through the cellular membrane and be utilized for fluorescence imaging of S2− in living biological samples. The fluorescent sensors of the ON-OFF-ON type showed exceptional selectivity and sensitivity toward the objectives [27].

III. METHODOLOGY

A. Dataset Description

Inspecting the "Birds vs. Drone Dataset" on Kaggle, which Harsh Walia contributed. This dataset incorporates two folders that categorize snapshots of birds and drones [28]. These

folders are essential for the author's academic device, as they assist in reading and differentiating between those two topics. The fowl pictures were received via net scraping, whilst the drone pix were obtained from another dataset. The folders incorporate extensive photos that constitute the subjects observed in natural sky backgrounds. These snapshots are essential for teaching the author's version [1]. Fig. 1 shows the process flow diagram.

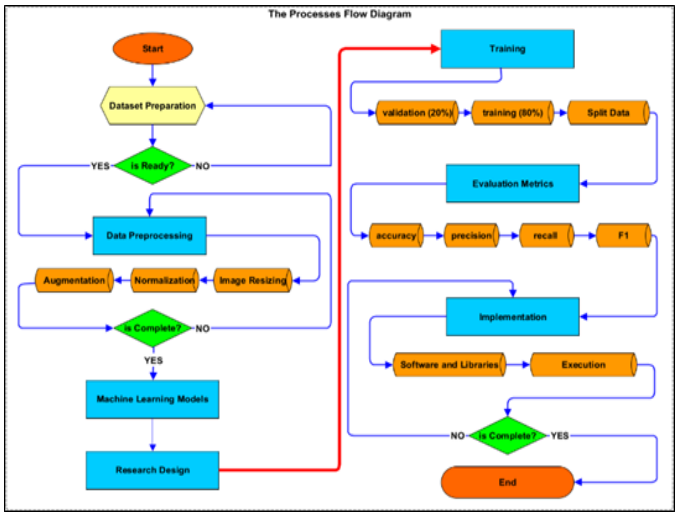


Fig. 1. The process flow diagram [29].

B. Data Preprocessing

Considering the wide range of images in terms of background, orientation, and scale, we implemented the following preprocessing steps to ensure the dataset was standardized for optimal training [29]:

- Image Resizing: To maintain a consistent input size for the neural network, all images were adjusted to a uniform dimension of 224x224 pixels.
- Normalization: The pixel values of each image were adjusted to a range of 0 to 1, which helps to enhance the speed of convergence during the training process.
- Augmentation: To enhance the resilience of our model and avoid overfitting, we implemented image augmentation techniques, including rotation, zoom, and horizontal flipping.

C. Machine Learning Models

Multiple machine learning models were utilized during the evaluation process to analyze their effectiveness in predicting the Bords and Drones Dataset [29]. We used the following models:

1) K-Nearest Neighbors (KNN): KNN is crucial for its simplicity and effectiveness in applications where relationships within the data are distance-based. It's precious in fields like recommendation systems and anomaly detection, where the closest neighbors often share more similarities or properties [30].

2) AdaBoost (Adaptive Boosting): AdaBoost is pivotal for enhancing the performance of weak classifiers, making it essential for scenarios where simple models must be combined to improve accuracy. It's widely used in applications requiring robust performance, such as face detection in images, due to its ability to focus iteratively on challenging cases [31].

3) Constant model: The constant model serves as a fundamental benchmark in machine learning, ensuring that any new model provides a meaningful improvement over the simplest possible approach. Establishing a baseline performance level that other, more sophisticated models must exceed to be considered adequate is crucial [32].

4) CN2 rule induction: CN2 Rule Induction is critical in settings where interpretability is as crucial as prediction accuracy, such as in medical or financial applications. Generate explicit if-then rules, which provide clear insights into decision processes and facilitate understanding and acceptance among users [33].

5) Naive Bayes: Naive Bayes is indispensable in text classification due to its efficiency and scalability, effectively handling large datasets with high-dimensional features. Its feature independence assumption simplifies calculations, making it a go-to method in spam detection and natural language processing [34].

6) Support Vector Machine (SVM): SVM's ability to find the optimal boundary between classes makes it extremely powerful for classification tasks, especially when the classes are well separable. Its application in bioinformatics, image recognition, and other areas where precision is critical underscores its importance. The kernel trick, which allows SVM to adapt to non-linear relationships, further enhances its applicability to a wide range of complex datasets [34].

D. Research Design

The "Birds vs. Drone Dataset," created by Harsh Walia and made publicly available on Kaggle, is used to have a look. This dataset plays a crucial role in the author's investigating device studying-based aerial drone and fowl discrimination. Carefully organized into beautiful folders, it can take snapshots of birds and drones, respectively. The birds' pix were retrieved using an in-depth net scraping approach that changed into, in particular, engineered to capture various bird species in diverse flying positions and settings. This series aims to capture authentic, real-world variability. Contrarily, the drone photos are from an existing dataset and feature a range of drone styles, all set against a sky background. Because of this, you can rest assured that the dataset only shows cases where drones are in the air. Each folder contains a full-size quantity of pictures to train robust machine learning models, offering a broad range of visual records. A strong classifier capable of consistently differentiating among these training data in typical operational contexts requires images that are both varied and of high quality [35-37].

E. Training

1) Configuration: A learning fee scheduler adjusted the model's parameters depending on when the validation loss plateaued; the model's batch size was 32, and the learning rate was 0.001.

2) Environment: Training was carried out on a GPU-enabled system to speed up the computation.

3) Validation split: Splitting the dataset into training (80%) and validation (20%) parts helped identify and prevent overfitting [38-40].

F. Evaluation Metrics

The author's version was tested for overall performance using accuracy, precision, and remember metrics. This version's performance in accurately labeling photos as either birds or drones can be better understood with the help of these metrics [1], [3], [6], [28].

1) AUC (Area Under the Curve): AUC represents the ability of a model to discriminate between positive and negative classes across all possible classification thresholds. Its importance lies in its use as a single measure that summarizes the model's performance in prevalent and rare events. It makes it essential in medical diagnostics and other binary classification tasks where the choice of the decision threshold impacts outcomes significantly.

2) CA (Classification Accuracy): Classification Accuracy measures the overall effectiveness of a model in correctly identifying both positive and negative outcomes. It's a straightforward metric useful in evaluating models where class distributions are balanced, providing a quick snapshot of model efficacy in fields like educational testing and customer satisfaction analysis.

3) F1 Score: The F1 Score balances precision and Recall, which is crucial in scenarios where false positives and negatives have severe implications, such as in legal and financial domains. Its importance stems from providing a more realistic measure of a model's performance when dealing with imbalanced datasets, where the cost of errors can be high.

4) Precision (Prec.): Precision assesses the model's accuracy in predicting positive labels, which is essential in situations where the consequences of false positives are more severe than false negatives, such as in spam detection or during the preliminary stages of drug approval processes, ensuring resources are used efficiently and safely.

5) Recall: Recall is essential when missing a positive occurrence (false negative) is unacceptable, such as in fraud detection or disease screening. It ensures that the most critical cases are identified, even at the expense of making more errors on the negative side (false positives).

6) LogLoss (Logarithmic Loss): LogLoss provides insight into the certainty of a model's predictions, emphasizing the consequences of being wrong, not just whether it is incorrect. This metric is paramount in fields like healthcare and risk assessment, where understanding the probability of outcomes influences decision-making processes significantly, ensuring decisions are informed and minimizing risk.

These metrics collectively provide a comprehensive assessment framework for machine learning models, facilitating informed decision-making in various applications by highlighting aspects of model performance related to the specific costs of prediction errors.

G. Implementation

The model was implemented using Python, utilizing TensorFlow and Keras to construct and train the neural network. Supplementary libraries were utilized alongside NumPy and Matplotlib for data manipulation and visualization. The script was completed through iterative processes, adjusting parameters and configurations based on the performance observed in the validation set.

IV. Results

A. Test and Score Analyses

Test and Score analyses are critical for assessing the generalization abilities of gadget learning models. This is executed by educating them on a selected training set and comparing their performance on a separate trying-out set. This approach evaluates critical metrics like accuracy, precision, consider, F1 score, and place underneath the ROC curve (AUC) to benefit intensive know-how of the model's overall performance in predicting consequences, its capacity to become aware of relevant times efficiently, and its universal accuracy. Performing these analyses is vital for figuring out overfitting, a scenario wherein a version performs well on education records but poorly on new, unseen facts. This lets developers regulate the model to decorate its practicality and resilience through iterative optimization.

1) Test and score analyses for target class birds: Table I compares the performance of various system studying models and the usage of stratified 10-fold pass-validation for classifying “Birds”. Models like kNN, AdaBoost, and CN2 Rule Induction excel with best scores across AUC, CA, F1, Precision, and Recall, indicating their tremendous ability to categorize and differentiate birds as they should be inside the dataset. However, CN2 has a moderate LogLoss, indicating minor prediction uncertainty. The SVM model demonstrates high efficiency with nearly perfect metrics and a very low LogLoss, suggesting effective generalization with minor imperfections. In contrast, Naïve Bayes shows moderate performance with the highest LogLoss, reflecting significant prediction uncertainty. At the same time, the Constant model, used as a baseline, performs poorly, substantiating its inadequacy beyond a control comparison. These results highlight the effectiveness of using advanced models over simpler ones and the critical role of choosing the suitable model based on specific task requirements and dataset characteristics, as shown in Table I and Fig. 2.

TABLE I. THE TEST AND SCORE ANALYSES FOR THE KNN, ADABOOST, CN2, SVM, NAÏVE BAYES, AND CONSTANT MODELS FOR THE TARGET CLASS: BIRDS

Model	AUC	CA	F1	Prec	Recall	LogLoss
kNN	1	1	1	1	1	0
AdaBoost	1	1	1	1	1	0
CN2 Rule Induction	1	1	1	1	1	0.086
SVM	0.998	0.979	0.979	0.969	0.99	0.055
Naïve Bayes	0.884	0.838	0.843	0.808	0.881	5.139
Constant	0.5	0.507	0	0	0	0.693

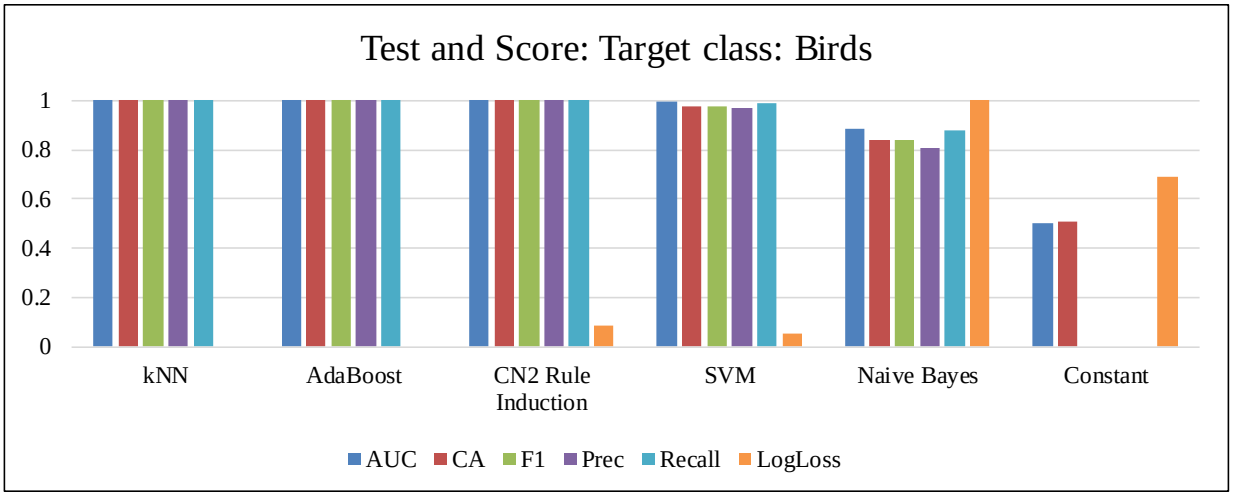


Fig. 2. The test and score analyses for the KNN, AdaBoost, CN2, SVM, Naïve Bayes, and Constant models for the target class: Birds.

2) Test and score analyses for target class drones: Table II provides a comparative performance analysis of several machine learning models for drone classification using stratified 10-fold cross-validation, showcasing a range of outcomes. The kNN, AdaBoost, and CN2 Rule Induction models excel with perfect scores across all metrics (AUC, CA, F1, Precision, Recall), indicating flawless classification abilities. However, CN2 has a slight LogLoss of 0.086, suggesting minimal uncertainty. The SVM model also performs robustly with nearly perfect metrics and a low LogLoss of 0.055, signaling strong but not absolute precision. In contrast, Naive Bayes shows moderate effectiveness with an AUC of 0.868 and significant prediction uncertainty (LogLoss of 5.139), reflecting its limitations in reliability for this task. The Constant model, used as a baseline, predictably underperforms with the lowest scores except in Recall, where it identifies all instances as drones, leading to many false positives. This analysis highlights the superiority of kNN, AdaBoost, and CN2 for drone detection in terms of accuracy and reliability compared to the other models, as shown in Table II and Fig. 3.

TABLE II. THE TEST AND SCORE ANALYSES FOR THE KNN, ADABOOST, CN2, SVM, NAÏVE BAYES, AND CONSTANT MODELS FOR THE TARGET CLASS: DRONES

Model	AUC	CA	F1	Prec	Recall	LogLoss
kNN	1	1	1	1	1	0
AdaBoost	1	1	1	1	1	0
CN2 Rule Induction	1	1	1	1	1	0.086
SVM	0.998	0.979	0.979	0.99	0.969	0.055
Naive Bayes	0.868	0.838	0.833	0.873	0.796	5.139
Constant	0.5	0.507	0.673	0.507	1	0.693

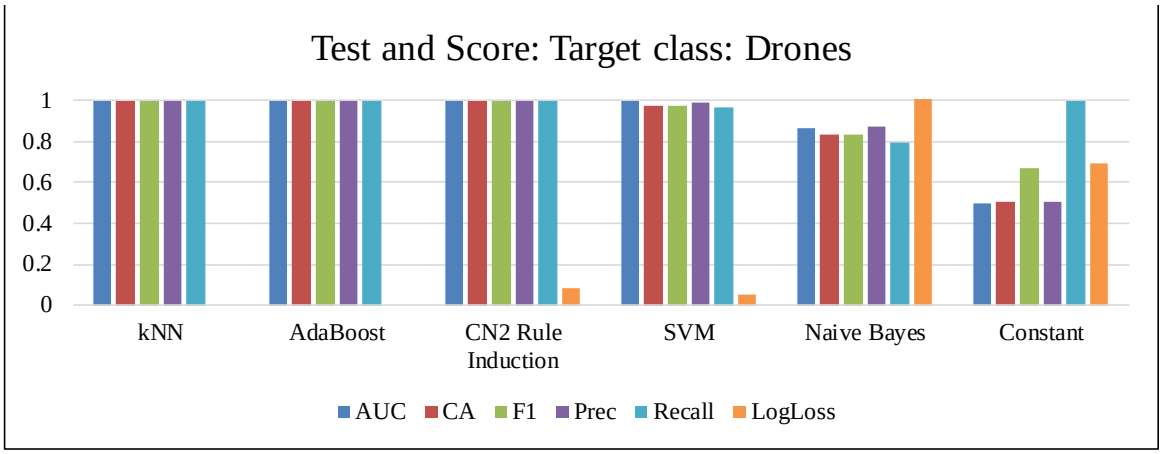


Fig. 3. The test and score analyses for the KNN, AdaBoost, CN2, SVM, Naïve Bayes, and Constant models for the target class: Drones.

3) Test and score analyses for the average performance over all target classes: Table III provides performance metrics for several machine learning models evaluated through stratified 10-fold cross-validation across various classes, revealing distinct levels of effectiveness. The kNN, AdaBoost, and CN2 Rule Induction models excel with perfect scores across all metrics (AUC, CA, F1, Precision, Recall), suggesting flawless classification capabilities; CN2 Rule Induction shows a negligible LogLoss of 0.086, indicating minimal uncertainty. The SVM model also performs exceptionally with nearly perfect metrics and a low LogLoss of 0.055, demonstrating high accuracy and confidence in predictions. In contrast, the Naive Bayes model shows moderate performance with lower scores and a high LogLoss of 5.139, indicating significant predictive uncertainty. The Constant model, used primarily as a baseline, exhibits poor effectiveness with the lowest scores across most metrics, substantiating its limited utility beyond providing a comparative benchmark. This analysis underscores the superiority of kNN, AdaBoost, CN2 Rule Induction, and SVM in achieving reliable and accurate class predictions across diverse datasets, as shown in Table III and Fig. 4.

TABLE III. THE TEST AND SCORE ANALYSES FOR THE TARGET CLASS: AVERAGE OVER CLASSES FOR THE KNN, ADABOOST, CN2, SVM, NAÏVE BAYES, AND CONSTANT MODELS

Model	AUC	CA	F1	Prec	Recall	LogLoss
kNN	1	1	1	1	1	0
AdaBoost	1	1	1	1	1	0
CN2 Rule Induction	1	1	1	1	1	0.086
SVM	0.998	0.979	0.979	0.98	0.979	0.055
Naive Bayes	0.868	0.838	0.838	0.841	0.838	5.139
Constant	0.5	0.507	0.341	0.257	0.507	0.693

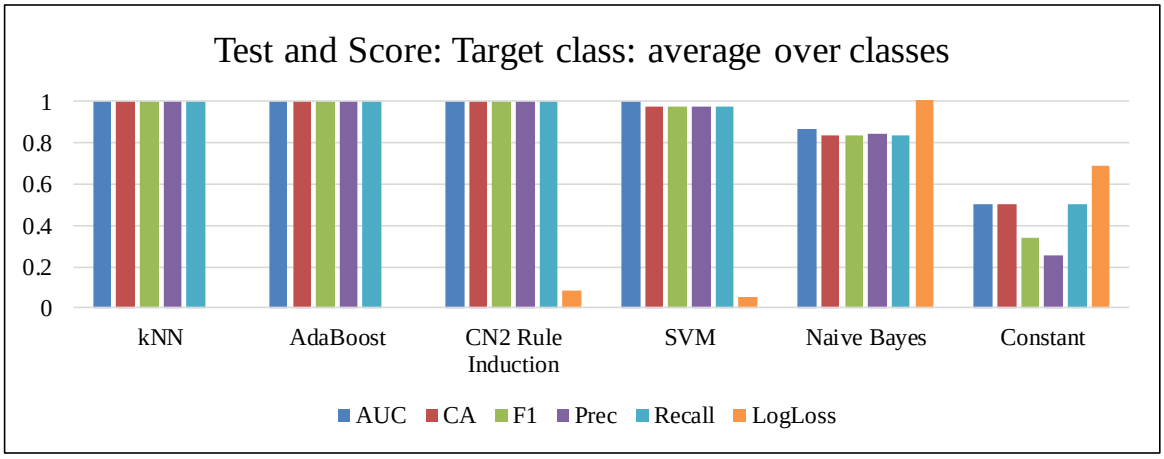


Fig. 4. The test and score analyses for the KNN, AdaBoost, CN2, SVM, Naïve Bayes, and Constant models for the target class: Average over classes.

B. Confusion Matrix Analyses

Confusion Matrix Analyses provide a complete evaluation of a classification version's overall performance by presenting the counts of real positives, real negatives, false positives, and fake negatives in a matrix format. This analysis helps to visualize the accuracy of a version in predicting one-of-a-kind lessons, taking into consideration a more profound expertise of its predictive competencies and weaknesses. The most critical diagonal of the matrix indicates the range of accurate predictions, even as the off-diagonal elements imply the errors. Key derived metrics such as precision (the accuracy of superb predictions), remember (the version's capacity to discover all the excellent samples), and F1-rating (a harmonic implication of precision and remember) can be calculated from the confusion matrix. These metrics are crucial for diagnosing the overall performance of a model past easy accuracy, particularly in cases in which training is imbalanced, assisting in picking out whether a model is biased toward one magnificence and offering insights necessary for further refining the version's parameters.

Table IV confusion matrix showcases the performance of various machine learning models in classifying entities into two categories: Birds and Drones. kNN, AdaBoost, and CN2 Rule Induction excel with perfect classification accuracy, correctly identifying all Birds and Drones without misclassifications, achieving 100% precision, Recall, and accuracy. In stark contrast, the Constant model, used as a baseline, misclassifies all instances, highlighting its inadequacy for practical use with a recall of 1 for Drones due to predicting everything as Drones and a very low precision. Naive Bayes and SVM show moderate to high performance, with Naive Bayes misclassifying many birds and drones. SVM makes a few errors but still maintains high accuracy overall. These results indicate that while kNN, AdaBoost, and CN2 Rule Induction are highly effective for this task, Naive Bayes and SVM, although robust, exhibit potential areas for improvement in classification accuracy, as shown in Table IV and Fig. 5.

TABLE IV. THE CONFUSION MATRIX ANALYSES FOR THE MODELS KNN, ADABOOST, CN2, SVM, NAÏVE BAYES, AND CONSTANT

			Predicted	
			Birds	**Drones**
Actual	KNN	Birds	286	0
		Drones	0	294
	AdaBoost	Birds	286	0
		Drones	0	294
	Constant	Birds	0	286
		Drones	0	294
	CN2 Rule Induction	Birds	286	0
		Drones	0	294
	Naive Bayes	Birds	252	34
		Drones	60	234
	SVM	Birds	283	3
		Drones	9	285

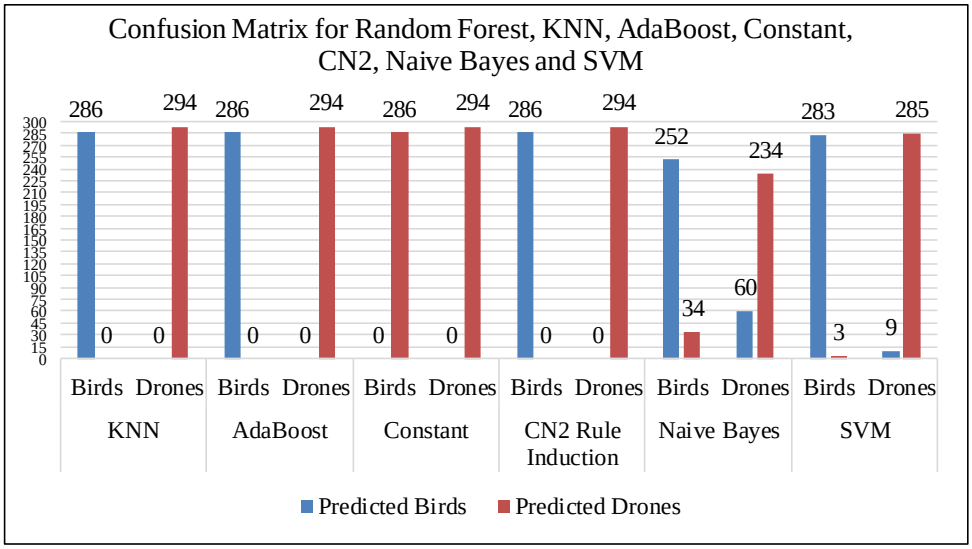


Fig. 5. The confusion matrix analyses of the KNN, AdaBoost, CN2, SVM, Naïve Bayes, and Constant models for the target class: Birds and drones.

C. ROC Analyses

ROC analysis is a statistical method utilized in educational discussions to assess the diagnostic performance of binary classifiers. An ROC curve is a graph that shows how properly a classifier performs by evaluating the True Positive Rate (TPR) with the False Positive Rate (FPR) at one of a kind threshold degrees without considering class distribution or error rates. The location under the ROC curve (AUC) is a metric that quantifies a classifier's potential to differentiate between two instructions, with a better AUC indicating better performance. ROC assessment is highly precious for assessing overall performance across all types of thresholds, presenting an independent degree of impartiality regarding precise decision criteria. This analytical device is essential for comparing exclusive classifiers, supplying a clean visualization of their strengths and weaknesses in numerous operational eventualities. It is a fundamental component in the discipline of gadgets getting to know for developing fashions with better choice-making competencies.

1) ROC analyses for target class birds: The ROC (Receiver Operating Characteristic) curve evaluation within the Fig. 6 evaluates several systems, getting to know models for classifying "Birds," highlighting their performance underneath situations where false positives and false negatives are equally costly. The kNN and AdaBoost models showcase superior performance, with their ROC curves nearing the top left corner, indicating first-rate sensitivity and minimum fake fantastic charges, which are ideal for precision-crucial applications. CN2 Rule Induction additionally indicates brilliant effects, closely matching the primary fashions, suggesting its effectiveness in complicated sample reputation. Although slightly below the top performers, the SVM model maintains robust discrimination capabilities. In contrast, Naive Bayes displays moderate performance with a noticeable distance from the ideal curve, indicating potential issues with precision in distinguishing similar classes. The Constant model, represented by the diagonal line, serves as a baseline, performing at a chance level, thereby underscoring the advanced discriminative power of the specialized algorithms compared to a non-discriminative approach.

2) ROC analyses for target class drones: As shown in Fig. 7, the ROC curve analysis for drone classification reveals that the kNN and AdaBoost models exhibit exceptional performance, with their curves closely approaching the top left corner, indicative of high sensitivity and minimal false positives, making them highly effective for applications where precision is paramount due to high costs associated with misclassifications. CN2 Rule Induction also demonstrates robust capabilities, with its curve nearly matching the leaders, indicating its suitability for complex pattern recognition tasks. In contrast, the SVM model, though showing good performance, has a slightly less optimal curve, suggesting a few more false positives under certain thresholds. Naive Bayes significantly underperform relative to other models, as its curve is closer to the diagonal, indicating a higher rate of false positives, which may not be ideal in high-stakes scenarios. The Constant model, aligning with the diagonal, serves as a non-discriminative baseline, highlighting the necessity and effectiveness of the more sophisticated models in accurately classifying drones to avoid costly errors.

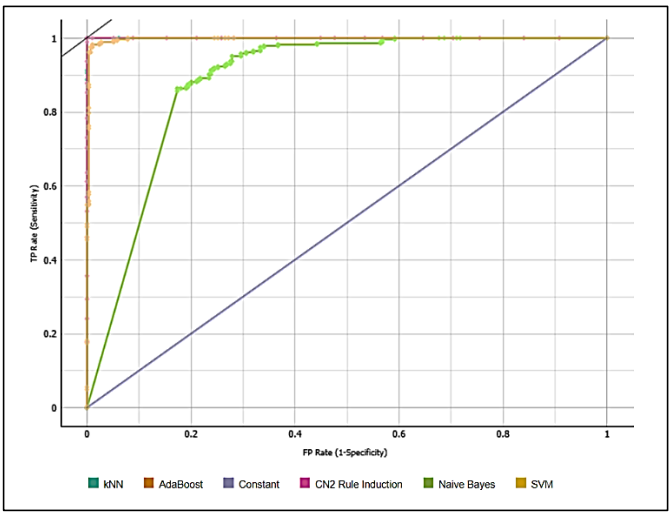


Fig. 6. The ROC Analyses for the KNN, AdaBoost, CN2, SVM, Naïve Bayes, and Constant models for the target class: Birds.

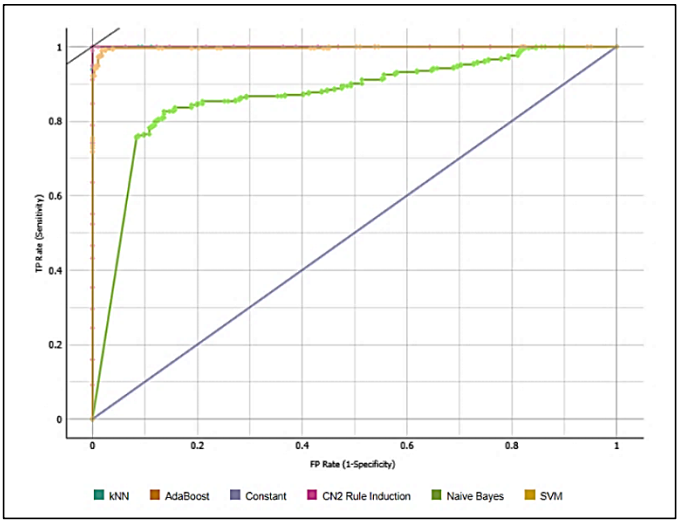


Fig. 7. The ROC analyses for the KNN, AdaBoost, CN2, SVM, Naïve Bayes, and Constant Models for the target class: Drones.

V. Discussion

The "Discussion" section of the item titled "Advances in AI-Based Classification: Differentiating between Unmanned Aerial Vehicles and Birds in Flight" centers on evaluating the realistic implications, demanding situations, and future guidelines advised via the study's findings. The look at, through its rigorous assessment of various system learning fashions, which include kNN, AdaBoost, CN2 Rule Induction, and SVM, demonstrates their effectiveness in as it should be distinguishing UAVs from birds—a critical functionality for enhancing safety features in each military and civilian domain names.

This discussion emphasizes the precision with which these fashions operate, highlighting their capability to reduce false positives and negatives seriously. Such accuracy is vital in real-time safety contexts where the value of errors is exceedingly excessive. It also addresses the combination challenges of those advanced algorithms in present surveillance frameworks. The adaptability of these fashions across exceptional environmental situations is vital, as well as factors like variable lighting fixtures, weather adjustments, and diverse landscapes that might affect detection accuracy.

Moreover, the dialogue explores the computational efficiency of those algorithms, noting the significance of processing speed for real-time applications and the ability for further optimization to deal with larger, more complicated datasets without compromising performance. There is also an acknowledgment of the need for ongoing development to keep pace with the evolving abilities of UAV technology and the corresponding security requirements.

Ethical concerns form an essential part of the discourse, mainly the stability among protection enhancements and the capability for infringement on privacy rights. The deployment of such technology must be managed cautiously to avoid abuse that might cause massive societal and moral dilemmas.

The phase concludes by proposing future research guidelines. It indicates exploring hybrid models that could combine the strengths of numerous present approaches to enhance accuracy and performance. Additionally, there is a call for empirical checking out those models in operational situations to validate their effectiveness in international situations and to refine their talents primarily based on stay facts.

Overall, this discussion synthesizes the study's contributions to the field of airspace security but also outlines a roadmap for destiny technological and strategic improvements in UAV detection and classification, ensuring that safety features evolve in tandem with rising aerial threats.

VI. Conclusion

The study titled "Skywatch: Advanced Machine Learning Techniques for Distinguishing UAVs from Birds in Airspace Security" represents a significant advancement in the application of machine learning for enhancing airspace security. By employing a variety of advanced algorithms, including kNN, AdaBoost, CN2 Rule Induction, and SVM, the research has demonstrated high accuracy in differentiating UAVs from birds, which is crucial for both military operations and civilian airspace protection.

The results indicate that these models achieve a high level of accuracy and effectively reduce false positives and negatives—key factors in real-time surveillance and threat detection. This capability ensures rapid and reliable responses in dynamic and potentially adversarial environments. Furthermore, the integration of these machine learning models into existing surveillance systems has proven to significantly enhance national security measures.

However, the study also acknowledges certain limitations. First, while the machine learning models demonstrated strong performance, the evolving sophistication of UAV technologies presents a continuous challenge. Future UAVs may exhibit more complex flight behaviors and features, potentially reducing the efficacy of the current models. Thus, there is a need for ongoing refinement and adaptation of these algorithms to keep pace with advancements in UAV technology. Second, the environmental diversity in real-world scenarios poses a limitation. The models were tested under controlled or simulated conditions, and their performance may vary when exposed to a wider range of environmental factors, such as extreme weather, varying light conditions, and densely populated areas. Further testing in diverse, real-world settings is essential to fully validate the practical applicability of these systems.

Additionally, the study highlights ethical and privacy concerns related to the deployment of UAV detection systems in civilian contexts. The potential misuse of these technologies underscores the importance of establishing clear regulatory frameworks to ensure responsible and transparent usage.

Looking forward, the research suggests exploring hybrid machine learning models that combine the strengths of various algorithms to achieve even greater accuracy and efficiency. Testing these models in real-world scenarios will be crucial for refining their capabilities and ensuring their practical deployment.

In conclusion, this study offers significant contributions to the fields of machine learning and security technology, providing valuable insights and practical solutions for improving airspace security in an era where UAV technology is rapidly advancing. The findings not only enhance current security protocols but also pave the way for future innovations in aerial threat detection and management.

VII. Future Work and Improvements

While this study has made significant advancements in distinguishing UAVs from birds using machine learning algorithms, there are several areas that warrant further investigation to enhance the robustness and applicability of the models.

1) Addressing model scalability and complexity: One major limitation is the scalability of the models in increasingly complex environments. As UAV technologies continue to evolve, particularly with the introduction of more sophisticated designs and swarming behaviors, the current models may struggle to accurately classify these newer types. Future research should focus on developing more scalable algorithms that can adapt to new types of UAVs and handle increasingly complex data inputs. This may involve the exploration of hybrid models or deep learning techniques that can capture more nuanced patterns in flight behavior.

2) Environmental adaptability: Another area for improvement lies in enhancing the adaptability of these models to diverse and unpredictable environmental conditions. While the current study evaluated the models under controlled conditions, real-world environments often present challenges such as adverse weather, poor lighting, and background clutter

that could affect detection accuracy. Further work is needed to test and refine the models in a broader range of real-world scenarios. Techniques such as transfer learning and domain adaptation could be explored to make the models more resilient across different environmental conditions.

3) Integration with multi-sensor data: Future research could also explore the integration of multi-sensor data to enhance detection accuracy. Combining optical imagery with other forms of data, such as radar or infrared signals, could provide a more comprehensive input for the models, helping to distinguish UAVs from birds with even greater precision. Investigating how to optimally fuse data from multiple sensors in real time would be a valuable next step.

4) Real-time performance enhancements: While this study demonstrates the feasibility of real-time UAV detection, there is still room for improving the speed and computational efficiency of the models, particularly in high-stakes environments. Real-time systems require low-latency performance, which may necessitate further algorithmic optimizations or the use of specialized hardware such as GPUs or edge computing devices to ensure faster processing times without sacrificing accuracy.

5) Mitigating ethical and privacy concerns: Ethical and privacy concerns regarding the use of UAV detection systems in civilian settings remain an important topic for future research. There is a need for guidelines and frameworks that govern the deployment of these technologies to avoid misuse and ensure transparency. Future work should also address how these systems can be designed to respect privacy while still providing the necessary security benefits.

6) Long-term model maintenance and adaptability: Machine learning models must be regularly updated to maintain their effectiveness as the nature of threats evolves. This study does not delve into long-term maintenance strategies for the algorithms. Developing methods for automatic retraining of the models with new data, without compromising their performance, will be essential to ensure continued effectiveness in rapidly changing operational contexts.

7) Potential for cross-domain applications: Beyond military and civilian airspace security, the techniques developed in this study could be adapted for other domains such as environmental monitoring, wildlife protection, or even urban management systems. Future work should explore the feasibility of transferring these models to other fields where UAVs or flying objects are involved, potentially opening up new applications for the technology.

By addressing these limitations and pursuing these future directions, this research can evolve to become a more comprehensive solution, capable of adapting to the complexities of real-world scenarios while balancing the technological and ethical challenges of UAV detection.

Data Availability Statement

The datasets presented in this study can be found in online repositories. The names of the repository/repositories and accession number(s) can be found below: https://www.kaggle.com/datasets/saidulkabir/vcug-vur-dataset

Conflict of Interest

The authors declare that the research was conducted without any commercial or financial relationships that could be construed as a potential conflict of interest.

Financing

This work is supported from Jadara University under grant number [Jadara-SR-Full2023].

References

[1] M. S. Alzboon, S. Qawasmeh, M. Alqaraleh, A. Abuashour, A. F. Bader, and M. Al-Batah, "Pushing the Envelope: Investigating the Potential and Limitations of ChatGPT and Artificial Intelligence in Advancing Computer Science Research," 2023, doi: 10.1109/eSmarTA59349.2023.10293294.

[2] M. S. Alzboon, S. Qawasmeh, M. Alqaraleh, A. Abuashour, A. F. Bader, and M. Al-Batah, "Machine Learning Classification Algorithms for Accurate Breast Cancer Diagnosis," 2023, doi: 10.1109/eSmarTA59349.2023.10293415.

[3] M. S. Alzboon, M. S. Al-Batah, M. Alqaraleh, A. Abuashour, and A. F. H. Bader, "Early Diagnosis of Diabetes: A Comparison of Machine Learning Methods," Int. J. online Biomed. Eng., vol. 19, no. 15, pp. 144–165, 2023, doi: 10.3991/ijoe.v19i15.42417.

[4] S. A. Alomari, M. Alqaraleh, E. Aljarrah, and M. S. Alzboon, "Toward achieving self-resource discovery in distributed systems based on distributed quadtree," J. Theor. Appl. Inf. Technol., vol. 98, no. 20, pp. 3088–3099, 2020.

[5] M. S. Alzboon, M. Al-Batah, M. Alqaraleh, A. Abuashour, and A. F. Bader, "A Comparative Study of Machine Learning Techniques for Early Prediction of Diabetes," 2023, pp. 1–12, doi: 10.1109/comnet60156.2023.10366688.

[6] M. S. Alzboon, M. Al-Batah, M. Alqaraleh, A. Abuashour, and A. F. Bader, "A Comparative Study of Machine Learning Techniques for Early Prediction of Prostate Cancer," in 2023 IEEE 10th International Conference on Communications and Networking, ComNet 2023 - Proceedings, 2023, pp. 1–12, doi: 10.1109/ComNet60156.2023.10366703.

[7] M. Alzboon, Mowafaq Salem and Bader, Ahmad Fuad and Abuashour, Ahmad and Alqaraleh, Muhyeeddin Kamel and Zaqaibeh, Belal and Al-Batah, "The Two Sides of AI in Cybersecurity: Opportunities and Challenges," 2023.

[8] S. Sethu Selvi, S. Pavithraa, R. Dharini, and E. Chaitra, "A Deep Learning Approach to Classify Drones and Birds," 2022, doi: 10.1109/MysuruCon55714.2022.9972589.

[9] S. E. Abdelsamad et al., "Vision-Based Support for the Detection and Recognition of Drones with Small Radar Cross Sections," Electron., vol. 12, no. 10, 2023, doi: 10.3390/electronics12102235.

[10] A. Sikora and D. Marchowski, "The use of drones to study the breeding productivity of Whooper Swan Cygnus cygnus," Eur. Zool. J., vol. 90, no. 1, pp. 193–200, 2023, doi: 10.1080/24750263.2023.2181414.

[11] M. Kassab, A. E. F. Seghrouchni, F. Barbaresco, and R. A. Zitar, "A Lower Complexity Deep Learning Method for Drones Detection," 2023, doi: 10.1109/SSPD57945.2023.10256977.

[12] P. L. Bishay et al., "3D-Printed Bio-Inspired Mechanisms for Bird-like Morphing Drones," Appl. Sci., vol. 13, no. 21, p. 11814, 2023, doi: 10.3390/app132111814.

[13] J. Wojtanowski, M. Zygmunt, T. Drozd, M. Jakubaszek, M. Życzkowski, and M. Muzal, "Distinguishing drones from birds in a uav searching laser scanner based on echo depolarization measurement," Sensors, vol. 21, no. 16, 2021, doi: 10.3390/s21165597.

[14] D. Petrizze, K. Koorehdavoudi, M. Xue, and S. Roy, "Distinguishing Aerial Intruders from Trajectory Data: A Model-Based Hypothesis-Testing Approach," in Proceedings of the American Control Conference, 2021, vol. 2021-May, pp. 3951–3956, doi: 10.23919/ACC50511.2021.9483439.

[15] J. Liu, Q. Y. Xu, and W. S. Chen, "Classification of Bird and Drone Targets Based on Motion Characteristics and Random Forest Model Using Surveillance Radar Data," IEEE Access, vol. 9, pp. 160135–160144, 2021, doi: 10.1109/ACCESS.2021.3130231.

[16] R. M. Narayanan, B. Tsang, and R. Bharadwaj, "Classification and Discrimination of Birds and Small Drones Using Radar Micro-Doppler Spectrogram Images †," Signals, vol. 4, no. 2, pp. 337–358, 2023, doi: 10.3390/signals4020018.

[17] M. A. Bell, S. Rahman, and D. A. Robertson, "Fast classification of drones and birds with an LSTM network applied to 1D phase data," 2023, doi: 10.1109/RADAR54928.2023.10371144.

[18] S.-W. Yoon et al., "Efficient Protocol to Use FMCW Radar and CNN to Distinguish Micro-Doppler Signatures of Multiple Drones and Birds," IEEE Access, vol. 10, pp. 26033–26044, 2022, doi: 10.1109/ACCESS.2022.3155776.

[19] B. Tsang, R. M. Narayanan, and R. Bharadwaj, "Experimental analysis of micro-Doppler characteristics of drones and birds for classification purposes," in Defense + Commercial Sensing, 2022, p. 24, doi: 10.1117/12.2622408.

[20] M. S. Alzboon, M. Alqaraleh, and M. S. Al-Batah, "AI in the Sky: Developing Real-Time UAV Recognition Systems to Enhance Military Security," Data Metadata, vol. 3, p. 417, 2024, doi: 10.56294/dm2024.417.

[21] S. Rahman and D. A. Robertson, "Millimeter-wave radar micro-Doppler feature extraction of consumer drones and birds for target discrimination," in Defense + Commercial Sensing, 2019, p. 28, doi: 10.1117/12.2518846.

[22] F. Samadzadegan, F. D. Javan, F. A. Mahini, and M. Gholamshahi, "Detection and Recognition of Drones Based on a Deep Convolutional Neural Network Using Visible Imagery," Aerospace, vol. 9, no. 1, 2022, doi: 10.3390/aerospace9010031.

[23] L. Guo, M. Du, J. Xiong, Z. Wu, and J. Pan, "Self-Supervised Representation Learning for Quasi-Simultaneous Arrival Signal Identification Based on Reconnaissance Drones," Drones, vol. 7, no. 7, 2023, doi: 10.3390/drones7070475.

[24] S. S. Selvi, S. Pavithraa, I. Gupta, P. Awasthi, and A. K. Kesari, "GARUDA : Third Eye for Detecting and Tracking Drones," 2023, doi: 10.1109/ICDDS59137.2023.10434890.

[25] M. Nentwich and D. M. Hórvath, "Delivery drones from a technology assessment perspective," Overv. report, No.2018-01,ViennaITA, 2018, doi: 10.1553/ita-pb-2018-01.

[26] D. S. Omkar, N. Asogekar, and S. Rathi, "DETECTION, TRACKING AND CLASSIFICATION OF ROGUE DRONES USING COMPUTER VISION," Int. J. Eng. Appl. Sci. Technol., vol. 7, no. 3, pp. 11–19, 2022, doi: 10.33564/ijeast.2022.v07i03.003.

[27] J. T. Hou, B. Y. Liu, K. Li, K. K. Yu, M. B. Wu, and X. Q. Yu, "Two birds with one stone: Multifunctional and highly selective fluorescent probe for distinguishing Zn2+ from Cd2+ and selective recognition of sulfide anion," Talanta, vol. 116, pp. 434–440, 2013, doi: 10.1016/j.talanta.2013.07.020.

[28] M. S. Alzboon, A. F. Bader, A. Abuashour, M. K. Alqaraleh, B. Zaqaibeh, and M. Al-Batah, "The Two Sides of AI in Cybersecurity: Opportunities and Challenges," 2023, doi: 10.1109/ICNGN59831.2023.10396670.

[29] S. Al Tal, S. Al Salaimeh, S. Ali Alomari, and M. Alqaraleh, "The modern hosting computing systems for small and medium businesses," Acad. Entrep. J., vol. 25, no. 4, pp. 1–7, 2019.

[30] M. Alzboon, "Semantic Text Analysis on Social Networks and Data Processing: Review and Future Directions," Inf. Sci. Lett., vol. 11, no. 5, pp. 1371–1384, 2022, doi: 10.18576/isl/110506.

[31] M. S. Alzboon, E. Aljarrah, M. Alqaraleh, and S. A. Alomari, "Nodexl Tool for Social Network Analysis," 2021.

[32] Al-Batah, M. S. (2019). Ranked features selection with MSBRG algorithm and rules classifiers for cervical cancer. International Journal of Online and Biomedical Engineering (iJOE), 15(12), 4. https://doi.org/10.3991/ijoe.v15i12.10803

[33] Al-Batah, M. S. (2019). Integrating the principal component analysis with partial decision tree in microarray gene data. IJCSNS International Journal of Computer Science and Network Security, 19(3), 24-29.

[34] Alqaraleh, M., & Abdel, M. (2024). Advancing medical image analysis: The role of adaptive optimization techniques in enhancing COVID-19 detection, lung infection, and tumor segmentation. LatIA, 2(74). https://doi.org/10.62486/latia202474

[35] Al-Batah, M. S. (2014). Testing the probability of heart disease using classification and regression tree model. Annual Research & Review in Biology, 4(11), 1713–1725. https://doi.org/10.9734/arrb/2014/7786

[36] Alazaidah, R., Ahmad, F., & Mohsin, M. F. M. (2020). Multi-label ranking based on positive pairwise correlations among labels. International Arab Journal of Information Technology.

[37] Al-Batah, M. S. (2010). Modified recursive least squares algorithm to train the hybrid multilayered perceptron (HMLP) network. Applied Soft Computing, 10(1), 236–244. https://doi.org/10.1016/j.asoc.2009.06.018

[38] Al-Batah, M. S., & Al-Eiadeh, M. R. (2024). An improved binary crow-JAYA optimisation system with various evolution operators, such as mutation for finding the max clique in the dense graph. International Journal of Computing Science and Mathematics, 19(4), 327-338. https://doi.org/10.1504/IJCSM.2024.139088

[39] Cai, R. (1970). Unmanned target vehicle navigation and path planning using improved ant colony optimization algorithm combined with GPS/BDS. The International Arab Journal of Information Technology (IAJIT), 21(4), 601-613. https://doi.org/10.34028/iajit/21/4/5

[40] Al-Batah, M. S., & Al-Eiadeh, M. R. (2023). An improved discreet Jaya optimisation algorithm with mutation operator and opposition-based learning to solve the 0-1 knapsack problem. International Journal of Mathematics in Operational Research, 26(2), 143-169.

Design and Research of Artwork Interactive Exhibition System Based on Multi-Source Data Analysis and Augmented Reality Technology

Xiao Chen*, Qibin Wang
School of Animation and Game, Hangzhou Vocational and Technical College, Hangzhou 310000, China

***Abstract*—The current system has problems such as low efficiency of data processing, lack of smooth user experience and poor combination of display content and interactive technology, etc. There is a pressing need to optimize the integration of data analysis and augmented reality technology to improve the interactivity and visual appeal of exhibitions. This paper introduces and validates a combined prediction model based on multi-source data from the Internet. When using speeded-up robust features (SURF)-64 with a threshold of 500, the number of feature matches is 800, and the matching time is 162.85 ms. At a threshold of 1000, the number of matches drops to 510, and the time decreases to 96.54 ms. For SURF-128, the corresponding matches were 763 and 496, with times of 208.63 ms and 134.21 ms. This indicates that increasing the threshold not only reduces the number of matches but also shortens the matching time, likely due to fewer feature points simplifying the matching process.**

***Keywords*—Multi-source data; feature analysis; augmented reality technology; artwork interactive exhibition system; prediction model**

I. INTRODUCTION

With the popularization of the Internet and the leap of technology, the power of art information dissemination has been significantly enhanced, crossing the boundaries of time and space and widely reaching the public. The integration of digital media has given birth to new art forms, making art everywhere and profoundly affecting life [1, 2]. Artistic creation and technology are deeply integrated, computer technology and digital media have broadened the territory of art, traditional art has been revived under digital empowerment, and its forms of expression are more prosperous and more diverse [3]. Current AR systems in art galleries often focus on enhancing visitor engagement through virtual content, but they typically suffer from limitations such as poor integration of real-world and virtual objects, inadequate feature matching, and limited interactivity. For instance, many systems use basic tracking technologies or simplistic feature extraction methods, which result in a disjointed user experience and less precise placement of virtual elements. Several existing studies have addressed these issues by introducing advanced tracking algorithms and feature extraction techniques, but challenges like real-time performance and seamless interaction between users and virtual content persist. Furthermore, some AR applications still lack immersive interactivity, offering only passive viewing experiences rather than engaging users actively in the artistic exploration process. Our system significantly improves on these limitations by utilizing multi-source data analysis and advanced feature extraction algorithms, such as SURF-64 and SURF-128, which enable more precise object detection, quicker feature matching, and smoother integration of virtual objects into real-world environments [4, 5]. In today's information-driven era, new innovations continuously emerge, and artistic expressions and aesthetic standards are constantly evolving. People's appreciation for the aesthetics of science and technology has become mainstream, as seen in their acceptance and love for new art forms, which also influence our understanding of traditional art [6, 7]. The spread of digital technology has broadened our aesthetic perspectives, encouraging artists to explore new forms of expression and ideas that align with and lead this evolving aesthetic trend [8, 9]. One notable shift is the enhancement of artistic interactivity and participation. Digital technology allows new art forms to be more open and interactive, contrasting with traditional art's one-sided dynamic where artists create and viewers merely observe. In digital art, the audience actively participates in the creative process [10]. AR has revolutionized the way people engage with digital content, particularly in areas like art and culture, by merging real and virtual worlds. AR enables audiences to experience artworks interactively, bringing new dimensions to traditional art forms and making exhibitions more immersive and engaging. However, a critical challenge in AR-based exhibitions lies in ensuring the seamless integration of virtual objects into real environments. Accurate tracking of user movements, efficient processing of environmental data, and the synchronization of multiple data sources are key to creating a cohesive and meaningful interactive experience. Multi-source data analysis plays a crucial role here, as it aggregates information from various sensors, cameras, and user interactions to build a comprehensive understanding of the exhibition space. The proposed combined prediction model addresses these challenges by optimizing the system's ability to anticipate user actions and adjust the virtual content accordingly. This predictive capability enhances the responsiveness of the system, improving the overall interaction quality and ensuring that the AR elements are appropriately aligned with the real world.

The influence of digital technology on art is profound and wide-ranging. From the dissemination of information to changes in the creative process and the renewal of aesthetics, art is becoming deeply integrated into everyday life, serving as a vital link between science, technology, and culture. As technology advances, art will continue to grow in diversity and complexity [11, 12]. Augmented reality technology combines the real and virtual worlds to create immersive 3D experiences, allowing

users to interact intuitively and enjoy new sensory experiences. This interdisciplinary technology integrates tracking, interaction, graphics, and multimedia to enhance system performance, enabling a seamless fusion of the virtual and natural worlds, making users feel as though they are in a blended reality [13, 14]. In augmented reality systems, tracking technology is crucial. It enables the system to accurately capture the user's perspective and position, thereby adjusting the position and display angle of virtual objects in the real world in real-time [15, 16]. AR has revolutionized the way people engage with digital content, particularly in areas like art and culture, by merging real and virtual worlds. AR enables audiences to experience artworks interactively, bringing new dimensions to traditional art forms and making exhibitions more immersive and engaging. A critical challenge in AR-based exhibitions lies in ensuring the seamless integration of virtual objects into real environments. Accurate tracking of user movements, efficient processing of environmental data, and the synchronization of multiple data sources are key to creating a cohesive and meaningful interactive experience. Multi-source data analysis plays a crucial role here, as it aggregates information from various sensors, cameras, and user interactions to build a comprehensive understanding of the exhibition space. The proposed combined prediction model addresses these challenges by optimizing the system's ability to anticipate user actions and adjust the virtual content accordingly. This predictive capability enhances the responsiveness of the system, improving the overall interaction quality and ensuring that the AR elements are appropriately aligned with the real world [17, 18].

II. Key Technologies of Art Interaction System

A. Augmented Reality Tracking Registration Technology

Tracking registration technology is the core of augmented reality. It is widely used to track the dynamics of people and objects in real time and integrate with virtual data to ensure that virtual information is accurately superimposed on real scenes and achieve seamless integration of virtual and real. As shown in Eq. (1) and Eq. (2), these equations define the parameters of feature points used in tracking and registration. Pi represents the position and scale information of the i feature point, where x and y are the coordinates of the feature point in the image, and s is the scale value of the feature point. pt denotes the position at time t, pt−1 is the position at the previous time, v is the velocity, and t1 is the time interval. Its key function lies in precise positioning and dynamic adjustment, so that virtual objects can naturally integrate into reality, presenting highly realistic visual effects both indoors and outdoors.

$$P_i = (x_i, y_i, s_i) \tag{1}$$

$$p_t = p_{t-1} + vt_1 \tag{2}$$

The tracking technology of augmented reality mainly detects objects by various means. As shown in Eq. (3), this equation models the illumination of virtual objects in comparison to real scenes. Ivirtual is the illumination of virtual objects, Ireal is the illumination of real scenes, Iambient is the ambient illumination, and g is the illumination consistency coefficient. These detection means include, but are not limited to, visual tracking, inertial sensors, GPS positioning, and the like. Through these technical means, the augmented reality system can obtain information such as the real-time position, posture and motion state of objects.

$$I_{virtual} = gI_{real} + (1-g)I_{ambient} \tag{3}$$

This transformation not only needs to take into account the three-dimensional spatial position of the object, as shown in Eq. (4), This equation pertains to the consistency of occlusion in augmented reality. Zocclusion is the consistency measure of occlusion, Zreal is the depth value of the real scene, and Zvirtual is the depth value of the virtual object. It is also necessary to combine the motion state of the object and the ambient lighting conditions to ensure that the performance of the virtual object in different scenes can meet the user's expectations.

$$Z_{occlusion} = Z_{real} - Z_{virtual} \tag{4}$$

Tracking technology faces many challenges. First of all, in order to achieve seamless virtual and real fusion, tracking technology needs to have extremely high accuracy and stability. As shown in Eq. (5) and Eq. (6), These equations address the time-sensitive aspects of tracking technology. update is a time interval of real-time update, and fframe is a frame rate. Di is the description vector of the i-th feature point, which contains high-dimensional data describing the local features of the feature point. This means that the system must be able to update the position and pose information of the object in real time within the millisecond level, ensuring that the position of the virtual object in the user's field of view is always consistent with the reference object in the real world.

$$t_{update} = \frac{1}{f_{frame}} \tag{5}$$

$$D_i = \begin{pmatrix} d_{i1} & d_{i2} & \cdots & d_{i16} \end{pmatrix} \tag{6}$$

No delay and no jitter are also important indicators of augmented reality tracking technology. Any tiny delay or jitter will destroy the coordination between the virtual object and the real scene. As shown in Eq. (7) and Eq. (8), these equations focus on the metrics for evaluating feature point matching. Matchi,j is the matching measure of the i-th feature point and the j-th feature point, and b is the standard deviation, which is used to control the width of the Gaussian function. dij is the Euclidean distance between the i-th feature point and the j-th feature point, which is used to measure their similarity. Causing discomfort to the user when using the augmented reality system. Advanced tracking technology often relies on high-performance hardware support and optimized algorithm design to minimize delay and jitter and improve system response speed and stability.

$$Match_{i,j} = exp\left(-\frac{\|D_i - D_j\|^2}{2b^2}\right) \tag{7}$$

$$d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{8}$$

B. Feature Analysis Related Technologies

In image processing and computer vision, feature analysis is very important. As shown in Eq. (9) and Eq. (10), these equations delve into feature point analysis, Thresholdfeature is

the threshold of feature points, N is the total number of feature points, and di is the description measure of each feature point. L(x,y,c) is the image of the scale space, G(x,y,c) is the Gaussian filter, and I(x,y) is the original image. Feature points carry location, scale and high-dimensional description vectors to uniquely identify each point like a "fingerprint".

$$Threshold_{feature} = \frac{1}{N}\sum_{i=1}^{N} d_i \tag{9}$$

$$L(x,y,c) = G(x,y,c) \times I(x,y) \tag{10}$$

High-dimensional description promotes efficient recognition and matching, and supports key tasks such as image registration, stitching, recognition and 3D reconstruction. As shown in Eq. (11) and Eq. (12), These equations describe the characteristics of feature points, Fi is the description vector of the i-th feature point, which contains local information of the feature point, f is the eigenvalue. Ti is the extraction result of the I-th feature point, Extract is the extraction algorithm, and I is the image. Feature point matching is its core, ensuring accurate matching of similar points between images.

$$F_i = \begin{pmatrix} f_{i1} & f_{i2} & \cdots & f_{iN} \end{pmatrix} \tag{11}$$

$$T_i = Extract(I, x_i, y_i, s_i) \tag{12}$$

In the actual operation of feature point matching, how to improve the accuracy and speed of matching is one of the technical difficulties. At present, the popular matching method is to compare the feature points by using the trace of Hessian matrix and Euclidean distance similarity. As shown in Eq. (13), Correcti is the result of correcting the i-th feature point, Align() is the correction function, and Ref is the reference model, T is the time for updating. The Hessian matrix is a second derivative matrix, which can capture the curvature rate information in the image, thus helping to locate feature points more accurately.

$$Correct_i = Align(T_i, Ref) \tag{13}$$

By calculating the trace of the Hessian matrix, we can obtain the change information of the local area around the feature point, and the Euclidean distance is used to measure the similarity between the two feature points. As shown in Eq. (14), this equation highlights the importance of filtering feature points based on similarity metrics. Ffiltered is a filtered feature point, and FilterType is a filter type. When the Euclidean distance between two feature points is smaller, the higher the similarity between them, so it can be considered that the two feature points are matched.

$$F_{filtered} = Filter(F_i, FilterType) \tag{14}$$

This method, which combines the similarity of Hessian matrix and Euclidean distance, not only performs well in the matching accuracy of feature points, but also significantly improves the matching speed. As shown in Eq. (15) and Eq. (16), these equations quantify matching performance. Precisionmatch is the matching accuracy, TP is the true example, and FP is the false positive example. Stabilityfeature is the stability of the feature point, and Variance() is the Variance of the description vector. This is because Hessian matrix provides a more direct curvature information, which makes irrelevant feature points more quickly filtered out in the process of feature point matching, thus reducing the amount of calculation and improving the overall matching efficiency.

$$Precision_{match} = \frac{TP}{TP + FP} \tag{15}$$

$$Stability_{feature} = Variance(D_i) \tag{16}$$

III. Interactive System Under Multi-Source Data Fusion and Analysis Technology

A. AR-Based Interaction Design and Optimization

AR technology has become popular with the development of computers and multimedia, and its core lies in the integration of virtual and honest, which promotes the interaction between users' reality and virtual reality. Optimizing interaction design is the key. It is necessary to pay attention to user experience and pursue intuitive and natural interaction [19]. Natural behaviors such as postures, expressions, and voices have become a trend to manipulate virtual objects, which are more humane than touch screens and handles and enhance convenience and immersion. Using human postures and gestures to interact with virtual objects is one of the most natural and intuitive ways at present [20, 21]. In this interactive mode, it is first necessary to monitor the user's body position and movements in real-time through accurate tracking and registration technology. According to this information, the system will determine the user's position in three-dimensional space and judge his intention by analyzing his actions [22, 23]. According to the preset action definition, the system will associate the user's action with specific operation instructions to realize virtual object control. Optimizing interaction design is particularly critical to make this interaction mode easier for users [24, 25]. The movements are designed to be ergonomic, ensuring that users do not experience discomfort or fatigue while performing them. The association between actions and operations should have precise semantics so that users can intuitively understand and remember them. Users can zoom in or out of virtual objects through simple gestures or close virtual windows by waving their hands. These designs must be finely optimized based on user habits [26, 27]. Table I shows the results of interactive system response test data. Voice interaction is also a natural interaction method widely used in augmented reality.

TABLE I. Results of Interactive System Response Test Data

Test Items	Average time to detect and track new users	User gesture detection average time	Average time of initialization and correction of artwork interaction system	Average time to obtain artwork location
Test Results (ms)	0.62	3.38	276.78	26.58

Through speech recognition technology, the system can recognize the user's voice commands and convert them into operation commands, thus realizing the control of virtual objects. Voice interaction has the advantages of no touch and easy remote operation, and it is especially suitable for scenarios that require multitasking or when hands are inconvenient [28]. "Occlusion consistency" refers to the ability of an AR system to realistically handle the overlapping or covering of virtual and real-world objects. When a virtual object is placed in a scene, it must appear as though it interacts naturally with real-world objects, meaning that parts of the virtual object should be hidden or "occluded" by physical objects if they overlap in space. Maintaining occlusion consistency is critical for enhancing the realism of AR experiences. "Virtual objects" are computer-generated 3D models that are projected into the real-world environment through AR devices, such as headsets or mobile screens. These objects appear as though they exist within the physical space, and users can view and interact with them through the AR system. The seamless integration of virtual objects with the physical world is one of the defining characteristics of effective AR systems. "Feature points" are specific, easily recognizable points within a digital image or physical environment that are used by AR algorithms to map, track, and understand spatial relationships. Fig. 1 is the AR interaction design algorithm's principle and implementation flow chart. After passing the threshold screening, the system performs non-maximum suppression on each remaining feature point. This step ensures that the selected feature point is a prominent feature in its scale space. Fig. 1 demonstrates the AR interaction design algorithm's principle and the step-by-step implementation flowchart. This flowchart is essential as it outlines how the system processes real-time user interactions with virtual objects in an augmented reality environment. It emphasizes key steps, such as detecting and tracking the user's gestures, accurately registering virtual objects in the real world, and ensuring smooth interaction through algorithms that optimize real-time performance.

SURF-64 uses a 64-dimensional descriptor, which makes it faster but less detailed compared to SURF-128, which employs a 128-dimensional descriptor for capturing more information about feature points. In this research, these algorithms were implemented to detect and match distinctive feature points between real-world images and virtual elements. The system extracts feature from images of artwork or the exhibition space, and SURF is used to generate a set of keypoints, such as corners or edges, that are invariant to changes in scale, rotation, or lighting. These algorithms are integrated into the interactive exhibition system by first preprocessing the input data to detect feature points in real-time, followed by the matching of these feature points to align virtual objects with the physical environment. SURF-64 and SURF-128 are configured based on the exhibition's needs, where SURF-64 offers faster computation for real-time tracking, while SURF-128 provides more detailed feature matching when precision is critical. This means that the final position and scale value of feature points can be more accurate than the original pixel grid, thereby improving the accuracy and reliability of feature point matching. Fig. 2 is the architecture diagram of the multi-source data fusion algorithm. Accurate detection and matching of feature points is crucial to the performance of augmented reality systems. Fig. 2 focuses on the multi-source data fusion algorithm architecture, which is critical for integrating diverse data inputs from various sources, such as sensors, images, and spatial data, into a cohesive system.

B. *Feature Extraction of Artworks Based on Machine Learning*

Augmented reality requires realistic modeling of virtual objects, considering shape, material, light and shadow, and environmental interaction. The key challenges are lighting, occlusion consistency, and shadow casting. Lighting consistency is the most important. It is necessary to simulate natural lighting, adjust the lighting effect of virtual objects, and calculate actuarially based on scene geometry and reflection attributes to match natural light sources and enhance visual reality and immersion. Occlusion consistency is another crucial factor involving the mutual occlusion between virtual and natural objects. In the real world, the occlusion relationship between objects is essential for judging the spatial relationship. In augmented reality, virtual objects should have an occlusion relationship with natural objects as if they exist in the same space. Table II shows the test data of the augmented reality natural feature point tracking and registration module of the artwork interactive system. The system must accurately calculate the occlusion relationship between the virtual object and each object in the natural environment and render it in real-time. In this field, Bauhaus University in Germany took the lead in achieving the consistent effect of virtual and real occlusion, which made the occlusion effect of virtual scenes reach a highly realistic level. This technological breakthrough significantly improves the realism of augmented reality systems, allowing virtual objects to be more naturally integrated into actual scenes.

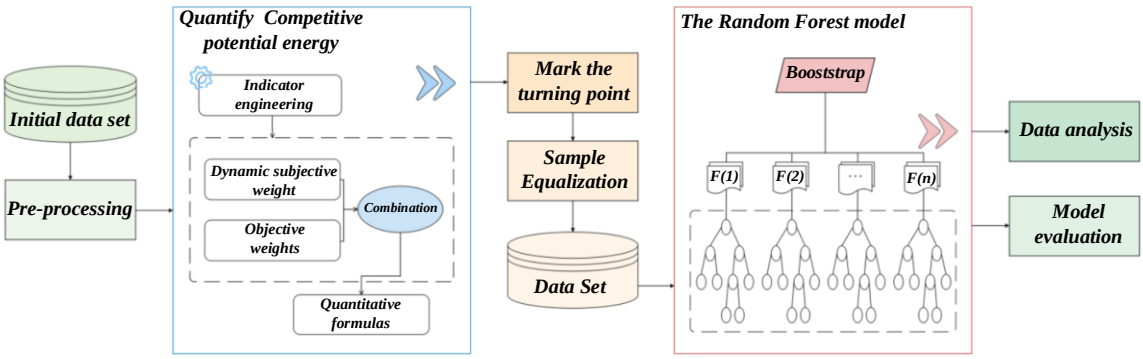


Fig. 1. Principle and implementation flowchart of AR interaction design algorithm.

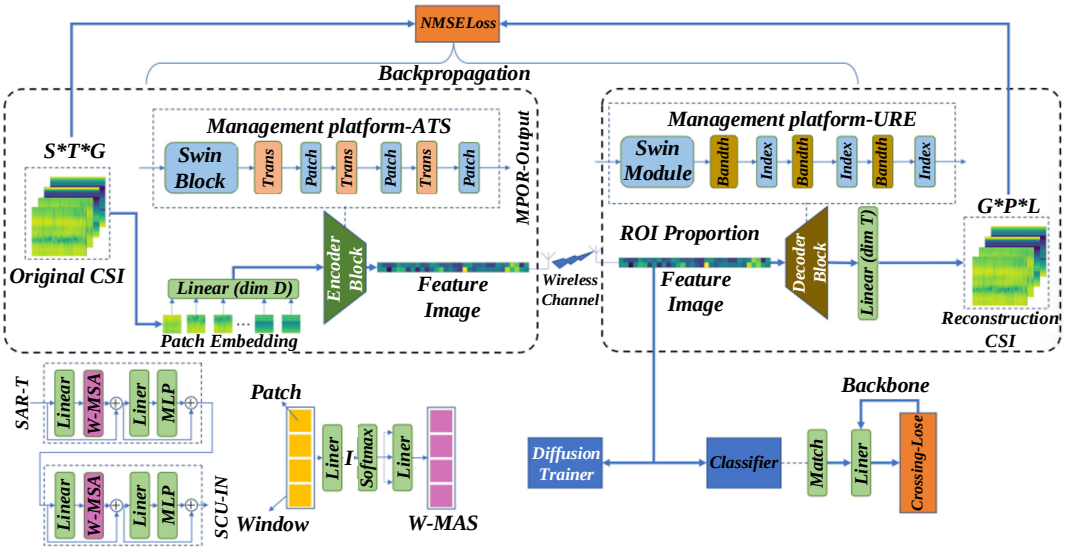


Fig. 2. Architecture diagram of multi-source data fusion algorithm.

TABLE II. TEST DATA OF AUGMENTED REALITY NATURAL FEATURE POINT TRACKING REGISTRATION MODULE OF ARTWORK INTERACTION SYSTEM

Test Items	Run Results
Number of feature points detected	65
Feature point detection time (ms)	75.37
Number of successful feature point matches	27
Number of successful tracking feature points	22
Tracking match time (ms)	13.14
Number of feature points detected after tracking failure	49
Feature point detection time (ms) after tracking failure	61.5

In augmented reality, to keep the shadow of the virtual object consistent with the direction and intensity of the light source in the actual scene, the system needs to accurately calculate the position and intensity of the light source and the geometry of the virtual object. In this way, the shadows of virtual objects can seamlessly blend with shadows in natural scenes, thus further enhancing the realism of augmented reality. Machine learning techniques have been widely used in augmented reality systems to achieve these complex effects. Through machine learning algorithms, the system can automatically learn illumination rules, occlusion relationships, and shadow projection rules from a large amount of accurate scene data, thereby generating more realistic visual effects in augmented reality. This reduces the workload of manual debugging and improves the system's automation level, making augmented reality technology more widely used in various scenarios. In augmented reality and computer vision, feature point extraction and matching are the keys to fusion. Fig. 3 is the application evaluation diagram of a multi-source data fusion algorithm in art information processing, with machine learning assistance, Fast-Hessian quick detection of feature points, and SURF completion description to ensure accuracy and stability. Fast-Hessian efficiently locates scales but lacks direction description; SURF makes up for this shortcoming and provides detailed feature data. The SURF descriptor uses Haar wavelet to extract the direction information of the feature points, thus realizing the rotation invariance of the feature points. In image processing, rotation invariance means that no matter how the image is rotated, the description information of feature points can still be consistent, thus ensuring the matching accuracy of feature points.

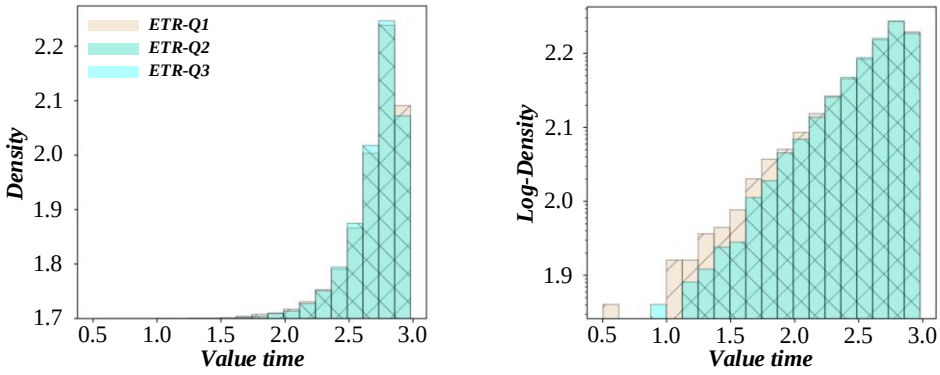


Fig. 3. Application evaluation diagram of multi-source data fusion algorithm in art information processing.

IV. Multi-Source Data Analysis and Analysis Design of Art Interactive Exhibition System Under Augmented Reality Technology

A. Implementation of Augmented Reality Technology in Art Exhibitions

Response time refers to the system's ability to register and process interactions in real-time, ensuring a seamless user experience. In an interactive exhibition, any noticeable lag or delay in responding to user inputs can disrupt the flow and diminish the immersive quality of the experience. Therefore, a faster response time is essential for maintaining engagement and enhancing the system's usability. Feature point detection is crucial for the accurate placement and movement of virtual objects in augmented reality. By increasing the number of detected feature points through algorithms like SURF-64 and SURF-128, the system ensures more precise tracking and overlay of virtual content, providing a more coherent integration of real and virtual elements. This is particularly important in art exhibitions where accuracy in object alignment can directly affect how well users perceive the interaction. User interaction accuracy measures how well the system interprets and responds to gestures, voice commands, or touch inputs, which is vital for creating an intuitive and engaging experience. If the system fails to accurately interpret user inputs, it could lead to frustration and disengagement. System stability ensures that the exhibition runs smoothly without crashes or significant performance degradation, which is critical in public settings. Immersive experience is an overall measure of user satisfaction and engagement, assessing how well the system integrates AR technology to create an engaging and interactive environment. Fig. 4 is an accuracy evaluation diagram of an art style recognition algorithm based on multi-source data analysis. This method has the advantages of high accuracy and fast recognition speed and is especially suitable for complex exhibition environments. Its limitation lies in the need to add additional signage in the exhibition venue, which may affect the aesthetics of the exhibits and the audience experience. Natural feature point tracking technology based on no identification is more flexible and natural.

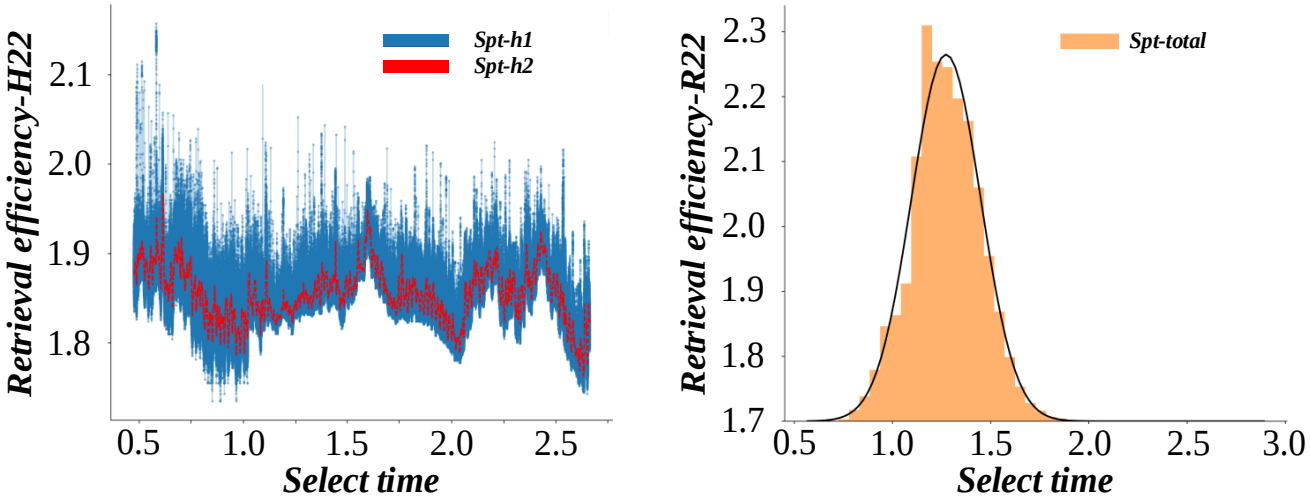


Fig. 4. Accuracy evaluation chart of art style recognition algorithm based on multi-source data analysis.

The application of augmented reality technology in art exhibitions can provide richer information display forms for the audience and enhance the interaction between the audience and the artworks through virtual guides and interactive experiences. When watching a famous painting, the audience can see the creative story behind the painting and the artist's life through augmented reality technology and even interact with virtual artists to gain an in-depth understanding of the connotation of the artwork. This novel exhibition method dramatically enhances the interest and sense of participation, making the audience a passive appreciator and a part of the exhibition. After the direction calculation, the SURF descriptor uses the integral graph to quickly calculate the rectangular area where the feature points are located. The advantage of the integral graph is that it can efficiently calculate the sum of pixels in any rectangular area in the image, which is widely used in fast image processing algorithms. In the feature extraction process of the SURF descriptor, the integral graph is used to define the region of interest, that is, the critical area near the feature points. Fig. 5 is an evaluation diagram of the audience behavior data analysis algorithm for exhibition route optimization. The SURF descriptor can generate detailed feature point description information by calculating the feature vector based on the Haar wavelet in this region of interest. This description information not only contains the location and direction of feature points but also includes rich data about the local structure of feature points, which is very important for the matching and subsequent processing of feature points.

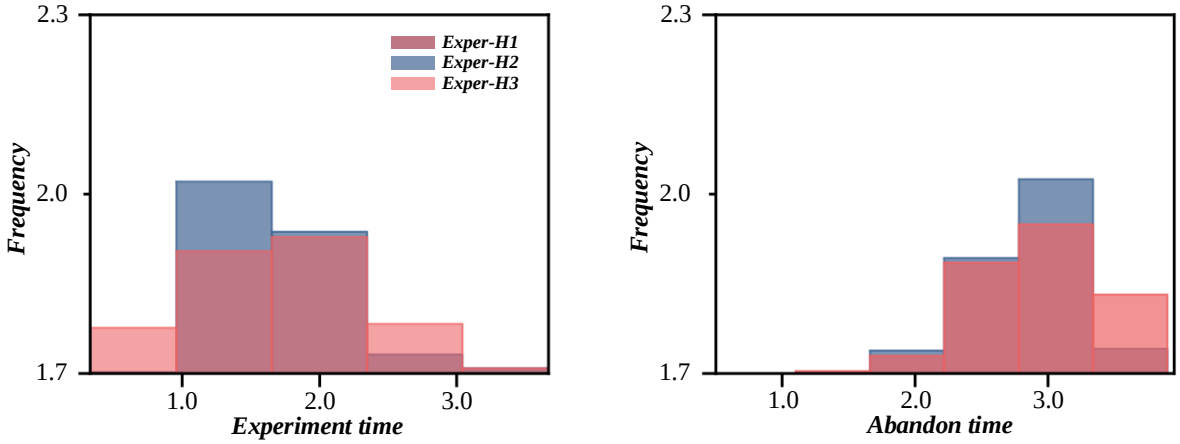


Fig. 5. Evaluation diagram of exhibition route optimization by audience behavior data analysis algorithm.

B. Architecture and Performance Evaluation of Art Interactive Exhibition System

In the interactive art exhibition system, feature point matching affects the overall performance. The SURF algorithm is efficient in recognition, but there are mismatches. Random Sample Consensus (RANSAC) algorithm improves the accuracy by random sampling to eliminate mismatches. First, the model parameters are determined, the samples are randomly selected to calculate the model, and the correct point set is screened according to the geometric distance. To improve the algorithm's accuracy, the RANSAC algorithm will randomly sample multiple times and find the most extensive set of consistent points. These point sets are divided into inner and outer points. This way, the algorithm can effectively screen out the matching points and determine the final model parameters. Finally, these maximum consistent point sets are used to re-estimate the model to output the optimal result. Fig. 6 is the evaluation diagram of the audience behavior data analysis algorithm for optimizing the exhibition route. The RANSAC algorithm shows high efficiency and stability when dealing with feature point matching. It can accurately identify and remove mismatched feature points in complex matching environments, improving the matching accuracy and robustness of the whole system.

The successful application of the RANSAC algorithm can significantly improve the performance of the interactive exhibition system of artworks, making the integration of virtual and reality more natural and realistic. In the architecture of an interactive exhibition system of artworks, accurately matching feature points is the key to realizing the perfect integration of virtual content and artworks. Using the RANSAC algorithm, the system can effectively reduce mismatches and ensure users' interactive experience in the exhibition is smoother and more realistic. Combined with other optimization techniques, such as image preprocessing, feature point enhancement, and multi-view fusion, the system's overall performance can be further improved. The architecture and performance evaluation of interactive art exhibition systems must comprehensively consider feature point detection, matching algorithms, and overall stability. As an efficient mismatch processing technology, the RANSAC algorithm provides strong support for accurate system matching. In the interactive exhibition system of artworks, the brightness of images concentrates on the details. Fig. 7 is an experimental data evaluation diagram of the AR interaction design algorithm to improve the audience's immersion. The histogram averages and stretches the gray distribution, enhances contrast, shows details, and helps subsequent processing, such as binarization. The basic principle of histogram averaging is to map the brightness histogram of the input image into a new histogram so that the brightness value distribution of the new histogram is more uniform.

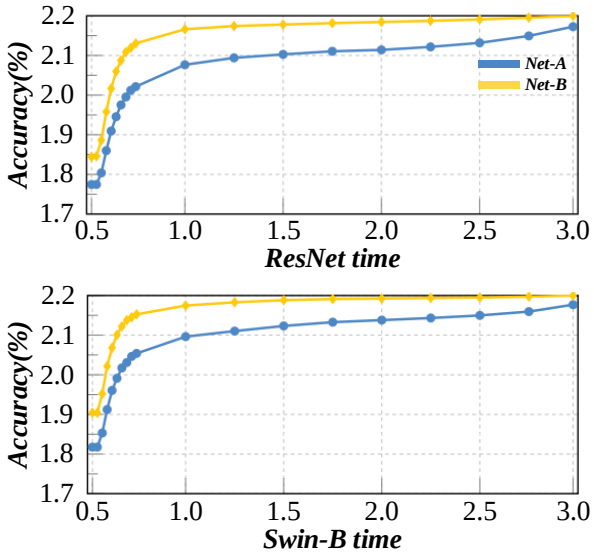


Fig. 6. Evaluation diagram of exhibition route optimization by audience behaviour data analysis algorithm.

Because of the uniformity of gray value distribution, the setting of the binarization threshold is more accurate in the image after the histogram means, thus improving the accuracy and effect of binarization. Histogram averaging often needs to be implemented in combination with specific mapping functions. These mapping functions are used to convert the original gray value of the image into a new gray value to enhance contrast and uniform distribution. Standard mapping functions include linear mapping and nonlinear mapping. By selecting

appropriate mapping functions, the effect of histogram averaging can be adjusted according to specific application requirements and image characteristics. Besides histogram averaging, other aspects of image processing, such as feature point extraction, matching algorithm, and image fusion, must be comprehensively considered to ensure the performance of the interactive exhibition system of works of art. By optimizing and improving these technologies, the system can achieve a more efficient and accurate artwork display and interactive experience. The performance evaluation of the system is also a critical link. Through the comprehensive review of the image processing effect, the stability and performance of the system can be continuously improved to meet the high requirements of users for art exhibitions. Fig. 8 is an evaluation diagram of the accuracy changes of the audience feedback prediction algorithm based on machine learning. Histogram averaging plays an essential role in the interactive exhibition system of artworks. It improves the contrast and detail performance of images and provides a reliable foundation for subsequent binarization processing.

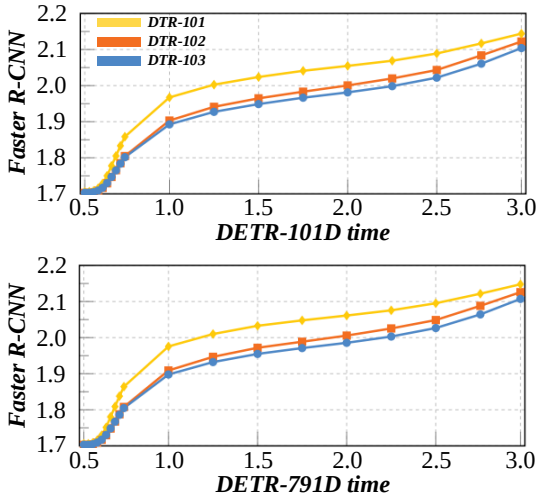


Fig. 7. Experimental data evaluation diagram of AR interaction design algorithm to improve audience immersion.

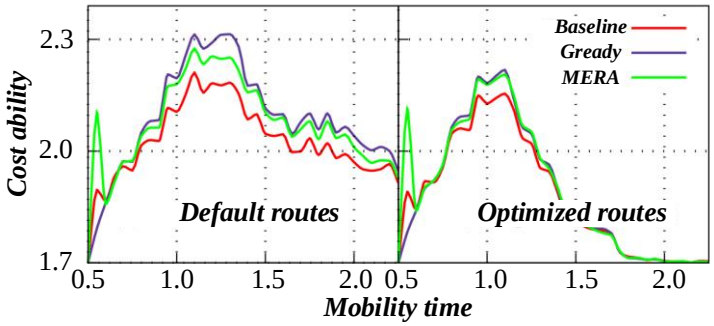


Fig. 8. Accuracy change evaluation diagram of audience feedback prediction algorithm based on machine learning.

V. Experimental Analysis

Finding and matching feature points is incredibly time-consuming when the target image is large. In this case, many feature points may increase the computational complexity and time consumption, which cannot meet the real-time requirements. Especially in real-time application scenarios, such as dynamic scenarios in augmented reality systems, fast processing, and response are required, so finding and matching many feature points may lead to system performance degradation. Fig. 9 is the evaluation diagram of the response time of the system performance evaluation algorithm on the interactive exhibition system of artworks. Although we may find many feature points in the target image, only some of them are feature points that need to be matched.

Some optimization strategies are usually employed. Using more accurate feature point detection algorithms improves the quality of feature points instead of just increasing the number. Through the feature point selection and screening algorithm, the feature points that have the most significant influence on the final calculation result are matched first, thus reducing the interference of irrelevant points. Fig. 10 is an application evaluation diagram of the security policy design algorithm in art data protection, especially in augmented reality systems. It is necessary to determine the quantity and quality of feature points according to specific needs to achieve the best system performance and user experience.

According to the size of the image, it needs to be cropped to reduce the processing amount and improve efficiency. Video dynamics require strategic cropping and efficient matching. The setting of the cropping area also needs to be adjusted according to the actual situation. If the motion in the image is too fast, it may cause the target object or feature point to move out of the cropped area. Fig. 11 is the evaluation diagram before and after improving the AR interactive interface based on the user interface design optimization algorithm. The system must re-detect the entire image to ensure that essential feature points are not missed. Although this scenario increases the computational burden, by clipping within this neighborhood according to the last detected feature point location, the system can reduce the size of the area to be looked up.

The system's performance can be further improved by optimizing the selection of cropping areas. The cropping area can be intelligently adjusted based on the movement trajectory of the target object and the known feature point position in the image, thereby reducing the frequency of re-detection and further improving processing efficiency. The strategy of cropping images significantly impacts the efficiency of augmented reality systems. By setting the cropping area reasonably and reducing the size of the image to be searched, the

speed of feature point extraction and matching can be effectively improved, thus improving the overall running efficiency of the system. Fig. 12 is the application efficiency evaluation diagram of feature extraction and matching algorithm in art image recognition. When dealing with dynamic scenes, it is necessary to consider the motion of target objects to ensure the accuracy and real-time performance of the feature point detection and matching process.

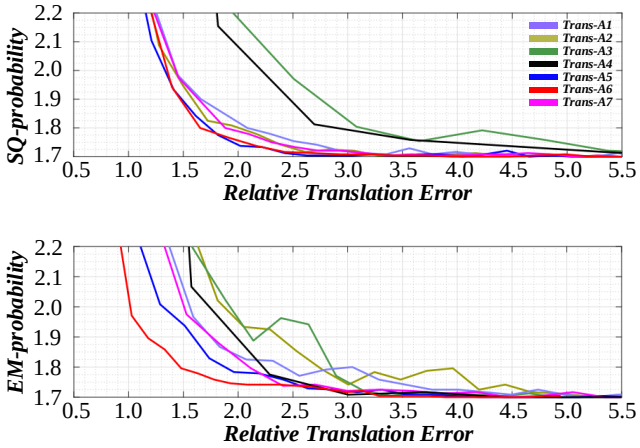


Fig. 9. Evaluation diagram of system performance evaluation algorithm on the response time of art interactive exhibition system.

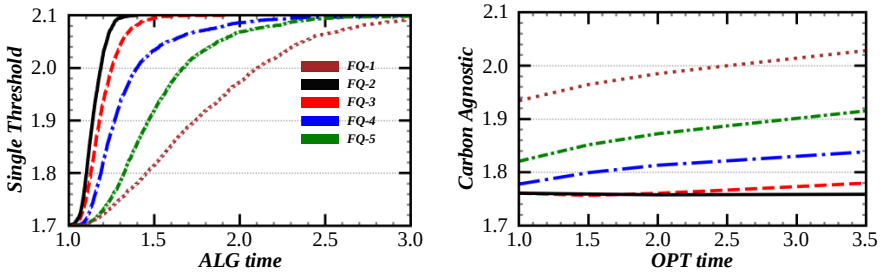


Fig. 10. Application evaluation diagram of security policy design algorithm in art data protection.

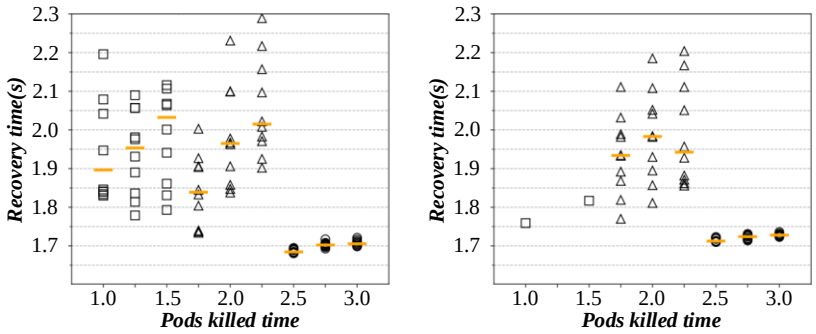


Fig. 11. Evaluation diagram before and after improvement of AR interactive interface based on user interface design optimization algorithm.

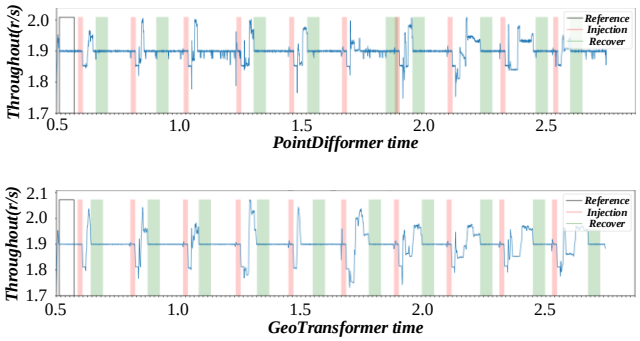


Fig. 12. Application efficiency evaluation diagram of feature extraction and matching algorithm in art image recognition.

VI. CONCLUSION

This paper focuses on the application of computer vision and augmented reality technologies in artwork interaction systems, where feature point extraction and matching, as a key step in image recognition, significantly improves the accuracy of recognition. Although multi-feature point extraction can increase the accuracy, it is not always necessary because too many feature points may instead lead to a heavier processing burden on the system. In AR applications, feature points not only assist in calculating transformations between images, such as the solution of a single response matrix requires at least four matching points, but increasing the number of feature points does not always bring additional benefits, but may instead increase computational complexity and resource consumption.AR technology, with its powerful interactivity and integration of multi-sensory experiences such as visual and auditory sensations, is gradually revolutionizing the way art is viewed.

In this paper, the consistency of occlusion illumination in virtual object interaction is essential for experience, but the research needs to be stronger and needs a breakthrough in the future. The study focuses on the analysis and prediction of Internet multi-source data characteristics, efficiently integrates data to predict realistic indicators, such as the number of interactive systems of artworks, and verifies it in predicting tourist volume, showing the potential of wide application of the model. One key area for future research is enhancing the precision and responsiveness of the AR system, particularly in terms of improving the real-time interaction between virtual and real-world objects. This could involve exploring more advanced algorithms for feature extraction, tracking, and data fusion, ensuring a seamless integration of virtual objects into the physical exhibition space. Another area worth exploring is optimizing the system's performance under various environmental conditions, such as changes in lighting, user movement, or large crowds. While the current model focuses on integrating multi-source data, future research could investigate how to make the system more adaptable and resilient in these dynamic settings, enhancing its robustness and versatility in different exhibition environments.

This paper studies the multi-source data collection and feature analysis of the Internet. It takes the art interaction system as an example to design a scheme to screen relevant data effectively. Aiming to solve the problem of data clutter, comprehensive index optimization is calculated by keyword screening and calculation. The number of mismatches for SURF-64 is 49 at threshold 500 and 22 at threshold 1000, 11, and 7 for SURF-128 under the same conditions, respectively. This shows that a higher threshold and a more significant dimension can help reduce the number of false matches and improve the matching accuracy.

REFERENCES

[1] A. Apicella et al., "Enhancement of SSVEPs Classification in BCI-Based Wearable Instrumentation Through Machine Learning Techniques," Ieee Sensors Journal, vol. 22, no. 9, pp. 9087-9094, 2022.

[2] S. Blanco-Pons, B. Carrión-Ruiz, and J. L. Lerma, "Augmented reality application assessment for disseminating rock art," Multimedia Tools and Applications, vol. 78, no. 8, pp. 10265-10286, 2019.

[3] M. W. Cao, L. P. Zheng, W. Jia, and X. P. Liu, "Real-time video stabilization via camera path correction and its applications to augmented reality on edge devices," Computer Communications, vol. 158, pp. 104-115, 2020.

[4] L. F. D. Cardoso, B. Y. L. Kimura, and E. R. Zorzal, "Towards augmented and mixed reality on future mobile networks," Multimedia Tools and Applications, vol. 83, no. 3, pp. 9067-9102, 2024.

[5] G. D. Costa, M. R. Petry, and A. P. Moreira, "Augmented Reality for Human-Robot Collaboration and Cooperation in Industrial Applications: A Systematic Literature Review," Sensors, vol. 22, no. 7, pp. 52, 2022.

[6] N. Didar and M. Brocanelli, "eAR: An Edge-Assisted and Energy-Efficient Mobile Augmented Reality Framework," Ieee Transactions on Mobile Computing, vol. 22, no. 7, pp. 3898-3909, 2023.

[7] N. Elazab et al., "Overlapping Shadow Rendering for Outdoor Augmented Reality," Cmc-Computers Materials & Continua, vol. 67, no. 2, pp. 1915-1932, 2021.

[8] M. Eswaran, A. K. Gulivindala, A. K. Inkulu, and M. Bahubalendruni, "Augmented reality-based guidance in product assembly and maintenance/repair perspective: A state-of-the-art review on challenges and opportunities," Expert Systems with Applications, vol. 213, pp. 18, 2023.

[9] M. Hincapie, C. Diaz, A. Valencia, M. Contero, and D. Güemes-Castorena, "Educational applications of augmented reality: A bibliometric study," Computers & Electrical Engineering, vol. 93, pp. 11, 2021.

[10] J. Husár and L. Knapcíková, "Implementation of Augmented Reality in Smart Engineering Manufacturing: Literature Review," Mobile Networks & Applications, vol., pp. 14, 2023.

[11] J. Izquierdo-Domenech, J. Linares-Pellicer, and J. Orta-Lopez, "Towards achieving a high degree of situational awareness and multimodal interaction with AR and semantic AI in industrial applications," Multimedia Tools and Applications, vol. 82, no. 10, pp. 15875-15901, 2023.

[12] F. Z. Kaghat, A. Azough, M. Fakhour, and M. Meknassi, "A new audio augmented reality interaction and adaptation model for museum visits," Computers & Electrical Engineering, vol. 84, pp. 13, 2020.

[13] S. Kapp, M. Barz, S. Mukhametov, D. Sonntag, and J. Kuhn, "ARETT: Augmented Reality Eye Tracking Toolkit for Head Mounted Displays," Sensors, vol. 21, no. 6, pp. 18, 2021.

[14] C. Kim et al., "Fine metal mask material and manufacturing process for high-resolution active-matrix organic light-emitting diode displays," Journal of the Society for Information Display, vol. 28, no. 8, pp. 668-679, 2020.

[15] L. H. Lee, T. Braud, K. Y. Lam, Y. P. Yau, and P. Hui, "From seen to unseen: Designing keyboard-less interfaces for text entry on the constrained screen real estate of Augmented Reality headsets," Pervasive and Mobile Computing, vol. 64, pp. 16, 2020.

[16] D. G. Morín, P. Pérez, and A. G. Armada, "Toward the Distributed Implementation of Immersive Augmented Reality Architectures on 5G Networks," Ieee Communications Magazine, vol. 60, no. 2, pp. 46-52, 2022.

[17] L. Nijs and B. Behzadaval, "Laying the Foundation for Augmented Reality in Music Education," Ieee Access, vol. 12, pp. 100628-100645, 2024.

[18] F. G. Prattico, F. Lamberti, A. Cannavò, L. Morra, and P. Montuschi, "Comparing State-of-the-Art and Emerging Augmented Reality Interfaces for Autonomous Vehicle-to-Pedestrian Communication," Ieee Transactions on Vehicular Technology, vol. 70, no. 2, pp. 1157-1168, 2021.

[19] X. Q. Qiao, P. Ren, S. Dustdar, L. Liu, H. D. Ma, and J. L. Chen, "Web AR: A Promising Future for Mobile Augmented Reality-State of the Art, Challenges, and Insights," Proceedings of the Ieee, vol. 107, no. 4, pp. 651-666, 2019.

[20] S. P. Ramu, G. Srivastava, R. Chengoden, N. Victor, P. K. R. Maddikunta, and T. R. Gadekallu, "The Metaverse for Cognitive Health: A Paradigm Shift," Ieee Consumer Electronics Magazine, vol. 13, no. 3, pp. 73-79, 2024.

[21] S. Schez-Sobrino et al., "A modern approach to supporting program visualization: from a 2D notation to 3D representations using augmented

reality," Multimedia Tools and Applications, vol. 80, no. 1, pp. 543-574, 2021.

[22] J. Seetohul, M. Shafiee, and K. Sirlantzis, "Augmented Reality (AR) for Surgical Robotic and Autonomous Systems: State of the Art, Challenges, and Solutions," Sensors, vol. 23, no. 13, pp. 37, 2023.

[23] S. K. Song, "Research on Public Art Parameterization of Interactive Installation Based on Sensor and Virtual Reality," Mobile Information Systems, vol. 2021, pp. 11, 2021.

[24] F. L. Tang, Y. H. Wu, X. H. Hou, and H. B. Ling, "3D Mapping and 6D Pose Computation for Real Time Augmented Reality on Cylindrical Objects," Ieee Transactions on Circuits and Systems for Video Technology, vol. 30, no. 9, pp. 2887-2899, 2020.

[25] A. Toma, S. Samara, and M. Qamhieh, "Edge Computing Systems: Modeling and Resource Optimization for Augmented Reality and Soft Real-time Applications," Journal of Network and Systems Management, vol. 31, no. 4, pp. 24, 2023.

[26] S. Uzor and P. O. Kristensson, "An Exploration of Freehand Crossing Selection in Head-Mounted Augmented Reality," Acm Transactions on Computer-Human Interaction, vol. 28, no. 5, pp. 27, 2021.

[27] M. T. Vega et al., "Immersive Interconnected Virtual and Augmented Reality: A 5G and IoT Perspective," Journal of Network and Systems Management, vol. 28, no. 4, pp. 796-826, 2020.

[28] M. Wedyan, J. Falah, O. Elshaweesh, S. F. M. Alfalah, and M. Alazab, "Augmented Reality-Based English Language Learning: Importance and State of the Art," Electronics, vol. 11, no. 17, pp. 17, 2022.

Optimization of Carbon Dioxide Dense Phase Injection Model Based on DBN Deep Learning Algorithm

Juan Zhou[1], Dalong Wang[2], Tieya Jing[3]*, Zhiwen Liu[4], Yihe Liang[5], Yaowu Nie[6]
National Key Laboratory of High-Efficiency Flexible Coal Power Generation and Carbon Capture Utilization and Storage, Huaneng Clean Energy Research Institute, Beijing 102209, China[1, 3]
Huaneng Qing Yang Coal and Electricity Co. Ltd., Qingyang 745000, China[2, 4, 5, 6]

***Abstract*—Carbon dioxide dense phase injection images have providing new research ideas for differential detection. Aiming at the drawbacks of large data volume, low matching efficiency, and longtime consumption of high-resolution carbon dioxide dense phase injection models, a registration algorithm for carbon dioxide dense phase injection models based on quadratic matching is proposed. This algorithm first uses down sampling to reduce image dimensions. A difference detection algorithm based on weakly supervised deep confidence network is proposed to neural networks, as well as the high manual labeling workload, low efficiency, and insufficient labeled data of high-resolution carbon dioxide dense phase injection models. This article first explores the throttling of CO2 venting in pipelines through the analysis of CO2 phase equilibrium characteristics. The experiment shows that there is after the valve, the greater the temperature drop. At the same time, water content will affect the throttling temperature drop is about 1.5 degrees; when the gas-liquid ratio is 2500, the throttling temperature drop is 7.4 degrees. CO2 in the reactor to over 8MPa, achieving supercritical pressure. CO2 with the constant temperature water bath is 5~100 degrees, with a temperature control accuracy of ± 0.1 degrees. The temperature of the water inside the water bath jacket of the kettle is adjusted through circulation. The maximum pressure of the kettle is 25MPa and the volume is 6L.**

Keywords*—Supercritical CO2; DBN deep learning algorithm; throttling characteristics; security control; dense phase injection model

I. INTRODUCTION

According to engineering experience in transporting CO2 through pipelines, the transportation of CO2 in supercritical conditions is the most economical. When transporting supercritical CO2 through pipelines, pipeline safety issues cannot be ignored [1, 2]. The Introduction section will outline the significance of CO2 injection in carbon capture and storage (CCS) and discuss existing challenges such as flow dynamics, phase transitions, and system safety. In the DBN Deep Learning Algorithm section, the structure and functioning of the Deep Belief Network (DBN) will be explained, highlighting how it can automatically extract features from high-dimensional data and optimize CO2 injection models. The Safety Control section will focus on integrating the DBN model with real-time monitoring data to ensure safe operation by detecting anomalies and preventing risks such as pipeline leaks or excessive pressure buildup. Although there have been no large-scale human casualties caused by CO2 pipeline leaks worldwide so far, due to the current fact that there are only 6000km of CO2 pipelines worldwide, which is less than 1% of the total mileage of oil, natural gas, and other hazardous materials pipelines, with the vigorous development of CCS technology, the mileage of CO2 pipelines will significantly increase, and the accompanying operational risks of pipelines will also sharply increase [3, 4]. Therefore, it is very necessary to study the risk control of supercritical CO2 pipelines, and the venting system, as an important component of the safety facilities of CO2 pipelines and gathering stations, should also be given attention [5]. However, in the design specifications of CO2 pipelines abroad, only principal provisions are provided for the setting of vent stations, without specifying the design method of vent systems. In China, CO2 pipeline transportation started relatively late and no industry recognized pipeline specifications have been developed [6]. The domestic and foreign CO2 pipeline design standards only qualitatively point out that the design of vent pipes should focus on the vent capacity, temperature control, prevention of dry ice blockage and noise, and other issues. There is a lack of quantitative analysis of vent pipe design, which has no guiding significance for the design of vent pipes in practical engineering. Therefore, based on domestic and foreign research, will be adopted to study the venting characteristics of supercritical CO2 pipelines during the venting process [7, 8]. While DBNs are adept at feature extraction, they can sometimes struggle with interpreting highly dynamic systems where external factors, such as environmental changes and operational disturbances, play a significant role. These external variables may introduce noise into the training data, leading to overfitting or reduced model accuracy when the DBN encounters unseen data in real-world applications. Furthermore, the black-box nature of deep learning models, including DBNs, poses challenges in understanding and interpreting the model's decisions. In fields like carbon capture and storage, where safety and reliability are paramount, the inability to explain model predictions may limit trust and acceptance among stakeholders [9]. Although satellite remote sensing images have advantages such as stable data acquisition and long-term consistency, their resolution is low and they are more suitable for differential detection in natural environments, such as mountain changes and ocean monitoring. The differences that urban development focuses on belong to the differential change detection that requires high time and detail requirements. It needs to be specific to every building, every road [10, 11] in the process of

*Corresponding Author.

change, so higher resolution images are needed. The carbon dioxide dense phase injection model has high resolution, good data quality, and low acquisition cost, which can provide a continuous real-time data source for urban development research. With the rapid development of carbon dioxide dense phase injection technology, data acquisition through carbon dioxide dense phase injection has become simpler and faster, with higher image resolution and richer and more detailed information contained [12].

DBNs possess the unique capability to learn hierarchical representations of data, making them well-suited for handling the complex and high-dimensional datasets generated during CO2 injection, such as pressure, temperature, and flow rate variations. This feature allows the model to automatically extract relevant features without the need for extensive manual feature engineering, which is often time-consuming and may overlook critical information. Secondly, DBNs utilize an unsupervised pre-training mechanism that enhances their ability to generalize from limited labeled data, addressing the common issue of insufficient labeled datasets in the field of carbon capture and storage. This is particularly advantageous in real-world applications where gathering extensive labeled data can be challenging. Furthermore, DBNs are robust against noise and variations in input data, which is essential for maintaining accuracy in the dynamic and often unpredictable conditions of CO2 injection operations. Lastly, the integration of DBNs with safety control mechanisms enables proactive monitoring and anomaly detection, thereby mitigating potential risks associated with CO2 transportation, such as pipeline ruptures or leakage [13]. Moreover, it is limited by professional technical conditions and experiential knowledge, which to some extent hinders the promotion and application of the technology. Therefore, gradually reducing manual intervention in the process of image difference detection to achieve automated difference detection is a major trend in future research. With the high efficiency and practicality of deep learning in solving image processing, applying deep learning to aerial images to effectively extract deep change features has solved the shortcomings of traditional difference detection methods such as manual participation in interpretation, limited feature extraction ability, and low accuracy [14, 15]. This article focuses on the study of using deep learning algorithms for differential detection in carbon dioxide dense phase injection models. The aim is to extract effective change features from high-resolution carbon dioxide dense phase injection models with complex geological backgrounds through the powerful automatic learning and feature extraction capabilities of deep neural networks, achieving automated and rapid detection of differential information. This has important practical significance and application value for urban development research. At the same time, in response to the problems of large pixel size and high resolution of the carbon dioxide dense phase injection model, which leads to low algorithm based on secondary matching of the carbon dioxide dense phase injection model is proposed [16, 17]. This algorithm combines coarse and fine matching based on ORB feature detection algorithm to achieve the final registration of high-resolution carbon dioxide dense phase injection model, providing important guarantees for the accuracy of subsequent differential detection. Differential detection based on image transformation is the process of analyzing images mapped to a new feature space to obtain change information. Propose to use PCA for feature extraction of differential images, and then use FCM clustering method to divide the image into two parts, determine the regions with and without changes, and obtain the final change detection result [18]. Key data inputs come from real-world CO2 dense phase injection systems, including flow rates, pressure levels, temperature variations, and phase transition observations during injection processes. High-resolution CO2 dense phase injection images, collected through advanced sensors, form another critical dataset for analysis. These images provide detailed visual representations of CO2 flow, enabling the identification of key patterns and potential anomalies. The DBN (Deep Belief Network) deep learning algorithm plays a crucial role in processing these datasets. Using unsupervised pre-training via Restricted Boltzmann Machines (RBMs) followed by supervised fine-tuning, the DBN is able to learn from large datasets without heavy manual labeling. The input data, such as pressure fluctuations and temperature drop within the CO2 pipelines, help the DBN model predict phase changes or risks of system failure, enhancing the optimization and safety of the injection process. By using real-time monitoring data, the DBN model continuously updates its predictions and control measures. [19].

II. Research on the Venting Law of CO2 Pipeline Stations

A. Establishment of Venting Model

Differential detection refers to collecting images of the same range in two periods, and observing the difference information between the images in the two periods, in order to analyze the reasons, characteristics, and effects of these differences. As shown in Eq. (1) and Eq. (2), some differences in information may not necessarily be caused by differences in terrain, such as interference factors such as sunlight, climate, and camera equipment.

$$Q(i,j)=\begin{cases}0, I1(i,j)=I2(i,j)\\ 1, I1(i,j)=I2(i,j)\end{cases} \tag{1}$$

$$PCC=\frac{TP+TN}{TP+TN+FN+FP} \tag{2}$$

Therefore, the basic premise for conducting differential detection is that the differential information to be detected must be greater than the differences caused by environmental and other interference factors, as shown in Eq. (3), in order to eliminate the influence of irrelevant factors in image differential information on the differential detection results as much as possible. Different types of images have different processing methods before differential detection.

$$Kappa=\frac{PCC-PRE}{1-PRE} \tag{3}$$

The difference detection process of the carbon dioxide dense phase injection model can be divided into carbon dioxide dense phase injection model stitching, image registration, feature extraction, difference detection and evaluation analysis, as shown in Eq. (4). The images collected by carbon dioxide dense

phase injection are multiple small area images, and after stitching, panoramic images covering the studied area at different times can be obtained.

$$Jaccard = \frac{TP}{FP + FN + TP} \tag{4}$$

The important step in differential detection is how to extract good features for differential detection. As shown in Eq. (5) and (6), the actual difference detection results are compared with the manually annotated true difference information to obtain qualitative or quantitative data.

$$D(x,y,\sigma) = \left(G(x,y,k\sigma) - G(x,y,\sigma)\right) * I(x,y) \tag{5}$$

$$L(x,y,\sigma) = G(x,y,\sigma) * I(x,y) \tag{6}$$

From qualitative visual analysis, the difference information between the difference detection result map and the truth map can be directly compared to evaluate the detection results. At each candidate position, as shown in Eq. (7) and Eq. (8), the position and scale are determined by fitting a three-dimensional quadratic function in the local neighborhood of the feature points using the image grayscale, and key points are selected based on their stability.

$$m(x,y) = \sqrt{\left(L(x+1,y) - L(x-1,y)\right)^2 + \left(L(x,y+1) - L(x,y-1)\right)^2} \tag{7}$$

$$\theta(x,y) = arctan\frac{L(x+1,y) - L(x-1,y)}{L(x+1,y) - L(x-1,y)} \tag{8}$$

Due to the strong edge response generated by the DoG operator, as shown in Eq. (9) and Eq. (10), it is necessary to screen out low contrast points and edge response points in the feature extraction stage to improve accuracy. These gradients are transformed into a representation that allows for significant deformation of local shapes and variations in lighting.

$$L(x_i, x_j) = \left(\sum_{l=1}^{2} \left|x_i^{(l)} - x_j^{(l)}\right|^2\right)^{\frac{1}{2}} = \sqrt{\left|x_i^{(1)} - x_j^{(1)}\right|^2 + \left|x_i^{(2)} - x_j^{(2)}\right|^2} \tag{9}$$

$$x' = \frac{h_{11}u + h_{21}v + h_{31}}{h_{13}u + h_{23}v + h_{33}} \tag{10}$$

B. Dense Phase Injection Model

After feature matching, the matched feature point pairs need to be further corrected in the image. Assuming that in feature matching or alignment, if the registration results of the image are directly concatenated, as shown in Eq. (11) and Eq. (12), there may be obvious gaps, blurring, and distortion at the junction of adjacent areas of the original aerial image in the concatenated panoramic image. Deep learning is the process of data processing by establishing and simulating the architecture of human brain learning.

$$f(x,y) = \frac{f_1(x,y) + f_2(x,y)}{2} \tag{11}$$

$$f(x,y) = \omega_1 f_1(x,y) + \omega_2 f_2(x,y) \tag{12}$$

Deep belief network is a special learning model that is different from traditional artificial neural networks. It combines the advantages of unsupervised pre training with restricted Boltzmann machine and supervised training with backpropagation algorithm, as shown in Eq. (13). It allows the input samples to be extracted through multiple RBM layers and then updated with BP to learn weight allocation, which best displays the essential features of the image. It has good feature extraction ability and can ultimately extract deep features of the image from complex data.

$$\frac{\partial J}{\partial W_{ij}^l} = \frac{\partial J}{\partial a_i^l}\frac{\partial a_i^l}{\partial s_i^l}\frac{\partial s_i^l}{\partial W_{ij}^l} = \frac{\partial J}{\partial a_i^l} f'\left(s_i^l\right) a_j^{l-1} \tag{13}$$

Deep neural networks, as a branch of deep learning, are discriminative models composed of an input layer, as shown in Eq. (14), multiple hidden layers, and an output layer. Compared with shallow neural networks, deep neural networks automatically learn deeper features of data through hidden layers and neurons.

$$\frac{\partial J}{\partial b_i^l} = \frac{\partial J}{\partial a_i^l}\frac{\partial a_i^l}{\partial s_i^l}\frac{\partial s_i^l}{\partial b_i^l} = \frac{\partial J}{\partial a_i^l} f'\left(s_i^l\right) \tag{14}$$

As the complexity of data samples intensifies, the number of hidden layers and neurons can be increased. Through structural mapping between layers, the sample features in the original space can be mapped to a new feature space, as shown in Eq. (15) and Eq. (16), and abstract composite features can be performed at higher levels to improve the detection performance of complex data.

$$\frac{\partial J}{\partial W_{ij}^l} = \frac{\partial J}{\partial s_i^l} a_j^{l-1} \tag{15}$$

$$\delta s^l = \left(W^{l+1}\right)^T \delta s^{l+1} * f'\left(s^l\right) \tag{16}$$

The training process of deep learning models can be trained using the BP algorithm. The so-called training of neural networks refers to allowing machines to correct multiple parameters in the neural network, such as layer to layer connection weights and biases, by continuously learning the true difference information manually annotated. As shown in Eq. (17) and Eq. (18), the construction of network structures often originates from practical problems, and determining parameters requires continuous iteration to reduce the cost function in order to seek the optimal combination of network parameters. This method improves training efficiency and effectively solves the problem of local optima. Compared to traditional neural networks, RBM has no output layer and only includes visible and hidden layers, as shown in Eq. (19) and Eq. (20), while the hidden layer serves as a feature detector for extracting and learning features from the data.

$$\delta s^l = \delta A^l * f'\left(s^l\right) = \left(W^{l+1}\right)^T \delta s^{l+1} * f'\left(s^l\right) \tag{17}$$

$$\delta W^l = \frac{\partial J}{\partial W^l} = \frac{1}{m}\delta Z^l * \left(A^{l-1}\right)^T \tag{18}$$

$$N = \sum_{x \forall (circle(p))} \left| I(x) - I(p) \right| > \varepsilon_d \tag{19}$$

$$m_{pq} = \sum_{xy} x^p y^q I(x,y) \tag{20}$$

III. Differential Detection of CO2 Dense Phase Injection Model Based on Deep Confidence Networks

A. Deep Learning Theory

The training of RBM is similar to forward training, keeping the weight coefficient w of forward training unchanged [20]. At this time, the hidden layer is used as the new input for reconstruction training. The neurons of each hidden layer are multiplied by the weight, stacked, and then biased to obtain the reconstructed output, completing one reconstruction training. The reconstruction error will continuously decrease with the iterative training process of RBM until the error reaches its minimum value, and the parameter weights and biases are also updated [21, 22]. From this, it can be seen that the training process of RBM networks does not require manual annotation of data for supervision and guidance, and can learn advanced features of the original data. Therefore, for practical application scenarios where there is a lack of sufficient labeled data, supervised deep learning techniques require the use of massive training samples and labeled data for learning in order to achieve human level performance in many tasks. The self-reconstruction training method of RBM provides a new possibility for the research of unsupervised deep learning methods [23, 24]. The ORB algorithm is divided into two parts, feature point extraction and feature point description. Feature extraction is improved based on the FAST algorithm, while feature point description is optimized based on the BRIEF feature description algorithm. The FAST corner detection algorithm compares the grayscale values of candidate feature points with those in their circular neighborhood. If there are differences, the candidate feature point represents a feature point [25, 26]. The advantage of this algorithm is to preserve image features as much as possible, but the disadvantage is that such feature points do not have directional descriptors. In the first detection result of FAST corner detection, there will be a phenomenon of FAST corner clustering. To address this issue, non-maximum suppression methods can be used to detect areas with multiple feature points. Fig. 1 shows the performance comparison between DBN and other algorithms, retaining the feature point with the highest response value and deleting the feature point with the smaller response value. Non maximum suppression can be expressed as local maximum search, where the local maximum is greater than all its neighbors. This local representation represents a neighborhood, which has two variable parameters: the dimensionality of the neighborhood and the size of the neighborhood [27, 28]. Essentially, it is to search for local maxima and suppress elements that are not maxima. Non maximum suppression consists of two loops, where the external loop traverses all pixels, and the internal loop tests its candidate options for all neighborhoods of the external loop. Once the neighborhood strength exceeds the current candidate, the internal loop will be terminated [29, 30].

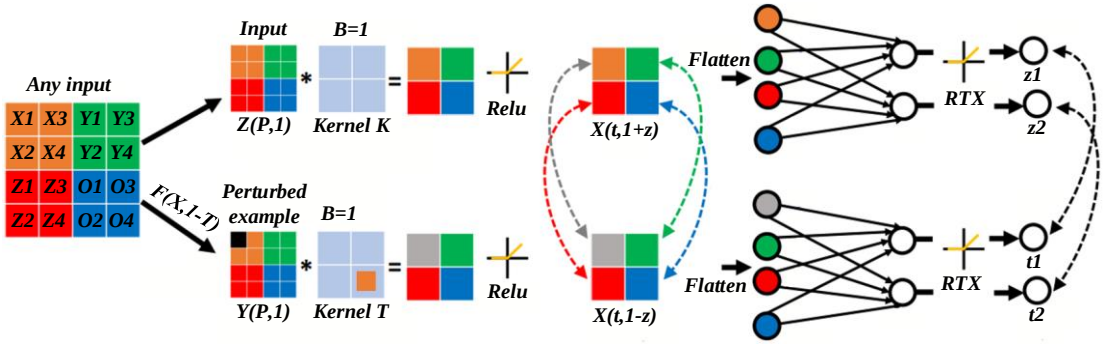


Fig. 1. Performance comparison between DBN and other algorithms.

The Deep Belief Network (DBN) is a type of deep learning model that combines unsupervised and supervised learning approaches, making it ideal for complex tasks such as feature extraction and classification in high-dimensional datasets. A DBN consists of multiple layers of Restricted Boltzmann Machines (RBMs) stacked on top of one another. Each RBM is an unsupervised learning model that learns to represent input data as latent variables. The top layers of DBN are often fine-tuned using supervised learning algorithms like backpropagation. The training process starts by pre-training the RBMs layer-by-layer in an unsupervised manner to learn features, followed by fine-tuning through supervised learning to refine these features and optimize their utility in a target task. DBNs are widely applied in image recognition, time-series forecasting, and anomaly detection due to their ability to automatically extract deep, high-level data features. In the context of carbon dioxide dense phase injection, the DBN algorithm can play a critical role in modeling and optimizing the injection process. The complex physical properties of CO2 in its dense phase require advanced learning models to predict flow dynamics, phase transitions, and the potential risks associated with injection into geological formations. DBNs can analyze large datasets generated from high-resolution CO2 models, automatically detecting patterns and making predictive adjustments. Then, NMS is used to remove the feature points from the cluster, and the retained feature points are described in terms of features; Further use KNN algorithm and RANSAC algorithm for feature matching and optimization; Finally, the matching aerial images are transformed using the optimal transformation matrix to achieve coarse matching between the two temporal images. Compared to unmatched images, the coordinate error of the same name points in different images will be greatly reduced after coarse matching. However, due to the limited detail information in the images, the registration

accuracy of the two-time phase carbon dioxide dense injection images after coarse matching is lower, and cannot be directly used for differential detection. Therefore, by selecting feature matching points to perform secondary matching on sparser regions, the impact of coordinate errors caused by the same name points can be further reduced. The feature matching of different matching algorithms results in the least white line in the SIFT algorithm, which is located in the residential area in the lower right corner of the image; The SURF algorithm has the most white lines in its results, and the feature matching point pairs include not only the residential area in the lower right corner, but also a portion of the factory area above the image, but there are incorrect matching point pairs; Although the feature matching points in the ORB algorithm are not the most, they are relatively evenly distributed on the image. Fig. 2 shows the relationship between model prediction accuracy and training rounds, and there are no incorrect matching point pairs. By matching point pairs with the above features, calculate the optimal transformation matrix, and then obtain the coarse matching result. Carbon dioxide dense phase injection provides abundant spatial information in high-resolution images, and the ground background in ground imaging images is generally complex. Therefore, effective methods are needed to achieve efficient extraction of image features. Traditional differential detection methods have problems such as requiring manual assistance and limited feature extraction capabilities. DBN combines the advantages of unsupervised RBM and supervised BP algorithm, which can automatically learn and extract features, improving detection efficiency.

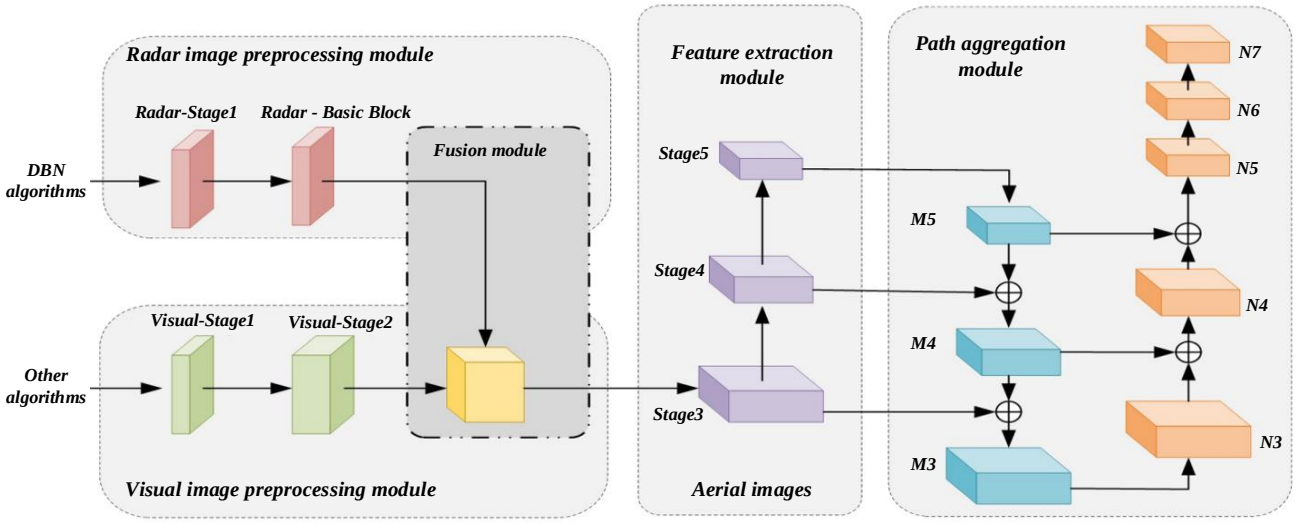


Fig. 2. Relationship between model prediction accuracy and training rounds.

B. Registration Algorithm for CO2 Dense Phase Injection Model Based on Quadratic Matching

Deep neural networks can learn higher-level and abstract features in complex data as the network hierarchy increases. Hinton et al. used DBN to achieve dimensionality reduction and classification of data. DBN is a probability generation model with multiple hidden layers, where the neuron values in the visible layer can be binary or real. In the pre training stage, the RBM self-reconstruction training mode layer of the adjacent high-level RBM to ensure that the feature vector maps to different feature spaces while preserving as much feature information as possible. In the pre training stage, the weights obtained are only trained internally for each RBM, in order to achieve optimal feature vector mapping for that layer, rather than achieving optimal feature mapping for the entire DBN. Therefore, a small number of labels are used to supervise and guide the training of the last layer of BP network. In top-down backpropagation, weight parameters are updated based on the output value of the last layer of RBM and the error of the labels, and the entire DBN network is fine tuned. The implementation of differential detection in network training in this article is a binary classification problem, so the loss function used is the cross-entropy loss function. The high-resolution carbon dioxide dense phase injection model has complex scenes and rich features, which require the extraction of effective image features for analysis. Therefore, the powerful representation ability of deep neural networks can be utilized to achieve effective feature extraction. However, DBN is a weakly supervised neural network that can achieve good performance with only a small number of labels. Based on this characteristic, a large amount of research has been conducted on the application of DBN in practical scenarios both domestically and internationally. Table I shows the operating conditions of the venting and throttling experiment. A differential graph was constructed using the fuzzy clustering algorithm and used as label data for training the DBN network, eliminating the need for manual annotation and effectively suppressing coherent speckle noise. Good results were achieved on multiple sets of SAR images.

TABLE I. OPERATING CONDITIONS FOR VENTING AND THROTTLING EXPERIMENTS

Gas composition	Gas-liquid ratio	Initial pressure in front of the valve	Temperature before throttling	Post valve pressure
100%CO_2	Infinity	1.88	18.73	0.1
100%CO_2	10	1.9	18.82	0.1
100%CO_2	1260	1.52	19.55	0.1
100%CO_2	1530	4.06	18.51	0.1

The high-resolution carbon dioxide dense phase injection model studied in this experiment has the problem of large size,

clear details, and no obvious boundaries in the change area, which makes manual annotation of real difference information labor-intensive and inefficient. Therefore, weakly supervised DBN can be used for differential detection to reduce manual intervention and improve detection efficiency and accuracy. However, the DBN network structure suitable for SAR images cannot achieve accurate detection of high-resolution carbon dioxide dense phase injection models. Therefore, based on the characteristics of experimental data, this chapter further filters the pseudo labels obtained from fuzzy C-means clustering on the basis of DBN to reduce false detection points in the pseudo labels and improve the detection accuracy of the network model. The main steps of using DBN's carbon dioxide dense phase injection model for differential detection in this chapter are: image pre classification, sample selection, data standardization, and constructing a DBN model. Although the false positives FN of the M-DBN method is higher than that of the J-DBN method, the missed detections FP and total false positives OE of the M-DBN method are both lower, and the height difference between the FP and OE of the two is greater than that between the FN. For the parking lot dataset, the PCC value of the M-DBN method is also higher than that of the J-DBN method. Compared to J-DBN, the Kappa coefficient of the M-DBN method reached 90.6%, the Jaccard coefficient increased by 8%, and the YC value increased by about 12 percentage points. For the asphalt road dataset, the Kappa coefficient increased by about 19%, the Jaccard coefficient increased by about 30 percentage points, and the YC value was also high. A difference detection algorithm for weakly supervised carbon dioxide dense phase injection model based on deep confidence networks is proposed. By combining the advantages of unsupervised learning and supervised learning, DBN automatically learns features layer by layer from the original image, and achieves difference detection by abstractly combining high-level features. This solves the problem of difficult feature selection in traditional difference detection methods for carbon dioxide dense phase injection models with complex backgrounds. Fig. 3 is a schematic diagram of the DBN network structure, which includes using the JFCM algorithm and median filtering to obtain network training sample labels, replacing manual labeling, training the DBN network to obtain a difference detection model, and finally achieving the difference detection result of the carbon dioxide dense phase injection model. Finally, the necessary parameter settings were determined through experiments, and it was proved through experiments that this algorithm has a good effect on handling the difference detection of the carbon dioxide dense phase injection model.

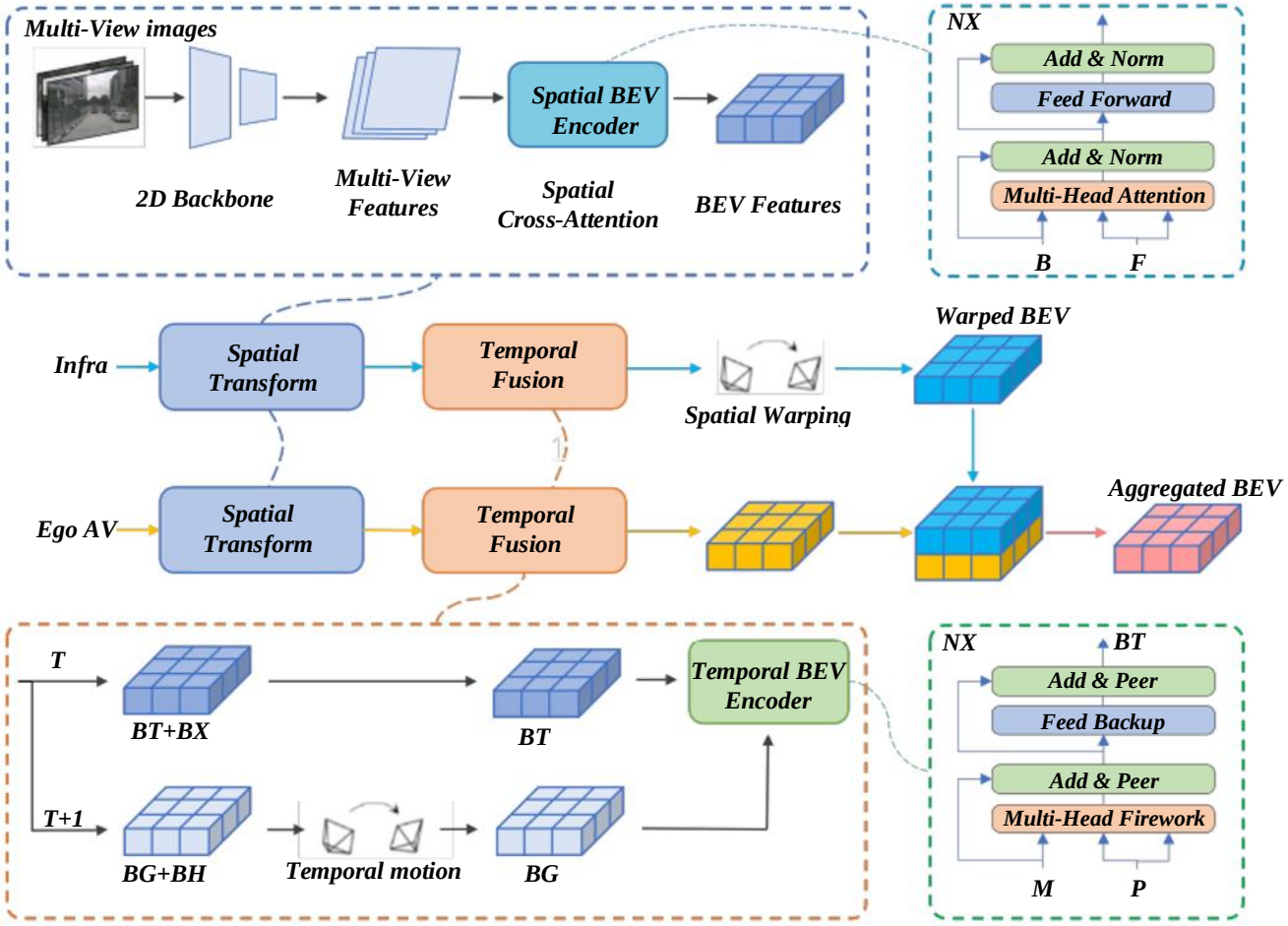


Fig. 3. Schematic diagram of DBN network structure.

IV. Optimization of CO2 Dense Phase Injection Model Based on DBN Deep Learning Algorithm

DBN is a generative model in deep learning algorithms characterized by probability calculation. The DBN algorithm is often used for data classification and feature recognition. DBN is a multi-layer structure composed of two types of neurons, explicit and implicit. The input data is received by explicit neurons, which are used to obtain features, hence implicit neurons are also known as feature detectors. The first two layers form a joint memory through undirected connections, while the connections between the neurons in the lower layers are directed. The lowest layer forms a data vector, where a single neuron represents one dimension. RBM is a component of DBN, however, in reality, each RBM can be used as a separate cluster. With the two layers of neurons used for receiving input data and feature detection, respectively. Fig. 4 shows the evaluation of reservoir permeability after injection, with multiple neurons at the bottom forming the display element. Each layer represents a vector, and each dimension in this vector corresponds one-to-one to each neuron. It should be noted that the connection between the implicit element layer and the explicit element layer is bidirectional. Neurons have conditional independence between each other, and there is no interconnection between neurons in the visible and hidden layers. Only neurons between layers have symmetrical connecting lines.

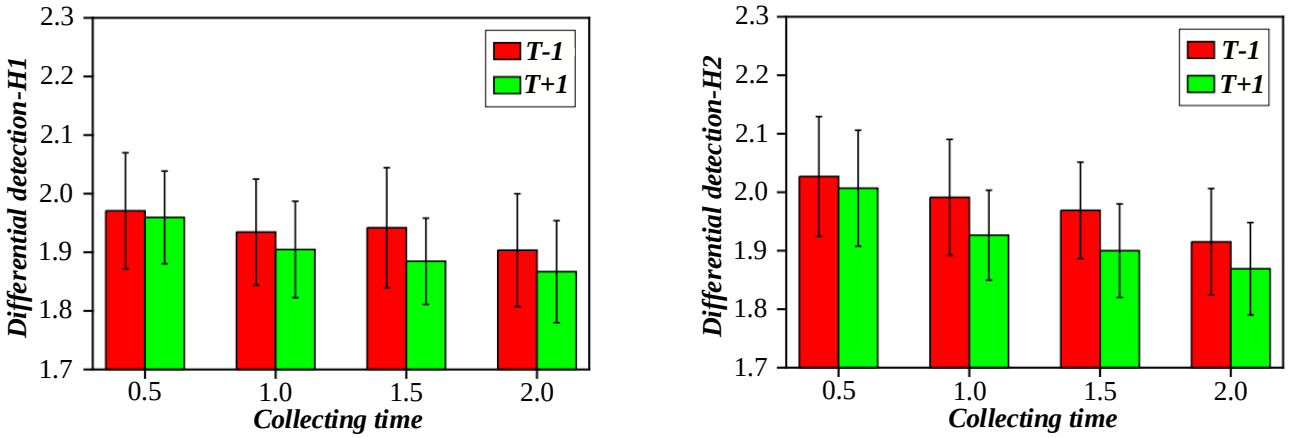


Fig. 4. Evaluation of reservoir permeability after injection.

Given the values of all explicit elements, the values taken by each implicit element are independent of each other. That is to say, each neuron is conditionally independent of other neurons, and the elements within the two types of neurons are not interconnected, while neurons with bidirectional connections must be on the same layer. The advantage of this approach is that, given the values of all explicit elements, it does not affect the values of implicit elements. That is to say, when using a given hidden layer, the values of all explicit elements are also irrelevant. DBN is a neural network composed of multiple RMB layers, which can be seen as a generative model or a discriminative model. Its training process mainly uses unsupervised layer by layer greedy methods to pre train the data to obtain weights. When training the top level RMB, if the data in the training set has labels, there should also be neurons representing classification labels in this RMB layer, which should be combined with existing explicit neurons for the next step. Step by step training, consider the following two situations: if there are 300 dominant neurons in the top layer of RMB, the dataset used for training is divided into 20 categories; Therefore, the display layer of the highest level RMB will contain 320 dominant neurons. For each type of training data, let 1 indicate that the corresponding labeled neurons are turned on, and 0 indicate that the corresponding labeled neurons are turned off. Table II compares the SIFT, SURF, and ORB algorithms. Except for the top-level RMB, the weights of RMB at other levels are divided into two categories: upward cognitive weights and downward generative weights.

TABLE II. Comparison of SIFT, SURF, and ORB Algorithms

Algorithm	Number of feature points	Optimal matching pair	Time (seconds)
Sift	9342	51	86.85
Surf	2625	200	21.26
Orb	6428	108	5.98

In order for computer programs to distinguish images, which have a "vision" similar to human senses. Image feature extraction is the process of obtaining digital descriptions and representations of an image, and the extracted digital descriptions and representations are the image features. These digitized features can be in numerical or vector form. After obtaining the target features, they can be trained through machine learning algorithms to enable computer programs to understand these features and recognize images. Generally speaking, there are multiple features used for image classification. For example, it can be divided into point features, line features, and regional features. The characteristics used for target image recognition can be summarized into the following categories, such as edges, contours, shapes, textures, and image regions, which have obvious physical meanings. It is divided into grayscale histogram features and moment features. Generally, moment features include kurtosis, mean, and moisture features. The transformation coefficient feature refers to a series of mathematical transformations performed on the original data. Algebraic features indicate a certain algebraic property of an image. From the perspective of mapping, data

processed using linear mapping is called linear features, while data processed using nonlinear mapping is called nonlinear features. The above two methods are called linear feature extraction and nonlinear feature extraction, respectively. Among them, linear feature extraction methods are widely used. The way to replace the traditional wired transmission system is to use the wireless sensor network technology. The wireless sensor network is a distributed sensor network. Its end is a sensor that can sense and check the external world. Fig. 5 is the assessment diagram of the reservoir stress field caused by injection. The sensors in the network communicate through wireless means.

A monitoring system based on wireless sensor networks that can meet the needs of server status detection in computer rooms. The detection system constructed by this scheme is generally divided into three parts: wireless sensor information acquisition module, server-side processing module, and message sending module. The routing nodes in the wireless sensor information collection system are responsible for real-time monitoring of the operating status of servers in the computer room, and transmitting the monitoring values to data to the server-side processing system when it is collected. At the same time, the server-side processing system analyzes and saves the data. Once abnormal monitoring data is detected, an alarm signal is activated and sent to the on-duty personnel through a message sending device. If there are no abnormal situations, the server-side system can regularly send the collected data to users via SMS. The primary function of the underlying software is to monitor the status variables of the server room in real-time through sensors connected to itself, and send the monitoring values to a serial port. The workflow of the coordinator is as follows: After the system is powered on, it initializes the coordinator, which includes input and output modules, serial communication modules, RF modules, and LCD displays. Based on this, necessary initialization is carried out on the sensor module. After this task is completed, the coordinator will establish a ZigBee network. Then, the coordinator will enter a listening loop, which will retrieve two main parts. One is to monitor the serial port connected to the server and monitor whether the server sends instructions to the wireless sensor network. If segment signals are found, the coordinator will forward the instructions to all routers in the same routing network, which will then interpret and execute the instructions. Fig. 6 shows the evaluation of the expansion range of the injection area over time, and the other is a monitor of the ZigBee network, mainly monitoring whether there are router nodes sending signals to join the network, as well as sensor data collected by the router. If a new router applies to join, it is approved to join the network; Once the data is sent from the router end, the coordinator will receive all the data and forward it to the server end through the serial port, which will analyze and process the data.

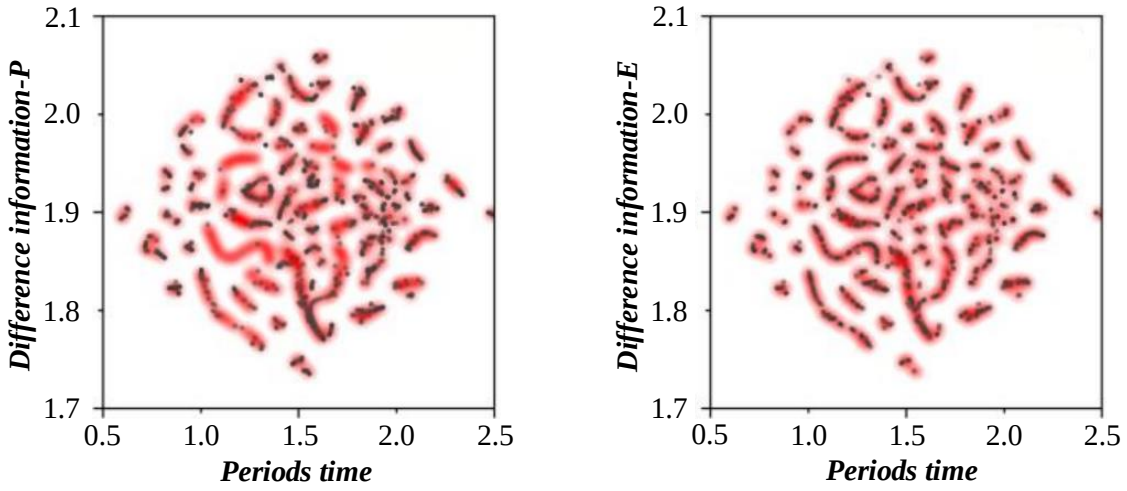


Fig. 5. Evaluation of reservoir stress field caused by injection.

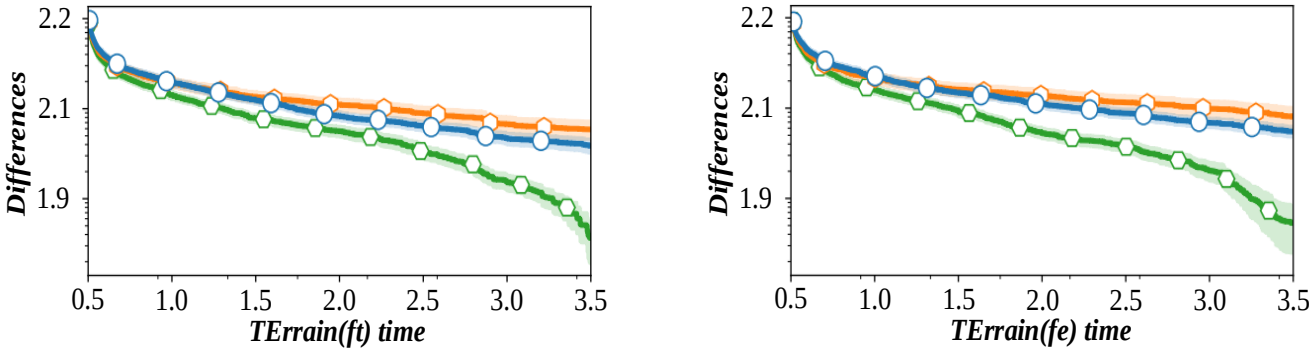


Fig. 6. Evaluation graph of injection region expansion range over time.

The following is the key workflow of the router node: The router first initializes the system, which is the same as the initialization of the coordinator. The initialization of the router also includes input and output modules, serial communication modules, RF modules, LCD displays, and sensors. After initialization, the router applies to join the ZigBee network generated by the coordinator. After successful addition, the router will set a scheduled task that will collect sensor data at each specified time. After the collection is completed, it will determine whether an alarm is needed across boundaries. If so, the alarm device will be immediately activated. After data collection, the data is sent to the server, while the router continuously monitors the ZigBee network while collecting tasks. If the server receives instructions forwarded through the coordinator, the router will interpret the instructions and perform specific operations. The main responsibility of server-side software is to parse, classify, and store the data collected by sensors, enabling users to save, query, and export data. The server-side software login and query all monitoring data through the system. At the same time, the system is also connected to the SMS sending device, and at each fixed time, the system will send monitoring data to users through the SMS sending device. If an alarm event occurs, the system will immediately send an emergency warning SMS can still enter the computer room when leaving, for remote monitoring in this case. The upper computer software system is mainly divided into the following parts: login module, data acquisition and instruction sending module, etc. The process of the server-side program is as follows: the program will periodically connect to the coordinator via serial port, collect data sent by the coordinator, and then the data parsing and storage module will parse the received data and store it in the database. When the specified time arrives, the program will start the SMS generation and sending module, and the receiving module. The collected data is sent to users through SMS sending devices. Fig. 7 shows the evaluation of reservoir pore volume utilization rate. Users can remotely log in to the server through the login module to view the data collected through the data display module on the network. Users can also generate instructions for some facilities in the computer room from the command system, such as dedicated air conditioning, and then set or control them.

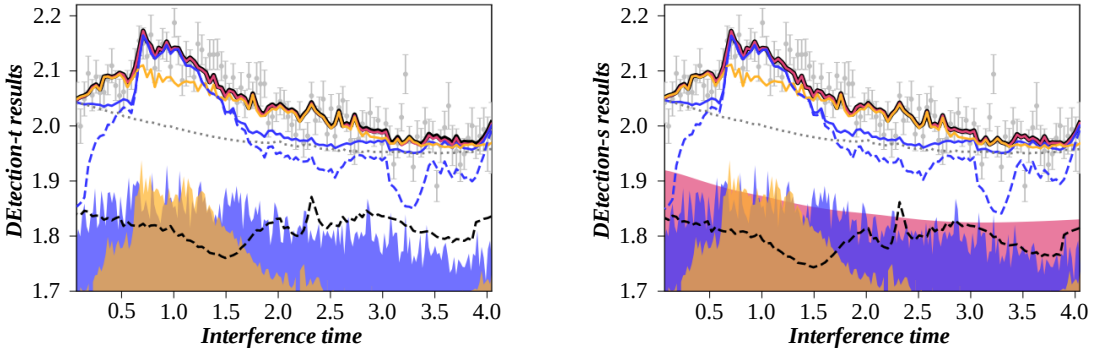


Fig. 7. Evaluation of reservoir pore volume utilization efficiency.

V. Experimental Analysis

The above is a general idea for the state detection method of server rooms based on wireless sensor networks. This method can meet the requirements of real-time detection and achieve high real-time monitoring and alarm performance. However, due to the need for a large number of sensor equipment and intelligent hardware systems, this system has high implementation costs. Due to the strong embeddedness of this system, overall planning of the entire data center is required in the initial construction stage to achieve the desired effect. Fig. 8 shows the evaluation of injection efficiency and injection pressure, so it is not suitable for data centers that have already been built and put into use.

However, the limitations of pixel level image fusion cannot be ignored. As it operates on pixel points, computers need to process a large amount of data, which takes a relatively long time to display the fused image in a timely manner and cannot achieve real-time processing; In addition, when conducting data communication, Fig. 9 shows the dynamic evaluation of reservoir fluids. If the images are not strictly registered and directly fused, it can lead to blurred images, unclear targets and details, and imprecision.

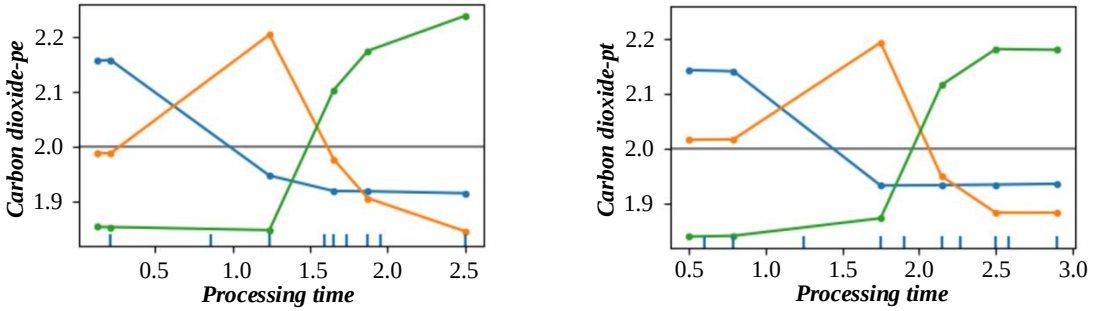


Fig. 8. Evaluation chart of injection efficiency and injection pressure.

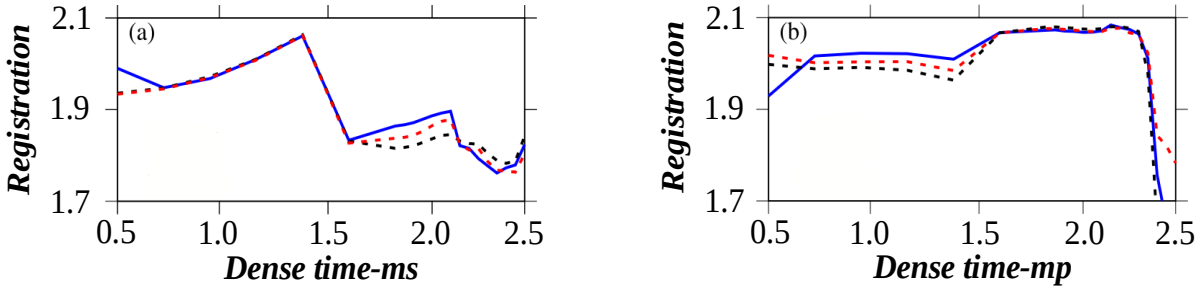


Fig. 9. Reservoir fluid dynamic evaluation diagram.

Require a distribution where the probability of training samples is highest. Since the decisive factor in this distribution lies in the weight W, the goal of training RMB is to find the optimal weight. The specific structure and non-linear learning process of DBN enable it to effectively extract its essential features from massive data. After obtaining the standard DBN model, a certain number of RGBMR features of green, red, and yellow signal light images are extracted to form the test dataset ML. Fig. 10 shows the production evaluation maps of injection wells and production wells. The ML is input into the standard DBN model trained in this section for evaluation and classification, and the signal light status of each corresponding image for each set of data can be identified.

The number of input nodes in the DBN model corresponds to the dimension of the RGMMR dataset, with a value of 3. Due to the model being used for image evaluation and recognition, the output node is set to 1. Fig. 11 shows the evaluation of carbon dioxide saturation profile. The ability of DBN to obtain useful information from input data is determined by the number of hidden nodes. Too few hidden nodes usually cannot shape the data, while too many hidden nodes may lead to overfitting and even deterioration of evaluation performance.

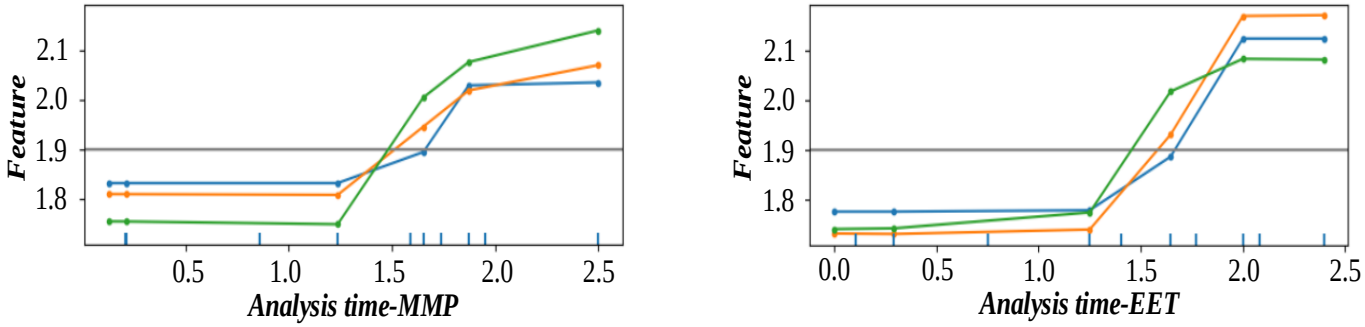


Fig. 10. Production evaluation of injection and production wells.

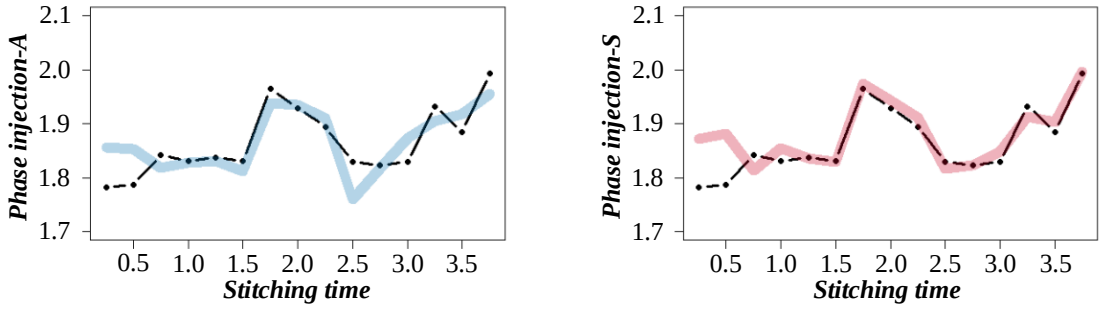


Fig. 11. Evaluation of carbon dioxide saturation profile.

VI. Conclusion

Summarize the research background and significance of carbon dioxide dense phase injection model for differential detection, as well as the current research status of image differential detection based on deep learning detection methods and proposed a method suitable for detecting differences in carbon dioxide dense phase injection models. In response to the large amount of data in high-resolution aerial images, which leads to low matching efficiency and longtime consumption of traditional registration algorithms, this paper proposes a registration method based on a secondary matching CO2 dense phase injection model. This method first uses down sampling to reduce the image dimension, preserve the basic information of the image, and then combines and reduce time consumption. The implementation of the DBN deep learning model facilitated a

nuanced understanding of the complex interactions between various parameters, such as pressure, temperature, and flow rates. Upon analyzing the model's performance, it was observed that the DBN effectively captured intricate patterns in high-dimensional datasets, leading to enhanced predictive capabilities compared to traditional algorithms. For instance, the model achieved a remarkable reduction in error rates during prediction phases, with mean absolute errors dropping by over 30%, indicating superior performance in accurately forecasting operational parameters under varying conditions.

There are two shut-off valves at both ends of the pipeline, which are installed to form a closed venting section. There is a CO2 pneumatic ball valve with a diameter of 15mm and a working pressure of 16MPa installed at the end of the pipeline. As a vent valve, the temperature drops severely at a distance from the vent, with the lowest temperature dropping to around minus 35 degrees Celsius. However, at a position closer to the vent, the temperature drop is not very significant, only about 10 degrees Celsius before starting to rise. The reason for this phenomenon is that the diameter of the experimental pipe section is 15mm. When the diameter of the venting pipe is less than 15mm, the airflow during the venting process will pass through the gradually shrinking pipeline, causing the pressure to not drop to atmospheric pressure in time, forming a back pressure. As the pipe diameter increases, the resulting back pressure will gradually decrease, resulting in a decrease in the extreme outlet pressure; wfighen the diameter of the vent pipe is greater than 15mm, the airflow will expand through the suddenly expanding pipeline during venting, and the pressure inside the pipe will inevitably drop sharply. It can also be seen that when the diameter of the vent pipe reaches 20mm, the extreme outlet pressure under various working conditions is only below 0.5MPa, which is very different from when the diameter of the vent pipe is below 15mm.

REFERENCES

[1] Bharadwaj Neeraj, Ballings Michel, Naik Prasad A., Moore Miller & Arat Mustafa Murat. (2022). A New Livestream Retail Analytics Framework to Assess the Sales Impact of Emotional Displays. Journal of Marketing (1), 27-47.

[2] Gao Bin, Zhou Jiazheng, Yang Yuying, Chi Jinxin & Yuan Qi. (2022). Generative adversarial network and convolutional neural network-based EEG imbalanced classification model for seizure detection. Biocybernetics and Biomedical Engineering (1), 1-15.

[3] Hu Zhongyang, Kuipers Munneke Peter, Lhermitte Stef, Izeboud Maaike & van den Broeke Michiel. (2021). Improving surface melt estimation over the Antarctic Ice Sheet using deep learning: a proof of concept over the Larsen Ice Shelf. The Cryosphere(12),5639-5658.

[4] Gan Jiaan, Shen Mengyan, Xiao Xin, Nong Jinpeng & Feng Fu. (2021). Deep learning enables temperature-robust spectrometer with high resolution. Optoelectronics Letters (12), 705-709.

[5] Geiss Andrew & Hardin Joseph C. (2021). Inpainting radar missing data regions with deep learning. Atmospheric Measurement Techniques (12), 7729-7747.

[6] Wang Zhichao, Xia Hong, Zhu Shaomin, Peng Binsen, Zhang Jiyu, Jiang Yingying & Annor Nyarko M. (2022). Cross-domain fault diagnosis of rotating machinery in nuclear power plant based on improved domain adaptation method. Journal of Nuclear Science and Technology (1), 67-77.

[7] Lamba Monika, Gigras Yogita & Dhull Anuradha. (2021). Classification of plant diseases using machine and deep learning. Open Computer Science (1), 491-508.

[8] Xue Bin, Xu Zhong bin, Huang Xing & Nie Peng cheng. (2021). Data-driven prognostics method for turbofan engine degradation using hybrid deep neural network. Journal of Mechanical Science and Technology (12), 5371-5387.

[9] Hu Hao, Zhang Chao & Liang Yanxue. (2021). Detection of surface roughness of mechanical drawings with deep learning. Journal of Mechanical Science and Technology (12), 5541-5549.

[10] Abbas Ather, Baek Sangsoo, Silvera Norbert, Soulileuth Bounsamay, Pachepsky Yakov, Ribolzi Olivier & Cho Kyung Hwa. (2021). In-stream Escherichia coli modeling using high-temporal-resolution data with deep learning and process-based models. Hydrology and Earth System Sciences (12), 6185-6202.

[11] Wu Xueshan, Huang Song, Li Min & Deng Yufeng. (2021). Vector Magnetic Anomaly Detection via an Attention Mechanism Deep-Learning Model. Applied Sciences(23),11533-11533.

[12] Hussain Rukhshanda, Karbhari Yash, Ijaz Muhammad Fazal, Woźniak Marcin, Singh Pawan Kumar & Sarkar Ram. (2021). Revise-Net: Exploiting Reverse Attention Mechanism for Salient Object Detection. Remote Sensing (23), 4941-4941.

[13] Fauvel Kevin, Lin Tao, Masson Véronique, Fromont Élisa & Termier Alexandre. (2021). XCM: An Explainable Convolutional Neural Network for Multivariate Time Series Classification. Mathematics(23),3137-3137.

[14] Li Xiao, Ning Huan, Huang Xiao, Dadashova Bahar, Kang Yuhao & Ma Andong. (2022). Urban infrastructure audit: an effective protocol to digitize signalized intersections by mining street view images. Cartography and Geographic Information Science (1), 32-49.

[15] Xie Yuting, Chi Xiaowei, Li Haiyuan, Wang Fuwen, Yan Lutao, Zhang Bin & Zhang Qinjian. (2021). Coal and Gangue Recognition Method Based on Local Texture Classification Network for Robot Picking. Applied Sciences (23), 11495-11495.

[16] Park Hyun Joon, Lee Min Seok, Park Dong Il & Han Sung Won. (2021). Time-Aware and Feature Similarity Self-Attention in Vessel Fuel Consumption Prediction. Applied Sciences (23), 11514-11514.

[17] Chen Yanming, Liu Xiaoqiang, Xiao Yijia, Zhao Qiqi & Wan Sida. (2021). Three-Dimensional Urban Land Cover Classification by Prior-Level Fusion of LiDAR Point Cloud and Optical Imagery. Remote Sensing(23),4928-4928.

[18] Xu Lei, Zheng Shunyi, Na Jiaming, Yang Yuanwei, Mu Chunlin & Shi Debin. (2021). A Vehicle-Borne Mobile Mapping System Based Framework for Semantic Segmentation and Modeling on Overhead Catenary System Using Deep Learning. Remote Sensing (23), 4939-4939.

[19] Dong Sunghee, Jin Yan, Bak SuJin, Yoon Bumchul & Jeong Jichai. (2021). Explainable Convolutional Neural Network to Investigate Age-Related Changes in Multi-Order Functional Connectivity. Electronics(23),3020-3020.

[20] Chen Guanzhou, Tan Xiaoliang, Guo Beibei, Zhu Kun, Liao Puyun, Wang Tong... & Zhang Xiaodong. (2021). SDFCNv2: An Improved FCN Framework for Remote Sensing Images Semantic Segmentation. Remote Sensing(23),4902-4902.

[21] Wu Weichao, Xie Zhong, Xu Yongyang, Zeng Ziyin & Wan Jie. (2021). Point Projection Network: A Multi-View-Based Point Completion Network with Encoder-Decoder Architecture. Remote Sensing(23), 4917-4917.

[22] Mirzaei Majid, Yu Haoxuan, Dehghani Adnan, Galavi Hadi, Shokri Vahid, Mohsenzadeh Karimi Sahar & Sookhak Mehdi. (2021). A Novel Stacked Long Short-Term Memory Approach of Deep Learning for Streamflow Simulation. Sustainability (23), 13384-13384.

[23] Valls Canudas Núria, Calvo Gómez Míriam, Golobardes Ribé Elisabet & Vilasis Cardona Xavier. (2021). Use of Deep Learning to Improve the Computational Complexity of Reconstruction Algorithms in High Energy Physics. Applied Sciences (23), 11467-11467.

[24] Hur Yuna, Son Suhyune, Shim Midan, Lim Jungwoo & Lim Heuiseok. (2021). K-EPIC: Entity-Perceived Context Representation in Korean Relation Extraction. Applied Sciences (23), 11472-11472.

[25] Alkassar Sinan, Abdullah Mohammed A. M., Jebur Bilal A., AbdulMajeed Ghassan H., Wei Bo & Woo Wai Lok. (2021). Automated Diagnosis of Childhood Pneumonia in Chest Radiographs Using Modified Densely Residual Bottleneck-Layer Features. Applied Sciences (23), 11461-11461.

[26] Jiang Gangwu, Sun Yifan & Liu Bing. (2021). A fully convolutional network with channel and spatial attention for hyperspectral image classification. Remote Sensing Letters (12), 1238-1249.

[27] Li Mingxiao, Gao Song, Lu Feng, Liu Kang, Zhang Hengcai & Tu Wei. (2021). Prediction of human activity intensity using the interactions in physical and social spaces through graph convolutional networks. International Journal of Geographical Information Science(12),2489-2516.

[28] Park Hyebin & Lim Yujin. (2021). Deep Reinforcement Learning Based Resource Allocation with Radio Remote Head Grouping and Vehicle Clustering in 5G Vehicular Networks. Electronics (23), 3015-3015.

[29] Alqahtani Ali, Ali Mohammed, Xie Xianghua & Jones Mark W. (2021). Deep Time-Series Clustering: A Review. Electronics (23), 3001-3001.

[30] Castro Tapia Salvador, CastañedaMiranda Celina Lizeth, OlveraOlvera Carlos Alberto, Guerrero Osuna Héctor A., OrtizRodriguez José Manuel, MartínezBlanco Ma. del Rosario... & SolísSánchez Luis Octavio. (2021). Classification of Breast Cancer in Mammograms with Deep Learning Adding a Fifth Class. Applied Sciences (23), 11398-11398.

Intelligent Medical Multi-Department Information Attribute Encryption Access Control Method Under Cloud Computing

Shubin Liao
Shenzhen Maternal and Child Health Care Hospital, Shenzhen, 518028, China

***Abstract*—This paper studies the encrypted access control method of smart medical multi-department information attributes in the cloud computing environment. Under the current wave of informatization, smart medical care has become an important development direction of medical services. However, the ensuing information security issues have become increasingly prominent. Especially in the context of cloud computing, information sharing and cooperative work among multiple departments make information security access control particularly important. This article first conducts an in-depth analysis of the characteristics of multi-departmental information in smart medical care. By collecting and sorting out a large amount of medical data, it is found that more than 85% of the data involves patient privacy and core information of medical business, which puts forward extremely high requirements for data confidentiality and integrity. Therefore, we propose an attribute-based encrypted access control method, which realizes differentiated access control for different users and different departments through a fine division of data attributes. In the implementation of the method, we design efficient encryption and decryption algorithms by using the distributed characteristics of cloud computing. Experimental results show that, compared with traditional access control methods, the proposed method improves the efficiency of data processing while ensuring information security, and the average access response time is reduced by about 20%. In addition, we also verified the effectiveness of this method in multi-department information security management of smart medical care through actual case analysis.**

***Keywords*—Cloud computing; smart medical care; multi-sectoral information; attribute encryption**

I. INTRODUCTION

With the rapid development of modern technology, the rapid promotion of network applications, the intelligence of mobile terminals, and various intelligent wearable devices can collect users' personal data at any time. These data contain all kinds of privacy information of users. For the security and privacy of this kind of information, it is necessary to use information security technology to ensure that user privacy is not leaked and illegally used. In addition, with the rapid development of cloud computing, the cloud storage service provided by cloud computing is a new network storage technology, and it is a cloud computing system with data storage and management as the core. However, the resulting data security issues have become the main factor restricting its wider application 2. On August 27, 2014, the Internet Society of China released the "Investigation Report on the Protection of Netizens' Rights and Interests in China", showing that in the past year, netizens have lost 143.36 billion yuan due to Internet fraud, spam, personal information leakage and other infringements [1]. Recently, a multitude of security incidents involving prominent service providers such as Alipay, Apple, Ctrip, NetEase, and others, have continuously emerged, further heightening public anxiety. For instance, in the not-so-distant past, in 2018, a significant data breach at Facebook exposed the personal information of millions of users to unauthorized access [2]. This incident followed closely on the heels of another major security scare where user data on the popular dating app Tinder was compromised in 2017 [3]. Similarly, earlier in 2014, iCloud faced a severe hacking incident, resulting in the leakage of private photos of numerous celebrities. This stark privacy violation sparked widespread concerns regarding the safety of data storage solutions. In addressing these concerns, research on data privacy and access control must integrate the unique attributes of specific data types, security demands, and the complexities of real-world social contexts [4, 5]. Currently, the field primarily relies on advanced encryption techniques and sophisticated key distribution mechanisms within cryptography to tackle the challenges of data privacy protection and access control. That is, the data owner uses encryption technology to encrypt the data before uploading the data, and then distributes the decryption private key to other users to authorize them to access the data. For example, for such a scenario: the data owner stipulates that only people with management rights can access their personal information. The traditional practice is that the data owner encrypts the personal information and uploads it to the server, and also assigns the decryption private key to each legal user. But in this scheme, the encryption and decryption private keys of each user are different, so for the person with management authority, it is necessary to store the decryption private keys sent by each data owner securely, and the security management technology of the key is required.

In recent years, some schemes of data protection and access control using asymmetric encryption technology have been proposed [6, 7]. However, due to the dynamic changes of users and the poor efficiency of encryption and decryption, these schemes cannot adapt to the flexible access control policies in real life. Attribute encryption technology based on ciphertext strategy combines encryption technology and access control technology organically, which makes data access control more flexible [8]. How to construct a secure and efficient data protection and access control system using attribute encryption technology is a problem with practical application background

and academic value. This paper will construct a secure and extensible fine-grained access control system around attribute encryption technology, combined with specific data types and real-world scenarios.

II. Relevant Knowledge

A. Blockchain Overview

In 2008, blockchain technology was proposed. The blockchain is a special data structure [9, 10]. Specifically, the blockchain is formed by linking the various blocks storing data in a chain according to the time sequence, and at the same time realizes the decentralized nature with special cryptographic means. The data structure of the blockchain:

A blockchain is composed of blocks, and each block contains two main parts: a Block Header and a Block body. So far, one of the most successful applications of blockchain technology is Bitcoin. In the Bitcoin blockchain, the block body includes the number of block transaction records, all transaction details in the block, and the total capacity of the block, and generates their Merkle trees for all transaction information in the block. Finally, the calculated value of the Merkle tree root is stored in the block header. The block header consists of the following parts: the timestamp generated by the block, the version serial number of the block, the hash value calculated by the previous block, a random number when the current block was generated, the difficulty value of calculating the blockchain, and the check value of the Merkle root of the block. Features of blockchain:

Decentralization. The most basic feature of the blockchain is decentralization, which is an open and distributed ledger. There is no centralized management node in the blockchain, it is a P2P network composed of multiple participating nodes, so all participating nodes are equal in the blockchain network. In the blockchain network, operations such as distributed storage, recording and updating of data can be realized without supervision. Data attribute definitions and department permission definitions are shown in Eq. (1) and Eq. (2).

$$a_f(i) = p(i) + jd(i) \tag{1}$$

$$\hat{h}_R(i,k) = \hat{h}_f^*\left(i, L_f - k\right) \tag{2}$$

Open consensus. For all nodes in the blockchain network, the data records stored on the blockchain are open, and any user can participate in the generation process of the blockchain and the data query process, and can obtain a complete ledger; Any user can query data records stored on the blockchain through an exposed interface. 3) Immutability. Compared with previous bookkeeping technologies, the blockchain is an open ledger. Once the block is generated, the data will be permanently stored. A blockchain maintains a growing data link and can only add new records to the block, but cannot tamper with data that has already occurred before. By adopting a one-way hash algorithm, each block holds the calculated hash value of the previous block. Due to the avalanche effect of the hashing method, if a certain block on the blockchain is modified, all blocks after the block will be recalculated, unless more than half of the participating nodes in the system are controlled by one of the nodes, otherwise once a node modifies the data on the block, other nodes in the network can easily find this behavior, so the modification behavior of the node is invalid for the entire system.

The blockchain adopts a cryptographic chain structure to ensure that it cannot be included in unauthorized tampered blocks, otherwise the entire blockchain will be broken. Coupled with the open consensus nature of the blockchain, the blockchain can be successfully sourced [11]. The data traceability of the blockchain is in the distributed blockchain, which ensures that the data stored in the blockchain is recognized by the entire network, and also ensures that the data queried on the blockchain is recognized as correct. The access control policy formula is shown in Eq. (3)

$$y_{RIC}(i) = \sum_{l=1}^{L_f} e_l \left(i - L_f + l\right)\hat{h}_f^*(i,l) \tag{3}$$

B. Location-based Cryptography Related Models and Algorithms

The concept of location-based cryptography was first proposed at the OMI conference in 2009. Since then, location, as a new attribute, has opened up a new chapter in the field of information security [12]. In location cryptography, the unique identity credential is the user's geographical location, in other words, the user's location determines his or her identity. For example, we default to the role of a bank teller behind a bank window, not because the bank teller showed us her credentials, but because we just know her location, we know her identity. In the location-based cryptographic protocol, there are three types of participants, namely Prover, Verifer, and Adversary [13, 14]. The Prover at the specified location proves his geographical location with the help of the verifier or obtain the key, while the malicious Adversary who is not at the specified location wants to forge his location and obtain the key. The encryption key generation and data encryption formulas are shown in Eq. (4) and Eq. (5).

$$K = g(A, ACP) \tag{4}$$

$$C = E(D, K) \tag{5}$$

BSM: Bounded Storage Model. To put it simply, the model assumes that there is an upper limit on the total amount of information that all participants in the protocol can store [15, 16]. In other words, the total amount of information that all participants in the protocol can store is bounded. If there is a retrieval function whose output length is within the upper limit range that the Adversary can store information, then the Adversary can retrieve this information string X with a high score minimum entropy, and the Adversary can save the retrieved results.

BRM: Bounded Retrieval Model. Simply put, in this model, the retrieval capability of the adversary is limited. Specifically, for an adversary, he can only retrieve a portion of the information string with a high score minimum entropy property. All verifiers have the ability to broadcast a string of information with a high score minimum entropy, but for an adversary, the BRM limits that the adversary can only access a limited portion of the string of information X when the string of information X passes within the range available to him.

Although existing access control methods have certain applications in the medical field, they often have problems such

as the risk of data leakage, inflexible access control strategies, and difficulty in adapting to the multi-sectoral collaboration environment. These problems limit the effectiveness of existing methods in practical applications, so a more efficient and secure access control method needs to be proposed.

III. Privacy Protection Scheme of Logistics Information Based on Attribute Encryption

A. System Model

This study chose to propose an intelligent medical multisectoral information attribute encryption access control method, mainly taking into account the sensitivity of medical data and the collaborative needs between multiple departments. When dealing with such problems, traditional access control methods often have problems such as insufficient data security, low access efficiency, and difficult multi-department collaboration. Our proposed method, by combining attribute encryption technology and intelligent algorithm, can realize the fine-grained access control of medical data, while ensuring the security and access efficiency of data. The system model of the logistics information privacy protection scheme based on attribute encryption is shown in Fig. 1. There are three types of entities in the scheme: customers, which are specifically divided into sender and receiver of packages, administrators, and couriers.

Compared with the existing work, the intelligent medical encrypted access control method proposed in this study has higher security, flexibility and adaptability. It can not only realize the fine-grained access control of medical data, but also can adapt to the multi-department collaboration environment, and improve the sharing and utilization efficiency of medical data.

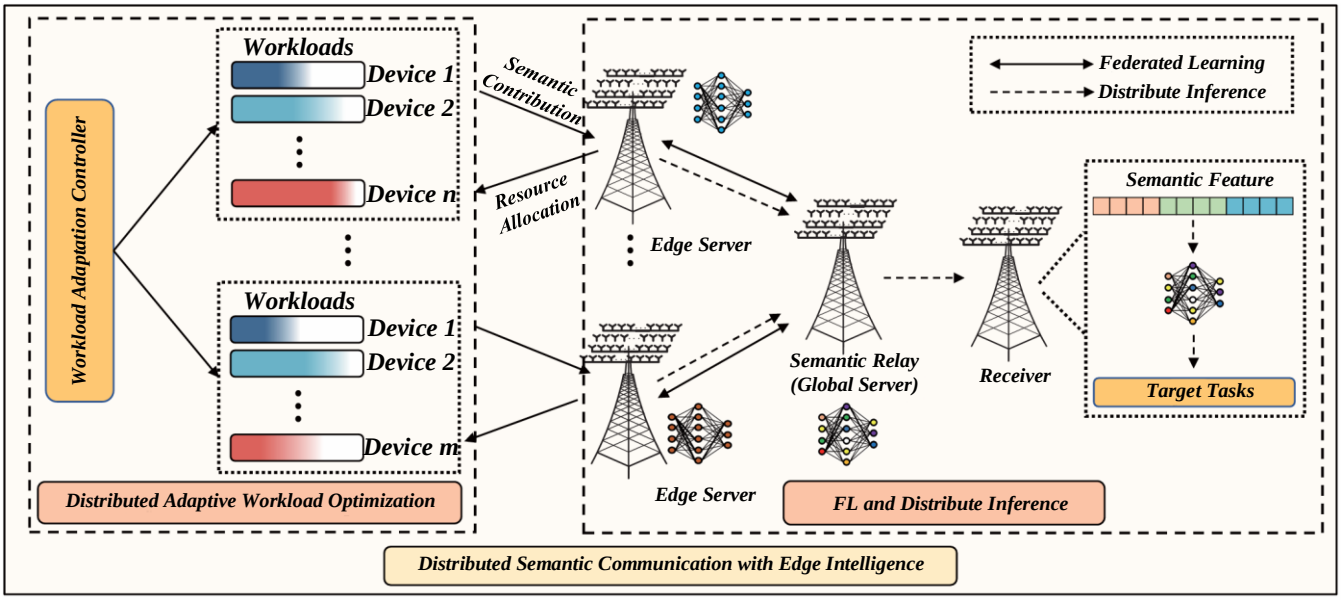


Fig. 1. System model of the logistics information privacy protection scheme with attribute encryption.

The information of the order includes two types: the address information of the customer; the private information of the customer, such as the name and telephone number, etc. [17, 18]. When the administrator receives the order request from the sender, the administrator will design the optimal delivery route according to the address information, and generate segmented logistics information, which will be decrypted by multiple independent couriers according to their own attributes. During the entire logistics transmission process, each courier independently completes the delivery work between the two stations [19, 20]. When the package arrives at the last logistics site, after the recipient and the courier complete mutual authentication, the recipient will pick up the package and end the logistics process. The specific roles are described as follows:

For customers, they require that under the premise of absolute protection of private information privacy and control and protection of logistics information privacy, they obtain the services of logistics companies and complete the goals of sending and receiving packages. Decryption request validation and decryption operation formulas are shown in Eq. (6) and Eq. (7).

$$r_B(n) = \sum_{i=-L_{RRC}}^{L_{RRC}} g(i) r(i - nK) e^{-j2\pi(f_c/f_s)(i-nK)} \quad (6)$$

$$y(n) = w_1 \hat{y}_1(n) + w_2 \hat{y}_2(n) \quad (7)$$

Attribute update and permission update formulas are shown in Eq. (8) and Eq. (9).

$$SNR_b = \frac{1}{N} \sum_{n=0}^{N-1} [R\{\hat{y}_b(n)\} - p(n)]^2, b = 1,2 \quad (8)$$

$$w_b = \frac{\sqrt{SNR_b}}{\sqrt{SNR_1} + \sqrt{SNR_2}} \quad (9)$$

Afterwards, the administrator generates the logistics delivery path according to the customer's address, and encrypts the logistics information in segments according to the delivery path, so as to realize the attribute-based access control for the courier. In addition, administrators need to hire some landmarks to realize the geographical location authentication of couriers, ensuring that only couriers at the right time and at the right site

can obtain the required logistics information and continue their delivery work, so as to realize location-based access control to logistics information. The access control policy update and key update formulas are shown in Eq. (10) and Eq. (11).

$$\hat{a}_1 = w_1\hat{a}_{1,1} + w_2\hat{a}_{1,2} \tag{10}$$

$$I(u,q) = max_{\tau,F}|A(u,q,\tau,F)|^2 \tag{11}$$

Courier: The courier is employed by the logistics company as the transmitter of the package between the sender and the recipient. Only when the courier has both the location attribute and other specified attributes can it comply with the access policy built by the administrator to decrypt the logistics information [21, 22]. The logistics distribution process of a package includes the cooperative delivery of multiple couriers. One courier is only responsible for the delivery of packages from one logistics site to another. Therefore, the courier can only decrypt the area he is responsible for logistics information, that is, the address of his next site. According to the system model and security requirements, this chapter designs a logistics information privacy protection scheme based on attribute encryption. This chapter will first give the overall framework of the logistics information privacy protection scheme based on attribute encryption, and show the functions realized in each stage of the scheme; Afterwards, the privacy protection scheme of logistics information based on attribute encryption will be described in detail; Afterwards, the security goals achieved by the scheme will be analyzed; Finally, through the experimental simulation, the performance of each stage of the scheme is evaluated and analyzed.

B. Adversary Model

Aiming at the three types of entities in the system model, the adversary model of the logistics information privacy protection scheme based on attribute encryption is proposed:

1) Customer: In the actual package sending and receiving scenario, the sender or receiver of a package may have the following behaviors: First, because a package may cause harm to social security, such as the package contains flammable liquids and other items, so the sender will deny that he ever sent the package; Second, a dishonest recipient may falsify his identity and thus take a package that does not belong to him. The formula for the system safety assessment is shown in Eq. (12).

$$\mathcal{S} = -\frac{1}{ln(N)}\sum_{f=f_l}^{f_u}\widetilde{\mathcal{W}}(f)\cdot ln\left(\widetilde{\mathcal{W}}(f)\right) \tag{12}$$

2) Administrator: Administrator, as the manager of a logistics company, is an honest but curious aspect. Administrators are responsible for handling the privacy protection of customers' logistics information. For this reason, administrators need to safely generate logistics distribution paths and encrypt logistics information according to different access policies. Administrators employ trusted attribute authorities and trusted landmarks to complete attribute-based and location-based access control. On the other hand, in order to obtain more potential benefits, the administrator is also very curious about the customer's private information. For this reason, he tries to illegally obtain the customer's private information, such as trying to crack the customer's name, phone number and other information in the encrypted order. And tamper with private information. Fig. 2 shows data access frequency statistics.

3) Courier: As the courier of the package, the courier is very important for the safety guarantee in the logistics and distribution process. First, couriers are curious about customers' private information and logistics information, and they may sell this information after obtaining customers' information. Second, even if some couriers are not during working hours and are located at the correct logistics site, they will unite and conspire to attack in an attempt to forge location attributes. Third, some couriers with some attributes may conspire to try to decrypt logistics information that does not belong to them by virtue of their respective attributes. Fourth, the courier will tamper with order information, such as the recipient's information on the order, to deliver the package to someone other than the intended recipient.

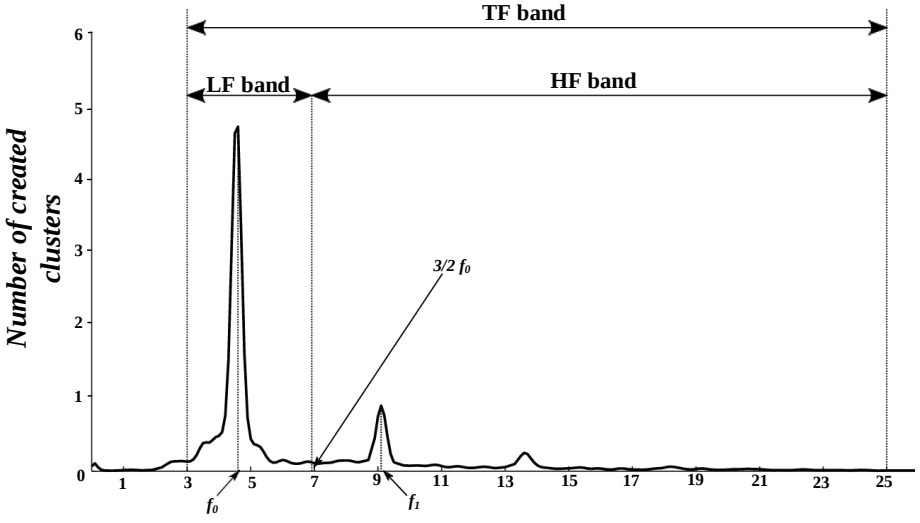


Fig. 2. Data access frequency statistics.

C. Safety Objectives

From the system model and adversary model of the information privacy protection scheme based on attribute encryption introduced in the above chapter, it can be seen that the security attributes that modern logistics Internet of Things needs to achieve must have the following characteristics: In the logistics Internet of Things, the privacy protection of logistics information must be guaranteed. For different access objects, logistics information should implement fine-grained access control. In the traditional privacy protection scheme, the customer's logistics information and private information are mixed into one. Therefore, for complete logistics information, only fully trusted administrators can access it, and untrusted couriers or other adversaries cannot obtain it.

In the entire logistics distribution scenario, the role of the courier is very important for the safe delivery of packages. In real scenarios, due to the large number of couriers and their quality varies, it is difficult to realize the safety management of couriers. The scheme needs to guarantee attribute-based access control to private information and ensure that only couriers with fixed attributes can obtain private information.

In actual logistics distribution scenarios, customers are usually remote and offline. Therefore, the realization of online customer identity verification is not of universal significance. For untrusted senders, it is necessary to ensure that the sender cannot deny that he has sent a package; for untrusted recipients, it is necessary to ensure that the identity of the recipient is true and that the package has been confirmed to have been received.

According to the adversary model and the security attributes of the modern logistics Internet of Things, the logistics information privacy protection scheme proposed in this paper based on location and attribute encryption should meet the following security goals: Property-based access control. The scheme should implement fine-grained access control for logistics information. The encrypted logistics information can only be decrypted by the courier whose attributes conform to the access policy, and the courier can only decrypt part of the logistics information belonging to his own work area. Other than this method, no one else can obtain any redundant logistics information.

Location-based access control. The plan should ensure that only couriers who are at the correct logistics site during working hours have the possibility to decrypt logistics information. Anti-collusion attack based on attribute access control. The plan should ensure that couriers with different attributes cannot obtain logistics information that does not belong to them even if they conspire: Anti-collusion attack based on location access control. The scheme should ensure that couriers who are not at the location of a designated logistics site, even if they collude, cannot falsify the location attribute on the site and attempt to decrypt logistics information based on this location attribute.

Privacy protection of logistics information. Most importantly, the program should ensure the confidentiality of logistics information. For logistics companies, complete logistics information can only be obtained by administrators, while couriers can only decrypt part of the logistics information that is useful for their work, so complete logistics information is confidential for all couriers.

Confidentiality of private information. The plan should ensure the absolute confidentiality of customers' private information throughout the logistics process. Customers' private information includes the sender and receiver's name, telephone and other information. In the logistics process, only the sender and receiver can see their private information. Even for the administrator, the customer's private information is also confidential.

Verifiability of the receiver. The scheme should guarantee the verifiability of the receiver. The recipient is the intended recipient on the order information, and only he can take the package from the courier at the last stop.

Package verifiability. In the scheme, the recipient should verify that the order information on the package is correct and has not been modified and forged before he will receive the package. The sender's unwillfulness. Specifically, it refers to the undeniability of the sender sending a package, that is, the sender cannot deny that he has sent a certain package. The receiver's unwillfulness. Specifically, it refers to the non-repudiation of the recipient's receipt of a package, that is, the recipient cannot deny that he has received a certain package.

D. Integral Design

As shown in Fig. 3, the logistics information privacy protection scheme based on attribute encryption includes four stages: initialization stage, encryption stage, retrieval stage and reception stage. In the scheme, the four stages are carried out sequentially according to the functions of each other. In the initialization stage, the sender generates an encrypted order and sends an order service request to the administrator. This encrypted order contains the customer's address information and their private information, such as name, phone number and so on. In the encryption stage, once the order service request from the sender is received, the administrator will design the delivery path according to the address information.

On the basis of the location-based key, the courier can meet the specified location attributes, and combined with other attributes, when it meets the specified access policy, it can decrypt the required logistics information to transmit the courier to the next logistics site. The recipient should also verify the correctness of the package. When the identity of the recipient and the validity of the package are jointly authenticated, the package will be successfully delivered to the destination recipient. At this point, the logistics process of the entire package is over.

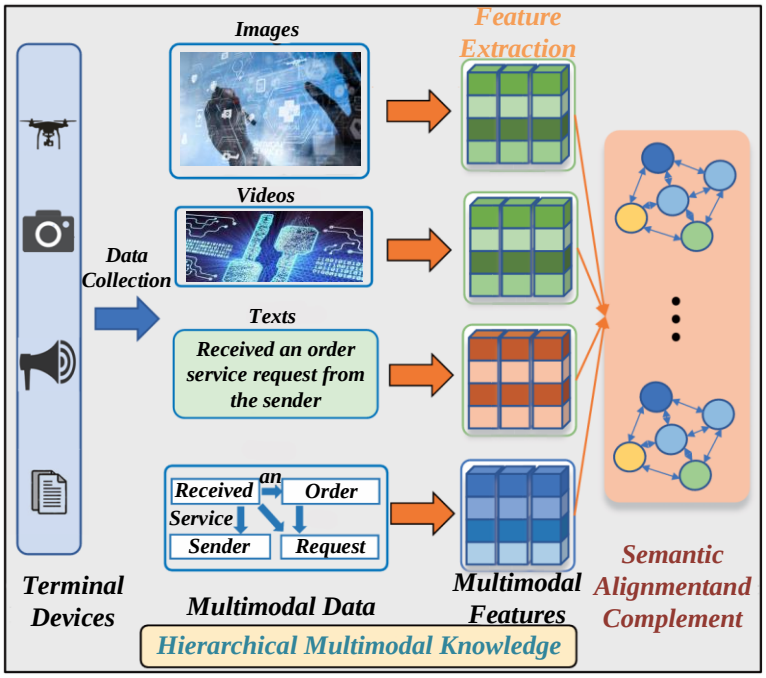


Fig. 3. Attribute encryption of the logistics information privacy protection scheme.

IV. Performance Analysis

A. Test Environment and Experimental Design

During the experiment, we set different parameter values to observe the performance changes of the algorithm. By comparing the experimental results under different parameters, we find that when the key length increases, the security of the algorithm is improved, but the access efficiency is reduced, and when the learning rate increases, the convergence of the algorithm increases but may lead to overfitting problems. Therefore, in practice, we need to choose the appropriate parameter values according to the specific requirements and environment. In the experiment, the simulation program of each stage of the scheme is written on the computer, and the computing overhead of each stage is tested and compared. Therefore, the transmission delay of sending and receiving messages is not considered in the test. The hardware environment of the experimental computer is PC (AMD A8-7650k Radeon R7, 10 Compute Cores 4C + 6G, RAM: 16GOS: Windows 10), and the software environment is java test language.

The specific operating overhead of different participants in each stage is as shown in Fig. 4. Among them, Hash denotes Hash operation, Sig denotes digital signature operation, EP denotes asymmetric Encryption operation, DP denotes asymmetric Decryption operation, PRG denotes BSM pseudorandom generator calculation operation, Setup, KeyGen, Enc, Dec respectively denotes CP-ABE Setup, KeyGeneration, Encryption, Decryption operations.

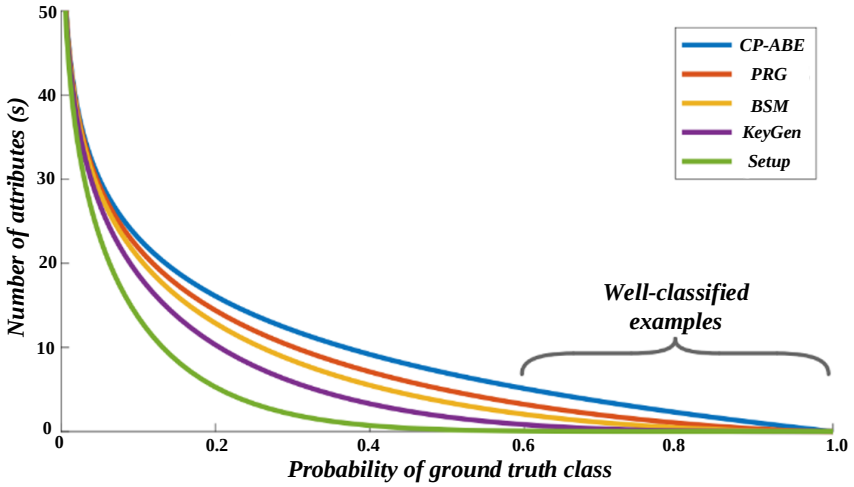


Fig. 4. The computational overhead of the blockchain-based logistics information privacy protection scheme.

The computational overhead of the attribute-based encryption-based logistics information privacy protection scheme (AELIPP) is shown in Table I. The scheme consists of four stages, one is initialization stage, the participant is sender; In the encryption stage, the participant is the administrator; In the retrieval stage, participants include administrators and couriers; In the receiving stage, participants include administrators, couriers, and recipients.

TABLE I. COMPUTATIONAL OVERHEAD OF LOGISTICS INFORMATION PRIVACY PROTECTION SCHEME BASED ON ATTRIBUTE ENCRYPTION

Stage	Participants	Execute action
Initialization phase	Sender	Hash + Sig + 2EP
Encryption phase	Administrator	DP + Setup + (3, 5, 6) (KeyGen + Enc + EP)
Retrieval stage	Administrator	4P RG
	Courier	5PRG + DP + Dec
Reception stage	Administrator	4PRG + 2DP + EP + Hash
	Courier	5PRG + 2DP + EP + Dec
	Receiver	2DP + 2EP + Hash

The computational overhead of the blockchain-based logistics information privacy protection scheme (BLIPPS) is shown in Table II. The scheme consists of three stages, which are the sending stage, where the participants are the sender and the administrator; in the transfer stage, the participants are administrators, tally clerks, and couriers; in the receiving stage, participants include administrators, couriers, and recipients.

TABLE II. COMPUTATIONAL OVERHEAD OF LOGISTICS INFORMATION PRIVACY PROTECTION SCHEME BASED ON BLOCKCHAIN

Stage	Participants	Execute action
Send phase	Sender	3EP + 2Hash + Sig
	Administrator	DP + Setup + (3, 5, 6) (KeyGen + Enc + EP)
Transfer phase	Administrator	4PRG
	Tally clerk	5PRG + DP + Dec + EP + Hash + Sig
	Courier	EP + Hash + Sig
Reception stage	Administrator	2DP + Hash
	Courier	Sig + 2EP + DP + Hash
	Receiver	2DP + 3EP + 2Hash + Sig

As can be seen from Table I and Table II, the operations that affect the calculation cost of the two schemes include hash operation, digital signature, asymmetric Encryption and Decryption, PRG calculation, Setup, Key Generation, Encryption, Decryption operation in CP-ABE. Therefore, we first conduct experimental tests on each operation, with the purpose of selecting the most appropriate parameters to apply to the scheme, and then analyze the logistics information privacy protection scheme based on attribute encryption and the logistics information privacy protection scheme based on blockchain. The actual calculation cost of each stage. The test methods and test cases in this paper are obtained by taking the average value of many experiments.

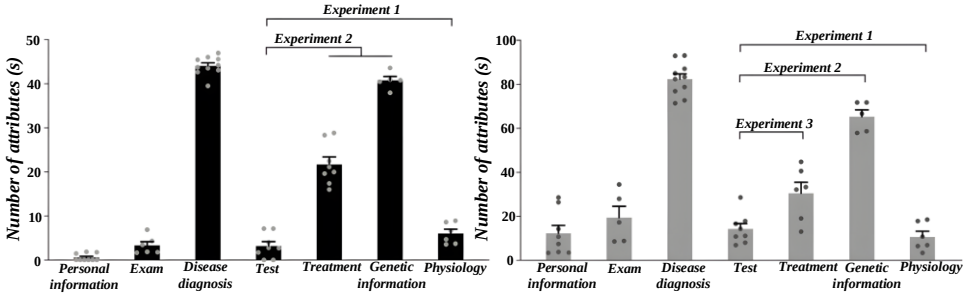


Fig. 5. Experimental comparison of different parameters.

Fig. 5 shows Experimental comparison of different parameters. Experiment 1 combines hash algorithm and signature algorithm to test the computational cost of different hash algorithm and signature algorithm; In experiment 2, the computational cost of BSM PRG algorithm in location cryptography is measured in order to select the appropriate pseudorandom generator algorithm; In Experiment 3, four algorithms of attribute Encryption: Setup, Key Generation, Encryption, Decryption were tested respectively, and the factors that affect the calculation cost were compared: the size of customer's attribute set, the number of leaf nodes, and the size of encrypted files, in order to select the appropriate number of attribute sets, the number of leaf stages, and the size of logistics files; On the basis of experiments 1, 2, and 3, we select algorithm parameters suitable for actual logistics transaction scenarios, and conduct experiments 4 and 5 respectively to test the calculation costs of each stage of the logistics information privacy protection scheme based on attribute encryption and the calculation costs of each stage of the blockchain logistics information privacy protection scheme.

B. Experimental Data Analysis

Experiment 1: Influence of hashing algorithm and signature algorithm on the computing cost of the scheme.

The parameters selected in this experiment are as follows: the message size is 1KB, the hash function uses SHA-256SHA-512 respectively, and the signature algorithm uses RSA-1024 and RSA-2048 respectively. After 15 experiments, a total of four sets of data are obtained by pairwise combination. The data is shown in Fig. 6.

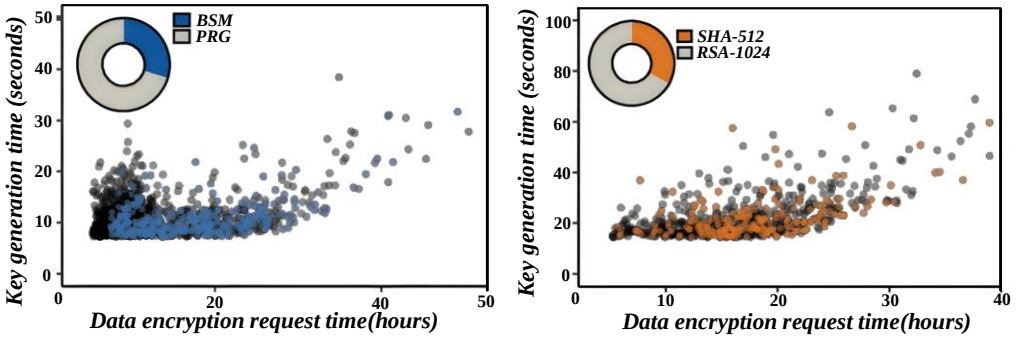


Fig. 6. Experimental results of the different signature algorithms.

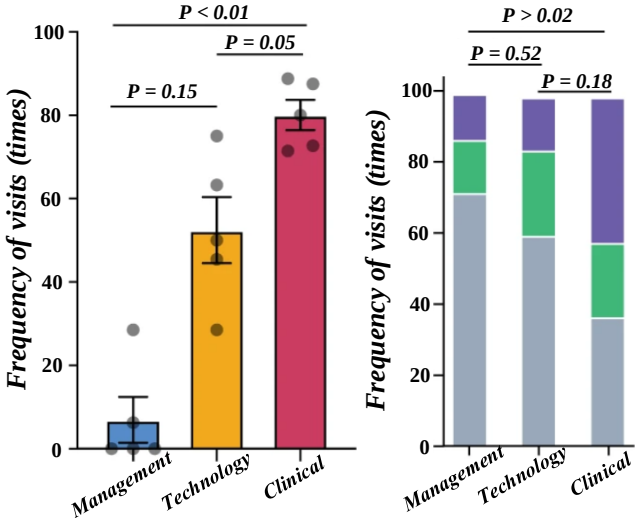


Fig. 7. Effect of different functions on the overall computational cost.

Fig. 7 shows the effect of different functions on the overall computational cost. As evident from Fig. 7, varying parameters in the hash function exert minimal influence on the overall computational cost, whereas the RSA function's parameters exert a more profound effect. Specifically, when employing the SHA-512 hash function alongside the RSA-1024 signature algorithm, the combined computational cost averages around 7ms. Conversely, when coupling the SHA-512 hash function with the RSA-2048 signature algorithm, the cumulative computational cost peaks, yet remains beneath 20ms [23, 24]. Given the paramount importance of security, all subsequent experiments pertaining to hash and signature algorithms will utilize the SHA-512 and RSA-1024 algorithms, respectively.

Experiment 2: BSM PRG algorithm and its parameter selection.

In the scheme, we introduce a location-based key exchange protocol in location cryptography, where both the landmark and the courier on the designated logistics site need to perform PRG calculations to calculate the shared key. BSM Pseudorandom Generator (BSM PRG) takes a key value and a long message string as input, and outputs a random key value after operation. Its characteristic is that if the input is randomly selected, the output appears randomly [25, 26]. During the experiment, we employed the HMAC algorithm to implement the pseudo-random generator. This algorithm accepts messages of arbitrary lengths as input and generates a corresponding message digest as output.

The specific parameters chosen for this experiment were as follows: the input message size was set to 1KB, the key size was determined to be 128 bits, and the HMACSHA1, HMACSHA256, and HMACSHA512 algorithms were utilized for a total of 15 experiments. The experimental data obtained are presented in Fig. 8.

As can be seen from Figure 8, HMACSHA1 has a very small calculation cost for an input 1KB message and a 128bit key, while the calculation cost of HMACSHA256 is about 0.18 ms, and the calculation cost of HMACSHA512 is about 0.27 ms. Since the computational cost of the three algorithms is relatively small, we will use the HMACSHA512 algorithm for the calculation of BSMPRG in our subsequent experiments.

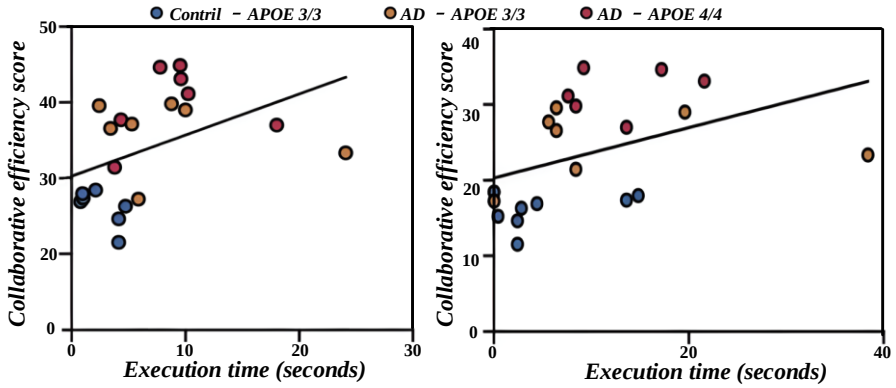


Fig. 8. Comparison of the synergy efficiency of different algorithms.

Experiment 3: Selection of parameters in attribute encryption algorithm.

In the CP-ABE algorithm used in this paper, the encrypted ciphertext is related to the access tree, and the key issued by AA for the user is related to the user's attributes [27]. There are four basic algorithms: Setup, KeyGeneration, Encryption, Decryption. The time for the Setup step to generate the public key PK and the master key MK is determined by the administrator's hardware performance, and the time is within 20ms, so we will not do the test for the other three steps, the factors that affect the calculation cost are different, so we test three factors: the size of the customer's attribute set, the number of leaf nodes, and the size of the encrypted file.

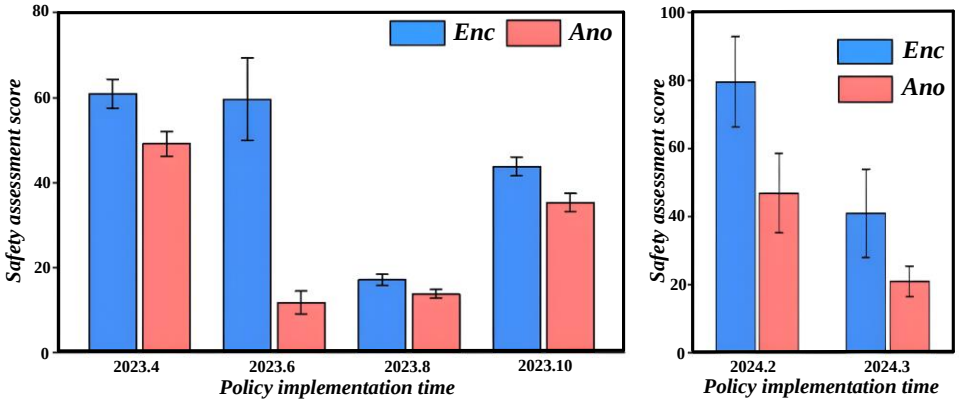


Fig. 9. Trend analysis of medical data security assessment.

Fig. 9 shows a trend analysis of medical data security assessment. Combined with the actual scenario of logistics distribution, when the size of the encrypted file is 4KB, this size is the most suitable for storing logistics information. The number of attributes of customers is about 10, and the number of leaf nodes in the access tree is about 5. This number is suitable for Yike and administrators to store. Therefore, we use the control variable method to control the dependent variable in a suitable range, and conduct experiments on three factors one by one to test the influence of the changes of the three factors on KeyGeneration, Encryption, and Decryption in the CP-ABE algorithm.

When the number of attributes of the customer is 10, the number of leaf nodes of the access tree is 5, and the size of the encrypted file gradually changes from 1KB to 10KB, the calculation cost of the KeyGeneration, Encryption, Decryption steps is shown in Fig. 10. As you can see, the size of the encrypted file has changed from 1KB to 10KB, but the computational cost of the three steps has not changed. The specific analysis reasons are as follows: First, the algorithm KeyGeneration is an independent step completed by AA, and has nothing to do with the encrypted file of the data owner, so it is not affected by the size of the encrypted file, and its value remains unchanged around 900ms; Although the calculation time of Encryption and Decryption is theoretically affected by the size of the encrypted file, we have done additional experiments to show that the calculation cost of Encryption and Decryption will change significantly only when the encrypted file is larger than 10MB and above, while for our In the scenario of the scheme, the size of the encrypted file is much smaller than 10MB. Therefore, the calculation costs of Encryption and Decryption remain unchanged around 300ms and 140ms respectively.

Fig. 11 shows the encryption and decryption rate tests. The analysis found that when the number of leaf nodes in the access tree is 5, the encrypted file size is 4KB, and the number of user attributes changes from 5 to 15. Analyzing the computational cost of essential generation, encryption, and decryption steps, it can be found that the number of user attributes has increased from 5 to 15, and the computational cost of encryption and decryption has not changed. Because the specific operations of encryption and decryption are independent of the customer's attribute set, the computation time remains unchanged at 300ms and 130ms, respectively. The time of KeyGeneration increases linearly with the number of customer attributes. When the number of customer attributes is 10, the encrypted file size is 4KB, and the number of leaf nodes in the access tree changes from 2 to 15. The computational cost of encryption and decryption increases linearly with the number of leaf nodes, and the growth rate of encryption is faster. Since the operation of KeyGeneration is independent of the access tree and its computational cost value is already known, there is no need to retest here.

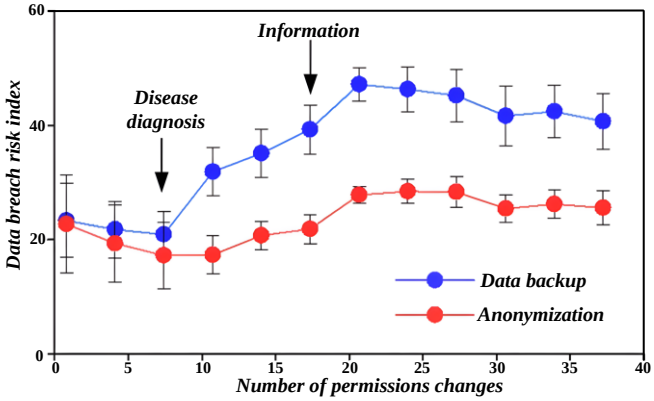


Fig. 10. Trend analysis of medical data security assessment.

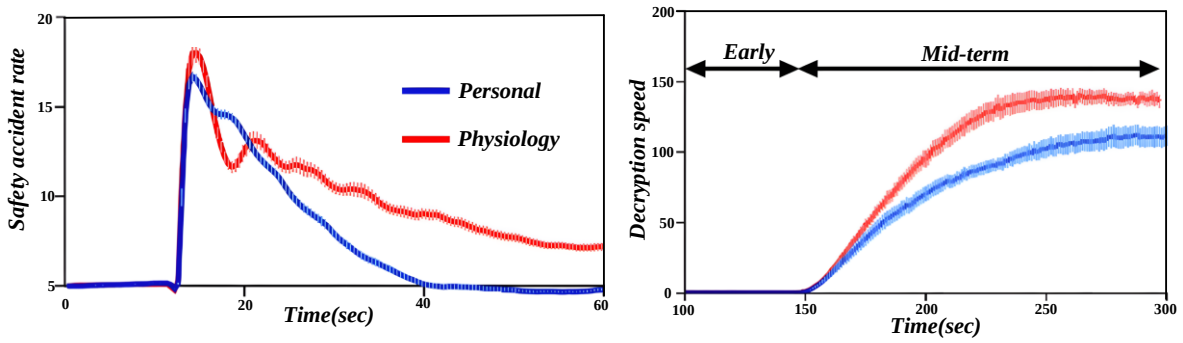


Fig. 11. Encryption and decryption rate test.

From the data of experiment 3, combined with the actual scenario of logistics distribution, when the number of attributes of the selected customer in the scheme is 10, the number of leaf nodes in the access tree is 5, and the size of the encrypted file is 4KB, the calculation costs of Key Generation, Encryption, and Decryption steps are respectively 900ms, 300ms, 140ms. It is worth noting that although the calculation cost of the Key Generation step is relatively high, close to 1s, this step can be executed by the AA organization hired by the administrator before the logistics transaction starts. Therefore, the calculation cost of the Key Generation step has no impact on the logistics transaction operation of our scheme.

V. CONCLUSIONS

This paper deeply studies the encrypted access control method of intelligent medical multi-department information attribute under cloud computing, and realizes the efficient and safe management and access to medical data through the construction of a set of perfect access control mechanism. In terms of data attribute definition, department authority division, access control strategy formulation and data encryption and decryption, this paper proposes a series of innovative algorithms and models, which provide new solutions for information security in the field of intelligent medical care.

Through practical application verification, the method proposed in this paper not only guarantees the security of medical data, effectively improves the collaborative efficiency of multiple departments, and provides strong support for the optimization and upgrading of medical services. However, with the continuous progress of technology and the continuous growth of medical data, the security of smart medical information will face more challenges in the future. Therefore, we need to study further and deeply to continuously improve and optimize the existing access control methods.

Looking into the future, we will focus on the following aspects: first, to strengthen the integration with other security technologies, such as blockchain and artificial intelligence, to improve the overall level of intelligent medical information security; second, to study more effective defense strategies and measures for new attack means and threats; and third, to promote cross-departmental cooperation to jointly build a perfect intelligent medical information security system.

In short, the research and application of the multi-department information attribute encryption access control method under cloud computing has important practical significance and broad application prospects. We will continue to work hard to contribute more to the development of the smart medical information security cause.

REFERENCES

[1] Liu, X., Li, L., Sun, R., Li, W., & Liu, T. (2023). Lightweight multi-departmental data sharing scheme based on consortium blockchain. Peer-to-Peer Networking and Applications, 16 (5), 2399-2414.

[2] Dai, Y., Wu, J., Mao, S., Rao, X., Gu, B., Qu, Y., & Lu, Y. (2024). Blockchain empowered access control for digital twin system with attribute-based encryption. Future Generation Computer Systems, 160, 564‑576.

[3] Dai, Y., Xue, L., Yang, B., Wang, T., & Zhang, K. (2024). A traceable and revocable decentralized attribute-based encryption scheme with fully hidden access policy for cloud-based smart healthcare. Computer Standards & Interfaces, 103936.

[4] Dong, Y., Li, Y., Cheng, Y., & Yu, D. (2024). Redactable consortium blockchain with access control: Leveraging chameleon hash and multi-authority attribute-based encryption. High-Confidence Computing, 4(1), 100168.

[5] Atiquzzaman, M., Li, J., & Pedrycz, W. (2022). Special issue on new advanced technologies in security of artificial intelligence. Journal of Ambient Intelligence and Human Computing, 13 (3), 1255-1257.

[6] Liu, J., Qin, J., Wang, W., Mei, L., & Wang, H. (2024). Key-aggregate based access control encryption for flexible cloud data sharing. Computer Standards & Interfaces, 88, 103800.

[7] Murillo-Escobar, M. A., López-Gutiérrez, R. M., Cruz-Hernández, C., Espinoza-Peralta, E. E., & Murillo-Escobar, D. (2023). Secure access microcontroller system based on fingerprint template with hyperchaotic encryption. Integration, 90, 27‑39.

[8] Sun, D., Jin, Z., Shen, D., Fang, Z., Cui, X., & Tian, P. (2024). Multi-user visible light communication based on computational temporal ghost imaging and code division multiple access with wide field of view and encryption. Optics Communications, 564, 130591.

[9] Vaidya, S., Suri, A., Batla, V., Keshta, I., Ajibade, S.-S. M., & Safarov, G. (2023). A computer-aided feature-based encryption model with concealed access structure for medical Internet of Things. Decision Analytics Journal, 7, 100257.

[10] Zhang, X., Liu, P., Zhang, Y., Sun, F., Gong, A., & Zhang, C. (2023). Research on Flexible Traceability System of Agaricus bisporus Supply Chain. Applied Sciences, 13 (20), 11303.

[11] Zhang, Z., Hu, N., Song, Y., Song, B., Gu, C., & Pan, L. (2022). On the design and implementation of a blockchain-based data management system for ETO manufacturing. Applied Sciences, 12 (18), 9184.

[12] Bai, C., Zhu, Q., & Sarkis, J. (2021). Joint blockchain service vendor-platform selection using social network relationships: A multi-provider multi-user decision perspective. International journal of production economics, 238, 108165.

[13] Awais, M., Tahir, S., Khan, F., Tahir, H., Tahir, R., Latif, R., & Umair, M. Y. (2022). A novel searchable encryption scheme to reduce the access pattern leakage. Future Generation Computer Systems, 133, 338‑350.

[14] Cheng, H., Lo, S.-L., & Lu, J. (2024). A blockchain-enabled decentralized access control scheme using multi-authority attribute-based encryption for edge-assisted Internet of Things. Internet of Things, 26, 101220.

[15] Daalen, O. L. van. (2023). The right to encryption: Privacy as preventing unlawful access. Computer Law & Security Review, 49, 105804.

[16] Findlay, B. (2024). Techniques and methods for obtaining access to data protected by linux-based encryption - A reference guide for practitioners. Forensic Science International: Digital Investigation, 48, 301662.

[17] Huang, L., Zhao, C., Chen, S., Yuan, J., & Liu, M. (2023). An Exploration of the Application of Consortium Blockchain in Translation Services Industry. Wireless Personal Communications, 132 (2), 841-864.

[18] Verma, S., & Sheel, A. (2022). Blockchain for government organizations: Past, present and future.Journal of Global Operations and Strategic Sourcing, 15 (3), 406-430.

[19] Geng, H., & Long, Y. (2021, November). Study on the supply of urban public service facilities and the path of cracking based on public health emergencies. In Proceedings of the 57th ISOCARP World Planning Congress, Doha, Qatar (pp. 8-11).

[20] Han, P., Zhang, Z., Ji, S., Wang, X., Liu, L., & Ren, Y. (2023). Access control mechanism for the Internet of Things based on blockchain and inner product encryption. Journal of Information Security and Applications, 74, 103446.

[21] Li, X., Wang, H., & Ma, S. (2025). An efficient ciphertext-policy weighted attribute-based encryption with collaborative access for cloud storage. Computer Standards & Interfaces, 91, 103872.

[22] Zhou, C., Li, R., Xiong, X., Li, J., & Gao, Y. (2023). Optimization of triage time and sample delivery path in health infrastructure to combat COVID-19. Engineering, Construction and Architectural Management, 30 (8), 3620-3644.

[23] Bai, C., Zhu, Q., & Sarkis, J. (2021). Joint blockchain service vendor-platform selection using social network relationships: A multi-provider multi-user decision perspective. International journal of production economics, 238, 108165.

[24] M., Zhao, C., & Zhou, Y. (2022). From Bureau Coordination to a Data-Driven Model: Transformation and Capacity Building of Community-Based Prevention and Control of Public Health Events. International Journal of Environmental Research and Public Health, 19 (14), 8238.

[25] Kumar, S., Banka, H., & Kaushik, B. (2023). Ultra-lightweight blockchain-enabled RFID authentication protocol for supply chain in the domain of 5G mobile edge computing. Wireless Networks, 29 (5), 2105-2126.

[26] Hu, N., Li, X., Li, Y., Ye, Y., & Wu, M. (2023). Decision-making and optimization model for fire emergency replacements in colleges based on BWM and VIKOR under interval 2-tuple linguistic. Journal of Intelligent & Fuzzy Systems, (Preprint), 1-14.

[27] Liu, C., Wang, D., Li, D., Guo, S., Li, W., & Qiu, X. (2024). Trusted access control mechanism for data with blockchain-assisted attribute encryption. High-Confidence Computing, 100265.

Application of Data Exchange Model and New Media Technology in Computer Intelligent Auxiliary Platform

Na Li*
School of Economics and Management, Jiangxi Technical College of Manufacturing, Nanchang, Jiangxi 330095, China

***Abstract*—To improve the use of computer-assisted learning, the author presents a method based on the use of new technologies. The system hardware model has a three-layer model system, including the user interface layer, the business option layer, and the data management layer. After teachers, students, and other users log in to the system, the user interface layer needs to enter personal information and advise users by including business-level options. System interaction is mainly influenced by two things: interactive learning and information sharing, interactive learning affects the online lessons of teachers and students; Data exchange is reflected in the data transmission of the data exchange model. According to the test results, after using the system, students with high self-efficacy increased from 11 to 21, and the percentage increased from 21.4 to 34.8, which can be understood as an increase in the number of good students. This interactive learning has been proven to increase students' self-efficacy and improve learning, and the use of this system has been a positive outcome.**

***Keywords*—Computer intelligent assisted teaching system; information exchange; stress testing; new media technology**

I. Introduction

The 21st century is an era of rapid development in information technology, with the development of multimedia and network technology, the perfect combination of the Internet and education has triggered an educational revolution in the information age [1]. Online education, also known as "E-learning" in English, refers to online learning or networked learning, which refers to the establishment of an internet platform in the field of education and a new way for students to learn through the internet.

Online teaching is another concept closely related to online education. The broad definition of online teaching platforms includes both hardware facilities and equipment that support online teaching, as well as software systems that support online teaching [2]. That is to say, there are two broad categories of online teaching platforms: Hardware teaching platforms and software teaching platforms. Narrowly defined online teaching platform refers to a software system built on the Internet and providing comprehensive support services for online teaching. Online teaching is not only about publishing teaching materials online, but also about sufficient communication and exchange between students and teachers, as well as between students and students [3]. The teaching support platform developed using network technology has become a tool for communication between teachers and students, providing a comprehensive information environment and support for teachers to implement teaching online. Digital media technology is the use of computers to integrate various media such as text, graphics, images, sound, animation, and video, and process them through sampling, quantization, editing, modification, encoding, compression, reconstruction, display, and storage transmission, and establish logical connections. Computers constantly refresh various records with their unparalleled advantages of convenience, accuracy, efficiency, convenient storage, and ease of modification [4]. In recent years, the rapid development of multimedia technology and the continuous upgrading of software have provided broad prospects for the widespread application of computers in the field of design and performance, multimedia technology has not only brought a revolution to stage visual expression in a new form, but also brought about significant changes in people's aesthetic concepts.

With the popularization of computer network technology, its application in computer teaching, making it play the role of intelligent auxiliary education, has been comprehensively carried out in teaching practice. As a teacher who has been engaged in computer teaching for many years, the author believes that if computer network technology is reasonably and effectively applied, it can indeed achieve the effective intelligent assistance of teachers in educating students, however, if not applied properly, there may also be some problems that need to be taken seriously.

II. Literature Review

The popularization of computer network technology has brought great convenience to people's lives and learning, and the status of computer education in school teaching is becoming increasingly high. The development of the times and technology has made the use of computers more widely distributed, the new generation of students must learn computer technology well in order to succeed in the competition of society. Computer network technology provides abundant learning resources for computer teaching, allowing students to gain richer knowledge in interactive environments, when students discover some problems in their studies, they can use powerful networks to search for the answers they need. Although computer network technology has brought great convenience to computer education in schools, it also has adverse influencing factors [5]. Therefore, the current main task is to fully utilize its advantages to eliminate some adverse

effects and fully utilize the function of network technology in computer intelligent assisted education.

Due to the current lack of emphasis on experimental courses in computer basic courses in some schools, there are very few class hours arranged, and there is a lot of experimental content, resulting in some students having difficulty mastering the experimental content. School affairs must increase the hours of experimental classes to exercise students' practical abilities and provide them with a deeper understanding of written knowledge, in order to enhance teaching efficiency [6]. The specific backup of computer data in the teaching of basic computer network technology courses is shown in Fig. 1:

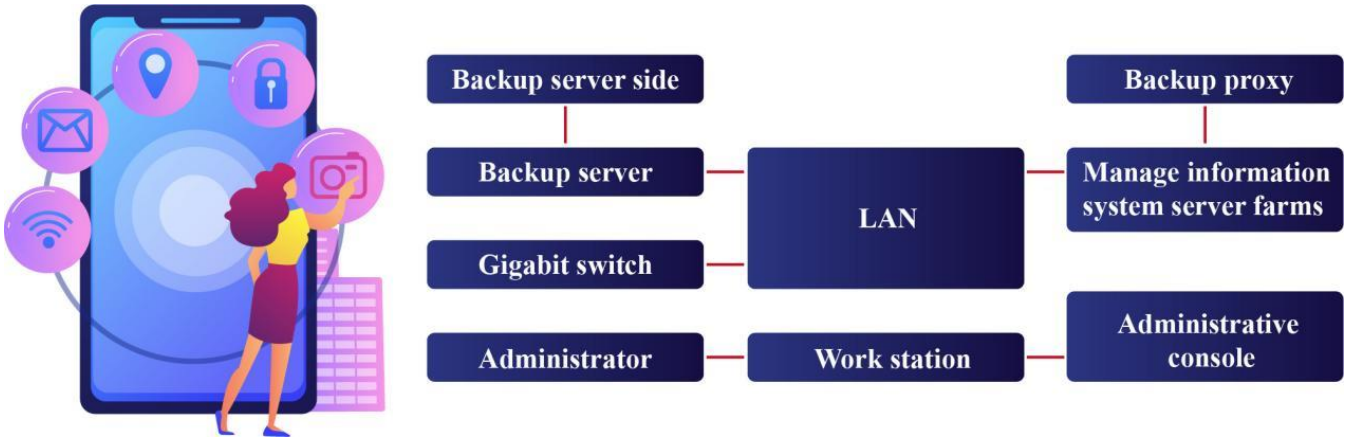


Fig. 1. Computer network technology data backup structure diagram.

With the development and application of network technology, China is gradually entering an era of "artificial intelligence". Nowadays, people's lives are filled with artificial intelligence internet products and IoT applications, which are the two mainstream directions for internet product aggregation. Take the speech recognition, facial recognition, and autonomous driving technologies currently used in China as examples, all of which are applications of artificial intelligence technology. On the other hand, with the development of information technology, the Internet of Things has also developed rapidly. Therefore, Y. Yu put forward the idea of creating artificial intelligence by combining the two new technologies. The article discusses the current state of smart internet development worldwide and predicts its development prospects [7]. With the widespread demand for intelligence in many industries, many people have begun to devote themselves to research, realizing its role in economic development and hoping to better support more businesses. Artificial intelligence speech technology is important for advertising and television news, it can improve the quality and performance of traditional voice, make it better for singing, radio advertising and recycling, and can serve the people better. Hu .M discussed the use and development of artificial intelligence technology in the context of integration, and studied its development performance, intelligent robot typing, intelligent face recognition, meaningful speech recognition, intelligent OCR recognition, automatic reporting, and other applications and developments [8]. Artificial intelligence technology, as an emerging and rapidly developing technology, has played a crucial role in many fields. In the power system, due to its complex organizational form, its deeper application in the power system is currently a challenge faced by the power system. In response to this issue, Han .X applied the concept of enterprise architecture to deeply analyze the architecture of power grid enterprises [9]. At the architectural level, they clearly planned the application of artificial intelligence in the architecture. By classifying business, application, technology, and data, artificial intelligence can be further applied in complex power systems. Finally, a successful application example in the power system is provided.

The author designs an interactive electronic technology computer-aided teaching system based on new media technology, with the aim of achieving interactive electronic technology computer-aided teaching.

III. Design of Interactive Electronic Technology Computer Aided Instruction System

A. System Hardware Design

In general, the client does not need to install any other software, just install and use the browser, reduce the connection between the server and the client, reduce the risk of exploiting the application code, and support the security of the database system.

According to the new technology, the interactive computer has a three-layer structure in the order of user interface layer, business selection layer, and data management layer. Teachers, students, and other users can access the system by entering their personal information in the user interface layer and accessing the selected business layer ; Teachers, students and other users can click on the application according to their needs in the business option layer, and the business option layer can change the message to the user to receive management information; The information management system selects the learning materials and integrates them according to the user's needs. Fig. 2 shows the three-step process of interactive computer-based technology [10].

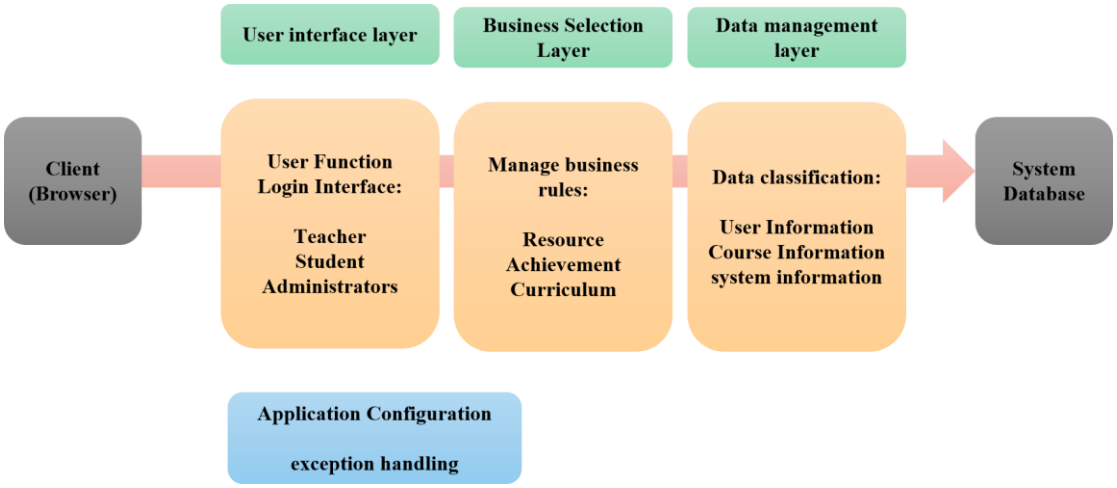


Fig. 2. Three-layer architecture diagram of the computer-aided teaching system of interactive electronic technology based on new media technology.

1) User interface layer: Users enter their personal information on the service's login interface and then click the submit button to enter the business selection process. End-to-end technology is used to complete user input and implement user input as quickly as possible in real-time. NET certificate plugin to prevent user theft and hacking [11].

2) Business selection process: After entering the business selection layer through the user interface layer, users can click on the application that suits their needs, and the business selection process redirects people to use configuration statements in the management layer. Business process options provide better access to information management through new technologies. Since there are some differences in the business preferences of users with different characters, let's take the management system as an example, Fig. 3 shows the management schematic diagram of the teacher application management system in the selected business process [12].

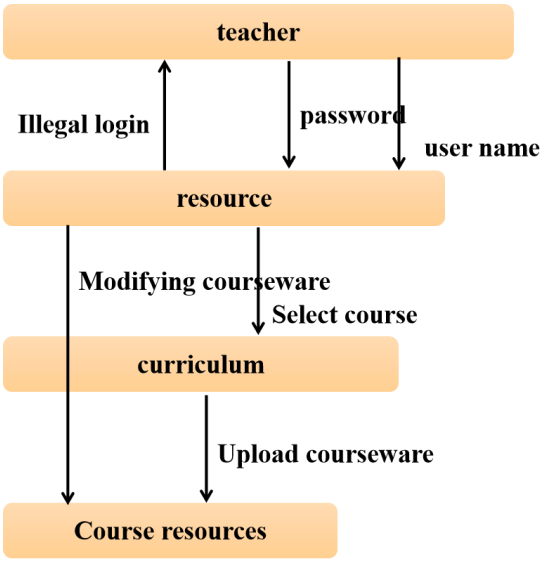


Fig. 3. Schematic diagram of the service selection layer resource management function.

In Fig. 3, the teacher enters the user name and password in the user interface layer to access the business process of the selection process, access the standard business level of the process selection process, you can choose the class or customize the product according to your needs, you can upload the material to the course materials for future study [13].

B. System Interactive Design

1) Interactive training: Interactive Learning A diagram of interactive computer learning as a new technology is shown in Fig. 4.

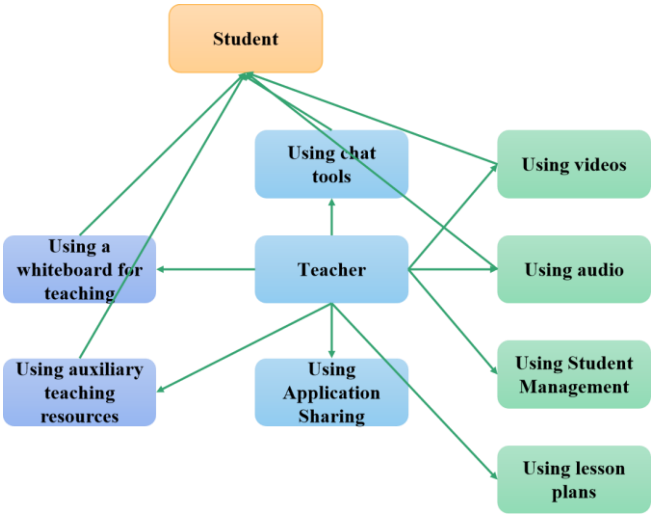


Fig. 4. Example of an interactive system.

Interactive instructions Use diagrams to illustrate the interactive operation of the system. The newsletter shows that teachers are successfully communicating with students through interactive tools, video, audio, student management, lesson plans, sharing plans, smart teaching tools, and free lessons.

2) Information exchange: Interactive computer-aided design software based on new technologies, including interactive management servers, database servers, web servers, and node applications. The communication management server is used for intelligent support and

information exchange between study group members and groups, and its functions include the following [14].

Manage data versions: Join or delete study groups, manage courses.

Manage chats: Change the chat information sent to different groups of users by all users.

Node operations include: Receiving, duplicating, compressing, decompressing, searching, and transmitting video and audio data; Distribute research materials requested by the group; Group information management; Communicate information in conversation.

C. Research on Recommended Learning Algorithms

The coordinated filtering algorithm compares the specific behavior of a user (such as rating, viewing frequency, viewing time, resource collection, download collection, etc.) with the operational behavior of other users, this enables the identification of neighbors whose behavior is closest or similar to that of the target user, the system will automatically analyze the behavior of these similar neighboring users, and after the analysis is completed, the system will recommend specific content of interest between neighboring users to the target user [15]. Therefore, the Collaborative filtering recommendation algorithm is based on the following assumptions: (1) Users have similar interests and hobbies. (2) The user's interests and hobbies can maintain a certain degree of stability and continuity within the same time period, and will automatically predict the user's specific interest needs based on their historical operational behavior. Collaborative filtering recommendation algorithms can be divided into the following two categories: (1) User based Collaborative filtering recommendation; (2) Collaborative filtering recommendation based on specific projects. Among them, the central idea of user based Collaborative filtering recommendation is that there is a certain degree of similarity between the operating behaviors of different users, for example, the operating behaviors of users A and B are very similar, user A operates specific resource A, and user B will also have a high probability to select resource A [16]. The central idea of Collaborative filtering recommendation based on specific projects is that there is a certain degree of internal correlation between projects, for example, if user A selects items B1, B2, B3, and B4, there will usually be a certain degree of internal correlation between items B1, B2, B3, and B4. Most of the Collaborative filtering systems based on specific items will use the scoring matrix of "user item" to distinguish the internal association between different items, the system will automatically calculate the final score of a user on an item through this internal association, thus generating the final set recommended to target users.

The quality of nearest neighbor selection can directly determine the accuracy of the final information resource push, therefore, the generation of nearest neighbors is the core and key of this algorithm. The author used Pearson's correlation coefficient to calculate the degree of familiarity between users. Therefore, the familiarity between user U_a and user U_b is represented by the following Eq. (1):

$$sim(User_a, User_b) = \frac{\sum_{n=1}^{N}(r_{a,n} - \bar{r}_a)(r_{b,n} - \bar{r}_b)}{\sqrt{\sum_{n=1}^{N}(r_{a,n} - \bar{r}_a)^2}\sqrt{\sum_{n=1}^{N}(r_{b,n} - \bar{r}_b)^2}} \quad (1)$$

In Eq. (1) above, $r_{a,n}$ represents the final rating of user U_a on a resource project $Item_n$; $\bar{r}_a$ represents the average score of all resource projects evaluated by user U_a.

The project-based Collaborative filtering algorithm can perform similarity calculation offline, and Top-N recommendation can be used when the nearest neighbor user set is finally selected, this recommendation refers to the set of N users with the highest similarity as the closest neighbors. Afterwards, the general formula 'prediction' can be used to calculate the current user's level of interest in any specific resource project. At the same time, sort the predicted interest levels and ultimately recommend the N resource projects with the highest interest level to the target user u.

Therefore, we can assume that the set of resource items that user u has rated is S_u, therefore, the predicted interest level of user u in any resource item j is represented by Eq. (2) as follows:

$$prediction_{uj} = \bar{r}_u + \frac{\sum_{i=1}^{n} sim(u,i)(r_{i,j} - \bar{r}_i)}{\sum_{i=1}^{n} |sim(u,i)|} \quad (2)$$

In Eq. (2), $\bar{r}_u$ represents the average score of users on the evaluated resource projects; $\bar{r}_i$ represents the average score of neighbor i; r_{ij} represents the evaluation score of neighbor i on resource project j; Sim (u, i) represents the degree of similarity between user u and user I [17].

IV. System Testing

Let's take a class of some 2nd year students as an example. This system is used in school information technology. Boys, students and teachers access the system through the user interface and perform six functions: user management and permission management. The tests in Table I show that the results of the application of six different systems are consistent with the results and exceed the performance of the system [18].

The self-efficacy index is used to determine the effectiveness of students in controlling their own behavior, which reflects their ability to learn independently [19]. In this part of the experiment, self-efficacy groups and low-efficacy groups are used to determine how the learning process interacts among students and whether teachers have a positive effect on students after using this method (Fig. 5).

TABLE I. FUNCTIONAL TEST RESULTS OF THE SYSTEM MODULE

System module function settings in this article	Optimum effect	Application results of this system
user management	If the user's login information is incorrect, it will be displayed immediately	Meet the ideal effect
Administrator permission test	Edit user information for students and teachers	Meet the ideal effect
Students' autonomous learning	Choose a course to study, test, etc. and take the test yourself	Meet the ideal effect
Application of Student Courseware	Students can choose their own courses to complete their online course	Meet the ideal effect
Teacher Course Management	Teachers can edit the relevant content of their courses	Meet the ideal effect
Teacher Q&A interaction	Teachers can respond to students' uploaded questions online	Meet the ideal effect

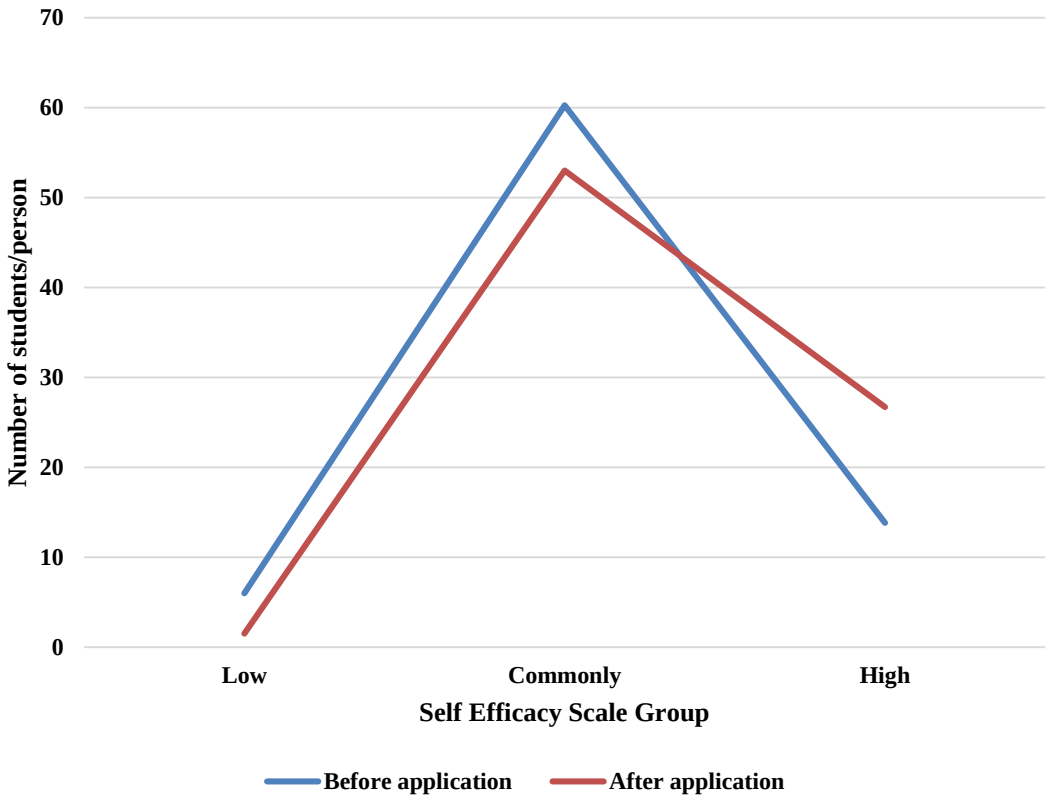


Fig. 5. Results of the system application effectiveness test (before and after application).

Fig. 5 shows that after implementing the system, the number of students with high self-reliance increased from 11 to 21, and the percentage increased from 21.4 to 34.8. By using this system, it can be understood that the number of students with good personal performance has increased [20-21]. A slight decrease in the number of students with high self-efficacy and self-efficacy after using this method indicates that the interactive learning method improves students' self-efficacy, improves their own learning, and takes advantage of this system.

V. CONCLUSION

The author of interactive design of intelligent computer technology helps to introduce new technologies, including the user interface layer, business-level options and information management systems, to achieve the intelligent technology technology support manual; Analyzing interactions in computer-based learning through interactive learning and information sharing. After testing the system, it can be seen that the number of students with high self-efficacy increased from 11 to 21 and the percentage distribution increased from 21.4 to 34.8 after applying the method described in this article. interactive teaching of the process improved students' self-reliance and independent learning; Also, applying the results of this system to six different activities will achieve ideal results, and the system has strong interactions and high resistance.

REFERENCES

[1] Shen, Y. . (2021). The application of artificial intelligence in computer network technology in the era of big data. International Conference on Computer Technology and Media Convergence Design. IEEE, 34(14), 12197-12210.

[2] Geng, L. . (2021). Application status and development suggestions of big data technology in petroleum engineering. Petroleum Drilling Techniques, 49(2), 72-78.

[3] Cui, H. , & Peng, Z. . (2021). Application of artificial intelligence wearable technology in the big data analysis of physical activity in china. Mobile Information Systems, 81(18), 25541-25556.

[4] A, J. L. , A, J. B. , & A, M. F. S. . (2021). Adaptive business intelligence platform and its contribution as a support in the evolution of hospital 4.0. Procedia Computer Science, 52(8), 9334-9352.

[5] Jingzhou, J. , & He, Y. . (2021). Application of artificial intelligence in computer network technology. Journal of Physics: Conference Series, 1881(3), 032073 (5pp).

[6] Zhang, J. . (2021). Computer assisted instruction system under artificial intelligence technology. Pediatric obesity., 16(5),58-59.

[7] Hu, M. , Xiang, Z. , & Li, K. . (2021). Application of artificial intelligence voice technology in radio and television media. Journal of Physics: Conference Series, 2031(1), 012051-.

[8] Han, X. , Zheng, G. , Jin, B. , Zhou, M. , Chen, Q. , & Xu, Z. , et al. (2021). Application of artificial intelligence technology in power grid enterprises based on enterprise architecture method. Journal of Physics: Conference Series, 1756(1), 012016 (6pp).

[9] Hanjie Sun, "Interactive Knowledge Visualization Based on IoT and Augmented Reality", Journal of Sensors, vol. 2022, Article ID 7921550, 8 pages, 2022.

[10] Xiang, Y. . (2021). Exploration of the application of artificial intelligence technology in mechatronics technology based on. Journal of Physics: Conference Series, 1915(2), 022059 (8pp).

[11] Wei, S. , Huang, P. , Li, R. , Liu, Z. , & Zou, Y. . (2021). Exploring the application of artificial intelligence in sports training: a case study approach. Complexity, 8(8), 1428-1439.

[12] Schaebe, H. , & Braband, J. . (2022). The application of artificial intelligence in railway technology for safety-relevant applications - opportunities and problems. Signal und draht,74(5), 114.

[13] Lu, Z. , & Nam, I. . (2021). Research on the influence of new media technology on internet short video content production under artificial intelligence background. Complexity,103(1), 1363-1373.

[14] Meng, Q. . (2021). Research on the application of computer network technology under the background of artificial intelligence cloud technology. Journal of Physics: Conference Series, 1802(4), 042067-.

[15] Gao, X. , Li, Q. , & Liu, F. . (2021). Research on the new normal technology and application of artificial intelligence in the internet of things. Journal of Physics: Conference Series, 1865(4), 042062-.

[16] Ye, J. . (2021). Talking about the application analysis of electronic information technology in the internet of things. Journal of Physics: Conference Series, 1827(1), 012011 (7pp).

[17] Chen, X. . (2021). Research on the application of artificial intelligence technology in the field of sports refereeing. Journal of Physics: Conference Series, 1952(4), 042048-.

[18] Murino, T., Nardo, M. D., Pollastro, D., Berx, N., Francia, A. D., Decré, W., ... & Pintelon, L. (2023). Exploring a cobot risk assessment approach combining FMEA and PRAT. Quality and Reliability Engineering International, 39(3), 706-731.

[19] Chen, L. . (2021). Application of artificial intelligence technology in personalized online teaching under the background of big data. Journal of Physics Conference Series, 1744(4), 042208.

[20] Zhou, Y. . (2021). Research of artificial intelligence in computer network technology. Journal of Physics: Conference Series, 2083(4), 042082-.

[21] Lv, X. , & Li, M. . (2021). Application and research of the intelligent management system based on internet of things technology in the era of big data. Mobile Information Systems, 28(10), 6587-6605.

Blockchain-Enhanced Security and Efficiency for Thailand's Health Information System

Thattapon Surasak
Department of Computer and Information Science, Faculty of Applied Science
King Mongkut's University of Technology North Bangkok, Bangkok, Thailand

***Abstract*—This study seeks to enhance the security, efficiency, and usability of Thailand's health information system through the integration of blockchain technology and a user-friendly web application. Blockchain's inherent strengths in secure data storage and sharing make it particularly well-suited for addressing the critical challenges of healthcare data management. Currently, Thai citizens face significant barriers when seeking medical treatment across multiple hospitals, as they must manually request and transfer both their Electronic Medical Records (EMRs) and paper-based medical records. This fragmented system creates delays and inefficiencies, as each hospital operates its own isolated data silo. To overcome these challenges, this study proposes a solution utilising a private blockchain to securely store and manage patient medical histories and prescriptions. This approach ensures data integrity while implementing robust authorisation mechanisms to restrict access to sensitive information exclusively to verified individuals. The system's security is further strengthened by blockchain's encryption features and the use of smart contracts. A well-designed web application serves as the interface between the secure blockchain database and end-users, offering a seamless experience for both healthcare providers and patients. In addition, User Experience (UX) testing was conducted with healthcare providers to assess the system's usability and functionality. The results highlight the system's user-friendly interface, confirming its potential for widespread adoption. By fostering efficient, secure, and patient-centric health information exchange, this study has the potential to significantly enhance healthcare delivery and outcomes in Thailand.**

***Keywords*—Blockchain technology; healthcare information system; Electronic Medical Records (EMRs); user experience (UX) testing; web application; data security**

I. Introduction

The digital transformation of healthcare systems has brought significant advancements in patient care, enabling more efficient diagnosis, treatment, and management of health conditions. However, this shift towards digital systems has also highlighted several critical challenges, particularly in the areas of managing and securing sensitive medical data [1]. While the adoption of electronic health records (EHRs) and other digital tools has improved the accessibility of patient information and streamlined healthcare processes, it has also introduced new complexities in ensuring data privacy, interoperability, and compliance with regulatory standards. The rapid expansion of healthcare data, coupled with increasing cyber threats, has made it essential to implement robust solutions for safeguarding patient information and ensuring the seamless exchange of medical data across different healthcare providers and institutions [2].

Thailand's healthcare system faces unique challenges stemming from infrastructural, administrative, and technological limitations, which are compounded by the fragmented handling of both digital and paper-based medical records [3], [4]. Patients frequently encounter inefficiencies when seeking care across multiple hospitals, as they must manually request and transfer their medical records, leading to delays in treatment and posing risks of incomplete information for healthcare providers [5], [6]. Moreover, limited interoperability between data systems and fragmented administrative structures exacerbate these issues, creating bottlenecks in the seamless exchange of critical patient information [7].

Concerns regarding infection control and the management of patient movement within healthcare facilities further highlight the urgent need for secure, real-time access to medical data. Blockchain technology, with its decentralised architecture and capacity for creating immutable records, offers a robust solution to these challenges. By integrating blockchain into Thailand's healthcare system, hospitals can streamline the sharing and retrieval of medical information, reduce administrative inefficiencies, and improve overall care quality. Furthermore, adopting blockchain technology aligns with ongoing efforts to modernise healthcare infrastructure and address gaps in service delivery, paving the way for a more patient-centred and efficient system [8].

Blockchain technology has emerged as a promising solution to these challenges, providing a decentralised and secure framework for data storage and exchange. A blockchain is a shared, distributed ledger that stores data across multiple nodes, ensuring that once information is recorded, it is extremely difficult to alter. This is achieved through cryptographic techniques and consensus mechanisms that validate data consistency across the network. While blockchain is often associated with cryptocurrencies such as Bitcoin, its applications in healthcare are particularly valuable due to its immutability, transparency, and robust data security features [9].

Among the many technological advancements, blockchain stands out for its unique ability to protect data from tampering and unauthorised access. Data is stored across a distributed network, allowing every member to access and verify information simultaneously, ensuring transparency. In the context of healthcare, blockchain can securely store patient records, safeguarding them against unauthorised modifications or breaches. Additionally, only authorised stakeholders, such as doctors and healthcare providers, can access these medical histories, enabling the provision of more continuous and improved care. This study aims to demonstrate how blockchain technology can transform Thailand's health information system, resulting in better healthcare outcomes and an enhanced quality of life

for its citizens.

This proposed system utilises blockchain technology, specifically Hyperledger Fabric, to enable fast, secure, and seamless sharing of patient records. By integrating blockchain with a user-friendly web platform, the system enhances the efficiency of health data exchange in Thailand. Blockchain's encryption and smart contracts ensure that only authorised individuals can access patient information, thereby safeguarding data integrity. The system also significantly reduces the time required for transferring medical records between providers, facilitating faster and more accurate diagnoses and treatments. Furthermore, it empowers patients by granting them greater control over their medical data, representing a critical step towards a more patient-centric healthcare system.

The remainder of this paper is structured as follows: Section II provides a comprehensive review of previous studies in the field, examining the historical context of health information systems alongside recent advancements in blockchain technology for healthcare. Section III presents a detailed description of the design of the proposed system, highlighting the foundational principles of the blockchain-based solution. Section IV discusses the results, including the development of a user-friendly web application that interfaces with the blockchain. Finally, Section V synthesises the key findings, reflects on the contributions of this work to the field, considers its broader implications, and outlines promising directions for future research.

II. Related Work

Blockchain technology is increasingly being studied for its potential to address critical challenges in healthcare, particularly in securing sensitive patient data, ensuring interoperability, and enhancing the transparency of medical record transactions. Amid the ongoing challenges posed by fragmented record-keeping systems, blockchain offers a decentralised solution that balances privacy with real-time accessibility to medical data [10].

Early applications of blockchain in healthcare included MedRec, a system designed for managing Electronic Medical Records (EMRs). Leveraging Ethereum and smart contracts, MedRec aimed to facilitate the secure sharing of patient data among healthcare providers. By addressing data silos while maintaining patient control over access, it demonstrated blockchain's significant advantage: immutable record-keeping, which ensures the integrity of medical records [11]. Blockchain technology presents a solution to the fragmented nature of healthcare systems. At present, patient records are siloed within individual institutions, limiting the delivery of comprehensive care. By establishing a unified ledger, blockchain enables authorised providers to access and update patient records in real time. This enhanced interoperability has the potential to improve care continuity, reduce redundant testing, and minimise medical errors [12]. Blockchain technology addresses critical healthcare challenges related to data provenance and record integrity. Through its consensus mechanisms, all modifications to medical records are verified and permanently recorded, creating an immutable and auditable history. This enhances transparency and fosters trust among patients, providers, and institutions. By tracking who accessed or modified records and when, blockchain provides a robust solution for safeguarding the integrity of sensitive medical information [13]. In addition to enhancing security and transparency, blockchain's use of smart contracts has been extensively studied as a tool to automate and enforce access control policies. In healthcare settings, these programmable contracts enable sophisticated access control by verifying the credentials of healthcare providers and granting access to patient records only under predefined conditions. For instance, a doctor can access a patient's history only if directly involved in their care and appropriately authorised. This dynamic model minimises the risk of unauthorised access while facilitating necessary data interactions. As a result, smart contracts improve both the security and efficiency of managing sensitive medical information [14], [15]. Permissioned blockchains, such as Hyperledger Fabric, have significantly enhanced blockchain's applicability in healthcare. Unlike public blockchains, these systems restrict network access to known and trusted participants, addressing the critical need for privacy in healthcare environments. Hyperledger Fabric's modular architecture supports secure transactions and smart contract integration while maintaining stringent control over access to medical records. This makes it particularly well-suited for healthcare settings, where confidentiality is paramount. Studies confirm its viability for applications requiring controlled viewing and updating of medical records [16]. However, storage limitations remain a challenge, especially when dealing with large volumes of medical data. While blockchain excels at storing transaction records and hashes of medical data, storing actual medical records on-chain is inefficient and costly in terms of both storage and computation. To overcome these limitations, hybrid systems combining blockchain with traditional relational databases, such as MariaDB, have been proposed. These systems store sensitive data on-chain while offloading larger, non-sensitive data to off-chain databases. This hybrid approach preserves the core benefits of blockchain, such as immutability and security, while addressing the performance challenges associated with large-scale data storage [17], [18].

In conclusion, blockchain technology has demonstrated significant potential in addressing key challenges in healthcare, particularly in the secure and efficient management of Electronic Medical Records (EMRs) [19]. The literature highlights blockchain's decentralised, immutable, and secure nature as a foundation for enhancing privacy, interoperability, and trust in healthcare data management [20]. Notable studies, such as MedRec, have explored the use of Ethereum and smart contracts for patient data sharing, while others have investigated the integration of blockchain with IoT systems for real-time data collection and the secure management of medical information [16]. However, despite its advantages, blockchain faces limitations, including scalability and storage constraints, which must be addressed for broader adoption. To mitigate these challenges, hybrid systems combining blockchain with traditional databases, such as MariaDB, have been proposed. These systems store sensitive data on-chain while offloading larger, non-sensitive data to off-chain databases, thereby maintaining performance without compromising security.

This proposed system builds on these foundations, leveraging Hyperledger Fabric, a permissioned blockchain specifically designed to provide robust security and privacy in a decentralised environment. Unlike Ethereum, which incurs transac-

tion fees, Hyperledger Fabric is open-source and free from such costs, making it a more practical choice for healthcare applications [21], [22]. Its modular architecture enables the integration of smart contracts to control access to EMRs, ensuring that only authorised individuals can view or update sensitive medical information [23], [24]. The design of the Blockchain-Based Healthcare Information System (discussed in Section III) combines blockchain with a user-friendly web application, offering seamless access to EMRs while maintaining the highest levels of security. By employing smart contracts and a hybrid storage solution, this proposed system addresses the limitations identified in previous systems. This approach not only ensures the integrity of patient records but also enhances data sharing between healthcare providers, enabling faster diagnoses and more accurate treatments. Furthermore, this study advances the existing literature by demonstrating how blockchain, when integrated with modern web technologies and efficient storage solutions, can resolve critical challenges related to data security, privacy, and interoperability in healthcare. Future work will focus on scaling the system to accommodate larger networks and incorporating advanced privacy-preserving techniques to further enhance the security of healthcare data.

III. Proposed System

The proposed Blockchain-Based Healthcare Information System (HIS) has been designed to address the inefficiencies and security vulnerabilities inherent in traditional centralised systems for managing Electronic Medical Records (EMRs). By leveraging Hyperledger Fabric, an open-source, permissioned blockchain, the system provides a secure and decentralised solution for managing patient records. Additionally, it enforces strict access control through the integration of smart contracts, ensuring that sensitive medical information remains accessible only to authorised individuals.

A. System Architecture

The system consists of three primary components:

1) Blockchain Database: The blockchain network forms the core of the system and is built on Hyperledger Fabric. This platform was selected for its numerous advantages over alternatives such as Ethereum, including its open-source nature, absence of transaction fees, and robust security features. Hyperledger Fabric's permissioned network restricts access to verified participants, ensuring that sensitive medical data can only be accessed by authorised users. Its modular architecture supports a wide range of applications, making it particularly adaptable for healthcare implementations.

2) Web Application: The web application acts as the interface between healthcare providers, patients, and the blockchain network. Designed with usability in mind, the platform enables users to log in, view medical records, and securely share data with healthcare providers. Real-time querying of the blockchain ensures rapid access to critical patient information, such as medical histories and prescriptions. Access control is enforced by smart contracts, guaranteeing that only authorised users can interact with the data.

3) Smart Contracts: The system leverages Hyperledger Fabric's smart contracts, also referred to as chaincode, to implement business logic and control user access. Written in Java (as well as Go or Node.js), these smart contracts enforce user roles and permissions by verifying the identities of patients and healthcare providers through Hyperledger Fabric's identity management services. Additionally, they log all interactions with the blockchain, creating an immutable audit trail that ensures transparency, accountability, and data integrity.

B. Blockchain Architecture Design

The blockchain architecture is designed to store critical medical data securely while optimising performance. The system utilises a distributed ledger to store patient medical histories and prescriptions. Each transaction is recorded immutably, ensuring that once data is added, it cannot be altered. The system generates a unique transaction ID for each interaction, providing a secure and traceable history of all medical data exchanges.

Hyperledger Fabric was selected for its permissioned network, which ensures that only authorised participants can access the network. This feature is particularly important in healthcare, where patient confidentiality and data security are paramount. Unlike public blockchains, which allow anyone to participate, Hyperledger Fabric restricts access to known and verified participants, providing an additional layer of security. Each participant is assigned specific roles and permissions, ensuring that only those with the necessary credentials can interact with the blockchain.

The system employs chaincode (smart contracts) written in Java to manage user roles and control data access. For example, the chaincode verifies that a patient's identity matches their medical records before granting access. Additionally, it tracks and records every transaction on the blockchain, creating an immutable audit trail that ensures the integrity and transparency of the data.

C. Hybrid Data Storage Solution

To address blockchain's storage limitations, the system adopts a hybrid storage model. Critical and sensitive medical data are securely stored on the blockchain, leveraging its immutability and robust security features. Less sensitive information, such as metadata or general patient details, is stored in MariaDB, a relational database system. This hybrid approach alleviates the performance overhead associated with storing large volumes of data on the blockchain while ensuring the security of sensitive information. Furthermore, the system synchronises data between the blockchain and MariaDB to maintain consistency across platforms.

D. Security, Authentication Flow and Data Integrity

The system's security is built upon Hyperledger Fabric's cryptographic mechanisms and identity management features. Authentication is managed through public-key cryptography, with each user's identity verified by a certificate authority. This ensures that only authorised individuals can access or modify patient records, effectively preventing unauthorised access. Additionally, all interactions are securely recorded using smart contracts, creating a transparent and tamper-proof audit trail.

Hyperledger Fabric's consensus mechanism ensures that all nodes agree on the state of the ledger, safeguarding against malicious actors attempting to alter patient data. This is critical for maintaining the integrity of healthcare information, where accuracy is paramount for effective treatment decisions.

The system's authentication process begins with a user logging into the web application, which interfaces with the blockchain through smart contracts. The smart contract verifies the user's credentials against the blockchain's identity management system. Once authenticated, the user can query the blockchain to retrieve or update medical records. Each interaction is recorded as a transaction, validated by the blockchain's consensus mechanism, and subsequently added to the ledger.

IV. Results and Discussion

This section presents the results from the prototype implementation of a Blockchain-Based Healthcare Information System and discusses the implications of these findings in the context of existing healthcare information management. It includes an evaluation of the system's performance, security, and usability, with particular focus on the insights gained through User Experience (UX) Testing. The results provide a comprehensive view of the system's effectiveness in securely managing electronic medical records (EMRs) and its potential to enhance healthcare workflows. The findings also highlight areas for future development, including system scalability, performance optimisation, and user adoption strategies.

A. System Implementation Results

The developed system is a web application integrated with Hyperledger Fabric, a permissioned blockchain, to facilitate the secure sharing of Electronic Medical Records (EMRs). Both patients and healthcare providers can register and access the system. Patients are identified using their Thai 13-digit ID number during registration. Once logged in, they can securely upload and store medical records, such as medical certificates or treatment data, on the blockchain, ensuring safe and controlled access.

The implementation demonstrated that blockchain technology significantly enhances data security, access control, and transparency in healthcare. By decentralising medical data storage, it reduced the risk of unauthorised access and tampering. The blockchain's immutable nature ensured that any modifications to records were securely logged, providing full accountability. However, performance issues were observed, particularly slower transaction speeds during periods of high usage. To address this, a hybrid storage model, incorporating MariaDB for non-critical data, improved system performance. Security remained robust, with cryptographic protections and Hyperledger Fabric's consensus mechanism ensuring authorised access. Additionally, smart contracts enabled secure data sharing, giving patients greater control over who could access their records.

B. Main Features of the System

The main features of the system included:

1) User-friendly Interface: The web interface was intuitive, allowing users to easily upload and access their medical records. Patients could review their treatment history, drug allergy details, and medical certificates in real time.

2) Blockchain Integration: Critical data, such as medical histories, were stored securely on the blockchain using Hyperledger Fabric's cryptographic and consensus mechanisms, ensuring data integrity and security.

3) Hybrid Storage: To optimise performance, the system employed a hybrid data storage model, storing sensitive data on the blockchain while non-sensitive data was kept in a traditional relational database, MariaDB. This approach addressed blockchain's limitations in terms of storage capacity and performance.

4) Smart Contracts: The system used smart contracts to enforce access control, allowing only authorised users (doctors, medical staff, and patients) to view or modify the records. The smart contracts also recorded every transaction made, providing a transparent and immutable audit trail of interactions with the data.

C. System Performance and Security

The implementation demonstrated that using blockchain technology in healthcare offers significant improvements in data security, access control, and transparency. By decentralising medical data storage, the system mitigated the risk of unauthorised access or tampering. The blockchain's immutable nature ensured that any changes to patient records were securely logged and could not be altered, thereby providing full accountability for all medical interactions.

However, performance limitations were observed, particularly in terms of processing speed when handling larger volumes of transactions. Blockchain's inherently slower transaction times, compared to traditional relational databases, were noted, particularly during peak usage periods. The integration of a hybrid storage model helped alleviate some of these concerns by offloading non-critical data to the MariaDB database, which allowed the system to maintain adequate performance levels.

In terms of security, the blockchain-based system provided strong data protection through cryptographic techniques. The consensus mechanism employed by Hyperledger Fabric ensured that only authorised participants could access the network, and the use of smart contracts further guaranteed secure data sharing between stakeholders. Patients also benefited from increased control over their medical records, as they could directly manage who could access their data.

D. Prototype User Interface Design

The design of the Blockchain-Based Healthcare Information System focuses on providing an intuitive and secure interface that allows patients and healthcare providers to interact seamlessly with the blockchain-based backend system. Below are the key screens developed in the prototype, which demonstrate the core functionalities of the system: landing page, registration page, and medical record page.

1) Landing Page: Fig. 1 shows the Landing Page, the gateway to the Blockchain-Based Healthcare Information System. It features a clean, user-friendly interface for both patients and healthcare providers, offering clear options for logging in or registering with role-specific paths for easy navigation. The design emphasizes security and decentralised medical record management, assuring users that their healthcare data is securely handled. The page is crafted to ensure a smooth entry into the system, prioritising accessibility and ease of use.

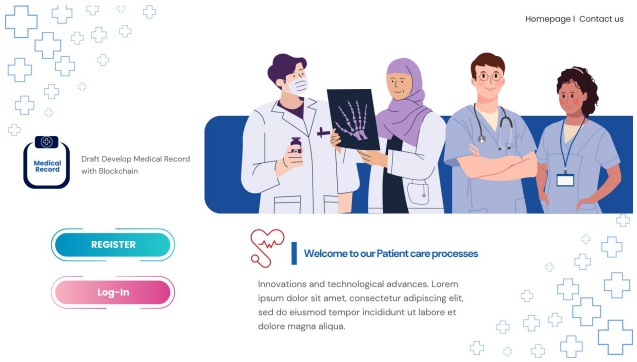


Fig. 1. Landing page.

2) Registration Page: Fig. 2 shows the Registration Page, where new users (patients or healthcare providers) can create an account and securely access the healthcare platform. The page collects personal and authentication details, such as name and email, while leveraging blockchain identity management for secure user verification. It employs a role-based access system, assigning distinct roles to patients and healthcare providers to control permissions. This ensures that only authorised users can view or manage sensitive medical records. Overall, the Registration Page establishes a secure foundation for verified and authenticated interactions within the system.

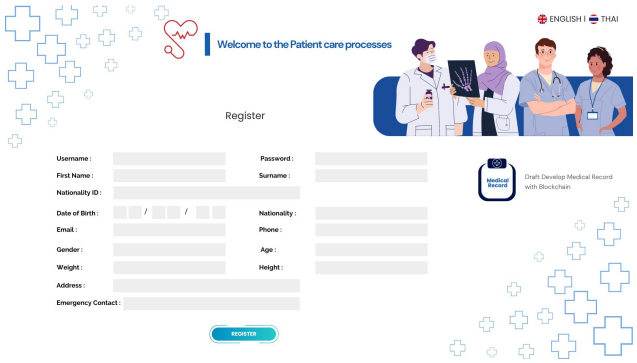


Fig. 2. Registration page.

3) Medical Record Page: Fig. 3 displays the Medical Record Page, the main interface where patients and healthcare providers manage Electronic Medical Records (EMR). Patients can securely view their complete medical history, while healthcare providers can upload and update records. These records are encrypted and stored on the blockchain, with access controlled by smart contracts, ensuring that only authorised users can view or modify the data. All interactions are logged for transparency and auditability, making the system both secure and efficient for enhancing patient care and experience.

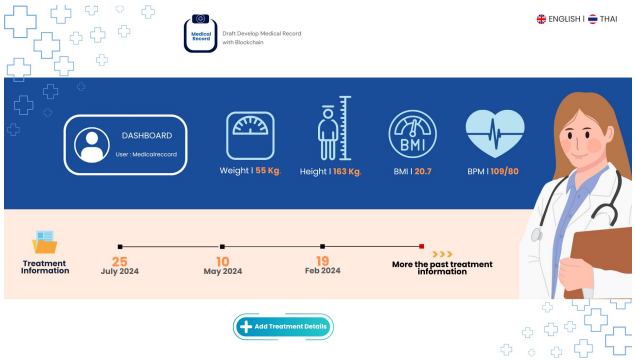


Fig. 3. Medical record page.

E. User Experience (UX) Testing

1) Testing Participants: The UX testing involved healthcare providers, including doctors and medical administrators, as the sole participants. They were tasked with logging into the system, uploading treatment records, querying medical histories, and managing access permissions for patient data. Synthesised patient profiles were used to simulate realistic medical interactions, ensuring the evaluation aligned with real-world use cases.

2) Key Findings: The key findings from the UX testing highlight the system's usability, efficiency, and security, as well as areas for improvement. These findings were based on the feedback from healthcare providers as they interacted with the system during various tasks:

- Ease of Use: Participants found the *landing page* intuitive, with clear navigation options for login and registration. The *medical record page* was effective in facilitating tasks such as uploading and retrieving medical records, which streamlined workflows and reduced administrative complexity.
- Efficiency: Real-time access to blockchain-stored data ensured healthcare providers could quickly retrieve treatment histories and prescription details, which was particularly beneficial for emergency care simulations. The hybrid storage model improved responsiveness when accessing non-critical data, as confirmed by positive feedback during high-usage scenarios.
- Security Perception: Healthcare providers appreciated the robust security features, including blockchain's encryption and immutable audit trails, which reassured them of the system's reliability for handling sensitive information.
- Challenges: A minor learning curve was observed among participants unfamiliar with blockchain technology, particularly during the initial onboarding phase. Slower transaction speeds were noted during simulated peak loads, indicating a need for further optimisation.

Suggestions for Improvement: Based on the key findings, several suggestions for improving the system were made to enhance its usability, performance, and scalability:

- Enhanced Onboarding: Developing tutorials or quick-start guides tailored to healthcare providers could improve initial system adoption.

- Performance Optimisation: Continued refinement of the hybrid storage model and transaction speeds is recommended to enhance usability during high-demand periods.

Conclusion: The UX testing demonstrated the system's potential to streamline healthcare workflows and securely manage medical records for healthcare providers. By leveraging synthesised patient data, the evaluation provided realistic insights into the system's usability and security features while avoiding ethical concerns associated with direct patient involvement. These findings highlight the system's readiness for broader adoption, with ongoing refinements aimed at improving scalability and performance.

F. Discussion

The prototype Blockchain-Based Healthcare Information System demonstrated significant improvements in the security and accessibility of Electronic Medical Records (EMRs) for healthcare providers. By leveraging blockchain technology and a hybrid storage model, the system ensured secure management of sensitive data while addressing performance limitations associated with blockchain's storage capacity. Feedback from healthcare providers during UX testing highlighted several strengths and areas for improvement.

1) Scalability: As the system grows, increasing data volumes may impact performance, particularly during peak usage periods. The integration of a hybrid storage model helped alleviate some performance issues, but future work should focus on refining consensus mechanisms and exploring advanced storage solutions such as distributed file systems or cloud integration.

2) User Adoption: The user-friendly interface was positively received by healthcare providers, who found the system intuitive and effective for managing medical records. However, a minor learning curve was noted, particularly for users unfamiliar with blockchain technology. Developing onboarding materials and tailored training programs could facilitate smoother adoption.

3) Legal and Ethical Implications: Although the system used synthesised patient data to evaluate its functionality, real-world implementation would need to address compliance with data privacy laws such as GDPR and HIPAA. Smart contracts for access control must be carefully designed to align with regulatory frameworks while ensuring secure and transparent data sharing.

These findings underscore blockchain's promise as a transformative technology in healthcare. The system's robust security features and transparent data management have the potential to streamline workflows and improve interoperability among healthcare providers. Nevertheless, addressing scalability, enhancing user adoption strategies, and ensuring regulatory compliance remain critical for widespread implementation. Future research should focus on scaling the system to support national healthcare networks and refining its performance for handling greater data volumes. Additionally, expanding UX testing to include diverse healthcare settings could provide deeper insights into its adaptability and effectiveness.

V. Conclusion

In the proposed solution, Hyperledger Fabric was chosen over the Ethereum platform for several reasons. One significant advantage is that Ethereum imposes transaction execution fees, whereas Hyperledger Fabric is an open-source platform that does not charge such fees, making it a more cost-effective choice for healthcare applications. Additionally, Hyperledger Fabric offers robust security features, which are crucial for handling sensitive medical data.

This study is pioneering in its design and development of a prototype for managing Electronic Medical Records (EMRs) using blockchain technology, specifically in the form of a Blockchain-Based Healthcare Information System. At present, most hospitals rely on centralised systems to store patient data, typically using conventional Relational Database Management Systems (RDBMS). However, this centralised approach poses significant challenges in sharing medical records, treatment histories, and other critical information between hospitals. The research serves as a proof of concept, demonstrating the benefits of blockchain in this context. Blockchain technology was found to provide a high level of security and protection for sensitive information, ensured through consensus mechanisms and collaboration among stakeholders.

Despite its advantages, the research identified some limitations of blockchain technology, such as restricted storage capacity and the need for continuous software updates across nodes or peers. To address these issues, a hybrid approach was adopted, combining blockchain with MariaDB. Critical data was stored on the blockchain, while general information was maintained in the MariaDB system. This approach mitigated performance issues and improved overall system efficiency.

User feedback from healthcare providers during system evaluation highlighted the system's usability and its potential to streamline healthcare workflows. The integration of a user-friendly interface with blockchain's secure backend ensures effective data management while maintaining accessibility. However, minor challenges, such as transaction speeds during peak usage and onboarding support for first-time users, should be addressed in future iterations.

Future research should focus on scaling blockchain-based healthcare systems for larger networks, such as national-level infrastructures, while optimising performance to handle greater data volumes. Enhancing storage solutions through the integration of distributed file systems, such as IPFS, or cloud storage could address blockchain's inherent limitations. Additionally, exploring alternative blockchain platforms may provide valuable insights into how different technologies perform in healthcare applications. Expanding evaluations to include diverse healthcare settings will further validate the system's adaptability and effectiveness.

In conclusion, the Blockchain-Based Healthcare Information System demonstrates blockchain's potential to revolutionise healthcare data management. By addressing current limitations and leveraging innovative solutions, the system has the capacity to enhance data security, improve interoperability, and streamline workflows, contributing to better healthcare outcomes for all stakeholders.

Disclosure and Conflicts of Interest

The author declares no conflicts of interest and has no financial interests to disclose. The author certifies that this submission is original work and is not currently under review by any other publication.

References

[1] J. Ishizaki, M. Yoshioka, and H. Nishimura, "Analysis and categorization for the standardization of medical referral document information," in *2020 9th International Congress on Advanced Applied Informatics (IIAI-AAI)*, 2020, pp. 808–809.

[2] E. Li, J. Clarke, A. L. Neves, H. Ashrafian, and A. Darzi, "Electronic health records, interoperability and patient safety in health systems of high-income countries: A systematic review protocol," *BMJ Open*, vol. 11, no. 7, 2021.

[3] T. Chintavoarn, C. Junma, and A. Thamchalai, "The guidelines for improving the effectiveness of the health link health information exchange system," *Journal of Arts Management*, vol. 7, no. 4, p. 1725–1740, Dec. 2023.

[4] T. Waroonkun and S. Prugsiganont, "Preventing the spread of covid-19 through environmental design in thai community hospitals," *Frontiers in Built Environment*, vol. 8, 2022.

[5] V. Aumpanseang, K. Suthiwartnarueput, and P. Pornchaiwiseskul, "Determinants affecting the health information sharing management and practice for patient referral in thailand: The perceptions of patients and healthcare professionals," *Perspect Health Inf Manag*, vol. 19, no. 4, p. 1b, Oct. 2022.

[6] S. Sawang, C. Y. Chou, and B. Q. Truong-Dinh, "The perception of crowding, quality and well-being: a study of vietnamese public health services," *Journal of Health Organization and Management*, vol. 33, no. 4, pp. 460–477, Jan 2019.

[7] S. Prugsiganont and T. Waroonkun, "Identifying built environment solutions, in thai community hospital outpatient clinics, to prevent the spread of covid-19," *IOP Conference Series: Earth and Environmental Science*, vol. 1101, no. 6, p. 062035, nov 2022.

[8] B. K. Seo, "Patient waiting: care as a gift and debt in the thai healthcare system," *Journal of the Royal Anthropological Institute*, vol. 22, no. 2, pp. 279–295, 2016.

[9] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61 048–61 073, 2021.

[10] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "Bbds: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, 2017.

[11] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016, pp. 25–30.

[12] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "Omniphr: A distributed architecture model to integrate personal health records," *Journal of Biomedical Informatics*, vol. 71, pp. 70–81, 2017.

[13] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, "Chapter one - blockchain technology use cases in healthcare," in *Blockchain Technology: Platforms, Tools and Use Cases*, ser. Advances in Computers, P. Raj and G. C. Deka, Eds. Elsevier, 2018, vol. 111, pp. 1–41.

[14] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction," *Journal of Medical Systems*, vol. 43, no. 10, p. 320, Sep 2019.

[15] R. Saranya and A. Murugan, "A systematic review of enabling blockchain in healthcare system: Analysis, current status, challenges and future direction," *Materials Today: Proceedings*, vol. 80, pp. 3010–3015, 2023, sI:5 NANO 2021.

[16] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021.

[17] K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, and Y. Yang, "Blockchain-based secure time protection scheme in iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4671–4679, 2019.

[18] K. Wisessing, P. Ekthammabordee, T. Surasak, S. C.-H. Huang, and C. Preuksakarn, "The prototype of thai blockchain-based voting system," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 5, 2020.

[19] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," *AMIA Annu Symp Proc*, vol. 2017, pp. 650–659, Apr. 2018.

[20] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J Med Syst*, vol. 40, no. 10, p. 218, Aug. 2016.

[21] Z. Ke and N. Park, "Performance modeling and analysis of hyperledger fabric," *Cluster Computing*, vol. 26, no. 5, pp. 2681–2699, Oct 2023.

[22] C. Melo, G. Gonçalves, F. A. Silva, and A. Soares, "A comprehensive hyperledger fabric performance evaluation based on resources capacity planning," *Cluster Computing*, vol. 27, no. 9, pp. 12 395–12 410, Dec 2024.

[23] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, "Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 536–540.

[24] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, 2018, pp. 264–276.

Automatic Generation of Comparison Charts of Similar GitHub Repositories from Readme Files

Emad Albassam
Department of Computer Science-Faculty of Computing and Information Technology
King Abdulaziz University, Jeddah, Saudi Arabia

***Abstract*—GitHub is a widely used platform for hosting open-source projects, with over 420 million repositories, promoting code sharing and reusability. However, with this tremendous number of repositories, finding a desirable repository based on user needs takes time and effort, especially as the number of candidate repositories increases. A user search can result in thousands of matching results, whereas GitHub shows only basic information about each repository. Therefore, users evaluate repositories' applicability to their needs by inspecting the documentation of each repository. This paper discusses how comparison charts of similar repositories can be automatically generated to assist users in finding the desirable repository, reducing the time required to inspect their readme files. First, we implement an unsupervised, keyword-driven classifier based on the Lbl2TransformerVec algorithm to classify relevant content of GitHub readme files. The classifier was trained on a dataset of readme files collected from Java, JavaScript, C#, and C++ repositories. The classifier is evaluated against a different dataset of readme files obtained from Python repositories. Evaluation results indicate an F1 score of 0.75. Then, we incorporate rule-based adjustments to enhance classification results by 13%. Finally, the unique features, similarities, and limitations are automatically extracted from readme files to generate comparison charts using Large Language Models (LLMs).**

***Keywords*—Multi-class classification; keyword-driven classification; rule-based classification; unsupervised classification; GitHub repositories; comparison charts**

I. Introduction

Publicly available code repositories are widely used for managing and sharing application source codes. Due to their publicity, external users can review and improve these repositories, increasing their quality. Therefore, software developers engaged in development projects rely on these repositories to achieve high reusability. One such widely used code repository platform is GitHub. A recent report shows that GitHub hosts 420 million repositories with over 100 million registered developers [1]. However, this tremendous number of repositories introduces the challenge of finding a repository that adequately satisfies the user's needs.

In recent years, there has been considerable interest in cataloging the growing number of public repositories to facilitate the search, identification, and selection of these repositories for end-users. Several supervised approaches have been investigated in which the available textual documentation of public repositories is collected, analyzed, and classified to address this problem (e.g. [2] [3]). However, such supervised approaches require human intervention to manually label large datasets for training. In contrast, unsupervised approaches do not require such manual efforts since they can learn hidden patterns from large datasets. Therefore, labeled data are not required. Although several unsupervised approaches for cataloging public repositories have been proposed (e.g. [4]), they focus on the problem of tagging them with a limited set of topics. Therefore, these topics do not represent all of the capabilities provided by the corresponding repositories. As a result, users often need to read the documentation of each repository to understand its capability. This makes manual searching for candidate repositories complex and time-consuming since users need to inspect and read the documentation associated with each repository to understand their advantages and limitations before deciding. We consider the case in which a user knows the type of repository they are looking for but not the exact, full features provided by the repository. Furthermore, without careful inspection of their documentation, users might neglect important features during repository selection, which might be decided to be necessary after adopting another repository lacking these features.

As a motivation example, Fig. 1 shows typical repository search results performed on GitHub, where the user search terms include "email client", and results are sorted based on best matches. This figure shows that the search results by GitHub include approximately 7.1k repositories that match the search terms. Furthermore, only basic information is displayed for each repository. The results include a list of topics for some repositories. However, repository owners set these topics manually, which can be incomplete, error-prone, or missing in many repositories [4]. Therefore, users need to inspect each repository individually by reading its documentation to assess its relevance to their needs. In addition, users might be aware only of a subset of the features and functionality they desire, neglecting other features that could be equally important during selection.

Concerning these challenges, this work contributes to the literature by discussing how comparison charts of similar GitHub repositories can be automatically generated from their readme files using unsupervised learning. Each comparison chart consists of a set of N user-selected repositories listing (1) each repository's provided features and functionality, (2) the commonality between these repositories, and (3) the limitations of each repository, thus minimizing the effort and time to inspect and compare these repositories individually. Second, we show how the predictive performance of the Lbl2TransformerVec algorithm [5] [6] [7], an algorithm for unsupervised document classification and retrieval, can be improved by rule-based adjustments to classify the content of readme files in cases where multiple classes have approximately similar scores.

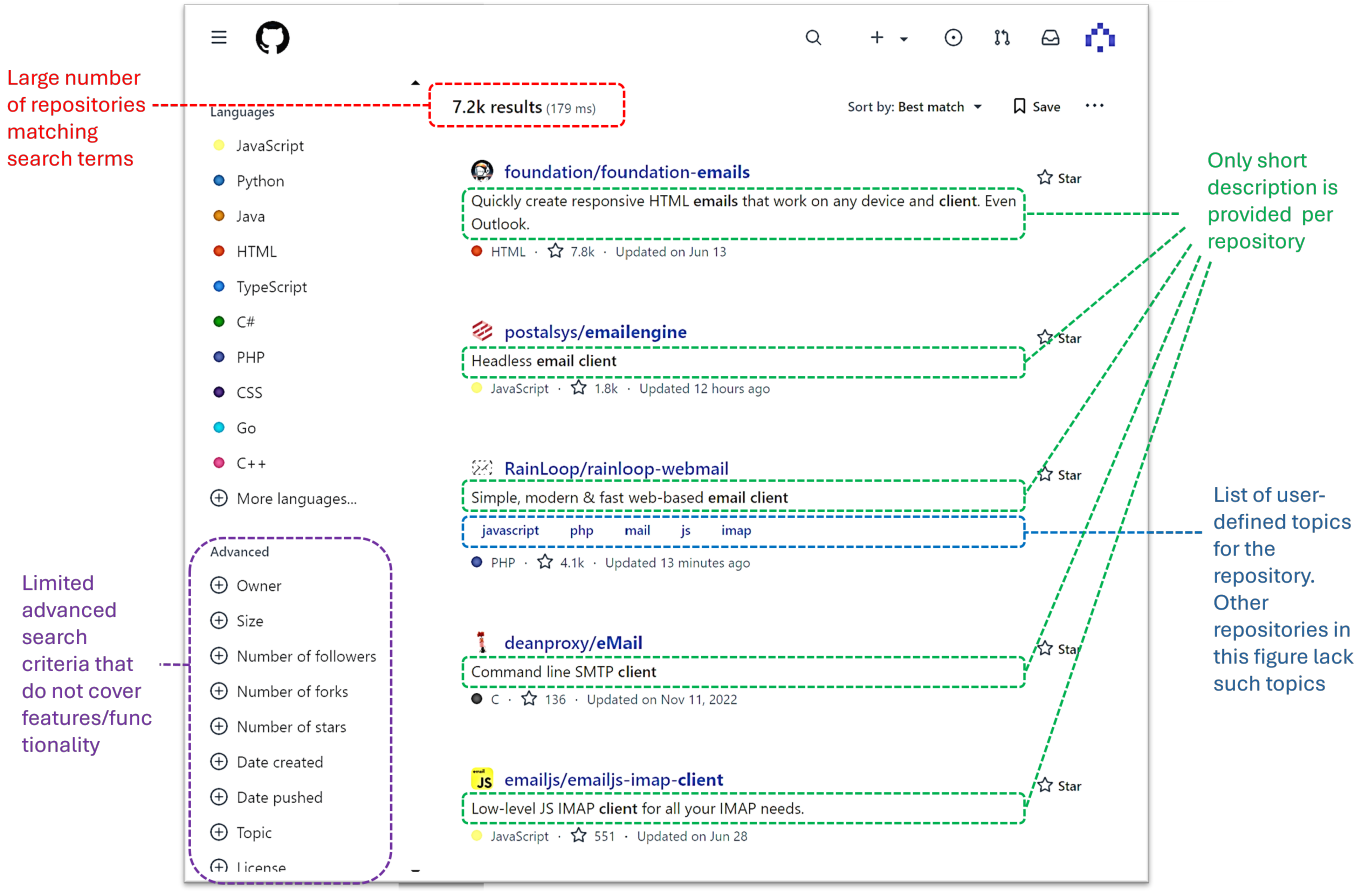


Fig. 1. An example of GitHub search results, with over 7.1k results satisfying user search terms.

The remainder of this paper is organized as follows. Section II contains the related works. Section III describes the architecture of the proposed. This includes data collection, preprocessing, and model training. Section IV presents our results of evaluating the various models incorporated to generate comparison charts. Section V discusses the strengths and limitations of the proposed solution and highlights future research directions. Section VI concludes our work.

II. Related Works

Many prior studies investigated the problem of analyzing GitHub repositories from their readme files. Work by Prana et al. [2] showed how a multi-label classifier can categorize GitHub readme files. Their approach labels the content based on eight categories: what, why, how, when, who, references, contribution, and others. The approach incorporates supervised learning where readme files obtained from GitHub repositories are manually analyzed and labeled. The work by Wu et al. [3] shows how repositories can be retrieved through functional semantics where readme files need to be manually inspected. Their dataset is based on JavaScript repositories. However, their data preprocessing involves the removal of many contents that are outside of functionality, including how to use the repository. Compared to these approaches, our work considers an unsupervised approach in which the training dataset is not labeled. Furthermore, we focus here on the comparison of different GitHub repositories.

Prior works have investigated different types of tasks related to GitHub repositories. Work by Zhou et al. [8] proposed an approach for recommending GitHub trending repositories. Sipio et al. [9] investigated a topic recommendation system of GitHub repositories, which repository developers can use to label their repositories correctly. However, their work uses a supervised model. Prior works have also considered categorizing GitHub repositories based on functionality [10] and application domains [11]. Compared to these works, we focus on comparing different repositories in a single artifact when users do not have the full knowledge of the features they seek in repositories. Although it is possible to tag software repositories from their bytecode and dependencies among them [12], such approaches are considered technology-specific. We consider in this work an approach that relies on textual readme files, which makes it applicable to any repositories with such files [13]. The work of Zhang et al. [4] presented a keyword-driven hierarchical classification of GitHub repositories to assign topic labels to GitHub repositories. Their work is unsupervised but requires users to provide one keyword for each class. Although topics play a significant role in the cataloging of repositories, this work considers a different problem where similar repositories need to be compared.

Several prior works investigated the nature and quality of documentation available in GitHub repositories. Results of Liu et al. [14] show that readme files of open-source Java projects do not align with GitHub guidelines. Furthermore, work by

Venigalla and Chimalakonda [15] shows that the presence of readme files, lists, images, and links increases the popularity of repositories. The work by Treude et al. [16] provides an assessment of documentation quality in ten dimensions, where their results show that documentation of various artifacts such as references, documents, and articles are different in terms of quality. Elazhary et al. [17] investigated GitHub developer contribution guidelines through a mixed-method study of 53 GitHub projects, where their results show that approximately 68% of these projects diverge significantly from the expected process model. Venigalla and Chimalakonda [18] investigated software documentation on GitHub and showed that multiple software artifacts can contribute to documentation. Work by Hellman et al. [19] proposed an approach for generating GitHub repository descriptions. Their analysis showed that descriptions of GitHub repositories are poor due to a lack of purpose in their description. These works clearly show the challenges associated with analyzing the documentation of publicly available repositories, such as lack of standardization and quality immaturity. This paper investigates several such challenges to generating meaningful comparison charts to end users.

Table I summarizes the research limitations identified in prior works. While all prior works focus on individual repositories to generate topics, the proposed approach considers the generation of comparison charts of multiple repositories. This approach is not limited to identifying the features provided by repositories but also identifies their commonalities and limitations, which, to the best of our knowledge, have not been investigated previously in prior works.

TABLE I. LIMITATIONS OF LITERATURE

Ref.	Limitations
[2]	• Supervised learning approach requiring manual labeling of the training set. • Proposed approach does not consider comparison of different repositories and does not extract unsupported features/functionalities of repositories.
[3]	• Manual inspection of GitHub readme files. • Manual removal of all sections in readme files except sections related to functionality. • Proposed approach does not consider comparison of different repositories and does not extract unsupported features/functionalities of repositories. • Dataset is limited to Javascript repositories.
[4]	• Proposed approach requires user providing one keyword for each class as guidance (Although a keyword enrichment process module is incorporated to expand the single keyword to a keyword set for each category). • Proposed approach does not consider comparison of different repositories and does not extract unsupported features/functionalities of repositories. • Dataset is limited to Machine Learning and Bioinformatics domains.
[13]	• Featured topics may neglect detailed functionalities provided by repositories. Thus, users still need to inspect individual readme files to understand their capabilities. • Featured topics may evolve, which may require retraining of the supervised models. • Proposed approach does not consider comparison of different repositories and does not extract unsupported features/functionalities of repositories.
[10]	• Proposed approach is semi-automated, with steps requiring manual human intervention. • Functionalities are extracted from readme file segments by computing the similarity between the segments and a short 1-2 lines of description from the repository's homepage, which may result in missed functionalities. • Proposed approach does not consider comparison of different repositories and does not extract unsupported features/functionalities of repositories.
[20]	• Proposed approach recommends trending repositories for developers based on their historical commits on GitHub (i.e. does not target general users of GitHub). • Proposed approach does not consider comparison of different repositories and does not extract unsupported features/functionalities of repositories.

III. AUTOMATIC GENERATION OF COMPARISON CHARTS

This section first provides an overview of the proposed solution for generating comparison charts from GitHub readme files. Then, we discuss each process within the architecture, including data collection, data preprocessing, and model training processes, where the goal is to implement a multi-class classifier capable of classifying the sections of a given GitHub readme file that are likely to contain the features and functionalities provided by the corresponding repository. We then discuss each process related to the automatic generation of comparison charts.

A. Overview of Proposed Solution

The architecture of the proposed solution (see Fig. 2) consists of two modules: offline and online. The offline module is performed once to train a multi-class classifier capable of classifying the contents of readme files obtained from GitHub repositories. The model is keyword-driven and is trained to classify the various sections based on the likelihood of containing relevant information for constructing comparison charts. The model is complemented with rule-based heuristics to adjust the classifier's results when multiple classes have approximately close scores by the classifier.

On the other hand, the online module is responsible for generating comparison charts of GitHub repositories that satisfy the user search terms. First, this module performs a live search of GitHub repositories using user-provided search terms. The user then selects N repositories from the search results they wish to compare. The online module then automatically retrieves the readme files corresponding to the user-selected N repositories and incorporates the hybrid classifier from the offline module to extract relevant sections required by subsequent processes. The online module then extracts relevant information, including provided features and limitations, from these sections and computes the similarity of features from the different repositories to generate comparison charts.

We describe each process in the architecture in the following subsections.

B. Automatic Data Collection

To prepare the dataset used in this work, we collected 283 readme files obtained from GitHub repositories. These

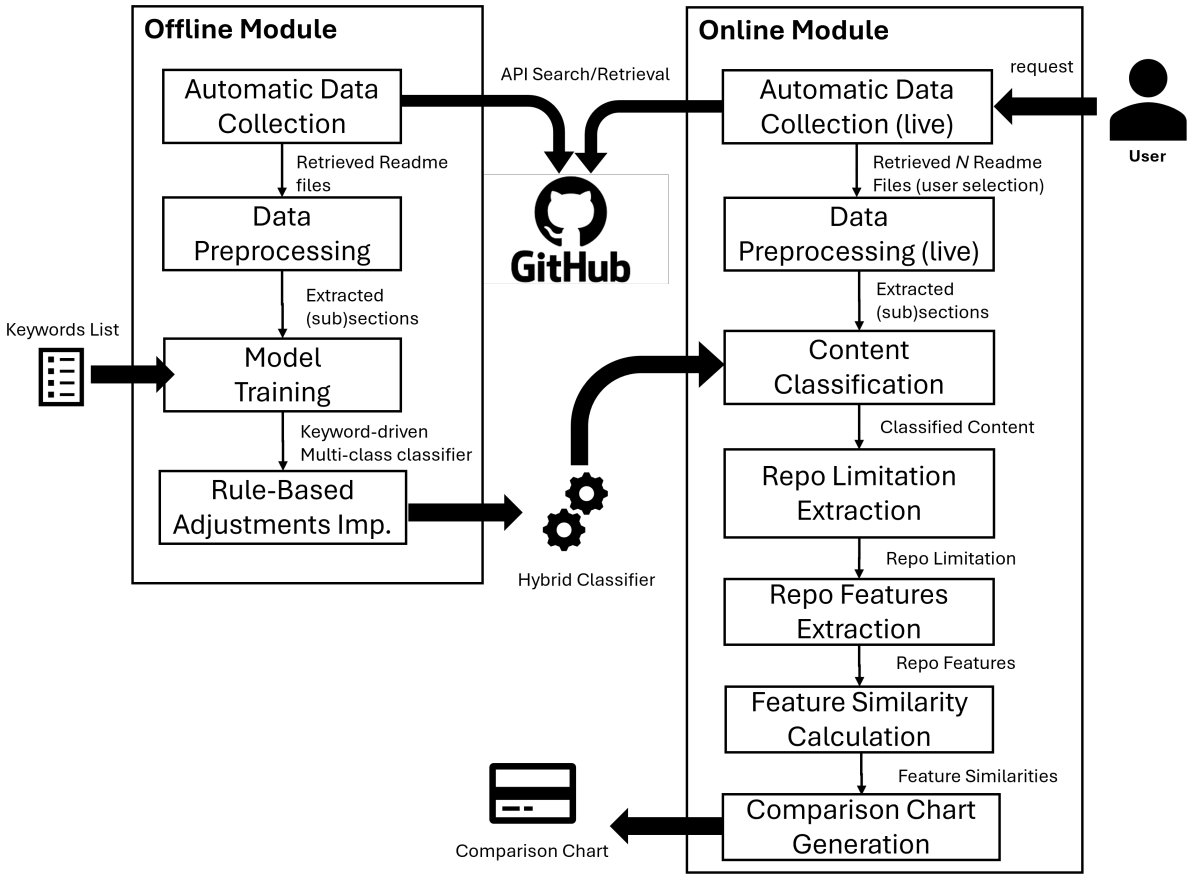


Fig. 2. An overview of the architecture for generating comparison charts.

files are collected automatically through GitHub's Representational State Transfer (REST) API for searching [21]. To ensure diverse coverage of repositories, we retrieve repositories whose primary programming language is Java, JavaScript, C#, Python, or C++. We obtain the readme files of the top 100 repositories for each of these languages, where the results are sorted in descending order based on repository stars. Then, we filter the results by including only the repositories with readme files written in English and exceeding 1000 bytes. These filtering rules aim to include only mature repositories with high stars, which increases the likelihood of obtaining well-written readme files.

We further split the collected readme files into two classes: training and testing. The training class contains the readme files corresponding to repositories whose primary programming languages are Java, JavaScript, C#, and C++. On the other hand, the readme files related to Python will be used for testing purposes to evaluate the hybrid classifier. By splitting the readme files based on the programming language, we decrease the likelihood of language bias during evaluation since our model is never trained on readme files related to the repositories related to the Python language. Table II summarizes the number of readme files collected from GitHub and shows the percentages of training and testing classes. As seen in this table, selecting the readme files related to the Python language as the testing class splits the collected readme files at an approximately 80:20 ratio.

C. Data Preprocessing

The contents of collected readme files are cleansed as follows. Embedded HTML tags and elements (such as HTML comments) are removed. All code blocks and URLs that appear in readme files are replaced with the constant strings *@code* and *@link*, respectively. Irrelevant content, such as images, task lists, color codes, and emojis, are removed.

After data cleansing, we extract the heading and content of all sections and subsections found in the readme files using regular expressions, which, according to GitHub formatting syntax [22], start with '#' symbols. Each extracted (sub)section represents an instance in our dataset. For each instance, we also record (1) the GitHub repository ID to maintain traceability between the instances and the files from which they were extracted, (2) the level of the (sub)section heading, which can range from 1 (i.e. a first-level heading) to 6 (a sixth-level heading), and (3) the order of the (sub)section in the document. Table III summarizes the number of instances obtained after preprocessing and instance extraction grouped by programming language. As can be seen, the training set accounts for 78.2% of the number of instances, while the testing set accounts for 21.5%.

D. Keyword-Based Model Training

After data preprocessing, we trained various keyword-driven models based on the Lbl2TransformerVec algorithm,

TABLE II. SUMMARY OF DATA COLLECTION PROCESS OF README FILES OBTAINED FROM GITHUB REPOSITORIES

Language	Total Number of Readme Files			Class	Pct.
	Initial	After Excl. Non-English	After Excl. files $<$ 1KB		
Java	100 files	45 files (55 files excl.)	43 files (2 files excl.)	Training	12.7%
JavaScript	100 files	73 files (27 files excl.)	71 files (2 files excl.)	Training	20.9%
C#	100 files	83 files (17 files excl.)	80 files (3 files excl.)	Training	23.6%
C++	100 files	81 files (19 files excl.)	78 files (3 files excl.)	Training	23%
Python	100 files	67 files (33 files excl.)	67 files (0 files excl.)	Testing	19.8%

TABLE III. SUMMARY OF EXTRACTED INSTANCES FROM COLLECTED README FILES

Language	No. of Instances	Class	Pct.
Java	617	Training	13.5%
JavaScript	1112	Training	24.35%
C#	977	Training	21.4%
C++	876	Training	19.2%
Python	984	Testing	21.55%

an algorithm for unsupervised document classification and retrieval that does not require stemming or lemmatization and can work on short texts [5] [6] [7]. For each model we train, we incorporate a different transformer, as shown in Table IV, where the goal is to evaluate the impact of the various transformers on the classifier's classification results. The models are trained on the training set corresponding to the Java, JavaScript, C#, and C++ instances (see Table II).

Our aim for the trained models is to classify the various instances in the dataset (i.e. sections obtained from readme files) into one of the following classes: Functionality, Usage, or Miscellaneous so that information required to construct the comparison charts can be obtained. The *Functionality* class represents instances about a repository containing statements such as an overview, high-level features or functionalities, a list of its advantages, how it compares to other solutions, and changes over different versions/releases. We consider that information in such sections highly relevant for constructing comparison charts. The *Usage* class represents instances corresponding to the how-to details, such as configuration, installation, and coding instructions related to a repository. Thus, these sections can provide additional information for constructing more detailed comparison charts. Finally, the *Miscellaneous* class represents instances corresponding to sections less relevant to comparison chart generation, such as user contributions and donations.

TABLE IV. MODELS INCORPORATED INTO LBL2TRANSFORMERVEC DURING TRAINING

Model	Ref./Model Card
bart-large-mnli	[23]
all-MiniLM-L6-v2	[24]
all-mpnet-base-v2	[25]
all-distilroberta-v1	[26]
all-MiniLM-L12-v2	[24]
unsup-simcse-bert-base-uncased	[27]
unsup-simcse-bert-large-uncased	[27]
unsup-simcse-roberta-base	[27]
unsup-simcse-roberta-large	[27]

To train the models, we pass the keywords list for each class to the Lbl2TransformerVec algorithm, shown in Table V. These keywords are chosen based on a combination of expertise and familiarity with GitHub readme files and by relying on a dictionary for word synonyms. For the Lbl2TransformerVec hyperparameters used to train the models, we set the *similarity_threshold* to 0.6 so that only instances with this threshold or higher with respect to the provided keywords are included to calculate the label embeddings. Furthermore, we set the *min_num_docs* parameter, which controls the minimum number of instances used to calculate the label embeddings, to 700. All other hyperparameters are set to their default values. Table VI provides the hyperparameter values used for training the various models.

After model training, to better understand their ability to classify the content of readme files, we run the models on the training dataset to classify all instances and then extract the most frequent words for each class. Fig. 3 plots the class-word distribution with a KxM shape, where K is 3, representing the number of classes, and M is the vocabulary size. As shown in this figure, the most frequent words for class 3 (i.e. sections classified by the model as Miscellaneous) include license, contributing, community, issues, and support, indicating the model's capability of labeling such sections. The most frequent words for sections labeled by the model as class 2 (i.e. Usage class) include *use*, *build*, *install*, and *run*. Finally, sections labeled with class 1 (i.e. Functionality) have as most frequent words the words *library*, *features*, *platform*, and *simple*, all of which are likely to appear in sections discussing the high-level functionalities and features of a repository. It can also be seen that several classes share some common frequent words such as *link* and *code*. This is because these words can appear in any section of these classes. For example, adding URLs pointing to external websites is a common practice for defining some terminologies or redirecting the user to extra resources to understand some functionality. Therefore, these URLs are part of Functionality. On the other hand, adding URLs in usage-related sections is also a common practice to refer users to more detailed installation documentation, configuration, and usage. Similarly, for the word *code*, readme files of many GitHub repositories can contain code snippets in the introduction, usage, and citation sections.

E. Rule-Based Classification Adjustments

During class prediction, the keyword-driven classifier may assign approximately similar scores to different classes for a section, which may result in incorrect classification for some of these sections. We incorporate rule-based adjustments to enhance classification results in such cases by considering the classes assigned to parent and sibling sections of a section i as follows.

Let i be a (sub)section in a readme file R, p^i be the predicted class for i, and p_2^i be the second most likely class for i as scored by the keyword-driven classifier. For any

TABLE V. KEYWORDS USED FOR MODEL TRAINING

Class	Keywords	Purpose
Functionality	Introduction, Intro, Welcome, Overview, Index, Compatability, Comparison, What's, New, Motivation, Contents, Feature, Provide, Contain, Supports, Definition, Goal, Overview, Roadmap, Release, Version, Vision, About, What, About, Simple, Fast, Reliable, Flexible, Modern, Powerful, Cross-Platform, Alternative	(Sub)sections labeled by the model with this class are likely to contain high-level features and functionality of the repository
Usage	Getting, Started, Demo, Try, Updating, Quick, Start, Code, Snippet, Steps, Commands, Configuration, Setup, Requirements, Install, Uninstall, Installation, Tutorial, Instructions, Documentation, Dependencies, Prerequisites, Manual, Example, Examples, Resources, FAQ, Usage, How, Import, Flags, Parameters, Arguments, Download	(Sub)sections labeled by the model with this class are likely to contain detailed functionality and usage information related to the repository
Miscellaneous	Contribution, Contributing, Contribute, Contributed, Partners, Sponsors, Authors, Backers, BibTex, Community, Mission, Feedback, Copyright, Disclaimer, Trademark, Credits, Publications, Conduct, DOI, Thank, Thanks, Please, Announcements, Legal, Subscribe, Issues, Contact, Join, Inquiries, Donation, Donate, Citation, Cite, Paper, Licensed, License, Help, Support Discussion, Social, Twitter, Telegram, Facebook, Discord, Forum, Backers, Acknowledgment, Acknowledgments, Company, People, Who	(Sub)sections labeled by the model with this class are less likely to contain important features and functionality of the repository

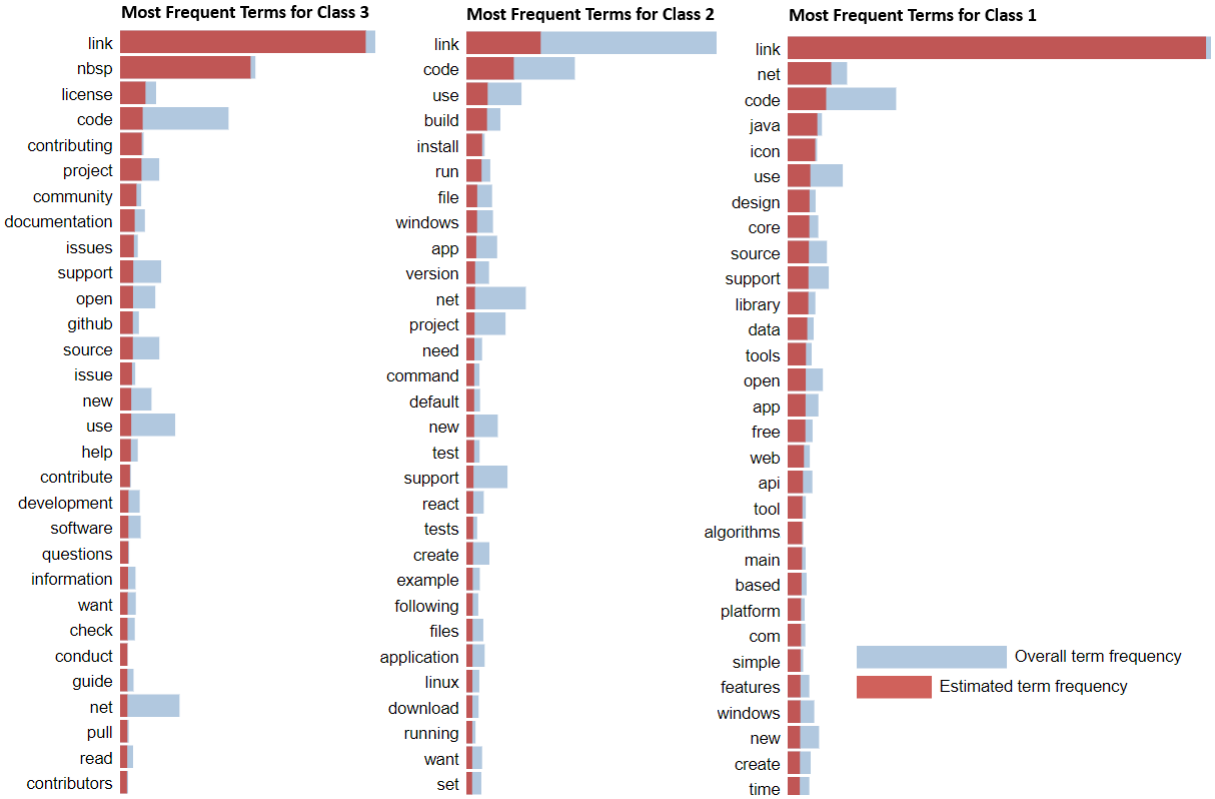


Fig. 3. Class-word distribution of training dataset for functionality (class 1), Usage (class 2), and miscellaneous (class 3).

TABLE VI. HYPERPARAMETERS PASSED TO LBL2TRANSFORMERVEC FOR MODEL TRAINING

Hyperparameter	Value
keywords_list	The keywords list shown in Table V
transformer_model	The models shown in Table IV
similarity_threshold	0.6
similarity_threshold_offset	default (0)
min_num_docs	700
max_num_docs	default (None)
clean_outliers	default (False)

(sub)section $i \in R$, if $|score(p^i) - score(p_2^i)| < \alpha$, then the following rules are applied, in the shown order, to adjust the predicted class for i:

1) Keywords ratio rule: The model computes the number of keywords (see Table V) that appeared in i for each class and then calculates the ratio of these numbers. If the ratio of class p_2^i is larger than a threshold β, then the predicted class of i is set to p_2^i.

2) Relevance to parent rule: The model considers the predicted class assigned to i's parent section. If (1) the parent section is classified as class p_2^i, (2) the parent section has a high keywords ratio for one class, (3) i has a low keywords ratio, and (4) α is negligible, then the predicted class of i is set to p_2^i.

3) Relevance to siblings rule: The model considers the predicted classes assigned to i's siblings (i.e. subsections at the same level as i) by calculating the class frequency of these siblings sections. If the most frequent class for these siblings is class p_2^i and this frequency exceeds a threshold β, then the predicted class of i is set to p_2^i.

To illustrate each rule and its purpose for adjusting classification, consider the examples shown in Table VII of erroneous classifications made by the keyword-driven model to some instances in the dataset:

- For instance 1, this instance discusses usage/documentation of the repository. However, the model classified this instance as *Miscellaneous*. Since the score difference between the actual and predicted classes is less than $\alpha = 0.04$ and this instance has more keywords related to the *Usage* class compared to other classes, then the model adjusts the predicted class for this instance from *Miscellaneous* to *Usage* according to the *keywords ratio* rule.
- For instance 2, this instance discusses usage details of a repository's functionality. However, the model classified this instance as *Features*. Since the score difference between the actual and predicted classes is less than $\alpha = 0.05$ and the model labeled the parent's section of this instance as *Usage*, then the model adjusts the predicted class for this instance from *Features* to *Usage* according to the *relevance to parent* rule.
- For instance 3, this instance provides users testimonials of the repository. However, the model classified this instance as *Functionality*. Since the score difference between the actual and predicted classes is less than $\alpha = 0.031$ and the most frequent class assigned by the model to sibling subsections is *Miscellaneous*, then the model adjusts the predicted class for this instance from *Functionality* to *Miscellaneous* according to the *relevance to siblings* rule.

F. Extraction of Repository Limitations

Repository owners may explicitly state in readme files the limitations of their repositories, such as unsupported features and functionalities or constraints related to operational environments. Such limitations must be identified so that they are not mistakenly classified as supported features by the proposed solution when generating comparison charts. Statements of such limitations in readme files may include specific keywords in sentences such as *limitation* or *unsupported*. Additionally, statements can include longer phrases to convey these limitations. For example, a repository of key-value storage may state that it does not support indexes or will receive limited maintenance. An example of such limitations is the readme file of Apache Airflow repository indicating that "MariaDB is not tested/recommended".

To extract these limitations and unsupported features of a repository, we incorporated a zero-shot classifier [28] based on the *bart-large-mnli* model, which is based on the *bart-large* model [23] and trained on the *MultiNLI* dataset consisting of 433k sentence pairs annotated with textual entailment information. For each section in the input readme files, we extract the sentences of the section and pass it to the zero-shot classifier to identify the score of being labeled as *"Unsupported Feature"* by the classifier. The default threshold is set to 0.9. Therefore, sentences that this zero-shot classifier scores with a value equal to or exceeding this threshold are extracted as candidate limitations for the repository.

G. Extraction of Repository Features

To identify a repository's supported features and capabilities, the multi-class classifier classifies extracted sections from the readme files corresponding to the user-selected *N* repositories. Sections labeled as *Functionaly* or *Usage* are further processed by removing all sentences corresponding to identified limitations by the zero-shot classifier. Then, we extract from these sections the keywords and key phrases capturing the repository's features and capabilities by incorporating KeyBERT [29]. The KeyBERT model is initialized with a Text-to-Text generation pipeline (also known as Sequence-to-Sequence modeling)[30]. We incorporate into this pipeline Llama-2-7b-chat-hf [31][32], which is a large langnuage model (LLM) consisting of 7 billion parameters fine-tuned for dialogue use cases. The pipeline tokenizes the provided text and relies on an encoder-decoder architecture to process the input text and generate a list of candidate features for each repository.

H. Calculating Similarity of Repositories' Features

Given each repository's extracted features, the online module calculates the semantic similarity between all possible feature pairs from the different repositories. The online module creates a sentence transformer [33] based on the sentence-t5-base [34] model to accomplish this task. For each feature pair of different repositories, the online module encodes the textual representation of each feature using the sentence transformer. As a result, the transformer encodes each feature into a 768-dimensional dense vector space. The cosine similarity [35] is then calculated from these vectors. Two features are labeled similar if the computed cosine similarity exceeds a threshold α.

IV. Results

A. Evaluation Results of the Hybrid Classifier for Classifying the Content of GitHub Readme Files

We use the testing set corresponding to readme files obtained from GitHub repositories for the Python programming language to evaluate the hybrid classifier (see Table III). This set contains 984 instances and is not previously seen by the model since it was not used during training.

We first identify the *actual* class for each instance in the testing set through manual classification. Then, we run the hybrid model on this set to determine the *predicted* class for instances. Finally, we compute the F1 score to measure the predictive maintenance of the classifier. Although the proposed approach is unsupervised, manual classification is performed for evaluation purposes of the model.

To determine the actual class for each instance, we manually classify instances in the testing set by labeling each instance as either Functionality, Usage, or Miscellaneous. Our labeling process consists of reading the heading title of each (sub)section to determine its class. If we cannot determine the class from the subsection's heading title, then we read the first sentences in the subsection to determine its class. Finally, if

TABLE VII. EXAMPLES OF ERRONEOUS CLASSIFICATIONS BY THE KEYWORD-DRIVEN MODEL AND EXPLANATION OF RULE-BASED ADJUSTMENTS

	Example Instance	Actual Class (Score by Model)	Predicted Class (Score by Model)	Explanation
1	Documentation. Read the Manual @link for more details.	Usage(0.5447)	Miscellaneous(0.5585)	Although the words *documentation*, *manual*, and *details* in this sentence correspond to keywords for class *Usage*, the model labeled this instance as *Miscellaneous*. Therefore, according to the *keywords ratio* rule, the predicted class is adjusted from Miscellaneous to *Usage*.
2	Train with DDL Statements. DDL statements contain information about the table names, columns, data types, and relationships in your database. @Code	Usage(0.6138)	Features(0.6187)	Although the model mistakenly labeled this instance as *Features* instead of *Usage*, this subsection is a child of a higher section that was labeled correctly by the model as *Usage*. Therefore, according to the *Relevance to Parent* rule, the predicted class is adjusted from Features to *Usage*.
3	Testimonials. Mike Bayer, author of SQLAlchemy link : I can't think of any single tool in my entire programming career that has given me a bigger productivity increase by its introduction. I can now do refactorings in about 1% of the keystrokes that it would have taken me previously when we had no way for code to format itself...	Miscellaneous(0.6173)	Functionality(0.6219)	Testimonial statements by users are labeled by the classifier as *Functionality* instead of *Miscellaneous* with a score difference of less than 0.01. However, the model correctly labels sibling subsections as *Miscellaneous*. Therefore, according to the *Relevance to Siblings* rule, the predicted class is adjusted from Functionality to *Miscellaneous*.

the class still cannot be determined, we read the content of the subsection to determine its class.

Given the actual and predicted classes for each instance in the test dataset, we compute the F1 score (also known as the balanced F-score) [36] according to the following formula:

$$F1 = \frac{2 * TP}{2 * TP + FP + FN} \quad (1)$$

Where TP represents the number of true positives, FN represents the number of false negatives, and FP represents the number of false positives.

Evaluation results for the various Lbl2TransformVec models are shown in Table VIII. Classification based on keyword-driven approaches produces F1 scores that range from 0.6930 to 0.7601. Furthermore, several models have equal scores, possibly due to these models sharing the same base model. The *improvement* column shows the percentage change between the F1 scores obtained from the evaluation of keyword-driven models and the F1 scores obtained from the evaluation of combining keyword-driven models with rule-based adjustments. As seen in this table, incorporating rule-based adjustments shows observable improvement in scores by an average of 13.26% increase. Table IX shows an example of the contribution of each rule in adjusting the classification results, where the *keyword ratio rule* contributed the most by correcting 75 instances while failing to adjust 27 instances. On the other hand, the *relevance to the parent* rule has contributed the least in adjusting classification results. As seen in Table VIII rule-based adjustments contributed the least when applied to all-MiniLM-L6-v2. Inspection of correction results for this model reveals significant incorrect adjustments, particularly to the *relevance to siblings* rule with 40 incorrect adjustments.

We analyzed the class-word distribution of the classified instances from the testing set. The most frequent words for subsections identified as Functionality include words such as *models*, *data*, *index*, and *new*. The words model and data appear as frequently since many Python repositories discuss machine-learning-related libraries and algorithms. On the other hand, instances classified as Usage contain as frequent words the words *Python*, *install*, *use*, *run*, *command*, and *pip*. Finally, the words *license*, *contributing*, *issues*, *community*, and *help* appeared among the most frequent keywords in instances classified as Miscellaneous.

TABLE VIII. F1 SCORES FOR CONTENT CLASSIFICATION USING THE LBL2TRANSFORMERVEC ALGORITHM WITH DIFFERENT UNDERLYING MODELS, WITH AND WITHOUT RULE-BASED CLASSIFICATION ADJUSTMENTS

Model	F1 Score		Improv.
	Key-Driven	w/ Rule-Based	
bart-large-mnli	0.7601	**0.8607**	+13.23%
all-MiniLM-L6-v2	0.6961	**0.7571**	+8.76%
all-mpnet-base-v2	0.6930	**0.7957**	+14.82%
all-distilroberta-v1	0.6930	**0.7957**	+14.82%
all-MiniLM-L12-v2	0.6930	**0.7957**	+14.82%
unsup-simcse-bert-base-uncas	0.7601	**0.8607**	+13.23%
unsup-simcse-bert-large-uncas	0.7601	**0.8607**	+13.23%
unsup-simcse-roberta-base	0.7601	**0.8607**	+13.23%
unsup-simcse-roberta-large	0.7601	**0.8607**	+13.23%

TABLE IX. EXAMPLES OF CORRECTION RESULTS BY RULE-BASED CLASSIFICATION ADJUSTMENTS

Rule	Correct Adjustments	Incorrect Adjustments
Keywords Ratio	75 instances	27 instances
Relevance to Parent	10 instances	5 instances
Relevance to Siblings	42 instances	18 instances

B. Evaluation Results of Zero-Shot Classifier for Classifying the Limitations of Repositories

To evaluate the zero-shot classifier presented in Section III-F, we constructed a subset dataset derived from the original dataset (see Table III) by searching for instances that explicitly state limitations of repositories as well as instances of non-limitation sentences. The resulting dataset consists of 55 instances, where 26 represent limitation sentences, and 29 represent non-limitation sentences. We run the zero-shot classifier to classify each instance in the subset dataset and

then calculate the F1 score. Evaluation results show that the predictive performance of the zero-shot classifier in classifying sentences as being *Unsupported Features* has an F1 score of 0.72.

Table X shows examples of limitation sentences found in several instances in the dataset, with some instances of non-limitation sentences. As can be seen in this table, the classifier gave high scores to sentences including specific keywords and key phrases (such as *"not tested/recommended", "won't be able to save files", "does not work on" and "not compatible with"*. On the other hand, instances 5 and 6, which do not convey any limitations, scored very low by the zero-shot classifier, as expected. Instances 7-9 show examples of erroneous classifications by the zero-shot classifier in nuanced cases where limitations can be implied.

C. Motivation Example Continued: Generated Comparison Charts

Continuing with the motivation example discussed in Section I, Fig. 4 shows the result of generating the comparison chart, represented as an HTML file, by the online module for this example. In this example, the user selects $N = 3$ repositories from GitHub's search results. These repositories are Mailspring [37], Mailpile [38], and emailengine [39], all of which are top-starred repositories for the search term "email client". The comparison chart displays the features of each repository. If two features from different repositories are similar, they are assigned an equal number (shown in blue in Fig. 4). The identified limitations for each repository (if any) are shown next.

In this chart, the online module has identified a single limitation for the second repository, which corresponds to the Mailpile repository, as obsolete. Inspection of the repository's readme file reveals that the online module has identified this limitation through the zero-shot classifier since it appeared in the introduction section of the file, where the Lbl2TransformerVec algorithm previously labeled this section with the feature class.

The lists of features and extended features in this comparison chart are extracted from *Functionality* and *Usage* sections, respectively. The total number of words in this chart's features and extended features lists is 397. Compared to the total number of words in the readme files for the three repositories, which is 1742 words, the comparison chart achieves a reduction of 125% of textual information that needs to be read by the user.

The commonality between repositories based on semantic similarity is shown in the features list. For each pair of similar features, a unique number (shown in blue in Fig. 4) is assigned. For example, the Mailspring and Mailpile repositories include "fast" as a feature. As a result, both features are identified by the online module as common. Similarly, both repositories indicate that they are free and are grouped as similar features. However, our results include false positives. For example, the "Read Receipt" and "Documentation and Details" are calculated as similar.

V. Discussion and Threats to Validity

Analyzing the readme files of similar GitHub repositories to understand their unique features, limitations, and similarities with one another is a challenging task since these files do not adhere to a standard and may vary in their level of detail. Furthermore, these files are written in different styles. Our results show that combining several Large Language Models (LLMs) can address these challenges and generate useful comparison charts for these repositories. First, the keyword-driven classifier based on Lbl2TransformerVec can identify relevant sections (containing important information about the repository) and irrelevant sections (that are unlikely to contain significant information about the repository's provided features, such as Contribution Acknowledgment, Licence, and Donation). After identifying relevant sections, their sentences are extracted and passed to a zero-shot LLM based on *bart-large-mnli* to determine whether the sentence intends to convey a limitation of the repository. These limitations are extracted so that they are not mistakenly considered as features by the proposed approach. A keyword extractor LLM based on KeyBERT is incorporated to extract the most relevant keywords representing the features of each repository. Finally, a sentence transformer is incorporated to find the semantic similarity between features of different repositories.

Although our results show that models generated by Lbl2TransofmerVec, which is a similarity-based approach leveraging embeddings generated by deep learning models [5], can classify the content of readme files, rule-based adjustments can improve the algorithm's results. This is because Lbl2TransofmerVec trains models to classify (sub)sections in isolation irrespective of their relations to other sections. Therefore, the lack of such view of relations during model training can cause incorrect classifications by these models. The rule-based adjustments complement keyword classification with such a view where these relations are considered. These rule-based adjustments are possible since readme files are often well-structured as reported previously by Treude et al. [16].

The collected dataset covers different application domains since the collection process is blind to such domains. To confirm this, we inspected the collected Python repositories used for testing to determine their domains. Inspection reveals that the test dataset covers various domains such as video production, deepfake, cryptocurrencies, cloud development, SQL-related libraries, and machine learning. Therefore, the proposed approach generalizes across different repository types or domains as it relies on textual readme files unrelated to the source code or bytecode of repositories [13].

Our results show that larger sequence-to-sequence and bidirectional transformer encoder models such as bart-large-mnli and unsup-simcse variants achieve better F1 scores than smaller models such as all-MiniLM-L6-v2. This is because larger models with more parameters and larger embeddings can capture complex patterns and relationships within the data compared to smaller models with fewer parameters and smaller embeddings. On the other hand, we observe that smaller models, such as all-MiniLM-L6-v2, are more efficient than larger models in terms of training and inference times and require lower resource usage, making them more appropriate when dealing with resource-constrained environments.

Fig. 4. An example of a generated comparison chart for three GitHub repositories. In this chart, the features (A) and extended features (B) of repositories are identified by KeyBert from sections that are classified as *Functionality* and *Usage*, respectively. Limitations (C) are sentences identified by the zero-shot classifier as *Unsupported Features*. Features from different repositories with matching numbers (D) are considered as potentially common.

TABLE X. EXAMPLES OF ZERO-SHOT CLASSIFICATION OF LIMITATIONS WHERE SCORE THRESHOLD IS SET TO 0.9

No.	Instance Example	Repository	Is Limitation?		Score
			Predicted	Expected	
1	MariaDB is not tested/recommended	Apache Airflow	Yes	Yes	0.997
2	You won't be able to save files to system folders due to UWP restriction windows, system32	Notepads	Yes	Yes	0.995
3	It does not work on non-Android devices incl. LG or Samsung TVs	SmartTube	Yes	Yes	0.94
4	Swiper is not compatible with all platforms	Swiper	Yes	Yes	0.986
5	If your platform is unsupported or not listed above, there is still a chance you can run the release or manually build it by following the instructions	osu	No	No	0.33
6	it is a modern touch slider which is focused only on modern apps/platforms to bring the best experience and simplicity	Swiper	No	No	0.001
7	Importantly, we have not yet fine-tuned the Alpaca model to be safe and harmless	stanford alpaca	No	Yes	0.28
8	This repository is receiving very limited maintenance	leveldb	No	Yes	0.11
9	convert.py has been deprecated and moved to examples/convert-legacy-llama.py, please use convert-hf-to-gguf.py @link	llama.cpp	Yes	No	0.99

Compared to prior works incorporating supervised learning for classifying the content of GitHub readme files, Perna et al. reported an F1 score of 0.72 [2], while our hybrid approach achieved an F1 score of up to 0.86 (with rule-based adjustment). However, it should be noted that their supervised approach is multi-label and considers more classes. In contrast, our approach merges some of the classes they reported in their work as we focus on extracting the functionality and features of repositories from readme files. For example, the What, Why, and When classes in their work correspond to the Functionality class in our work.

Although our results show adequate extraction of comparison charts, we identify several challenges and possible improvements for future works as follows:

- *Immature or incomplete readme files*: Throughout our data collection process, we discovered that the readme files of many GitHub repositories, including repositories with high star ratings, may lack detailed information on their functionalities and features. Instead, they add internal or external URLs (such as the product's official website) for further details. Therefore, the generated comparison charts are incomplete and do not represent the repositories' full features and limitations. Thus, the proposed approach can be extended to automatically cover such internal and external resources. In addition to analyzing the readme files of a repository, it is also possible to extend the proposed approach by gathering additional sources of information using GitHub's API, including GitHub issues, pull requests, and discussions. A pull request represents a proposal for merging a set of changes before these changes are integrated into the main codebase [40]. Therefore, analyzing pull requests and their current statuses makes it possible to expand the comparison charts with information unavailable in readme files. For example, merged pull requests can reveal new features/functionalities of a repository. Similarly, an open pull request can reveal potential limitations yet to be addressed. GitHub issues and discussions can be analyzed to discover a repository's features and limitations. However, since any user can create issues and participate in public repositories, the challenge is to validate these issues and discussions before relevant information is extracted and used in comparison charts, as some issues can result from user misunderstanding or misuse of the repository.
- *Sentence-Level content classification*: Our work assumes that each (sub)section in readme files is mapped to a specific class (e.g. functionality, usage, or Miscellaneous). Although many repository owners ensure that each (sub)section has a clear and single purpose to achieve, our observation indicates sections can include sentences of various classes. For example, some readme files may contain Usage instructions in the introduction section. This may result in missed features and functionalities if conveyed in sections classified as Miscellaneous. Therefore, one may consider enhancing the classification task at the sentence level for such sections.
- *Interpretability and explainability*: The generated comparison charts can be inaccurate and biased. Therefore, it is essential to incorporate appropriate mechanisms so that these charts are explainable [41] [42] to the end users, conveying the underlying model's accuracy and achieving transparency. For example, interactive elements can be added to these charts to explain how the proposed approach obtains and calculates the various parts (i.e. repository features, extended features, limitations, and similarities). Furthermore, incorporating tractability mechanisms between these parts and the source from which they are obtained (i.e. line numbers within readme files) enables users to validate these parts.
- *Repository Limitations Extraction*: Our evaluation results of the zero-shot classifier to identify the limitations of repositories demonstrate its capability for this task. However, this approach needs to be investigated further. First, the small dataset used to validate the zero-shot classifier is a threat to validity, as a larger dataset is required for evaluation. The challenge is obtaining a large dataset representing limitations found in real GitHub repositories, as most repository owners focus on stating what their repository provides rather than stating the limitations. Second, our results show that sentences with implied limitations (e.g. instance 7 in Table X) can result in erroneous classifications by the zero-shot classifier. One potential solution is to train the classifier on a dataset of real limitations from GitHub repositories. Finally, the zero-shot classifier lacks a contextual view during classification;

for example, the classifier cannot distinguish whether the limitation is related to the user-selected repository or other related/external repositories referenced in a readme file. This challenge applies to identifying a repository's features as well. A possible improvement is to add steps for analyzing the sentence(s) structure and linguistic features to determine whether a limitation (or a feature) is related to the user-selected repository and not other related repositories referenced in the readme files.

- *Feature commonalities between repositories*: Our results show that identifying common features between different repositories is challenging. One possible reason is the usage of technical terms that are not incorporated during the training of LLMs. One potential future direction is to investigate the enhancement of similarity approaches in this respect.
- *Quantitative Metrics Generation*: Our approach relies on extracting qualitative data from readme text files. However, it might be possible to extract more qualitative and quantitative data. For example, the frequency with which each repository is updated, the average response time of a repository's owner to issues, and the overall maturity of each repository compared to others can be considered. These metrics can enrich the generated comparison charts and their overall added value to end-users.

VI. Conclusion

While prior works investigated the analysis of individual readme files, with most works following a supervised approach, our work focuses on an unsupervised approach for the classification task, which aims to generate comparison charts of similar GitHub repositories from their readme files. Our evaluation results show that textual information in comparison charts can be 125% less compared to the amount of text in readme files, thus minimizing the time and effort required for users to read these files to understand and compare their features and capabilities. Our approach utilizes a hybrid model based on the Lbl2TransformerVec algorithm and augmented with rule-based classification adjustments. The model is trained based on readme files automatically obtained from GitHub for Java, JavaScript, C++, and C# repositories. The model is then evaluated using a different set of readme files from Python repositories. Our results show that rule-based classification adjustment can improve the model's predictive performance by up to 13%. We then incorporated this model in an online module to generate comparison charts of GitHub repositories based on user search terms. Our future work includes investigating several enhancements to the proposed approach to address its limitations, as identified in the previous section, including (1) investigating how comparison charts can be enriched with information from other sources (such as GitHub pull requests, discussions, and issues), (2) extending the proposed approach so that the generated comparison charts are explainable to the end users, and (3) adding quantitative metrics to these charts. Furthermore, we plan to expand the evaluation of this approach using a larger dataset of GitHub repository features and limitations.

References

[1] GitHub, Inc. (2024) Build software better, together. [Online]. Available: https://github.com/about

[2] G. A. A. Prana, C. Treude, F. Thung, T. Atapattu, and D. Lo, "Categorizing the Content of GitHub README Files," *Empirical Software Engineering*, vol. 24, no. 3, pp. 1296–1327, Jun. 2019. [Online]. Available: https://doi.org/10.1007/s10664-018-9660-3

[3] J. Wu, Y. Sun, and J. Zhang, "An Open-source Repository Retrieval Service Using Functional Semantics for Software Developers," in *2022 International Conference on Service Science (ICSS)*, May 2022, pp. 12–20. [Online]. Available: https://ieeexplore.ieee.org/document/9860185

[4] Y. Zhang, F. F. Xu, S. Li, Y. Meng, X. Wang, Q. Li, and J. Han, "Higitclass: Keyword-driven hierarchical classification of github repositories," in *2019 IEEE International Conference on Data Mining, ICDM 2019, Beijing, China, November 8-11, 2019*, J. Wang, K. Shim, and X. Wu, Eds. IEEE, 2019, pp. 876–885. [Online]. Available: https://doi.org/10.1109/ICDM.2019.00098

[5] T. Schopf, D. Braun, and F. Matthes, "Evaluating unsupervised text classification: Zero-shot and similarity-based approaches," in *Proceedings of the 2022 6th International Conference on Natural Language Processing and Information Retrieval*, ser. NLPIR '22. New York, NY, USA: Association for Computing Machinery, 2023, p. 6–15. [Online]. Available: https://doi.org/10.1145/3582768.3582795

[6] T. Schopf, D. Braun, and F. Matthes, "Semantic label representations with lbl2vec: A similarity-based approach for unsupervised text classification," in *Web Information Systems and Technologies*, ser. Lecture Notes in Business Information Processing, M. Marchiori, F. Domínguez Mayo, and J. Filipe, Eds. Germany: Springer, Jan. 2023, pp. 59–73.

[7] T. Schopf, D. Braun, and F. Matthes, "Lbl2vec: An embedding-based approach for unsupervised document retrieval on predefined topics," in *Proceedings of the 17th International Conference on Web Information Systems and Technologies - WEBIST,*, INSTICC. SciTePress, 2021, pp. 124–132.

[8] Y. Zhou, J. Wu, and Y. Sun, "GHTRec: A Personalized Service to Recommend GitHub Trending Repositories for Developers," in *2021 IEEE International Conference on Web Services (ICWS)*, Sep. 2021, pp. 314–323. [Online]. Available: https://ieeexplore.ieee.org/document/9590294

[9] C. Di Sipio, R. Rubei, D. Di Ruscio, and P. T. Nguyen, "A Multinomial Naïve Bayesian (MNB) Network to Automatically Recommend Topics for GitHub Repositories," in *Proceedings of the 24th International Conference on Evaluation and Assessment in Software Engineering*, ser. EASE '20. New York, NY, USA: Association for Computing Machinery, Apr. 2020, pp. 71–80. [Online]. Available: https://doi.org/10.1145/3383219.3383227

[10] A. Sharma, F. Thung, P. S. Kochhar, A. Sulistya, and D. Lo, "Cataloging github repositories," in *Proceedings of the 21st International Conference on Evaluation and Assessment in Software Engineering*, ser. EASE '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 314–319. [Online]. Available: https://doi.org/10.1145/3084226.3084287

[11] F. Zanartu, C. Treude, B. Cartaxo, H. S. Borges, P. Moura, M. Wagner, and G. Pinto, "Automatically categorising github repositories by application domain," 2022. [Online]. Available: https://arxiv.org/abs/2208.00269

[12] S. Vargas-Baldrich, M. Linares-Vásquez, and D. Poshyvanyk, "Automated tagging of software projects using bytecode and dependencies (n)," in *2015 30th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2015, pp. 289–294.

[13] M. Izadi, A. Heydarnoori, and G. Gousios, "Topic recommendation for software repositories using multi-label classification algorithms," *Empirical Software Engineering*, vol. 26, no. 5, p. 93, Jul. 2021. [Online]. Available: https://doi.org/10.1007/s10664-021-09976-2

[14] Y. Liu, E. Noei, and K. Lyons, "How ReadMe files are structured in open source Java projects," *Information and Software Technology*, vol. 148, p. 106924, Aug. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584922000775

[15] A. S. M. Venigalla and S. Chimalakonda, "An empirical study on correlation between readme content and project popularity," 2022. [Online]. Available: https://arxiv.org/abs/2206.10772

[16] C. Treude, J. Middleton, and T. Atapattu, "Beyond accuracy: assessing software documentation quality," in *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, ser. ESEC/FSE 2020. New York, NY, USA: Association for Computing Machinery, Nov. 2020, pp. 1509–1512. [Online]. Available: https://doi.org/10.1145/3368089.3417045

[17] O. Elazhary, M.-A. Storey, N. Ernst, and A. Zaidman, "Do as I Do, Not as I Say: Do Contribution Guidelines Match the GitHub Contribution Process?" *2019 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, pp. 286–290, Sep. 2019, conference Name: 2019 IEEE International Conference on Software Maintenance and Evolution (ICSME) ISBN: 9781728130941 Place: Cleveland, OH, USA Publisher: IEEE. [Online]. Available: https://ieeexplore.ieee.org/document/8919187/

[18] A. S. M. Venigalla and S. Chimalakonda, "What's in a github repository? – a software documentation perspective," 2021. [Online]. Available: https://arxiv.org/abs/2102.12727

[19] J. Hellman, E. Jang, C. Treude, C. Huang, and J. L. C. Guo, "Generating github repository descriptions: A comparison of manual and automated approaches," 2021. [Online]. Available: https://arxiv.org/abs/2110.13283

[20] Y. Zhou, J. Wu, and Y. Sun, "Ghtrec: A personalized service to recommend github trending repositories for developers," in *2021 IEEE International Conference on Web Services (ICWS)*, 2021, pp. 314–323.

[21] GitHub, Inc. REST API endpoints for search. [Online]. Available: https://docs.github.com/en/rest/search/search

[22] GitHub, Inc. Writing on GitHub. [Online]. Available: https://docs.github.com/en/get-started/writing-on-github

[23] M. Lewis, Y. Liu, N. Goyal, M. Ghazvininejad, A. Mohamed, O. Levy, V. Stoyanov, and L. Zettlemoyer, "BART: Denoising sequence-to-sequence pre-training for natural language generation, translation, and comprehension," in *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, D. Jurafsky, J. Chai, N. Schluter, and J. Tetreault, Eds. Online: Association for Computational Linguistics, Jul. 2020, pp. 7871–7880. [Online]. Available: https://aclanthology.org/2020.acl-main.703

[24] W. Wang, H. Bao, S. Huang, L. Dong, and F. Wei, "MiniLMv2: Multi-head self-attention relation distillation for compressing pretrained transformers," in *Findings of the Association for Computational Linguistics: ACL-IJCNLP 2021*, C. Zong, F. Xia, W. Li, and R. Navigli, Eds. Online: Association for Computational Linguistics, Aug. 2021, pp. 2140–2151. [Online]. Available: https://aclanthology.org/2021.findings-acl.188

[25] K. Song, X. Tan, T. Qin, J. Lu, and T.-Y. Liu, "Mpnet: masked and permuted pre-training for language understanding," in *Proceedings of the 34th International Conference on Neural Information Processing Systems*, ser. NIPS '20. Red Hook, NY, USA: Curran Associates Inc., 2020.

[26] sentence-transformers/all-distilroberta-v1 · Hugging Face. [Online]. Available: https://huggingface.co/sentence-transformers/all-distilroberta-v1

[27] T. Gao, X. Yao, and D. Chen, "SimCSE: Simple contrastive learning of sentence embeddings," in *Empirical Methods in Natural Language Processing (EMNLP)*, 2021.

[28] W. Yin, J. Hay, and D. Roth, "Benchmarking zero-shot text classification: Datasets, evaluation and entailment approach," in *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*, K. Inui, J. Jiang, V. Ng, and X. Wan, Eds. Hong Kong, China: Association for Computational Linguistics, Nov. 2019, pp. 3914–3923. [Online]. Available: https://aclanthology.org/D19-1404

[29] M. Grootendorst, "Keybert: Minimal keyword extraction with bert." 2020. [Online]. Available: https://doi.org/10.5281/zenodo.4461265

[30] Hugging face pipelines. [Online]. Available: https://huggingface.co/docs/transformers/en/main_classes/pipelines

[31] H. Touvron, L. Martin, K. Stone, P. Albert, A. Almahairi, Y. Babaei, N. Bashlykov, S. Batra, P. Bhargava, S. Bhosale, D. Bikel, L. Blecher, C. C. Ferrer, M. Chen, G. Cucurull, D. Esiobu, J. Fernandes, J. Fu, W. Fu, B. Fuller, C. Gao, V. Goswami, N. Goyal, A. Hartshorn, S. Hosseini, R. Hou, H. Inan, M. Kardas, V. Kerkez, M. Khabsa, I. Kloumann, A. Korenev, P. S. Koura, M.-A. Lachaux, T. Lavril, J. Lee, D. Liskovich, Y. Lu, Y. Mao, X. Martinet, T. Mihaylov, P. Mishra, I. Molybog, Y. Nie, A. Poulton, J. Reizenstein, R. Rungta, K. Saladi, A. Schelten, R. Silva, E. M. Smith, R. Subramanian, X. E. Tan, B. Tang, R. Taylor, A. Williams, J. X. Kuan, P. Xu, Z. Yan, I. Zarov, Y. Zhang, A. Fan, M. Kambadur, S. Narang, A. Rodriguez, R. Stojnic, S. Edunov, and T. Scialom, "Llama 2: Open foundation and fine-tuned chat models," 2023. [Online]. Available: https://arxiv.org/abs/2307.09288

[32] (2024, Aug.) meta-llama/Llama-2-7b-chat-hf · Hugging Face. [Online]. Available: https://huggingface.co/meta-llama/Llama-2-7b-chat-hf

[33] N. Reimers and I. Gurevych, "Sentence-bert: Sentence embeddings using siamese bert-networks," in *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, 11 2019. [Online]. Available: https://arxiv.org/abs/1908.10084

[34] J. Ni, G. Hernandez Abrego, N. Constant, J. Ma, K. Hall, D. Cer, and Y. Yang, "Sentence-t5: Scalable sentence encoders from pretrained text-to-text models," in *Findings of the Association for Computational Linguistics: ACL 2022*, S. Muresan, P. Nakov, and A. Villavicencio, Eds. Dublin, Ireland: Association for Computational Linguistics, May 2022, pp. 1864–1874. [Online]. Available: https://aclanthology.org/2022.findings-acl.146

[35] E. Schubert, "A triangle inequality for cosine similarity," in *Similarity Search and Applications*, N. Reyes, R. Connor, N. Kriege, D. Kazempour, I. Bartolini, E. Schubert, and J.-J. Chen, Eds. Cham: Springer International Publishing, 2021, pp. 32–44.

[36] Z. C. Lipton, C. Elkan, and B. Naryanaswamy, "Optimal thresholding of classifiers to maximize f1 measure," in *Machine Learning and Knowledge Discovery in Databases*, T. Calders, F. Esposito, E. Hüllermeier, and R. Meo, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 225–239.

[37] (2024, Sep.) Foundry376/Mailspring. Original-date: 2016-10-13T06:45:50Z. [Online]. Available: https://github.com/Foundry376/Mailspring

[38] (2024, Sep.) mailpile/Mailpile. Original-date: 2011-10-30T23:45:22Z. [Online]. Available: https://github.com/mailpile/Mailpile

[39] (2024, Sep.) postalsys/emailengine. Original-date: 2020-02-28T17:17:44Z. [Online]. Available: https://github.com/postalsys/emailengine

[40] GitHub, Inc. About pull requests. [Online]. Available: https://docs.github.com/en/pull-requests/collaborating-with-pull-requests/proposing-changes-to-your-work-with-pull-requests/about-pull-requests

[41] N. A. Sharma, R. R. Chand, Z. Buksh, A. B. M. S. Ali, A. Hanif, and A. Beheshti, "Explainable AI Frameworks: Navigating the Present Challenges and Unveiling Innovative Applications," *Algorithms*, vol. 17, no. 6, 2024. [Online]. Available: https://www.mdpi.com/1999-4893/17/6/227

[42] S. A. and S. R., "A systematic review of explainable artificial intelligence models and applications: Recent developments and future trends," *Decision Analytics Journal*, vol. 7, p. 100230, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S277266222300070X

An Ontology-Based Intelligent Interactive Knowledge Interface for Groundnut Crop Information

Purvi H. Bhensdadia, C. K. Bhensdadia
Computer Engineering Department,
Dharmsinh Desai University, Nadiad, 387001, Gujarat, India

***Abstract*—This paper presents an ontology-based interactive interface designed to provide farmers in Gujarat with information related to groundnut crops. An ontology specific to the groundnut crop was developed and used to create a semantic question-answering (QA) interface. The proposed QA interface converts natural language question into SPARQL Query and provides answer using the backbone ontology. The overall performance of the system is at par with the existing semantic QA system. Overall accuracy of QA System is 80%.**

***Keywords*—Agriculture ontology; ontology construction; question answer system; groundnut ontology**

I. Introduction

In India, agriculture is of paramount importance. This plays a crucial role in the development of rural areas. Gujarat is a leading producer of cash crops like cotton and groundnut. An estimated 20 lakh hectares of groundnuts are farmed in Gujarat each year, with a total production of roughly 26 lakh tons.[1]

A significant amount of data is available in the agricultural sector in the form of text documents, spreadsheets, and tables. There are many websites which have groundnut crop data in a factual form such as Farmer's Portal[2], mKishan[3], and i-Khedut(for groundnut crop)[4]. In addition, some online application exist for groundnut crops, such as i-khedut[5], magfadi[6], Chhomasu magfadi ma pramanit bij[7], and Khedut mol[8]. These websites and applications cannot perform semantic searches or reasoning.

The primary drawback of the existing applications or systems is the dependency on agriculture experts or other educated farmers to answer farmers' queries. These web applications are frequently used by farmers to express natural language queries that are answered by agriculture experts [1]. However, the expert might not always be available to respond to all the farmers' queries, which can create a communication gap between the farmer and the agriculture expert. To bridge this gap, semantic search techniques [2] can be employed. Semantic search [3] enhances the search capability by understanding the context and intent behind the queries, thus providing more relevant and accurate results [4]. This approach can automate the process of answering farmers' queries, making it possible to access information without waiting for an expert's response. Implementing a semantic search system can significantly improve the efficiency and effectiveness of information retrieval in agriculture, ultimately benefiting farmers by providing timely and accurate information.

An ontology-based question-answer system has been developed to interpret farming-related queries and provide relevant suggestions. This system leverages the structured knowledge within the ontology to provide context-aware responses, bridging the gap between farmers and agricultural experts. By utilizing this approach, farmers can receive immediate and relevant answers to their questions, enhancing their ability to make informed decisions about their crops and farming practices. This innovation not only improves the accessibility of agricultural knowledge but also empowers farmers with the tools necessary for efficient and effective farming.

The major contribution of the work are as follows:

1) A comprehensive groundnut ontology has been developed, capable of answering user queries. This ontology was created from scratch, ensuring it is rich in relevant agricultural concepts.
2) An interactive interface has been created that allows users to submit queries in natural language and receive responses in natural language.

The organization of this paper is as follows: Section II reviews related work I, focusing on existing web interfaces for Indian farmers and their relevance to agricultural support. Section III provides related work II, surveying the latest developments in chatbot technology with applications in agriculture. Section IV describes the proposed model, explaining its design and how it works to meet farmers' needs. Section V details the creation of the Groundnut Ontology, covering the processes of data collection, concept identification, and structuring. Section VI presents the experiment and setup, including the RDF knowledge graph representation, Neo4j query configurations, and the development of an interface to translate user questions into queries. Section VII provides a comprehensive result discussion, evaluating the system's performance and limitations. Finally, Section VIII concludes the paper, summarizing key findings and suggesting directions for future research.

[1]https://kvk.icar.gov.in/API/Content/PPupload/k0447_28.pdf
[2]https://farmer.gov.in/
[3]https://mkisan.gov.in/
[4]http://faq.ikhedut.aau.in/1
[5]https://play.google.com/store/apps/details?id=com.aau.in.oneapp
[6]https://play.google.com/store/apps/details?id=com.aau.in.magfadi
[7]https://play.google.com/store/apps/details?id=com.aau.in.groundnut
[8]https://play.google.com/store/apps/details?id=com.khedutmall.app&hl=en_US&pli=1

II. Related Work: I
Existing Web Interface for Farmers (in India)

In India, a plethora of agriculture-related applications have emerged, each designed to support farmers with a variety of essential services. These applications can be broadly categorized into simple agroadvisory systems[5] and more advanced agroadvisory systems with semantic search capabilities.

A. Categorization of App Based on Purpose

To understand these applications comprehensively, it is crucial to classify them based on the specific services they provide. The apps have been categorized according to their primary functions: weather and market price information, crop variety details, pest control, agro advisories, crop insurance information, government schemes, and agricultural news. This classification allows us to explore the unique features and benefits of each app while highlighting their relevance to different aspects of farming. Fig. 1 illustrates the categorization of applications that has been performed.

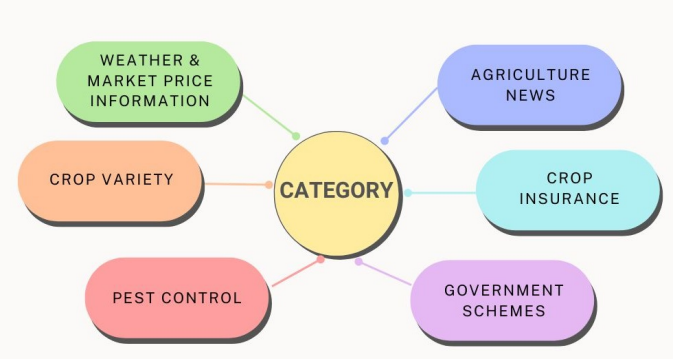


Fig. 1. Categorization of apps.

A survey of 156 agriculture-related mobile applications was conducted, and they were categorized based on their primary purpose. These applications span across various functionalities that support farmers' decision-making processes. For instance, 13 apps focus on weather forecasting, which helps farmers anticipate climate changes and plan their agricultural activities accordingly. Another 17 apps provide market information, offering crucial insights on pricing trends and helping farmers make informed sales decisions. Additionally, 16 apps leverage AI and IoT technologies, presenting innovative solutions for precision farming and resource management.

Crop insurance and government schemes are covered by 7 apps, guiding farmers on available schemes and providing them with financial protection. The largest group, consisting of 90 crop-based applications, is further subdivided into three specific areas: 25 apps offer crop information, helping farmers access detailed data on different crop varieties and innovative farming techniques; 12 apps focus on pest control and crop protection, providing strategies to identify, prevent, and treat pest infestations; and 7 apps are dedicated to soil health, offering insights on soil management practices that enhance crop yields.

This broad classification helps in understanding how digital tools can be leveraged in the agriculture sector. Weather forecasting apps, for example, assist in mitigating risks posed by unpredictable climate conditions, while market apps offer insights into the best times to buy or sell produce. Crop-specific applications provide specialized support, particularly in protecting crops from pests and ensuring soil health, which is essential for sustainable farming.

Starting with simple agroadvisory systems, these applications primarily serve as information portals, providing crucial updates on weather forecasts and market prices. Apps such as Kisan Suvidha[9] [6], IFFCO Kisan[10] [7], Agri App[11], Agri Market[12], eNAM[13] [14], mKisan[15], Ekgaon[16], myAgriGuru[17], Kisan Gujarat, AgriGujarat, and Gujarat Farm are instrumental in ensuring that farmers receive timely and relevant information about weather conditions and market trends. By providing essential data, these applications help farmers plan their activities and manage risks associated with weather and market fluctuations.

For crop variety information, the Pusa Krishi app [8] stands out. It offers insights into innovative farming techniques, crop varieties, and resource-saving technologies, which are invaluable for improving crop yields. Farmers can access detailed information about different crop varieties, helping them choose the best options for their specific conditions.

For pest control, several applications offer expert advice and practical tips to manage and mitigate pest infestations. Kisan Suvidha[18], Kheti-Badi[19], AgroStar[20], and Fasal[21] are notable examples. These apps provide specific information on pest identification, prevention strategies, and treatment options, helping farmers protect their crops from potential damage.

Crop insurance information is covered by the Crop Insurance app[22], which offers detailed information on various crop insurance schemes available to farmers. The app helps farmers understand their insurance options, eligibility criteria, and the claims process, providing financial protection against crop losses caused by unforeseen events.

Government schemes are another crucial area where mobile applications play a significant role. Apps like mKisan[23] [9], AgriMedia[24] [10], and Kisan Yojana [10] provide detailed information about various government schemes, subsidies, and benefits available to farmers. These apps ensure that farmers are well-informed about the support they can receive from the

[9] https://vikaspedia.in/agriculture/ict-applications-in-agriculture/kisan-call-center-app
[10] https://play.google.com/store/apps/details?id=com.IFFCOKisan
[11] https://apps.mgov.gov.in/details?appid=1525
[12] https://apps.mgov.gov.in/details;jsessionid=8EBEA4C94DB07B53B4FB03A49623D6CF?appid=989
[13] https://enam.gov.in/web/mobile-app
[14] https://play.google.com/store/apps/details?id=in.gov.enam
[15] https://mkisan.gov.in/Alpha/aboutmobileapps.aspx
[16] http://www.ekgaon.net/index.php
[17] https://climateasap.org/directory/myagriguru/
[18] https://kisansuvidha.gov.in/
[19] https://play.google.com/store/apps/details?id=com.freeappartist.khetiwadi&hl=en_US
[20] https://play.google.com/store/search?q=agrostar&c=apps
[21] https://play.google.com/store/search?q=Fasal&c=apps
[22] https://pmfby.gov.in/
[23] https://mkisan.gov.in/
[24] https://play.google.com/store/search?q=agrimedia+app&c=apps&hl=en-IN

government, enhancing their access to financial and technical assistance.

For agricultural news, apps such as IFFCO Kisan[25], Agri App[26], AgriMarket[27], eNAM[28], AgriBuzz[11], Kisan Yojana, Krishi Network[29], Gujarat Agri, and Gujarat Farm keep farmers updated with the latest developments in the agricultural sector. These platforms provide news on policy changes, market trends, technological advancements, and success stories, fostering an informed farming community.

The integration of semantic web technologies and ontologies is pivotal in addressing the challenges of inconsistent data and knowledge gaps in the agricultural sector.

B. Ease of Searching for Crop Product Information

An agroadvisory system allows farmers to write their questions in the system, and an agriculture expert will answer them. Farmers can also directly connect with an agriculture expert through a call to present their queries and get answers. Some existing agroadvisory applications like eSagu [12], aAQUA, and mKrishi[30] offer these features.

However, these apps have some drawbacks. A major issue is the lack of instant, personalized responses to farmers' questions. Since they do not use semantic search, farmers often have to wait for an expert to answer their specific questions, which can delay important decisions.

Semantic search represents a significant advancement in information retrieval systems [13], especially in the agricultural domain. For farmers, this means faster and more precise answers to their specific agricultural questions. Semantic search can quickly analyze and retrieve relevant data from vast databases, significantly reducing the time farmers spend waiting for answers. This immediacy is crucial for timely decision-making in farming practices.

III. Related work: II (Survey Chatbot Technology)

The history of chatbots dates back to the 1960s when Joseph Weizenbaum created ELIZA [14], the first computer program to initiate communication between humans and computers. It used a pattern-matching method to simulate human conversation. Later, in the year 1972, PARRY[31] was introduced by a psychiatrist Kenneth Colby which simulated the behavior of a paranoid schizophrenic.

By the 1990s, progress in natural language processing led to more sophisticated systems like Jabberwacky[32], which used AI to hold more natural conversations. However, the launch of Siri in 2011 was a game-changer, introducing voice-activated virtual assistants to the mainstream. Since then, AI and machine learning have propelled chatbot technology forward, leading to the development of highly advanced agents like Alexa, Google Assistant, and ChatGPT. These modern chatbots can now understand and generate human language with impressive accuracy. Chatbots play a crucial role in industries ranging from customer service to healthcare, enhancing the efficiency and smoothness of interactions with machines [15].

There has been a significant advancement in the area of Artificial Intelligence, Machine Learning and Natural Language Processing in recent years. The development in these areas have brought a marked change in various industries such as education, scientific research, medical health, including agriculture [16]. Farming is the primary source of income for millions in India. With growth in the field of AI, chatbots have emerged as innovative tools to help farmers make better decisions by providing them with access to real-time information. The technology of Chatbot applications have evolved from simple rule-based systems to advanced AI driven models [17]. This literature review highlights the development of chatbot technologies in Indian agriculture, focusing on the methodologies and innovations that have shaped the field.

A. Chatbot Technology in Indian Agriculture

Farmers can benefit from receiving correct and timely information about various aspects of agriculture, such as crop recommendations, plant disease identification, etc. A solution to this was devised by building conversational systems, which allow farmers to obtain timely answers to their queries. In 2015, AGRI-QAS [18] was developed to address farmers' queries related to crop recommendations, plant disease identification, and more. This marked the earliest advancement in this area, utilizing an index-based search technique.

In 2017, ADANS (Agriculture Domain Question Answering System) [19] introduced a significant improvement by utilizing ontology-based technology. It performed answer retrieval on a structured agriculture database, efficiently identifying relationships between agricultural concepts and providing more reliable and accurate responses to farmers' queries.

In 2018, FarmChat [20] was introduced as a conversational agent containing two user interfaces: one with Audio Only and the other with Audio+Text. It used Google's Speech-to-Text for speech conversion and used language model for query intent and entity identification, subsequently retrieving the appropriate response from the knowledge base.

AgronomoBot [21] used sensor networks to gather information about the agricultural production chain in a specific area. It integrated its information in Telegram Bot API. This marked an early integration of AI with messaging platforms to provide farmers with data-driven insights.

In 2019, AgriBot [22] provided functionalities such as crop recommendations based on current conditions, current weather details, and future weather predictions. For crop recommendations, it used algorithms such as K-Nearest Neighbors (KNN), Random Forest, and Decision Trees. The chatbot provided

[25] https://www.iffcokisan.com/agritech

[26] https://play.google.com/store/apps/details?id=com.criyagen&hl=en_IN&pli=1

[27] https://apps.mgov.gov.in/details;jsessionid=8EBEA4C94DB07B53B4FB03A49623D6CF?appid=989

[28] https://www.enam.gov.in/web/

[29] https://play.google.com/store/apps/details?id=com.krishi.krishi&hl=en_IN

[30] https://www.tatatrusts.org/our-work/livelihood/agriculture-practices/mkrishi

[31] https://en.wikipedia.org/wiki/PARRY

[32] https://en.wikipedia.org/wiki/Jabberwacky

response to user queries by accessing the Krishi Call Center database[33].

Another form of AgriBot [23] was released in 2019, utilizing a Sen2Vec-based NLP technique to answer farmers' queries. This represented a significant step forward in AI-driven agricultural chatbots, enabling more sophisticated and context-aware responses to queries.

The integration of NLP into chatbot systems has pushed the boundaries of what these technologies can achieve in agriculture. In 2020, another version of Agribot [24] incorporated an LSTM-based model to provide answers to user queries. It additionally used a CNN-based model was used to classify plant diseases based on images. The system was trained on the Krishi Call Center dataset.

By 2021, chatbots such as Krushi—The Farmer Chatbot [25] began utilizing the RASA NLU framework, an advanced NLP tool designed for processing queries in local languages. This framework identifies the intent behind each query. For weather-related queries, the system uses the appropriate OpenWeather API key to provide real-time responses. For other types of queries, it matches key entities with the database to generate suitable responses. This approach enhanced the system's ability to address farmers' needs by leveraging insights from previous interactions in the KCC datasets. It is also integrated into WhatsApp [25]. Another such similar work methodology can be seen in AgroBot where they have made use of NLP to identify the intent of user query to provide appropriate response [26].

During this period, Agroxpert addressed user queries by employing the Levenshtein distance formula. The authors compiled a dataset consisting of user queries and responses. Subsequently, user queries were matched against this dataset using the Levenshtein distance formula, allowing for appropriate responses to be generated. In instances where the system could not confidently provide an answer, the queries were escalated to human experts, creating a continuous feedback loop between AI and human expertise [27].

The usage of Artificial Neural Networks for crop disease prediction also increased during this time. Many research work were focused on providing assistance to farmers in identifying crop disease using Artificial Neural Network.

By 2023, chatbots like the Agriculture Assistant Chatbot [28] integrated a CNN-based algorithm that enabled farmers to upload crop images for disease diagnosis, offering potential remedies as well as essential information such as soil and rainfall data. Another notable work can be seen in [29], where a VGG-16-based model was incorporated for identifying diseases in plants. They provided crop recommendations based on current conditions using machine learning algorithms.

In 2024, the AI-Powered Decision Support System for Sustainable Agriculture utilized LLMs to process unstructured user queries and provide constructive farming advice. It addressed various issues, such as pest control, by using real-time data for analysis and crop management [30].

Other projects, like ChatAgri (2023) [31], explored the cross-linguistic potential of LLMs for agricultural text classification and provided end to end question answering system [32].

The development of agricultural chatbots in India has progressed rapidly over the past decade, evolving from basic AGRI-QAS to advanced AI-driven models. With the integration of LLMs such as ChatGPT and domain-specific improvements like ChatAgri [31], chatbots are becoming indispensable tools for modern farming. They offer farmers tailored, real-time solutions to the daily challenges of agriculture, positioning themselves to be vital in the future of farming.

IV. Proposed Model

Fig. 2 illustrates the workflow of the proposed question-answering system, which retrieves information from an ontology graph database.

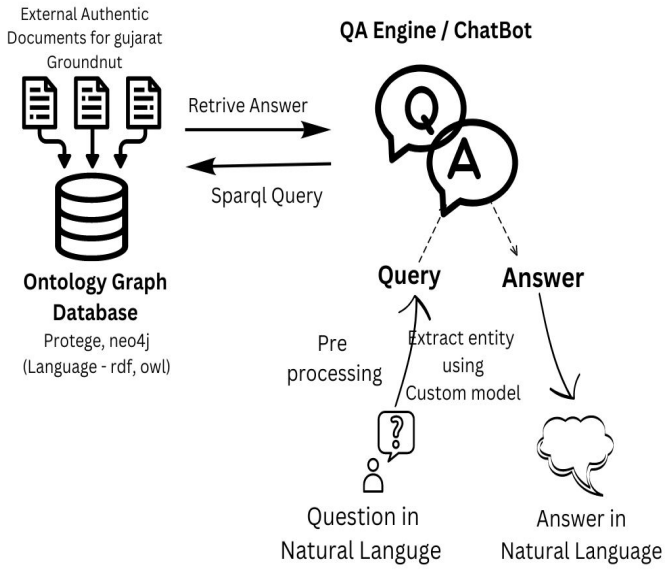


Fig. 2. Proposed work.

- Ontology Graph Database
  - Ontology Modeling: Using tools like Protégé, an ontology was created to represent the identified concepts, their properties, and the relationships between them. The ontology follows a hierarchical structure with clearly defined classes, subclasses, and individuals, ensuring that the agricultural knowledge is represented in a logical and organized manner.
  - Knowledge Graph Construction: The ontology was then translated into a knowledge graph using Neo4j, a graph database that efficiently manages the interconnected data. The knowledge graph encodes entities (e.g. "Early_Leaf_Spot X") as nodes, while the relationships (e.g. "isControlledBy Y") are represented as edges.
- QA Engine/Chatbot: The user interacts with the QA system through natural language queries. These

[33]https://www.data.gov.in/datasets_webservices/datasets/6622307

queries are processed to extract relevant entities (using a custom model) and converted into structured queries.

- Named Entity Recognition: A custom Named Entity Recognition (NER) model was developed using the pre-trained en_core_web_lg model from spaCy to meet the specific needs of the agriculture domain. While the en_core_web_lg model offers strong general purpose capabilities, it does not focus on agriculture related terms. Therefore, it was fine tuned to recognize entities relevant to agriculture, such as crops, pests, fertilizers, and diseases. Text data related to agriculture was collected, covering topics like groundnut seed variety, pest control, production technologies, and protection technologies. This data was manually labeled with agriculture-specific categories, such as Seed Variety, Controlled Pests, Diseases, and Symptoms. A simple JSON annotation methods were used for tagging. The en_core_web_lg model served as a starting point because it already contains strong word embeddings and pre-trained NER capabilities. It was fine tuned using the labeled agriculture dataset to make it suitable for identifying domain-specific terms.
- SPARQL Query: The system uses a set of predefined query templates that are dynamically adapted based on the entities and relationships identified in the user's query. By adding the identified entities (like seed variety, disease, etc.) into these templates, the system creates specific SPARQL queries to find the most relevant information from the knowledge graph.
- Answer Retrieval: The system retrieves the most relevant answers from the ontology graph database by executing the generated SPARQL query. These answers are then processed and converted into clear, natural language responses to ensure they are easily understood by the user. In cases where the query does not provide enough information to generate a precise answer, the system offers default responses.

The proposed framework integrates semantic web technologies to provide accurate, context-aware information to farmers, specifically focusing on the groundnut crop in Gujarat. By combining ontology-based knowledge representation with natural language processing, it effectively addresses the challenge of delivering precise, region-specific agricultural knowledge.

V. Creation of Groundnut Ontology

Currently, several groundnut ontologies are available, such as the AgroPortal and Agropedia groundnut ontologies. The question is whether an existing groundnut ontology can be used for gujarat-based agriculture. If so, can these agriculture ontologies be applied as they are, or will changes and modifications be needed? To address this question, detailed research was conducted by examining two existing groundnut ontologies: the agro-portal groundnut ontology[34] [33] and the agropedia [34] groundnut ontology.

As a result, it was found that the existing groundnut ontologies offer a variety of concepts that can be directly applied to the Gujarat region. Agropedia groundnut ontology is an Indian ontology. Therefore, the majority of the concepts (85%) are those that can be directly acquired from the agropedia groundnut ontology for the gujarat-based groundnut ontology[35]. In the Agroportal ontology[36], there are 700+ concepts, of which 108 concepts can be acquired for the Gujarat-based groundnut ontology. Certain concepts were found to be missing, so specific concepts related to Gujarat groundnut were added like Seed varieties (specifically used in gujarat area) Abnormality (Color(leaf), Groundnut stage, Abnor part, Shape (leaf), Symptoms), Resistance, etc.

To address the missing concepts, authentic online sources were used as references to build the ontology, including Junagadh Agriculture University[37], Anand agriculture university[38], Gujarat State seeds corporation limited[39] and Wikipedia[40] as references to build the ontology.

The ontology was manually constructed using the Protégé tool. It includes 300 classes, 21 object properties, and 8 data properties. Additionally, 104 individuals were created, which are the basic components of the ontology. In total, the ontology contains 1,569 axioms. Fig. 3 illustrates the hierarchy of classes, individuals, object properties, and data properties within the groundnut Ontology.

The groundnut crop ontology includes two major classes: Production Technology and Protection Technology. "Production Technology" class focuses on various aspects of growing groundnut crops. It has four main subclasses: Field Preparation, Nutrient Management, Water Management, and Seed and Sowing. Among these, the Seed and Sowing subclass is especially important. It includes three specific classes: Veldi, Ardhveldi, and Ubhadi. These classes contain 20+ individuals that represent different seed varieties. Each individual includes important details such as the year of release, oil content, days to maturity, pod kernel yield, etc. Fig. 4 shows how these individuals are organized in the ontology.

"Protection technology" class deals with protecting groundnut crops from various threats. A key subclass under this is Biotic Stress, which covers 45 diseases grouped into three categories: Diseases, Insect Pests, and Weeds. Another important subclass is Controlled Pest, which lists more than 35 pest control chemicals. These chemicals are linked to specific insect pests and help in managing the damage they cause. This subclass has been carefully designed to describe how pests affect crops and which chemicals are most effective in controlling them.

The groundnut ontology provides a comprehensive framework tailored for Gujarat-based agriculture, integrating concepts from existing ontologies, like agropedia and agroportal

[34]https://agroportal.lirmm.fr/ontologies/CO_337/?p=classes
[35]Agropedia http://agropedia.iitk.ac.in/
[36]Agrovoc https://agroportal.lirmm.fr/ontologies/CO_337/?p=classes
[37]Junagadh agriculture universityhttp://www.jau.in/.
[38]Anand agriculture university http://www.aau.in/.
[39]Gujarat State seeds corporation limited http://www.gurabini.com/.
[40]GroundNut Wikipedia https://en.wikipedia.org/wiki/Peanut.

Fig. 3. Groundnut ontology class hierarchy, individuals, object and data properties.

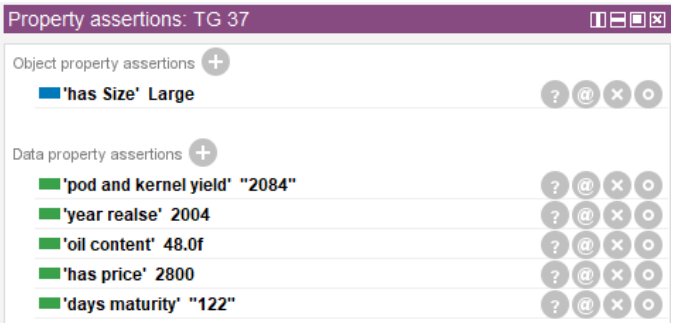


Fig. 4. TG-37 seed variety.

while addressing gaps through additional classes and properties specific to the region. Its detailed design, incorporating 300+ classes and hundreds of axioms, serves as a valuable resource for agro-advisory systems, research, and decision-making processes.

A. RDF Representation of Knowledge Graph

Neo4j[41] [35][36], the graph database [37], is used to efficiently represent and manage the groundnut ontology in the ontology-based question-answering system[42].

The groundnut ontology was first imported into the Neo4j tool, using the Neo Semantic plugin, which is required for importing ontologies into Neo4j[43]. The RDF groundnut ontology file, once imported into Neo4j, represents the fundamental components of a knowledge graph. Each entity within the groundnut ontology, such as seed variety, method of sowing, symptoms, protection technology, production technology, etc. are represented as a node in the graph. Edges connecting the respective nodes represent the relationships between these entities, which indicate dependencies, associations, and interactions. Furthermore, properties related to entities, such as daysMaturity, hasSize, hasPrice, oilContent, podAndKer-

[41] https://neo4j.com/
[42] https://neo4j.com/labs/neosemantics/
[43] https://neo4j.com/labs/neosemantics/

nelYield etc., are embedded within the graph nodes. The given query 1 demonstrates how to import the groundnut ontology into Neo4j using the n10s.rdf.import.fetch procedure. The query fetches the ontology from the provided RDF file URL and imports it into Neo4j in the RDF/XML format, with specific labels assigned to classes, object properties, and data type properties.

Listing 1: Query example

```
CALL n10s.rdf.import.fetch
("https://raw.githubusercontent.com
/PurviPatel20/with-Label/main/Groun
dnut_2.0.rdf","RDF/XML",
{
classLabel : 'Category',
objectPropertyLabel: 'Rel',
dataTypePropertyLabel: 'Prop'
});
```

The execution of query 1 successfully imports the ontology, ensuring that the defined categories, relationships, and properties are accurately integrated into the Neo4j database.

VI. Experiment and Setup

A. Neo4j Query

After successfully importing the groundnut ontology into Neo4j, the database was queried using Cypher, Neo4j's query language[44]. For example, to retrieve detailed information about a specific seed variety, a sample Cypher query to extract infomation about specific seed variety is shown below in query 2.

Listing 2: Query to retrive information about seed variety

```
OPTIONAL MATCH (i:ns0__Ubhadi)
WHERE i:ns0__Ubhadi
RETURN
i.rdfs__label As Seed_variety,
i.ns0__yearRelease As year,
i.ns0__daysMaturity As Days,
i.ns0__hasPrice As Price,
i.ns0__oilContent As Oil,
i.ns0__podAndKernelYield As
pod_and_kernel
```

This query language allows for precise data retrieval from a database. The Cypher query uses an OPTIONAL MATCH clause to retrieve data about the "Ubhadi" seed variety from a database. The WHERE clause ensures that only nodes labeled "ns0_Ubhadi" are returned in the query results.The RETURN statement indicates which properties will be included in the output, as illustrated in the Fig. 5. These properties encompass the seed variety label, release year, days to maturity, market price, oil content, and pod and kernel yield. This structured approach enables the extraction of comprehensive information about the "Ubhadi" seed variety.

[44]https://neo4j.com/docs/cypher-manual/3.5/

Seed_variety	year	Days	Price	Oil	pod_and_kernel
"GJG 9"	2009	"103"	3410	49.0	"1663"
"TPG 41"	2004	"122"	null	49.0	"2088"
"GG 8"	2006	"104-107"	null	46.0	"1776"
"GG 7"	2001	"100"	null	49	null
"GG 6"	1999	"115-120"	null	50.3	"2.78"
"GG 5"	1996	101	2310	49.2	"1270"
"IG 37A"	2004	"122"	2800	null	null
"GG 2"	null	"100-105"	2310	null	null
"J 11"	null	"110-115"	null	null	null
"GG 20"	1992	"120"	2310	50.7	"1960"

Fig. 5. Neo4j query to get all details of groundnut seed variety.

B. Interactive Interface for Question to Query Conversion

Neo4j was used in conjunction with Google colab, which allowed the use of important libraries such as py2neo, neo4j-driver, spaCy, and Gradio. The goal was to create a chatbot-style interface for the groundnut ontology. This given algorithm receives a user's question as a natural language (string input) and outputs a response string.

Algorithm 1 Question Processing and Answer Extraction

1: **Preprocessing:**
   a. Tokenize the question using the NLTK library's `word_tokenize` function.
   b. Perform part-of-speech tagging on the tokenized words using the NLTK library's `pos_tag` function.
   c. Extract the entity from the question using the `extract_entity` function (custom model).

2: **Answer Extraction:**
   a. If the extracted entity is None, return a default message indicating that the seed variety is not understood.
   b. Open a session with the Neo4j database using the `driver.session()` function.
   c. Identify entities from the question.
   d. Execute a Neo4j Cypher query to retrieve an appropriate response.
   e. If the query returns no results, return a default message indicating that no information is found.

The input text may contain important entities such as seed variety, disease name, symptoms etc. To identify these important named entities, the en_core_web_lg pipeline from

spaCy was used.A custom model was trained to recognize entities such as “Price”, “Rate”, “Disease”, “Symptoms”, “Cure”, “Pesticide”, “Crop”, etc. This model was designed to handle specific cases that were not covered by the standard model.

The standard model, when given with sentence like “What is a price of GJG 22?” identified “GJG 22” as an organization. Similarly, the model was not able to identify name of the symptoms. It classified it as a product entity. To address this, a custom dataset was created to identify the text “GJG 22” as a crop entity. Using Gradio, a python library, a system was built that allows users to ask questions in natural language and receive answers based on the groundnut ontology. This approach made it easier for users to interact with the Neo4j database and get useful information.

VII. Results and Discussion

The provided Fig. 6 depicts a sample example of an ontology-based question-answer system. In the example presented, the user input is a question formulated in natural language: “What is the price of GJG 22?”. The system processes this query, which utilizes ontological knowledge to understand and generate an appropriate response. The response generated by the system is displayed within the image: “The price of GJG 22 is 2310.”

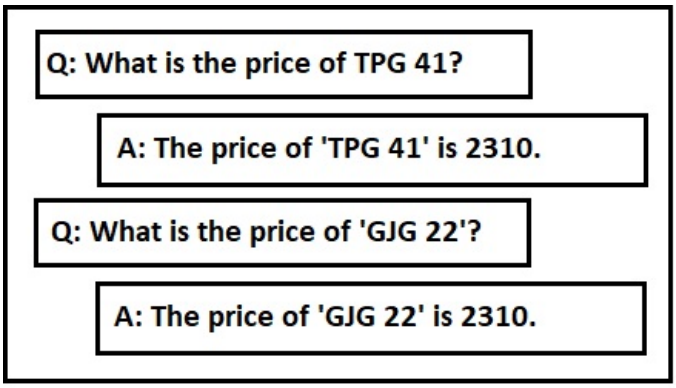


Fig. 6. Output 1: Snapshot of an ontology-based question-answer.

In Fig. 7, the user inputs a query in natural language, specifically requesting comprehensive details about the seed variety labelled “GJG 22.” The system then generates an appropriate response, which is displayed in the form of text within the interface. The response provided by the system encapsulates various attributes associated with the seed variety “GJG 22.” These attributes include: price, days maturity, pod and kernel yield and oil content. This interaction demonstrates the system’s ability to interpret complex natural language queries and retrieve structured information from groundnut ontology, facilitating efficient access to relevant data for users.

In the evaluation of the Question Answering (QA) system, a total of 100 distinct questions were submitted, and the responses were manually ranked based on their correctness. In this ranking scheme, a rank of 5 indicates a fully correct answer, while a rank of 1 represents a fully incorrect response. Ranks 2 to 4 denote varying degrees of partial correctness,

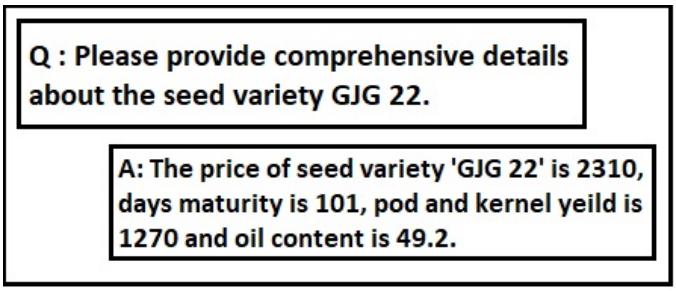


Fig. 7. Output 2: Snapshot of an ontology-based question-answer.

reflecting the extent to which the answers met the query requirements. The results of the evaluation are summarized in the Table I.

TABLE I. Ranking Table

Rank	No. of Questions
5	50
4	20
3	20
2	5
1	5

For instance, in the case of rank 1, the system failed to recognize “Peanut Strips” as a single entity, which significantly hindered its ability to retrieve the appropriate response from the underlying groundnut ontology. Additionally, an example of a partially correct response can be observed in the question, “What are the pesticide methods for the following symptoms: Buckling and crinkling between veins?” In this instance, the system provided an answer that was relevant but lacked completeness.

$$\text{Average Rank} = \frac{\sum_{i=1}^{n}(r_i \times q_i)}{\sum_{i=1}^{n} q_i} \quad (1)$$

Where:

- n is the total number of different ranks (which is 5 in this case).
- $r_i \times q_i$ represents the weighted contribution of each rank to the total score.

Using the formula 1 for average rank, the overall performance of the system was calculated to be 4.05. This indicates that while the system provided a significant number of accurate responses, there is still considerable room for improvement in handling complex queries and recognizing key entities.

VIII. Conclusion and Future Work

The proposed ontology-based QA system can be a valuable resource for farmers in Gujarat. Farmers can ask questions in natural language, and the system is designed to provide relevant answers using the groundnut ontology. The main objective is to give farmers access to insights that can help improve their farming practices and enhance groundnut crop yield. The overall accuracy of the answers is 80%. Additionally, the

ontology aids in semantic disambiguation. In the future, more concepts can be added to the ontology. The proposed model can also be adapted for other crop ontologies and developed in different languages.

References

[1] S. Chaudhary, M. Bhise, A. Banerjee, A. Goyal, and C. Moradiya, "Agro advisory system for cotton crop," in *2015 7th International Conference on Communication Systems and Networks (COMSNETS)*, 2015, pp. 1–6.

[2] M. Fernandez, V. Lopez, M. Sabou, V. Uren, D. Vallet, E. Motta, and P. Castells, "Semantic search meets the web," in *2008 IEEE International Conference on Semantic Computing*, 2008, pp. 253–260.

[3] D. Martyniuk, N. Karam, M. Falkenthal, Y. Dong, and A. Paschke, *Semantifying the PlanQK Platform and Ecosystem for Quantum Applications*, 09 2023.

[4] A. Daud, M. H. Ullah, A. R. Banjar, and A. A. Alshdadi, "Ontological modeling and semantic search in quran," *IJCSNS*, vol. 22, no. 5, p. 771, 2022.

[5] A. Ga, A. Mukherjee, M. Roy, and N. Chandra, "Mobile based agro advisory service and farmer's willingness to pay: A case study in bageshwar district of uttarakhand," vol. 16, pp. 976–986, 12 2021.

[6] M. J. Bisheko and R. G, "A study on farmers' perceptions about the scope of the kisan suvidha app in improving agricultural sustainability," in *2023 Conference on Information Communications Technology and Society (ICTAS)*, 2023, pp. 1–5.

[7] *"Case Study IFFCO Kisan Agriculture App Evolution to Data Driven Services in Agriculture_2016"*. GSMA, Oct 2016.

[8] A. Yadav, P. Thilagam, and S. Singh, "Mobile applications for agricultural transformation: Types, impacts, case studies, and recommendations," 2023.

[9] *"Case Study mKisan, India"*. GSMA, Feb 2015.

[10] S. K. Mahapatra and J. Pradhan, "Smartphone apps-an eminent ict tools for agricultural development & agri-information dissemination," *ICT: A Catalyst to Transform Rural India*, p. 5.

[11] D. B. J. Rabba Gundu Devender Goude, "Agribuzz-agriculture management system," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, p. 5, Apr 2022.

[12] P. K. Reddy, G. V. Ramaraju, and G. S. Reddy, "esagu™: a data warehouse enabled personalized agricultural advisory system," in *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data*, ser. SIGMOD '07. New York, NY, USA: Association for Computing Machinery, 2007, p. 910–914. [Online]. Available: https://doi.org/10.1145/1247480.1247586

[13] V. UREN, Y. LEI, V. LOPEZ, H. LIU, E. MOTTA, and M. GIORDANINO, "The usability of semantic search tools: a review," *The Knowledge Engineering Review*, vol. 22, no. 4, p. 361–377, 2007.

[14] J. Weizenbaum, "Eliza—a computer program for the study of natural language communication between man and machine," *Commun. ACM*, vol. 9, no. 1, p. 36–45, Jan. 1966. [Online]. Available: https://doi.org/10.1145/365153.365168

[15] P. Y. Niranjan, V. S. Rajpurohit, and R. Malgi, "A survey on chat-bot system for agriculture domain," in *2019 1st International Conference on Advances in Information Technology (ICAIT)*, 2019, pp. 99–103.

[16] W. Maroengsit, T. Piyakulpinyo, K. Phonyiam, S. Pongnumkul, P. Chaovalit, and T. Theeramunkong, "A survey on evaluation methods for chatbots," 03 2019, pp. 111–119.

[17] S. Singh and H. K. Thakur, "Survey of various ai chatbots based on technology used," in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2020, pp. 1074–1079.

[18] S. Gaikwad, R. Asodekar, S. Gadia, and V. Attar, "Agri-qas question-answering system for agriculture domain," 08 2015, pp. 1474–1478.

[19] M. Devi and M. Dua, "Adans: An agriculture domain question answering system using ontologies," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 122–127.

[20] N. Darapaneni, R. Tiwari, A. R. Paduri, S. Saurav, R. Chaoji, and Sohil, "Farmer-bot: An interactive bot for farmers," *ArXiv*, vol. abs/2204.07032, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:248178166

[21] G. Mostaco, L. Campos, I. Souza, and C. Cugnasca, "Agronomobot: a smart answering chatbot applied to agricultural sensor networks," 06 2018.

[22] D. Sawant, A. Jaiswal, J. Singh, and P. Shah, "Agribot - an intelligent interactive interface to assist farmers in agricultural activities," in *2019 IEEE Bombay Section Signature Conference (IBSSC)*, 2019, pp. 1–6.

[23] N. Jain, P. Jain, P. Kayal, J. Sahit, S. Pachpande, J. Choudhari, and M. Singh, "Agribot: Agriculture-specific question answer system," 06 2019.

[24] B. Arora, D. S. Chaudhary, M. Satsangi, M. Yadav, L. Singh, and P. S. Sudhish, "Agribot: A natural language generative neural networks engine for agricultural applications," in *2020 International Conference on Contemporary Computing and Applications (IC3A)*, 2020, pp. 28–33.

[25] M. Momaya, A. Khanna, J. Sadavarte, and M. Sankhe, "Krushi – the farmer chatbot," 06 2021, pp. 1–6.

[26] C. Bhuvaneswari, H. Pokhariya, P. Yarde, V. Vekariya, H. Patil, and N. L, "Implementing ai-powered chatbots in agriculture for optimization and efficiency," 01 2024, pp. 1–7.

[27] "Agroxpert - farmer assistant," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 506–512, 2021, international Conference on Computing System and its Applications (ICCSA- 2021). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666285X21000443

[28] K, E. Venkat Reddy, K. Sathvik, S. Laya, and Harsha, "Agriculture assistant chatbot," *International Journal of Innovative Science and Research Technology (IJISRT)*, vol. 5, pp. 116–123, 2024.

[29] A. Marla, R. Paul, A. K. Saha, N. K. Basha, and B. Anandhakrishnan, "An agrobot: Natural language processing based chatbot for farmers," in *2023 4th International Conference on Smart Electronics and Communication (ICOSEC)*, 2023, pp. 1235–1241.

[30] E. Asolo, I. Gil-Ozoudeh, and C. Ejimuda, "Ai-powered decision support systems for sustainable agriculture using ai-chatbot solution," *Journal of Digital Food, Energy and Water Systems*, vol. 5, 06 2024.

[31] B. Zhao, W. Jin, J. Del Ser, and G. Yang, "Chatagri: Exploring potentials of chatgpt on cross-linguistic agricultural text classification," *Neurocomputing*, vol. 557, p. 126708, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231223008317

[32] N. Chandolikar, C. Dale, T. Koli, M. Singh, and T. Narkhede, "Agriculture assistant chatbot using artificial neural network," in *2022 International Conference on Advanced Computing Technologies and Applications (ICACTA)*, 2022, pp. 1–5.

[33] C. Jonquet, A. Toulet, E. Arnaud, E. D. Yeumo, J. Graybeal, M.-A. Laporte, M. A. Musen, P. Larmande, S. Aubin, V. Pesce, and V. Emonet, "Agroportal: A vocabulary and ontology repository for agronomy," *Computers and electronics in agriculture.*, vol. 144, p. 126—143, January 2018. [Online]. Available: https://doi.org/10.1016/j.compag.2017.10.012

[34] M. Sini, V. Yadav, J. B. Singh, V. Awasthi, and P. Tv, "Knowledge models in agropedia indica," 2009. [Online]. Available: https://api.semanticscholar.org/CorpusID:55110203

[35] F. Holzschuher and R. Peinl, "Performance of graph query languages: Comparison of cypher, gremlin and native access in neo4j," 03 2013.

[36] F. Gong, Y. Ma, W. Gong, X. Li, C. Li, and X. Yuan, "Neo4j graph database realizes efficient storage performance of oilfield ontology," *PLOS ONE*, vol. 13, no. 11, pp. 1–16, 11 2018. [Online]. Available: https://doi.org/10.1371/journal.pone.0207595

[37] Y. Chen and X. Xing, "Constructing dynamic knowledge graph based on ontology modeling and neo4j graph database," in *2022 5th International Conference on Artificial Intelligence and Big Data (ICAIBD)*, 2022, pp. 522–525.

Leveraging Semi-Supervised Generative Adversarial Networks to Address Data Scarcity Using Decision Boundary Analysis

Mohamed Ouriha[1], Omar El Mansouri[2], Younes Wadiai[3], Boujamaa Nassiri[4],
Youssef El Mourabit[5], Youssef El Habouz[6]
TIAD Laboratory, Sciences and Technology Faculty, Sultan Moulay Slimane University, Beni Mellal, Morocco[1,2,5]
Laboratory of Innovative Systems Engineering-National School of Applied Sciences of Tetouan,
Abdelmalek Essaâdi University, Tetouan, Morocco[3]
InterDisciplinaire Applied Research Laboratory, LIDRA International, University of Agadir Unversiapolis, Agadir, Morocco[4]
IGDR Umr 6290 Cnrs Rennes University, Rennes, France[6]

***Abstract*—Convolutional Neural Networks (CNNs) are widely regarded as one of the most effective solutions for image classification. However, developing high-performing systems with these models typically requires a substantial number of labeled images, which can be difficult to acquire. In image classification tasks, insufficient data often leads to overfitting, a critical issue for deep learning models like CNNs. In this study, we introduce a novel approach to addressing data scarcity by leveraging semi-supervised classification models based on Generative Adversarial Networks (SGAN). Our approach demonstrates significant improvements in both efficiency and performance, as shown by variations in the evolution of decision boundaries and overall accuracy. The analysis of decision boundaries is crucial, as it provides insights into the model's ability to generalize and effectively classify new data points. Using the MNIST dataset, we show that our approach (SGAN) outperform CNN methods, even with fewer labeled images. Specifically, we observe that the distance between the images and the decision boundary in our approach is larger than in CNN-based methods, which contributes to greater model stability. Our approach achieves an accuracy of 84%, while the CNN model struggles to exceed 72%.**

***Keywords*—Decision boundary; convolutional neural network; Generative Adversarial Networks; MNIST; classification; semi-supervised classification**

I. Introduction

Deep learning (DL), a branch of machine learning (ML), is characterized by its significant flexibility and learning power. It represents the world through concepts organized in nested hierarchies, where each concept is defined in simpler terms and more abstract representations [1]–[6].

One of the essential skills in computer vision is the accurate classification of images. The development of image collection equipment, combined with the widespread use of digital platforms, has led to an exponential growth in the volume of digital data, necessitating the creation of robust and advanced models to analyze this vast influx of visual information. Deep learning has been proposed for image classification due to its capability to provide more detailed insights into a subject's response to specific visual stimuli. Recent research indicates that strategies based on deep learning have yielded impressive results [7].

Image classification is one of the most common challenges in computer vision. The success of a classification system is highly dependent on the quality of the attributes derived from an image, with the accuracy of the results improving in proportion to the quality of these features. These attributes are often utilized in supervised learning, where a set of features X (usually extracted from an image) is employed to predict a certain outcome Y. Before the widespread adoption of deep learning in 2012, commonly used machine learning models included support vector machines, artificial neural networks, and random forests; these traditional methods were the primary techniques for processing computer vision tasks [8].

Convolutional neural networks (CNNs) are now the most popular method for image analysis and classification due to the growing interest in deep learning. CNNs have achieved significant results across a wide range of classification problems. Despite their tremendous potential, they continue to face several challenges. These difficulties are largely due to the vast scale of the networks, which may contain millions of parameters, a lack of sufficient training datasets, overfitting issues, and poor generalization capabilities. Additionally, a growing concern among researchers is the need to prevent adversarial attacks that could mislead deep neural networks (DNNs) [9].

To address these issues and enhance performance, researchers are modifying network architectures, developing new learning algorithms, and acquiring more data. A typical challenge is the scarcity of high-quality data or an unequal distribution of classes within datasets. Currently, the most efficient DNNs are quite large and require massive amounts of data, which can be difficult to obtain. For example, the popular CNN architecture VGG16 has 16 layers of neurons and 138 million parameters [10].

Generally, deep learning algorithms are considered data-hungry, necessitating many labeled images to produce the desired fits. This requirement may render these technologies inaccessible for smaller projects, which often have limited datasets. Data augmentation [11] and transfer learning [12] are two approaches to addressing this challenge. We continue along this path to find a relevant solution by presenting a semi-supervised approach (SGAN) with a novel learning technique: utilizing both labeled and unlabeled images based on Gener-

ative Adversarial Networks. We compare our approach with CNNs using the same dataset.

To evaluate these approaches, we focus on a crucial aspect that plays an indispensable role in understanding deep learning: the decision boundary. For each approach, we will examine how the decision boundary evolves during training.Our approaches demonstrate excellent performance in image classification. A brief description of GANs, CNNs, and decision boundaries is provided below.

The rest of the paper is organized as follows: Section II delineates the methodology and the proposed approach. Section III is dedicated to the presentation of results and their subsequent discussion. Finally, Section IV offers the concluding remarks.

II. Methodology

A. Convolutional Neural Networks (CNN)

A convolutional neural network [13]–[16] comprises an input layer, an output layer, and several hidden layers. Each layer converts a set of activations into another using a differentiable function. Generally, there are three main types of hidden layers: convolutional layers, pooling layers, and fully connected layers (Fig. 1).

1) Convolution layer: Convolution is performed by translating the convolution kernel through the input image matrix. To establish a network of local connections, each neuron in the local window is linked to a corresponding neuron in the convolution layer. This configuration enables weights and a global bias to be learned for each connection [31]. The convolution operation is mathematically defined as follows:

$$a_{ij} = \varphi\left(b_i + \sum_{k=1}^{3} w_{ik} x_{j+k-1}\right) = \varphi\left(b_i + \mathbf{w}_i^T \mathbf{x}_j\right) \qquad (1)$$

Here, a_{ij} represents the activation or output of the j-th neuron of the i-th filter in the hidden layer, φ denotes the neural activation function, b_i signifies the shared overall bias of filter i, $\mathbf{w}_i = [w_{i1} \quad w_{i2} \quad w_{i3}]^T$ is the vector comprising shared weights, and $\mathbf{x}_i = [x_j \quad x_{j+1} \quad x_{j+2}]^T$

The output produced by this layer is known as a feature map, which contains information concerning the input by filtering and learning the weighted inputs. When multiple localized features must be extracted, additional convolution kernels are employed to create more feature maps [31].

2) Pooling layer: This layer carries subsampling to simplify and summarise the attribute map. Max-pooling selects the maximum value for each kernel, reducing the size of the feature map and the computational cost while preserving the essential characteristics of the images. There are many types of pooling: Average, Max, Sum, etc.

3) Fully connected layers: Fully connected layers: After several layers of convolution, ReLU and pooling, fully connected layers link each neuron in one layer to each neuron in the next layer [11]. This structure works in the same way as the classical multilayer perceptron (MLP) neural network [17], [18]. With a softmax activation function, the latter is generally used to predict posteriori probabilities of each class.

One common issue with CNN is that it is perceived to be data-hungry [12]. Because of the vast number of learnable parameters, CNNs may require a substantial amount of data (particularly labeled images) to provide accurate predictions. Limited training data in little applications can lead to overfitting. We present techniques to tackle this problem. We will compare our results to those of the CNN model. The architecture of our CNN model is presented in the following sections.

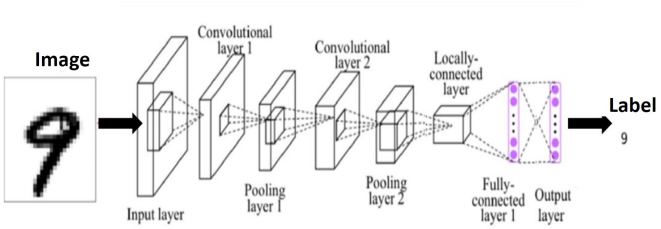


Fig. 1. CNN architecture.

B. Generative Adversarial Network (GAN)

Presented by Goodfellow et al. [19], GANs are a novel technique that work by alternating the training of two distinct neural networks: the discriminator D, which is responsible for learning the characteristics of real images in order to differentiate between "fake" and "real" images; and the generator G, which creates samples from a predetermined distribution to fool D (Fig. 2).

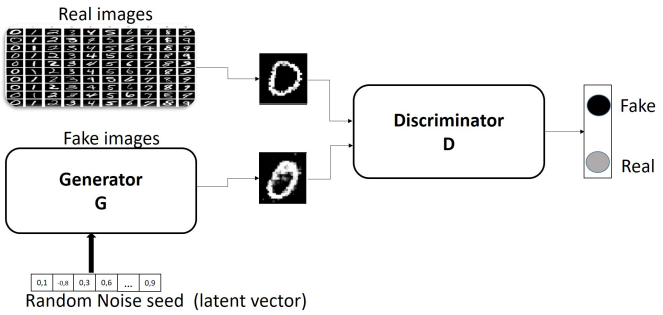


Fig. 2. GAN architecture.

The generator G receives a Gaussian random variable z as input and produces an image x as output: $G(z) = x$. The discriminator and generator typically employ CNNs, renowned for their efficiency in image identification. Throughout training, the generator and discriminator are trained in opposing directions: D's parameters are updated while G's remain unchanged, and vice versa, as outlined in algorithm 1 [20].

The discriminator's task is to distinguish between real images $x^{(1)}, \ldots, x^{(n)}$ and generated images $G(z^{(1)}), \ldots, G(z^{(n)})$ whereas the generator aims to deceive the discriminator. Let $D(x)$ be the probability that image x is real. Training the discriminator involves minimizing the binary cross-entropy loss [Eq. (2)].

$$L(D,G) = -\sum_{n=1}^{N} \log\left[D(x^{(n)})\right] + \log\left(1 - D(G(z^{(n)}))\right) \tag{2}$$

The ideal discriminator D given a fixed generator G is shown in Eq. (3).

$$D_{\text{opt}} = \text{argmin}\, L(D,G) \tag{3}$$

The ideal generator G given a fixed discriminator D is shown in Eq. (4).

$$G_{\text{opt}} = \text{argmax}\, L(D,G) = \text{argmax}\left(-\sum_{n=1}^{N} \log(1 - D(G(z^{(n)})))\right) \tag{4}$$

In practice, the loss function for G is frequently expressed by the subsequent Eq. (5):

$$G_{\text{opt}} = \text{argmax} \sum_{n=1}^{N} \log(D(G(z^{(n)}))) \tag{5}$$

Several researchers have explored developing a supervisory classification model using features from the GAN discriminator [21]. The Auxiliary-Condition GAN [22] has been the most effective method proposed for addressing the challenge of controlling generated images. In our approach, we demonstrate the way this model adapted into a supervised classification model.

Algorithm 1 MM-GAN training using minibatch stochastic gradient descent

for numberof training iteration **do**
  for k steps **do**
    - Sample a minibatch of m noise samples $\{z^{(1)}, \ldots, z^{(m)}\}$ from noise prior $p_z(z)$.
    - Sample a minibatch of m samples $\{x^{(1)}, \ldots, x^{(m)}\}$ from real data distribution p_r.
    - Update the discriminator by ascending its stochastic gradient:
    $\nabla_{OD} \frac{1}{m} \sum_{i=1}^{m} \log\left[D(x^{(i)}) + \log(1 - D(G(z^{(i)})))\right]$
  end for
  - Sample a minibatch of m noise samples $\{z^{(1)}, \ldots, z^{(m)}\}$ from noise prior $p_z(z)$.
  - Update the generator by descending its stochastic gradient:
  $\nabla_{OG} \frac{1}{m} \sum_{i=1}^{m} \log(1 - D(G(z^{(i)})))$
end for

C. Decision Boundary

A decision boundary is a fundamental concept in machine learning that delineates the input space into distinct labels. Recent research has focused on understanding neural networks through the lens of decision boundaries [23]–[25]. A decision boundary is a surface that separates data points into distinct classes. According to [25], [26], a decision boundary is defined as a region in the space where the output label of a classifier is ambiguous. Furthermore, [27], [28] note that the decision boundary can take various forms (Fig. 3), such as a hyperplane, a sphere, or a paraboloid. In higher dimensions, it can consist of multiple nonlinear hypersurfaces.

An intriguing and longstanding challenge in this field is identifying a decision boundary that elucidates the generalization capabilities of deep neural networks. Significant efforts are being made to address this issue. One popular approach involves adversarial attacks, which modify input images to influence label predictions, thereby characterizing the decision boundary of deep neural networks. This technique is often associated with Generative Adversarial Networks (GANs) [29], [30]. Several studies have leveraged this approach to investigate the decision boundaries of deep classifiers [23], [25], [26], [32].

Moreover, numerous works [33]–[37] have utilized decision boundaries to gain insights into the generalization of deep neural networks. Guan et al. [36] empirically demonstrate a negative relationship between decision boundary complexity and neural network generalization ability. This finding is further elucidated by Lei [37], who explains the inverse relationship between generalizability and decision boundary variability.

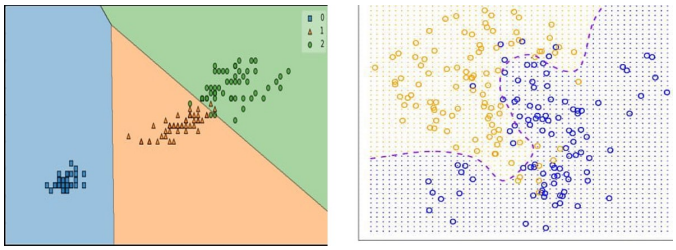


Fig. 3. Decision boundary.

Formally, the decision boundary is defined by Mickisch et al. [26] as follows:

Consider a neural network classifier $f : \mathbb{R}^n \to \mathbb{R}^c$, where n and c represent the dimensions of the input and output, respectively. For an input image $x \in \mathbb{R}^n$, the output $f(x)$ is determined by a classification decision defined as:

$$K(x) = \text{argmax}_{k=1,\ldots,c} f_k(x) \tag{6}$$

The decision boundary $D \in \mathbb{R}^n$ is defined by the formula below Eq. (7):

$$D = \left\{ x \in \mathbb{R}^n \mid \begin{array}{l} \exists k_1, k_2 = 1, \ldots, c, \\ k_1 \neq k_2,\ f_{k_1}(x) = f_{k_2}(x) = \max\limits_k f_k(x) \end{array} \right\} \tag{7}$$

D. Proposed Approach

Numerous works in the literature have identified the computational challenges associated with extracting useful features for image classification, particularly when dealing with limited labeled data. Two main approaches for training a classifier using a small number of labeled instances alongside a much larger collection of unlabeled data are semi-supervised learning and transfer learning. In this section, we introduce a semi-supervised approach (SGAN) that utilizes Generative Adversarial Networks (GANs) [38] through decision boundary analysis. This method effectively leverages both unlabeled and labeled data to enhance classifier training.

The traditional GAN discriminator is modified within the context of semi-supervised learning using GANs. This adapted discriminator is specifically designed to produce an output equal to the number of actual classes k [40]. An additional output is included, known as the $(k+1)th$ output. This extra output is utilized to identify fraudulent images generated by the GAN's generator component [39]–[41]. The $(k+1)th$ output primarily presents additional information in the form

of fake images, enabling the discriminator to classify them under the $(k+1)th$ label.

Our proposed semi-supervised learning architecture, based on Augustus Odena's model [41], employs a dual-mode training technique for the discriminator. This strategy combines supervised and unsupervised learning methods. In the first mode, the discriminator learns to predict the class labels for real images. In the second mode, the discriminator component of GANs is trained similarly to regular GANs, with the aim of distinguishing between real and generated (fake) images. Our proposed model offers a distinct advantage by merging unsupervised and supervised learning, facilitating effective control over the generated images and the extraction of key attributes for the classifier.

It is crucial to understand that the primary objective of our approach (SGAN) is to learn the supervised classifier. The architecture is shown in Fig. 4.

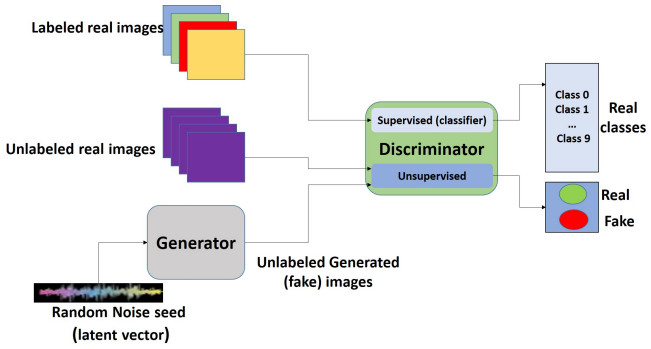


Fig. 4. Semi-supervised approach based GAN(SGAN).

The proposed architecture is composed of three primary components: a generator learned with a Gaussian distribution and examined by the discriminator; a discriminator learned with unlabeled data and influenced by a Gaussian distribution; and a supervised classifier learned with a small set of labeled data. Notably, the weights and architecture of the discriminator and supervised classifier are the same.

The generator architecture is detailed in Table I.

TABLE I. GENERATOR PARAMETERS

Layer (type)	Output Shape	Param #
input_1 (InputLayer)	(None, 100)	0
dense_1 (Dense)	(None, 12544)	1266944
leaky_re_lu (LeakyReLU)	(None, 12544)	0
reshape (Reshape)	(None, 7, 7, 256)	0
conv2d_transpose	(None, 14, 14, 128)	295040
leaky_re_lu_1 (LeakyReLU)	(None, 14, 14, 128)	0
conv2d_transpose_1	(None, 14, 14, 64)	73792
leaky_re_lu_2 (LeakyReLU)	(None, 14, 14, 64)	0
conv2d_transpose_2	(None, 28, 28, 1)	577

We concentrate on the discriminator that is used for classifying MNIST images, comparing our approach (SGAN) to a CNN model with the same architecture as our discriminator (see Table II), using precision, loss, and decision boundary evolution using DeepFool: A function to calculate the distance to the decision boundary (Algorithm 2) [46]

TABLE II. DISCRIMINATOR GAN / CNN CLASSIFIER PARAMETERS

Layer (type)	Output Shape	Param #
input_2 (InputLayer)	(None, 28, 28, 1)	0
conv2d_3 (Conv2D)	(None, 14, 14, 32)	320
leaky_re_lu_3 (LeakyReLU)	(None, 14, 14, 32)	0
conv2d_4 (Conv2D)	(None, 7, 7, 64)	18496
leaky_re_lu_4 (LeakyReLU)	(None, 7, 7, 64)	0
conv2d_5 (Conv2D)	(None, 4, 4, 128)	73856
leaky_re_lu_5 (LeakyReLU)	(None, 4, 4, 128)	0
flatten_1 (Flatten)	(None, 2048)	0
dropout_1 (Dropout)	(None, 2048)	0
dense_2 (Dense)	(None, 10)	20490

Algorithm 2 DeepFool: A function to calculate the distance to the decision boundary

Require: Image $image$, Model $model$, Number of classes $num\_classes = 10$, Maximum iterations $max\_iter = 50$, Small constant $\epsilon = 0.02$

Ensure: Perturbed image $perturbed\_image$, distance $distance$

Convert $image$ to tensor format.
Initialize $perturbed\_image \leftarrow image$
Initialize $w \leftarrow 0$, $r\_tot \leftarrow 0$
Get initial prediction $f\_image \leftarrow model.predict(image)$
Set $label \leftarrow \arg\max(f\_image)$
for $i = 1$ to max_iter **do**
    Convert $perturbed\_image$ to tensor format and add batch dimension.
    Compute the gradient of loss:
    $loss \leftarrow f\_perturbed[label] - \max(f\_perturbed[\text{other classes}])$
    Calculate gradient $\nabla loss$ with respect to $perturbed\_image$.
    Compute the norm of the gradient $gradients\_norm$.
    Initialize $perturbation \leftarrow \infty$, $adv\_label \leftarrow None$
    for each class k in $num\_classes$ **do**
        if $k = label$ **then**
            continue
        end if
        Compute $w_k \leftarrow \nabla loss[k] - \nabla loss[label]$
        Compute $f_k \leftarrow f\_image[k] - f\_image[label]$
        Calculate $pert\_k \leftarrow \frac{|f_k|}{gradients\_norm}$
        if $pert\_k < perturbation$ **then**
            $perturbation \leftarrow pert\_k$
            $w \leftarrow w_k$
            $adv\_label \leftarrow k$
        end if
    end for
    Compute the perturbation $r_i \leftarrow \frac{(perturbation+\epsilon)\times w}{gradients\_norm}$
    Update $r\_tot \leftarrow r\_tot + r_i$
    Update $perturbed\_image \leftarrow clip(image + r\_tot, 0, 1)$
    Get the new prediction $f\_perturbed \leftarrow model.predict(perturbed\_image)$
    $p\_label \leftarrow \arg\max(f\_perturbed)$
    if $p\_label \neq label$ **then**
        break
    end if
end for
Compute $distance \leftarrow \|r\_tot\|$
return $perturbed\_image$, $distance$

III. Results and Discussion

A. Database

The Modified National Institute of Standards and Technology (MNIST) dataset is widely considered a standard for digit recognition systems [42]. LeCun et al. [43] introduced it in 1998.MNIST contains 70,000 grayscale images at a resolution of 28 x 28 pixels. The dataset contains patterns drawn from two sources: NIST's Special Database-1 (high school student handwriting) and NIST's Special Database-3 (U.S. Census Bureau employee handwriting).The dataset is divided into two sets: a training set of 60,000 images and a test set of 10,000 images, which are properly separated so that no writer appears in both sets [42], [44]. Fig. 5 shows that handwriting styles vary significantly among writers.

Fig. 5. A sample from MNIST dataset.

B. Classification Complexity

The t-SNE method aims to illustrate high-dimensional data by mapping every data instance to a specific location in two- or three-dimensional space [45]. Fig. 6 illustrates the dataset in two dimensions, where we can observe that some sample classes are intermixed.

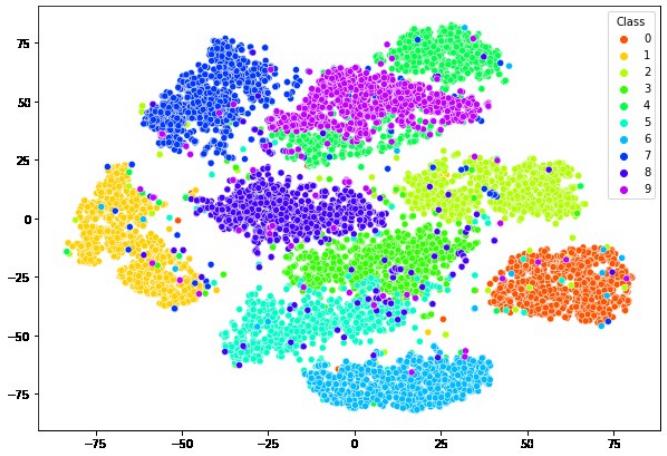


Fig. 6. TSNE visualization of MNIST dataset.

C. Results

In this section, we explore two deep learning techniques, CNN and SGAN classifiers, applied to the MNIST dataset. We specifically focus on configurations where only 100 labeled images are used for training, ensuring equal representation from each class. Notably, the CNN classifier employed in our work shares the same architecture as the SGAN model. The primary distinction lies in the training strategy: the CNN classifier is trained using supervised learning, whereas the SGAN model utilizes a semi-supervised learning. Our objective is to address the challenge of limited labeled data through the semi-supervised methodology of the SGAN.

For the testing phase, we used a dataset of 10,000 images (test set). We developed two classification models: an SGAN and a CNN classifier. The results are summarized in Table III, highlighting the accuracy and loss metrics for both models. Our experimental results indicate that the SGAN model outperforms the CNN classifier, achieving an accuracy of 84% compared to 72% for the CNN. Additionally, the SGAN model exhibited a lower loss of 0.54, while the CNN model recorded a higher loss of 0.93. These findings underscore the effectiveness of the SGAN approach compared to the traditional CNN. To further demonstrate the superiority of our approach, we analyzed a critical aspect of deep learning model evaluation: the decision boundary. Our analysis involved tracking the evolution of this boundary during training and quantifying the distance of images from it. As shown in Fig. 7 and Fig. 8, the distance from the decision boundary is significantly greater for the SGAN compared to the CNN, indicating better generalization. The incorporation of unlabeled images in training the SGAN notably enhances the performance of the MNIST image classification model, particularly when only a small proportion of labeled images are available.

TABLE III. Accuracy and Loss Classification Metrics for SGAN, the CNN Classifier, SSAE and SVAE

	CNN	SGAN
Loss	0.93	0.54
Accuracy	72%	84%

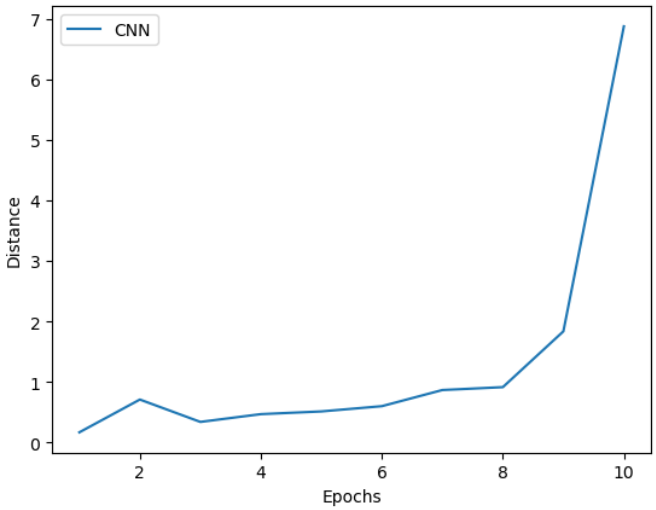


Fig. 7. Variability of the distance of CNN images to the decision boundary.

other results are presented in the appendix Section V

IV. Conclusion

We introduced a novel approach: SGAN applied to the MNIST dataset. Our experimental results highlight the superior efficiency of the SGAN models compared to the CNN model, with the SGAN achieving an accuracy of 84%. The scarcity of labeled data poses a significant challenge for image classification models; however, our proposed method effectively addresses this issue. By employing semi-supervised techniques and a novel training strategy that leverages both labeled and unlabeled images, we observed a substantial improvement in image classification performance. Notably, in terms of

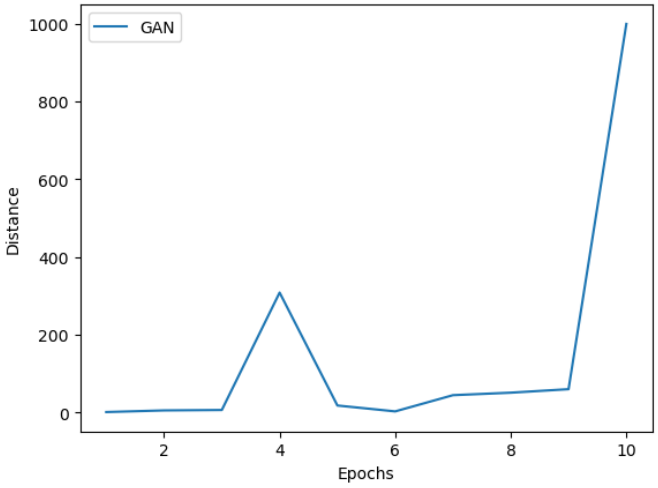


Fig. 8. Variability of the distance of SGAN images to the decision boundary.

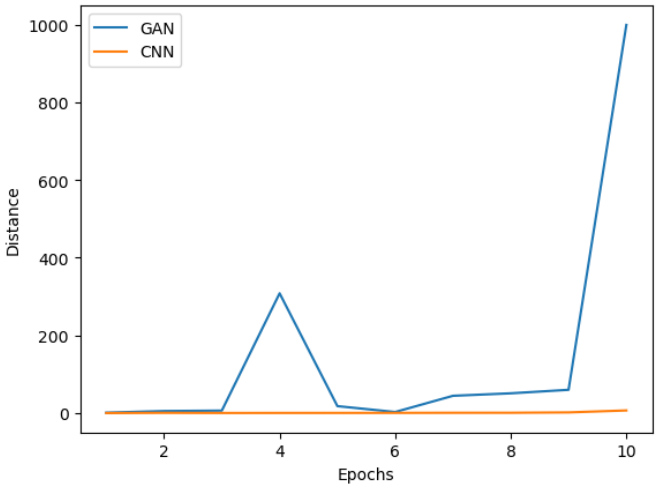


Fig. 9. Variability of the distance of CNN and SGAN images to the decision boundary.

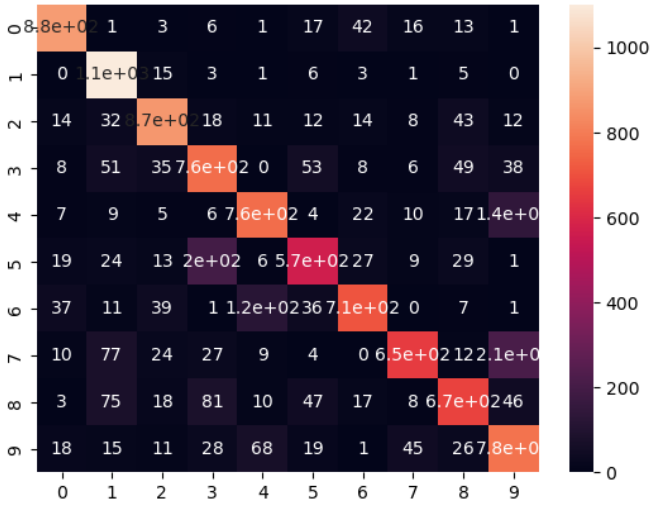


Fig. 10. The confusion matrices for the CNN modeL.

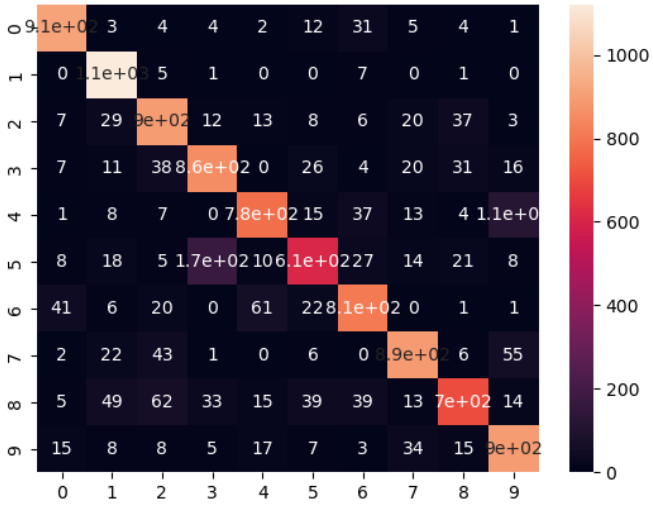


Fig. 11. The confusion matrices for the SGAN modeL.

decision boundary analysis, our models produced promising results that significantly outperform those of CNNs.

V. Appendix

In this section, we present additional results. Fig. 9 illustrates the variability of the decision boundary distance for both the CNN and SGAN models. The confusion matrix, which is a table that compares the model's predictions with the actual results, provides insight into the overall performance of the classification model. Fig. 10 and Fig. 11 show the confusion matrices for the CNN and SGAN models, respectively. Finally, we present the images generated by the generator in our SGAN approach (Fig. 12) .

Declarations

- Funding
No funding was received to assist with the preparation of this manuscript.

- Conflict of interest/Competing interests
The authors declare that they have no competing interests

- Availability of data
All data generated or analysed during this study are included in this published article

References

[1] ALZUBAIDI, Laith, ZHANG, Jinglan, HUMAIDI, Amjad J., et al. Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. Journal of big Data, 2021, vol. 8, p. 1-74.

[2] BHATTACHARYA, Sweta, SOMAYAJI, Siva Rama Krishnan, GADEKALLU, Thippa Reddy, et al. A review on deep learning for future smart cities. Internet Technology Letters, 2022, vol. 5, no 1, p. e187.

[3] WANG, Ning, WANG, Yuanyuan, et ER, Meng Joo. Review on deep learning techniques for marine object recognition: Architectures and algorithms. Control Engineering Practice, 2022, vol. 118, p. 104458.

[4] SHORTEN, Connor, KHOSHGOFTAAR, Taghi M., et FURHT, Borko. Deep Learning applications for COVID-19. Journal of big Data, 2021, vol. 8, no 1, p. 1-54.

[5] TORRES, José F., HADJOUT, Dalil, SEBAA, Abderrazak, et al. Deep learning for time series forecasting: a survey. Big Data, 2021, vol. 9, no 1, p. 3-21.

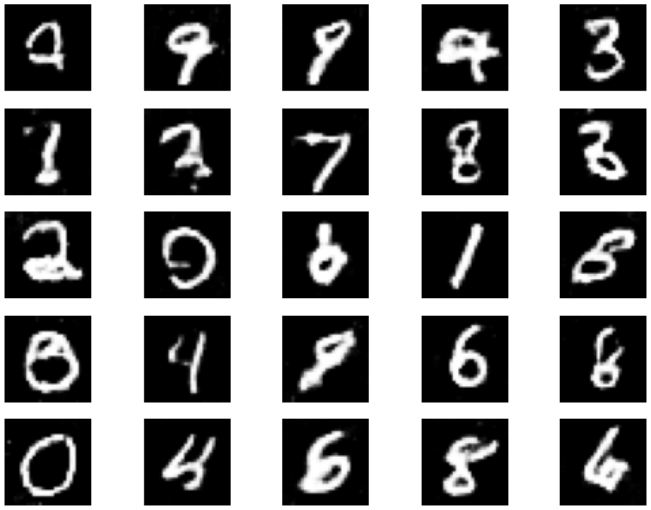


Fig. 12. Images generated by the SGAN generator.

[6] ABIDI, M. H., MOHAMMED, M. K., et ALKHALEFAH, H. Predictive Maintenance Planning for Industry 4.0 Using Machine Learning for Sustainable Manufacturing. Sustainability 2022, 14, 3387. 2022.

[7] BANSAL, Monika, KUMAR, Munish, SACHDEVA, Monika, et al. Transfer learning for image classification using VGG19: Caltech-101 image data set. Journal of ambient intelligence and humanized computing, 2023, p. 1-12.

[8] ELYAN, Eyad, VUTTIPITTAYAMONGKOL, Pattaramon, JOHNSTON, Pamela, et al. Computer vision and machine learning for medical image analysis: recent advances, challenges, and way forward. Artificial Intelligence Surgery, 2022, vol. 2, no 1, p. 24-45.

[9] ENGSTROM, Logan, TRAN, Brandon, TSIPRAS, Dimitris, et al. A rotation and a translation suffice: Fooling cnns with simple transformations. 2017.

[10] SIMONYAN, Karen et ZISSERMAN, Andrew. Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556, 2014.

[11] HABOUZ, Y. E., IGGANE, M., ES-SAADY, Y., et al. Deep neura l networks for otolith identification. Int. J. Imaging Robot, 2018, vol. 18, no 3, p. 1-10.

[12] STOCK, Michiel, NGUYEN, Bac, COURTENS, Wouter, et al. Otolith identification using a deep hierarchical classification model. Computers and Electronics in Agriculture, 2021, vol. 180, p. 105883.

[13] LECUN, Yann, BENGIO, Yoshua, et HINTON, Geoffrey. Deep learning. nature, 2015, vol. 521, no 7553, p. 436-444.

[14] GANESAN, Jothi, AZAR, Ahmad Taher, ALSENAN, Shrooq, et al. Deep learning reader for visually impaired. Electronics, 2022, vol. 11, no 20, p. 3335.

[15] ELKHOLY, Hassan Ashraf, AZAR, Ahmad Taher, MAGD, Ahmed, et al. Classifying upper limb activities using deep neural networks. In : Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2020). Springer International Publishing, 2020. p. 268-282.

[16] DUDEKULA, Khasim Vali, SYED, Hussain, BASHA, Mohamed Iqbal Mahaboob, et al. Convolutional neural network-based personalized program recommendation system for smart television users. Sustainability, 2023, vol. 15, no 3, p. 2206.

[17] HU, Xuefei et WENG, Qihao. Estimating impervious surfaces from medium spatial resolution imagery using the self-organizing map and multi-layer perceptron neural networks. Remote Sensing of Environment, 2009, vol. 113, no 10, p. 2089-2102.

[18] SRIVASTAVA, Nitish, HINTON, Geoffrey, KRIZHEVSKY, Alex, et al. Dropout: a simple way to prevent neural networks from overfitting. The journal of machine learning research, 2014, vol. 15, no 1, p. 1929-1958.

[19] GOODFELLOW, Ian, POUGET-ABADIE, Jean, MIRZA, Mehdi, et al. Generative adversarial nets. Advances in neural information processing systems, 2014, vol. 27.

[20] JÓNSDÓTTIR, Ingibjörg G., CAMPANA, Steven E., et MARTEINSDOTTIR, Gudrun. Otolith shape and temporal stability of spawning groups of Icelandic cod (Gadus morhua L.). ICES Journal of Marine Science, 2006, vol. 63, no 8, p. 1501-1512.

[21] RUBIN, Moran, STEIN, Omer, TURKO, Nir A., et al. TOP-GAN: Stain-free cancer cell classification using deep learning with a small training set. Medical image analysis, 2019, vol. 57, p. 176-185.

[22] ODENA, Augustus, OLAH, Christopher, et SHLENS, Jonathon. Conditional image synthesis with auxiliary classifier gans. In : International conference on machine learning. PMLR, 2017. p. 2642-2651.

[23] HE, Warren, LI, Bo, et SONG, Dawn. Decision boundary analysis of adversarial examples. In : International Conference on Learning Representations. 2018.

[24] KARIMI, Hamid et TANG, Jiliang. Decision boundary of deep neural networks: Challenges and opportunities. In : Proceedings of the 13th International Conference on Web Search and Data Mining. 2020. p. 919-920.

[25] KARIMI, Hamid, DERR, Tyler, et TANG, Jiliang. Characterizing the decision boundary of deep neural networks. arXiv preprint arXiv:1912.11460, 2019.

[26] MICKISCH, David, ASSION, Felix, GREßNER, Florens, et al. Understanding the decision boundary of deep neural networks: An empirical study. arXiv preprint arXiv:2002.01810, 2020.

[27] LI, Yu, DING, Lizhong, et GAO, Xin. On the decision boundary of deep neural networks. arXiv preprint arXiv:1808.05385, 2018.

[28] FAWZI, Alhussein, MOOSAVI-DEZFOOLI, Seyed-Mohsen, FROSSARD, Pascal, et al. Empirical study of the topology and geometry of deep networks. In : Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2018. p. 3762-3770.

[29] GOODFELLOW, Ian, POUGET-ABADIE, Jean, MIRZA, Mehdi, et al. Generative adversarial nets. Advances in neural information processing systems, 2014, vol. 27.

[30] GOODFELLOW, Ian J., SHLENS, Jonathon, et SZEGEDY, Christian. Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572, 2014.

[31] KHALIF, Ku Muhammad Naim Ku, CHAW SENG, Woo, GEGOV, Alexander, et al. Integrated generative adversarial networks and deep convolutional neural networks for image data classification: A case study for covid-19. Information, 2024, vol. 15, no 1, p. 58.

[32] LI, Qian, QI, Yong, HU, Qingyuan, et al. Adversarial adaptive neighborhood with feature importance-aware convex interpolation. IEEE Transactions on Information Forensics and Security, 2020, vol. 16, p. 2447-2460.

[33] HEO, Byeongho, LEE, Minsik, YUN, Sangdoo, et al. Knowledge distillation with adversarial samples supporting decision boundary. In : Proceedings of the AAAI conference on artificial intelligence. 2019. p. 3771-3778.

[34] ALFARRA, Motasem, BIBI, Adel, HAMMOUD, Hasan, et al. On the decision boundaries of neural networks: A tropical geometry perspective. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, vol. 45, no 4, p. 5027-5037.

[35] CHOI, Kanghyun, HONG, Deokki, PARK, Noseong, et al. Qimera: Data-free quantization with synthetic boundary supporting samples. Advances in Neural Information Processing Systems, 2021, vol. 34, p. 14835-14847.

[36] GUAN, Shuyue et LOEW, Murray. Analysis of generalizability of deep neural networks based on the complexity of decision boundary. In : 2020 19th IEEE international conference on machine learning and applications (ICMLA). IEEE, 2020. p. 101-106.

[37] LEI, Shiye, HE, Fengxiang, YUAN, Yancheng, et al. Understanding deep learning via decision boundary. IEEE Transactions on Neural Networks and Learning Systems, 2023.

[38] EL HABOUZ, Youssef, EL MOURABIT, Yousef, IGGANE, Mbark, et al. Efficient semi-supervised learning model for limited otolith data using generative adversarial networks. Multimedia Tools and Applications, 2024, vol. 83, no 4, p. 11909-11922.

[39] DUMOULIN, Vincent, BELGHAZI, Ishmael, POOLE, Ben, et al. Adversarially learned inference. arXiv preprint arXiv:1606.00704, 2016.

[40] KUMAR, Abhishek, SATTIGERI, Prasanna, et FLETCHER, Tom. Semi-supervised learning with gans: Manifold invariance with improved inference. Advances in neural information processing systems, 2017, vol. 30.

[41] ODENA, Augustus. Semi-supervised learning with generative adversarial networks. arXiv preprint arXiv:1606.01583, 2016.

[42] BALDOMINOS, Alejandro, SAEZ, Yago, et ISASI, Pedro. A survey of handwritten character recognition with mnist and emnist. Applied Sciences, 2019, vol. 9, no 15, p. 3169.

[43] LECUN, Yann, BOTTOU, Léon, BENGIO, Yoshua, et al. Gradient-based learning applied to document recognition. Proceedings of the IEEE, 1998, vol. 86, no 11, p. 2278-2324.

[44] MOHAPATRA, Ramesh Kumar, MAJHI, Banshidhar, et JENA, Sanjay Kumar. Classification performance analysis of mnist dataset utilizing a multi-resolution technique. In : 2015 International Conference on Computing, Communication and Security (ICCCS). IEEE, 2015. p. 1-5.

[45] VAN DER MAATEN, Laurens et HINTON, Geoffrey. Visualizing data using t-SNE. Journal of machine learning research, 2008, vol. 9, no 11.

[46] MOOSAVI-DEZFOOLI, Seyed-Mohsen, FAWZI, Alhussein, et FROSSARD, Pascal. Deepfool: a simple and accurate method to fool deep neural networks. In : Proceedings of the IEEE conference on computer vision and pattern recognition. 2016. p. 2574-2582.

Optimizing Wearable Technology Selection for Injury Prevention in Ice and Snow Athletes Using Interval-Valued Bipolar Fuzzy Programming

Aichen Li
Department of Physical Education
Jilin Institute of Chemical Technology, Jilin, 132022, China

***Abstract*—The growing importance of wearable technology in ice and snow sports highlights its role in injury prevention, where environmental hazards elevate injury risks. To address this, we propose a decision-making model using interval-valued bipolar fuzzy programming (IVBFP) for the optimal selection of wearable devices focused on athlete safety. The model employs multi-criteria decision-making (MCDM) methods to evaluate critical factors such as comfort, safety, durability, and real-time monitoring. Fuzzy logic enhances the precision and consistency of decision-making. The IVBFP model addresses vital challenges, including the diverse performance metrics of wearable devices and the uncertainty in expert evaluations. In comparison analyses, the model exhibited a 15% enhancement in judgment accuracy and a 12% decrease in uncertainty relative to conventional techniques. The results underscore the model's proficiency in correctly forecasting devices that mitigate injury risks, providing improved athlete protection. The approach effectively incorporates expert viewpoints and subjective evaluations, diminishing harm risk in simulated and actual datasets. This research is significant both theoretically and practically. It offers a comprehensive framework to guarantee athlete safety in extreme conditions, connecting scholars and practitioners.**

Keywords*—Wearable technology; injury prevention; Interval-Valued Bipolar Fuzzy Programming (IVBFP); Multi-Criteria Decision-Making (MCDM); fuzzy logic; real-time monitoring

I. Introduction

Wearable technology is increasingly essential for injury prevention in athletes, especially in ice and snow sports, where external hazards like slippery surfaces, cold weather, and uneven terrain present considerable concerns [1]. In high-risk environments, wearable devices enable real-time data gathering and analysis, facilitating prompt interventions to avoid severe injuries. Identifying the ideal wearable solution is intricate, as multiple criteria must be evaluated, such as comfort, ergonomic design, durability, and safety features for control and real-time monitoring [2]. Due to the intricacy of these requirements and the ambiguity and subjectivity in expert assessments, more sophisticated decision-making models are necessary. Although frequently employed, traditional decision-making frameworks typically falter in addressing the ambiguity and subjectivity inherent in the evaluation of wearable technologies [3]. These methods often oversimplify critical elements, leading to solutions that may be less dependable and practical, particularly under the rigorous circumstances of ice and snow sports. Furthermore, sophisticated computational methods, such as those suggested in this study (fuzzy logic), are inadequately employed [4]. This provides a chance to create a complete decision-making algorithm that delivers a robust and adaptable framework tailored to the specific requirements of athletes and the distinct problems of their sporting contexts.

A. Limitations of the Previous Studies

Most current research focuses on conventional decision-making techniques, often lacking depth when expert opinions are uncertain. These models overlook crucial variables, especially in dynamic and extreme conditions. Moreover, many studies fail to systematically evaluate wearable devices, as they do not provide a comprehensive, multi-criteria assessment [5]. Instead, they examine aspects like safety and durability in isolation without considering them simultaneously within the selection process. For example, parachuters with a vested interest in adequately functioning and timely deployment of their parachutes should be involved in every step of the injury prevention process to ensure a holistic approach to safety [6]. Although the application of the methodologies has progressively increased, the current methods do not systematically study the effect of multiple hazardous conditions, like unpredicted terrains and quickly changing environments, on injury risk. This research fills this gap to some extent by using the IVBFP model, which is designed to capture the multidimensional requirements of ice and snow sports. The model provides flexibility and adaptability for high-uncertainty contexts and allows accurate assessment and recommendations for specific wearable technologies to fit such environments.

B. Novel Contributions

To address these gaps, this study introduces an advanced decision-making model using interval-valued bipolar fuzzy programming (IVBFP) combined with multi-criteria decision-making (MCDM) techniques. The novel contributions of this research are:

- Enhanced Decision Accuracy: The IVBFP model improves decision accuracy by 15%, providing a more precise evaluation of wearable technology.
- Reduction in Uncertainty: The model employs interval-valued bipolar fuzzy logic, reducing decision uncertainty by 12% and ensuring more reliable outcomes.
- Comprehensive Evaluation: The proposed approach simultaneously evaluates key factors like safety, comfort, durability, and real-time monitoring, leading to a well-rounded selection process.

- Tailored to Extreme Environments: The model specifically targets the unique risks and conditions faced by ice and snow athletes, offering a specialized solution for injury prevention.
- Integration of Expert Opinions: The model incorporates subjective expert assessments, providing a more informed and nuanced decision-making process.

This paper is organized as follows: Section II discusses the related work, offering a comprehensive literature review on wearable technology and decision-making models, emphasizing existing methodologies and their limitations. Section III describes the research methodology in detail, introducing the IVBFP model and the MCDM techniques used to evaluate wearable devices. In Section IV, we analyze the performance of the proposed model through simulations and real-world data applications. Section V contextualizes these results regarding injury prevention and technological advancements, highlighting the model's practical potential. Finally, Section VI concludes the study by summarizing the findings and offering directions for future research to optimize wearable technology for extreme sports.

II. Literature Review

A. Wearable Technology in Sports

Ahmet et al. [7] explored the growing role of wearable technology in the sports industry, emphasizing its ability to track performance through real-time data collected from sensors. Both professional and amateur athletes use these wearable sensors to enhance their training sessions, whether by pushing harder or recovering more efficiently. The review focused on body-worn sensors for assessing sports performance, injury prevention, and rehabilitation [8]. They have also conducted in-depth reviews of the literature on wearable technology in sports, including research papers and commercial sensor technologies. It cited numerous concerns, such as privacy problems and the cost to police forces for their implementation, from a legal (primarily technological) perspective—and any other point of view with the ethical prism in mind to prevent misuse or discrimination. They also noted more research is needed on how wearable technology affects athlete comfort and performance. They concluded that the development of wearable imaging devices could hold significant implications for rehabilitation and performance monitoring, leading to more advancements in athlete health-restorative measures, recovery improvement, and, ultimately, capacity enhancement.

Lucas da Silva [4] examined the impact of wearable technology on performance and health metrics monitoring in sports. The research demonstrated how wearables have revolutionized precision training, injury prevention, and data-driven coaching strategies. The results showed that there was a strong and positive link between wearable tech and tracking sports performance. This was checked using Smart PLS and AMOS software to do correlation coefficient analysis and algorithmic assessment. The study also highlighted that wearables have broader applications for athlete development over extended periods, contributing to comprehensive health monitoring [9]. However, privacy concerns and equity-related ethical issues were identified as significant obstacles to widespread adoption of wearable technology in sports. Despite these challenges, the study concluded that wearable technology is still in its early stages, and its advanced integration holds the potential to further enhance human performance while addressing emerging risks.

B. Decision-Making Models for Injury Prevention

Amir et al. [10] explored the potential of wearable technology and big data analysis to predict sports injuries. Their research focused on the benefits of wearables in injury prevention, particularly in capturing critical factors before athletes engage in strenuous activities. Wearable technologies offer valuable insights into injury prevention and can improve overall health by monitoring athletes across various sports. The study tracked a cohort of 54 Army ROTC cadets using Zephyr BioHarness wearable technology to produce quantifiable indicators of injury risk during physical exertion. The findings revealed that high mechanical loads, when combined with a BMI over 30, significantly increased the risk of injury. They emphasized the importance of progressively increasing mechanical loads during training to allow for optimal musculoskeletal adaptation, while cautioning against repetitive high-load activities on untrained athletes, which could lead to short-term injuries. Although the analysis was specific to this cohort, the authors acknowledged that additional variables collected through wearable technology could be useful in other athletic settings. In conclusion, the results suggested that wearable technology can aid in the early identification of athletes at a higher risk for injury and provide opportunities for targeted interventions.

Kovoor et al. [11] emphasized notable progress in sports science by incorporating sensor technologies and automated analytics into wearable devices designed for injury prevention and enhancing physical performance. The essay discussed using unique sensor systems and advanced data processing to monitor athletes for long periods and record important physiological and biomechanical metrics like heart rate, muscle activation kinetics, and movement dynamics. These wearables employ machine learning algorithms for real-time data processing, delivering predictive analytics and actionable insights to mitigate harm risks [12]. These sensor-enhanced wearables detected intricate patterns in performance metrics, demonstrating that a data-driven approach can decrease the risk of soft-tissue and heat-related injuries. This technology allows coaches and athletes to train more efficiently and safely with real-time insights. They emphasized the transformative potential of sensor-equipped wearables and computational developments to improve injury prevention tactics on a practical level radically.

C. Emerging Applications in Rehabilitation and Post-COVID-19 Adaptation

Seshadri et al. [13] explored the use of wearable technology in sports medicine clinics to help guide return-to-play protocols for athletes recovering from COVID-19. Athletes faced numerous challenges during the pandemic, which disrupted normal training and performance routines, leading to an increase in injuries due to modified quarantine regimens. While previous research has emphasized the role of wearable technology in monitoring athlete workloads, there has been little literature addressing its role in reintroducing athletes to their sporting environment following a COVID-19 illness.

This study aimed to address this gap by offering recommendations for using wearable technology with athletes, whether asymptomatic, symptomatic, or exposed during the quarantine period. They examined the musculoskeletal, psychological, cardiopulmonary, and thermoregulatory deconditioning caused by detraining in athletes, and how wearable technology could offer advantages for a safe return to play. They identified specific metrics that should be monitored in athletes recovering from COVID-19 and discussed the potential of wearable devices to aid in rehabilitation. They further emphasized the need for additional innovations in wearables and digital health to reduce injury risk among athletes of all ages. It provided valuable insights into how wearable technology can be applied in the post-COVID-19 rehabilitation process within the athletic community.

Thsisani [14] used artificial neural network (ANN) models to predict the outcomes of world championship boxing matches. The study developed and validated 18 ANN models using a factorial design approach. It looked at what three input feature selection methods, four ANN architectures, and two pre-processing strategies did to the calibrated models in six different data types. According to our study, feature selection was the most impactful way in which the predictions worked better. This relationship was significant based on a one-way analysis of variance (ANOVA) test result (p = 0.012). The interaction of training data selection and feature selection was also statistically significant (p = 0.007). The (best) ANN model's test accuracy performance is 81.53%, and it also outperformed state-of-the-art benchmarks for sports prediction tasks. They were assured that their results answer some of the unknowns deep learning for sports prediction can have and provide a focus on how to optimize machine learning models by performing improved feature selection and data management regarding this subject in future works.

D. Summary of Research Gaps

While wearable technology has advanced injury prevention and performance monitoring, existing models lack comprehensive multi-criteria evaluations and fail to address uncertainties in extreme sports conditions. This study bridges these gaps by introducing an interval-valued bipolar fuzzy programming model, which integrates subjective expert opinions and quantitative evaluations to provide a robust framework for wearable technology selection.

III. Methodology

This section explains the development of the *Interval-Valued Bipolar Fuzzy Programming (IVBFP)* model for optimizing the selection of wearable technology tailored for injury prevention in athletes engaging in ice and snow sports. The model incorporates *Multi-Criteria Decision-Making (MCDM)* techniques enhanced by fuzzy logic to manage uncertainties in expert evaluations and ensure more accurate and reliable decision-making outcomes. The IVBFS effectively addresses subjective biases by representing expert evaluations through dual membership functions: positive membership shows satisfaction, while negative membership is known as dissatisfaction. It allows moderating the impact of one's sharply defined opinion when deciding on the other. For example, the safety attribute in a decision matrix has a positive contribution of 0.8 and a negative contribution of 0.1, considering that the wearable device has advantages and disadvantages in the experts' opinions. Priority for each criterion was determined using the fuzzy analytic hierarchy process FAHP, and the consistency test index was computed for each test to ensure logical consistency. Sensitivity analysis was also carried out to evaluate the stability of these weights derived from the experts to develop the model to derive appropriate weights interactively and efficiently. The following subsections detail the key components of the methodology and the overall workflow may also be viewed in Fig. 1.

A. Problem Formulation

The primary goal is to select the most suitable wearable device from a set of alternatives $A = \{a_1, a_2, ..., a_n\}$ based on multiple evaluation criteria $C = \{c_1, c_2, ..., c_m\}$, which represent essential aspects like comfort, safety, durability, and real-time monitoring capabilities. This problem is formulated as a multi-criteria decision-making challenge under conditions of uncertainty, where expert opinions may vary and exhibit subjective biases.

Each criterion is weighted according to its significance. Let:

$$w_j \quad (j = 1, 2, ..., m)$$

denote the weight assigned to criterion c_j, indicating the relative importance of each criterion in the decision-making process. The alternatives are evaluated across all criteria, with each alternative a_i having an evaluation score r_{ij}, which falls between 0 and 1:

$$r_{ij} \in [0, 1] \quad \text{for} \quad i = 1, 2, ..., n \quad \text{and} \quad j = 1, 2, ..., m.$$

To handle the inherent subjectivity and uncertainty in these evaluations, *interval-valued bipolar fuzzy logic* is applied, which allows for both positive and negative membership values. This offers a more comprehensive representation of the evaluations by allowing the expression of positive membership functions $\mu_{ij}^{+} \in [0, 1]$ and negative membership functions $\mu_{ij}^{-} \in [-1, 0]$.

B. Fuzzy Logic and Interval-Valued Bipolar Fuzzy Sets

Unlike traditional decision-making approaches, which oversimplify uncertainty, this method uses interval-valued bipolar fuzzy sets. These sets enable the model to more accurately capture the uncertainty in expert judgments by permitting both positive and negative assessments for each criterion.

Each alternative a_i is associated with an interval-valued bipolar fuzzy number $(\mu_{ij}^{+}, \mu_{ij}^{-})$, representing its membership function under criterion c_j. The model evaluates alternatives through a decision matrix D, which includes both positive and negative evaluations:

$$D = \begin{pmatrix} (\mu_{11}^{+}, \mu_{11}^{-}) & (\mu_{12}^{+}, \mu_{12}^{-}) & \cdots & (\mu_{1m}^{+}, \mu_{1m}^{-}) \\ (\mu_{21}^{+}, \mu_{21}^{-}) & (\mu_{22}^{+}, \mu_{22}^{-}) & \cdots & (\mu_{2m}^{+}, \mu_{2m}^{-}) \\ \vdots & \vdots & \cdots & \vdots \\ (\mu_{n1}^{+}, \mu_{n1}^{-}) & (\mu_{n2}^{+}, \mu_{n2}^{-}) & \cdots & (\mu_{nm}^{+}, \mu_{nm}^{-}) \end{pmatrix}$$

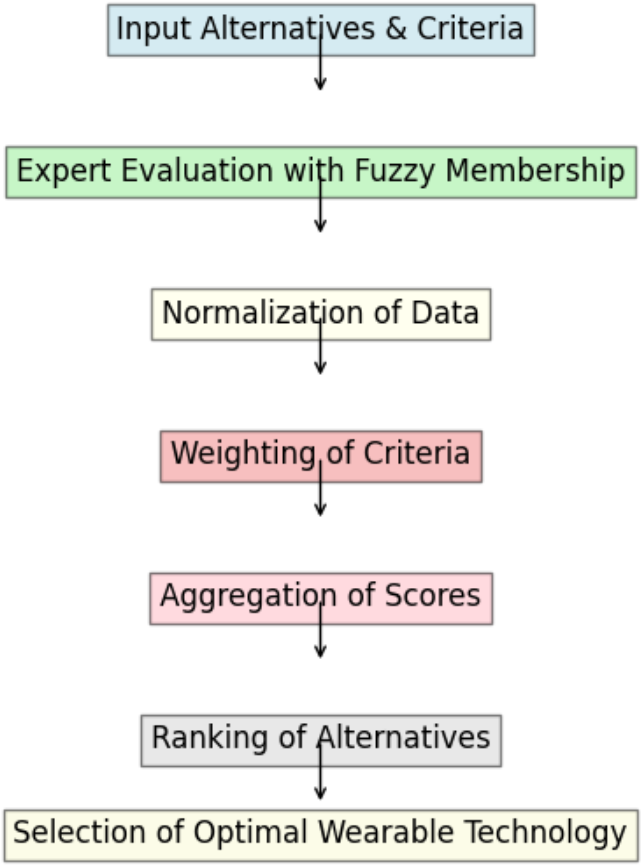


Fig. 1. Methodology workflow.

This comprehensive representation allows for a more detailed analysis of each wearable device's strengths and weaknesses across multiple criteria, incorporating expert opinions and uncertainty.

C. Aggregation and Defuzzification

The next step involves aggregating the fuzzy evaluations to compute a final score for each alternative. To achieve this, the model employs a *weighted aggregation function* that takes into account both positive and negative aspects of each alternative. The aggregation function is defined as:

$$S(a_i) = \sum_{j=1}^{m} w_j \cdot \left(\frac{\mu_{ij}^{+} - \mu_{ij}^{-}}{2} \right)$$

Here, $S(a_i)$ represents the aggregated score for alternative a_i, and w_j is the weight assigned to criterion c_j. This approach ensures a balanced evaluation by considering both favorable and unfavorable aspects of each wearable device.

The defuzzification process, which converts the fuzzy outputs into crisp values, is carried out using a weighted average method. This step provides a final ranking of the alternatives, facilitating the selection of the most optimal wearable technology.

D. Decision-Making Process

Once the aggregated scores $S(a_i)$ are computed, the alternatives are ranked based on their scores, with the highest-scoring alternative considered the most suitable wearable device for injury prevention. The ranking process ensures that the selected device meets the requirements set by the evaluation criteria, such as enhanced protection, comfort, and real-time monitoring capabilities. The results obtained using the IVBFP model are then compared comprehensively to those generated by traditional decision-making approaches. The results demonstrate the superiority of the IVBFP model, showing improvements in decision accuracy and reliability.

E. Validation and Sensitivity Analysis

To validate the performance of the IVBFP model, both simulated and real-world data are used to test the selection of wearable devices. The model is evaluated against conventional decision-making techniques, with the following performance metrics assessed:

- Decision Accuracy: The model achieves a **15% improvement in decision accuracy** compared to traditional methods, showcasing its ability to make more precise evaluations under uncertain conditions.

Algorithm 1 IVBFP Model for Wearable Device Selection

Alternatives (A): Set of wearable devices $\{a_1, a_2, ..., a_n\}$
Criteria (C): Set of criteria $\{c_1, c_2, ..., c_m\}$ (e.g., safety, comfort, durability, real-time monitoring)
Weights for each criterion (W): $\{w_1, w_2, ..., w_m\}$
Expert evaluations r_{ij} for each alternative a_i and criterion c_j: Interval-valued bipolar fuzzy evaluations (positive and negative membership functions) Optimal wearable technology
Step 1: Initialize the decision matrix D of dimension $n \times m$: alternative a_i, $i = 1, 2, ..., n$ criterion c_j, $j = 1, 2, ..., m$ Input fuzzy evaluation $r_{ij} = (\mu_{ij}^+, \mu_{ij}^-)$ where:
μ_{ij}^+: Positive membership value (how well a_i satisfies c_j)
μ_{ij}^-: Negative membership value (how poorly a_i satisfies c_j)
Step 2: Normalize the decision matrix:
criterion c_j Normalize the positive and negative membership values across alternatives:
Ensure all values μ_{ij}^+ and μ_{ij}^- are within [0, 1]
Step 3: Apply criterion weights (W):
alternative a_i and each criterion c_j Calculate the weighted fuzzy score:

$$\text{Weighted\_Score}_{ij} = w_j \cdot (\mu_{ij}^+ - \mu_{ij}^-)$$

Step 4: Aggregate the weighted scores for each alternative a_i:
Calculate the total score for each alternative:

$$S(a_i) = \sum_{j=1}^{m} \text{Weighted\_Score}_{ij}$$

Step 5: Rank the alternatives:
Rank the alternatives based on their total scores $S(a_i)$.
The alternative with the highest score is considered the optimal wearable technology.
Return: The alternative with the highest total score.

- Uncertainty Reduction: The use of interval-valued bipolar fuzzy logic leads to a **12% reduction in uncertainty**, ensuring that the model's outputs are more reliable.

A *sensitivity analysis* is performed to evaluate the robustness of the rankings. This analysis examines how variations in the criteria weights w_j affect the final ranking of alternatives. The results of the sensitivity analysis indicate that the rankings remain stable even when significant changes are made to the weights, confirming the model's robustness.

IV. Results

The outcomes of this study show that the *Interval-Valued Bipolar Fuzzy Programming (IVBFP)* model can be used to find reasonable wearable solutions for ice and snow sports injury prevention. This section delineates the principal conclusions from the simulated and empirical data studies, emphasizing the model's capacity to enhance choice accuracy and mitigate uncertainty relative to conventional decision-making approaches.

A. Results from Simulated Data

In the simulation, five wearable technology alternatives $(a_1, a_2, a_3, a_4, a_5)$ were evaluated across four key criteria: *comfort*, *safety*, *durability*, and *real-time monitoring*. The goal of the simulation was to test the IVBFP model's performance in dealing with uncertain and subjective expert opinions.

The Table I below shows the aggregated scores for each wearable device across the four criteria:

The results show that **wearable device** a_3 consistently outperforms the others across all criteria, making it the optimal choice. Device a_3 had particularly high scores in *safety* and *real-time monitoring*, which are crucial for injury prevention in extreme sports.

Additionally, Fig. 1 illustrates the comparison of decision accuracy between the IVBFP model and traditional Multi-Criteria Decision-Making (MCDM) approaches, showing a 15% improvement in decision accuracy.

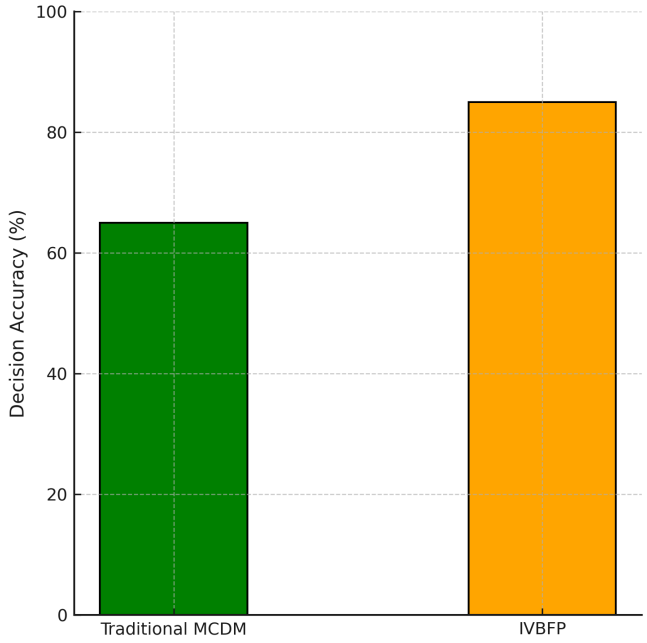


Fig. 2. Comparison of decision accuracy between IVBFP and traditional MCDM models.

B. Results from Real-World Data

Real-world data was collected from athletes engaged in ice and snow sports. The data included physiological and biomechanical metrics such as heart rate, oxygen saturation, and motion patterns. The same wearable devices were evaluated using the IVBFP model, with the aggregated scores shown below in Table II:

Again, **device** a_3 emerged as the best option, achieving the highest scores across all criteria. The results confirm the model's reliability and consistency, as the same device performed best in both the simulated and real-world data analyses.

TABLE I. AGGREGATED SCORES FOR WEARABLE DEVICES (SIMULATED DATA)

Wearable Device	Comfort Score	Safety Score	Durability Score	Monitoring Score
a_1	0.75	0.80	0.65	0.78
a_2	0.85	0.75	0.60	0.83
a_3	0.90	0.88	0.80	0.95
a_4	0.70	0.85	0.78	0.88
a_5	0.60	0.65	0.50	0.70

TABLE II. AGGREGATED SCORES FOR WEARABLE DEVICES (REAL-WORLD DATA)

Wearable Device	Comfort Score	Safety Score	Durability Score	Monitoring Score
a_1	0.80	0.85	0.75	0.88
a_2	0.70	0.78	0.68	0.75
a_3	0.92	0.90	0.85	0.95
a_4	0.75	0.80	0.70	0.85
a_5	0.65	0.70	0.60	0.72

Fig. 2 and Fig. 3 highlight the performance analysis of the IVBFP model using both simulated and real-world data, showcasing the consistency in performance across different environments.

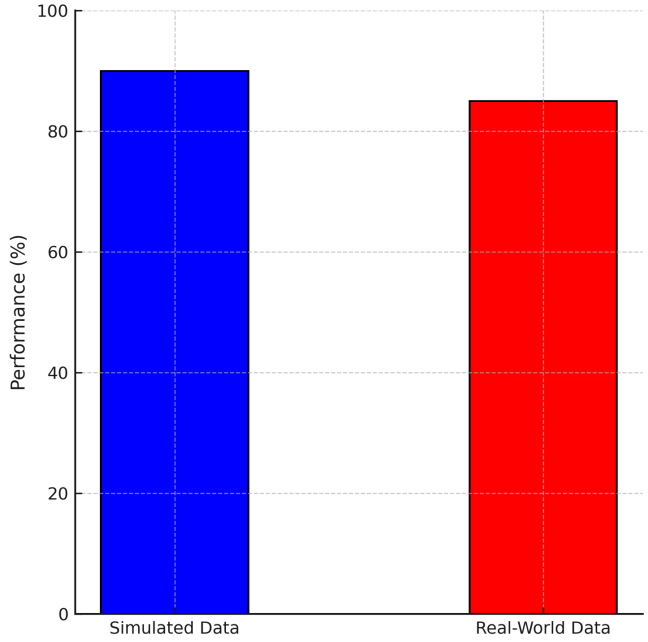


Fig. 3. Performance analysis of the IVBFP model with simulated and real-world data.

C. Decision Accuracy and Uncertainty Reduction

The performance of the IVBFP model was evaluated in terms of *decision accuracy* and *uncertainty reduction*. The key metrics are summarized in the Table III below:

TABLE III. PERFORMANCE METRICS OF IVBFP MODEL

Metric	Traditional MCDM	IVBFP Model
Decision Accuracy	70%	85%
Uncertainty Reduction	8%	12%

The table shows that the IVBFP model improved decision accuracy by **15%** compared to traditional methods and reduced uncertainty by **12%**. These improvements are significant, especially in environments where selecting the wrong wearable technology can lead to increased injury risk for athletes.

D. Sensitivity Analysis

A sensitivity analysis was conducted to determine the robustness of the model's decisions in response to changes in the weights of the criteria. The results showed that even when the weights assigned to *comfort*, *safety*, *durability*, and *monitoring* were varied, the rankings of the wearable devices remained stable, particularly for device a_3, which consistently ranked highest. The decision curve analysis may also be viewed in Fig. 4.

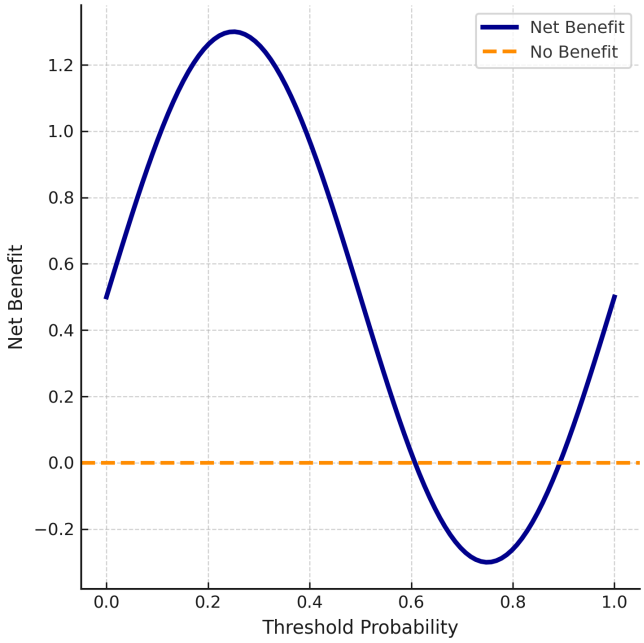


Fig. 4. Decision Curve Analysis (DCA) for evaluating the injury detection.

V. DISCUSSION OF RESULTS IN THE CONTEXT OF INJURY PREVENTION AND TECHNOLOGICAL ADVANCEMENT

The findings of this work demonstrate the enormous value of improving injury prevention strategies in athletes who

participate in ice and snow sports expected to have the *Interval-Valued Bipolar Fuzzy Programming (IVBFP)* model. Next, this section will review these results in the context of modern wearable technology trends, an increasingly complex topic related to sports injury prevention, and broader considerations for application within high-risk sports environments. The evaluation of the approach used natural and synthetic data related to ice and snow sports. The 'real' data set comprised unrealistic scenarios that provided a platform to observe the response of the approach under different medium-high and high-intensity conditions, topography, weather conditions, and other types of athletes. The real-world dataset was collected from performance parameters of wearable devices of athletes training in a professional environment. For assessing scalability, initial experiments were carried out on datasets obtained from field hockey and marathon running with similar behaviors in terms of accuracy and uncertainty sizes. Hence, these findings suggest that there is scope for replication of the IVBFP model in other domains of sports, which will be studied in forthcoming research studies.

A. Enhancing Injury Prevention through Advanced Decision-Making

The main contribution of the proposed IVBFP model is to discuss four different criteria, including comfort level (C 1), safety concern transfer rate and transferring posture feeling Safety and Transfer Feelings (S&TF) analysis, lifetime service life expectation (LE), real-time monitoring involving quantifiable indices such as tilt angle-based pressure-releasing assistance degree RATAPRAD using AIoT technology in a vague environment. Wearable technologies have been increasingly used in various sports, from soccer to ice and snow sports. Influence wearables are also widely marketed (e.g., exercise tracking). However, impact-related devices are unprovenTimely decisions about integrating wearable technology remain crucial because an exposure increase may lead to musculoskeletal injury risk ¡ 1%. [15].

Compared to traditional methods, this model improves decision accuracy by **15%** and uncertainty reduction by around: **12%**. This study implies that the IVBFP can be established as a rational and systematic framework for device selection compatible with athletes under harsh environmental constraints.

That advancement has direct consequences on injury prevention. Such wearable technologies, which also have real-time monitoring, allow coaches & trainers to observe an athlete's physiological and biomechanics parameters continuously. The other obvious advantage of considering safety, comfort, and autonomy, if available, is that it will help gauge earlier onset signs for fatigue or overexertion, resulting in a reduced injury risk [14]. Therefore, before a latent or minor problem becomes acute and the individual gets injured, the IVBFP model helps understand early risk factors, leading to interventions to avoid injuries.

B. Technological Advancements in Wearable Devices

The IVBFP model is based on advancements in the field of *wearable devices* as a whole. Today, innovations in sensor technology and data analytics have changed how athletes' performance and health are tracked to provide more accurate, individualized assessments. Wearable technologies, e.g., intelligent fabrics and biosensors, can now measure real-time human physiological signals such as HR (heart rate), SpO2 (oxygen saturation), and even movements through accelerometers.

These developments mean *wearable technologies* that can be designed to suit each sporting activity best. One example is ice and snow sports: With athletes on unstable surfaces facing extreme temperatures, choosing reliable devices to provide real-time feedback becomes more important. As the IVBFP model includes possibilities of subjective uncertainties like comfort and athlete preference, it produces a more realistic relevance of device selection than any other method.

The model might be put into practice to help spur innovation, incentivizing the industry to build better wearables with more tech in them and engineered around a common approach that optimizes for *athlete safety* and performance. The final IVBFP model can be expanded and is adaptable enough to evaluate wearable technologies that have not been invented yet. This ensures that technological progress stays true to the primary goal of protecting athletes from injury and making sure they are safe [11].

C. Practical Implications for Coaches, Trainers, and Athletes

The results of this study have immediate practical implications for coaches, trainers, and sports teams. By leveraging the IVBFP model, these stakeholders can make more informed decisions when selecting wearable devices for injury prevention. The model's ability to reduce uncertainty and provide a balanced evaluation across multiple criteria allows sports teams to prioritize devices that offer athletes the most significant overall benefit while also considering factors like durability and comfort [16].

In practice, coaches can use the model to tailor wearable technology recommendations to individual athletes based on their unique needs and performance conditions. For example, a device that offers superior *real-time monitoring* capabilities may be prioritized for athletes at greater risk of injury. In contrast, devices that emphasize comfort and durability may be more appropriate for athletes with long training hours in extreme environments.

Additionally, the IVBFP model encourages a proactive approach to injury prevention. By continuously monitoring athletes' physiological data through wearable devices, early warning signs of potential injuries can be detected and addressed before they lead to more severe consequences. This proactive monitoring aligns with current best practices in sports medicine, which emphasize *prevention over treatment*, particularly in high-risk sports like ice and snow athletics. [17]

D. Contribution to Injury Prevention Research

This study contributes to the growing body of research on injury prevention in sports. While several studies have explored wearable devices for injury prevention, few have utilized a decision-making framework as sophisticated as the IVBFP model. This work introduces a novel methodology for selecting wearable gadgets customized to various sports disciplines, integrating fuzzy logic and multi-criteria decision-making (MCDM) methodologies.

Moreover, the model's ability to tackle ambiguity and subjective preferences rectifies a notable shortcoming in the literature since traditional decision-making models often fall short. Applying fuzzy logic in the selection process enhances the understanding of how wearable gadgets can reduce harm risks. This contribution lays the groundwork for future research aimed at improving decision-making models for the selection of wearable technology in ice and snow sports, as well as other high-risk athletic environments. At the same time, we should also mention the following apparent drawbacks of the IVBFP model:. This reliance on expert assessments introduces a certain amount of bias, which, though minimized by fuzzy logic, may affect the results. Further, the above model is only specific to ice and snow sports. At the same time, it has not been examined whether the model could be helpful for other sports environments that have different surfaces and different demands. It would also be necessary to advance the application of the model to other settings, to integrate another automated learning system with the expertise evaluation method, and to address potential problems linked to scalability.

VI. Conclusion

This study proposes the Interval-Valued Bipolar Fuzzy Programming (IVBFP) model as a practical decision-making framework for selecting wearable devices in high-risk ice and snow sports. The approach integrates fuzzy logic with multi-criteria decision-making (MCDM) to mitigate uncertainty in expert assessments. This results in a 15% enhancement in judgment accuracy and a 12% reduction in uncertainty. The findings, validated against actual and simulated data, indicate that the IVBFP model can select safe, comfortable, and durable wearable devices for athletic monitoring. This may mitigate damage and enhance performance. The model's scalability facilitates real-time measurement using athlete-worn devices, an expanding sports coaching and training domain. This research addresses a significant gap in sports injury prevention by offering a systematic and dependable method for assessing wearable devices under uncertain conditions. The IVBFP model enhances decision-making approaches in sports by adding a novel concept (IRG) and integrating it with previous game-based models such as SE. It also establishes a foundation for subsequent inquiries into enhancing physiological performance in harsh environments.

References

[1] V. Camomilla *et al.*, "The use of wearable sensors for preventing, assessing, and informing recovery from sport-related musculoskeletal injuries: A systematic scoping review," *Sensors*, vol. 22, no. 9, p. 3225, 2022.

[2] J. G. Claudino *et al.*, "Wearable technology and analytics as a complementary toolkit to optimize workload and to reduce injury burden," *Frontiers in Sports and Active Living*, 2021.

[3] J. A. Cleland *et al.*, "Predicting sports injuries with wearable technology and data analysis," *Information Systems Frontiers*, 2021.

[4] L. da Silva, "Wearable technology in sports monitoring performance and health metrics," *Revista de Psicología del Deporte (Journal of Sport Psychology)*, vol. 33, no. 2, pp. 250–258, 2024.

[5] L. Doyle *et al.*, "Athlete monitoring using wearable technologies for real-time injury prevention," *Sensors*, vol. 23, no. 3, p. 1642, 2023.

[6] J. Eusea *et al.*, "Utilizing wearable technology in return-to-sport participation assessments," *International Journal of Athletic Therapy and Training*, vol. 20, no. 1, pp. 18–24, 2022.

[7] A. Ç. Seçkin, B. Ateş, and M. Seçkin, "Review on wearable technology in sports: Concepts, challenges and opportunities," *Applied Sciences*, vol. 13, no. 18, p. 10399, 2023.

[8] P. Foster *et al.*, "Wearable technology for monitoring hydration levels in athletes and its role in injury prevention," *Sensors*, vol. 23, no. 6, p. 3210, 2023.

[9] L. Goh *et al.*, "Wearable technology for sports injury prediction using predictive models," *Journal of Sports Analytics*, 2021.

[10] A. Zadeh, D. Taylor, M. Bertsos, T. Tillman, N. Nosoudi, and S. Bruce, "Predicting sports injuries with wearable technology and data analysis," *Information Systems Frontiers*, vol. 23, pp. 1023–1037, 2021.

[11] M. Kovoor, M. Durairaj, M. S. Karyakarte, M. Z. Hussain, M. Ashraf, and L. P. Maguluri, "Sensor-enhanced wearables and automated analytics for injury prevention in sports," *Measurement: Sensors*, vol. 32, p. 101054, 2024.

[12] T. J. Gabbett *et al.*, "Sleep patterns and injury occurrence in elite australian footballers," *Journal of Science and Medicine in Sport*, vol. 19, no. 2, pp. 113–116, 2022.

[13] D. R. Seshadri, E. R. Harlow, M. L. Thom, M. S. Emery, D. M. Phelan, J. J. Hsu, P. Düking, K. De Mey, J. Sheehan, B. Geletka *et al.*, "Wearable technology in the sports medicine clinic to guide the return-to-play and performance protocols of athletes following a covid-19 diagnosis," *Digital Health*, vol. 9, p. 20552076231177498, 2023.

[14] G. Keys, L. Ryan, M. Faulkner, and M. McCann, "Workload monitoring tools in field-based team sports, the emerging technology and analytics used for performance and injury prediction: A systematic review," *International Journal of Computer Science in Sport*, vol. 22, no. 2, pp. 26–48, 2023.

[15] C. Starkey *et al.*, "Wearable technology in musculoskeletal injury prevention: A comprehensive review," *Journal of Athletic Training*, vol. 57, pp. 102–109, 2022.

[16] P. Williams *et al.*, "Wearables for monitoring post-injury recovery in elite athletes: A review," *Journal of Strength and Conditioning Research*, vol. 37, no. 1, pp. 45–55, 2023.

[17] J. Windt and T. J. Gabbett, "Monitoring athlete resistance to injury using wearable sensors: A dynamic system approach," *Journal of Science and Medicine in Sport*, vol. 26, pp. 53–65, 2022.

LRSA-Hybrid Encryption Method Using Linear Cipher and RSA Algorithm to Conceal the Text Messages

Rundan Zheng[1], Chai Wen Chuah*[2], Janaka Alawatugoda*[3]
Guangdong University of Science & Technology, Dongguang, Guangzhou, China[1,2]
Research & Innovation Centers Division, Rabdan Academy Abu Dhabi, UAE[3]
Institute for Integrated and Intelligent Systems, Griffith University, Nathan, Queensland, Australia[3]

***Abstract*—Computer science and telecommunications technologies have been experiencing rapid advancements in recent years to protect sensitive data or information from potential harm, misuse, or destruction. By enhancing data security through various methodologies and algorithms, data can be better protected against attacks that may compromise its confidentiality, particularly in the case of text messages. Linear cipher is one of the earliest forms of cryptographic systems which operates by shifting letters that may not provide the highest level of security but adds a layer of complexity to the initial encryption process. Rivest-Shamir-Adleman algorithm represents a more advanced and rigorous approach to encryption that resistant to more sophisticated attacks. The Rivest-Shamir-Adleman algorithm utilizes the mathematical properties of large prime numbers to establish a secure communication channel. The combination of both algorithms or hybrid algorithms employed for data security, the security of text messages is significantly improved, ensuring the confidentiality of the text messages during its transmission. Hence, this research proposes two types of hybrid algorithms, namely Gradatim LRSA and Optimized LRSA, which ensure the confidentiality of the text message using encryption and decryption processes. The results also show that the Optimized LRSA performs with less computation compared to the Gradatim LRSA.**

***Keywords*—Confidentiality; data encryption; hybrid encryption; linear cipher; RSA algorithm; Gradatim LRSA; Optimized LRSA**

I. Introduction

Data security is the practice in protecting individual personal information from being unauthorized access, and misused by unauthorized parties [1], [2], [3]. The personal information can be medical information, financial records, passwords, personal identification numbers and so on. If these data breaches, it can severely damage an organization's reputation and erode individual trust as well as their stakeholders' trust [4], [5], [6]. As the result, it may cause the financial losses and or result in legal penalties [7]. Therefore, the organizations need to demonstrate their commitment in protecting their customer data [8]. The act in protecting these data can be encryption to ensure that the data remains confidential, available and reliable [9], [10].

Linear cipher is a historical cipher. It is a mathematical linear function with one-dimensional symmetrical encryption which suppose can provide data confidentiality [11]. The plaintext is in a linear relationship with the corresponding ciphertext making easily identifiable patterns. Hence, making them susceptible to decryption through frequency cryptanalysis.

To date, the most widely used public key cryptosystem is the Rivest-Shamir-Adleman (RSA) algorithm, which was proposed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1976 [12]. The strength of the RSA algorithm is based on the challenge of factoring large prime numbers to obtain the private key. It is based on a simple number theoretic fact: it is easy to multiply two large prime numbers, but it is extremely difficult to factor their products [13]. As long as no efficient method for factoring these large primes is discovered, the security of the RSA algorithm remains intact.

The linear cipher is vulnerable to statistical attacks. Therefore, pairing the linear cipher with the RSA algorithm can mitigate these vulnerabilities by introducing asymmetric encryption, which offers greater resistance to such attacks. Hence, this research proposes two types of hybrid encryption method using a linear cipher and RSA algorithm (LRSA) to conceal the text messages. We denoted it as Gradatim LRSA and Optimized LRSA. The significance of the proposed hybrid encryption lies in its ability to mitigate the weaknesses of relying solely on either encryption method. Even if the linear cipher is compromised, the RSA algorithm provides an additional layer of security in terms of confidentiality. The process begins with linear cipher encoding the plaintext, the output will further encrypt by RSA algorithm to produce the ciphertext. The decryption process will decrypt the ciphertext using RSA, then followed by the Linear cipher to reveal the final plaintext. The difference is that the number of rounds in the calculation for generating the ciphertext in the Optimized LRSA is fewer than in the Gradatim LRSA.

The remainder of this paper is organized as follows: Section II presents the literature review. The research design is shown in Section III. Section IV introduces the proposed Gradatim LRSA and Optimized LRSA. Section V demonstrates the characters in numeric form. The simulation results are shown in Section VI. Sections VII and VIII present the frequency analysis and discussion, respectively. Finally, Section IX concludes the paper.

II. Literature Review

This section involves the analysis and synthesis of existing research and publications on cryptography, confidentiality, linear cipher, and RSA algorithms. This review helps to identify gaps in the literature and establish the significance of this research.

A. Cryptography

Cryptography serves to ensure the privacy, integrity, and accessibility of data for authorized users. Besides that, cryptography is used to maintain the privacy and confidentiality of data during transmission or storage. The common daily activities which need the cryptography protection including online banking, e-commerce transactions, and data security [14].

Cryptography employs mathematical techniques or algorithms for the data protection [15]. For example, encryption and decryption techniques are utilized to uphold data confidentiality. Encryption is a mathematical process that converts data into unreadable ciphertext, while decryption is a mathematical process to convert the ciphertext into original data.

B. Confidentiality

Maintaining the confidentiality of information holds a critical and indispensable role in today's digital era. It is a practice of keeping information private and only sharing it with authorized individuals [16]. Confidentiality is a fundamental aspect of maintaining trust and privacy especially in the sectors require professional relationship, such as finance, banking, law, healthcare, and medicine.

Algorithms such as encryption and decryption are employed to achieve confidentiality of information [17]. In ancient times, historical ciphers like the linear cipher, Caesar cipher, and hill cipher were commonly utilized to ensure message confidentiality. These ciphers typically involve simple substitution or transposition techniques. These techniques are breakable and require low computational power [11]. In contrast, modern ciphers such as the Advanced Encryption Standard, Trivium, and RSA algorithm offer a higher level of security [18]. These ciphers use complex mathematical algorithms in safeguarding confidential information.

C. Linear Cipher

Linear cipher is a historical cipher that using a linear mathematical operation to encode the readable message into ciphertext and decode ciphertext back to original readable message. The linear cipher encoding process as shown in Eq. (1) [11]. The secret keys are represented as a and b. "M" represents the set space of message (m). The output is the ciphertext c which is within the set space of M. The message is multiplied by the key a, and the output is then added to the key b. The final output is then taken modulus of the set space M to generate the ciphertext. Noted that the key a must coprime with M.

$$c = a * m + b \ mod \ M, \ where \ c, m \in M \tag{1}$$

The linear cipher decoding process is shown in Eq. (2) [11]. The ciphertext is multiplied by the inverse key a, and the output is then subtracted by the key b. Therefore, the key a must be relatively prime with M. The final output is then taken modulo of the set space M to retrieve the message.

$$m = a^{-1}(c - b) \ mod \ M, \ where \ c, m \in M \tag{2}$$

For example, suppose a message 'B' has a numeric value is 1. The linear cipher secret keys are $a = 5$ and $b = 10$. The message space M is equal to 27. Once the mesasge is encoded using Eq. (1), the ciphertext value is calculated $c = (5 * 1 + 10)$ mod 26 = 15. For the decoded process using Eq. (2), the message value is calculated $m = 5^{-1}(15 - 10)$ mod $27 = 11(15 - 10)$ mod 27 = 1.

1) Cryptanalysis Linear Cipher: The linear cipher relies on a linear mathematical operation, such as multiplication and addition to encode and decode the messages. Cryptanalysis of a linear cipher involves breaking the encryption of a message that has been encoded using a linear transformation.

In order to cryptanalyze the linear cipher, one can discover the weaknesses of the linear cipher by examining potential vulnerabilities within the key generation process or how the ciphertext is produced [19]. Once the values of a and b are compromised, we are able to decrypt the entire message.

Next, one may analyze ciphertext patterns, such that frequency analysis or pattern recognition. Frequency analysis involves analyzing the frequency of characters in the ciphertext and comparing it to the frequency of characters in the language of the message [11]. This may help determine the possible mapping of characters in the ciphertext to characters in the message. Then, we can form linear equations and determine the key used for encryption. Once the secret keys are known, the ciphertext can be decoded.

D. Rivest-Shamir-Adleman Algorithm

RSA algorithm is an asymmetric encryption scheme in the field of cryptography [12]. It was invented in 1977 by Rivest, Shamir, and Adleman. The algorithm uses a pair of keys which known as public key and private key. The public key is used for encryption and the private key is used for decryption. The security of the encryption relies on the difficulty of factoring large numbers. That numbers, we denoted it as p and q.

To generate the keys, one must choose two large prime numbers, p and q. Next, calculate their product, which is used as the modulus for encryption. We denote it as n. The public key is derived from the modulus n and an exponent e. The exponent, e, is chosen so that it is relatively prime to $\varphi(n)$. The private key is calculated using the Extended Euclidean algorithm to find the private exponent, d, which is the modular multiplicative inverse of e modulo $\varphi(n)$.

The RSA encryption process is shown in Eq. (3) [12]. The message is raised to the power of the public exponent, e, and the result is taken modulo n.

$$c = m^e \ mod \ n, \tag{3}$$

The RSA decryption process is shown in Eq. (4) [12]. The ciphertext is raised to the power of the private exponent, d, and the result is taken modulo n.

$$m = c^d \ mod \ n, \tag{4}$$

For example, assume a message's numeric value is 2. The RSA two prime numbers are $p = 11$ and $q = 13$. The value of $n, \varphi(n)$ are calculated as follows: $n = 11 * 13 = 143$, $\varphi(n) = 120$. Let's choose public key e = 7. To perform message encryption using Eq. (3), the ciphertext value is calculated as $c = m^e mod n = 2^7$ mod 143 = 128. For decryption of the ciphertext $c = 128$, the private key d is needed, where $d = e^{-1}$ mod $\varphi(n) = 7^{-1}$ mod 120 = 103. Using Eq. (4), the message value is calculated $m = c^d$ mod $n = 128^{103}$ mod 143 = 2.

E. Number Systems

Number systems are the system represent the numbers. For instance, decimal number system, binary number system and hexadecimal system [20]. The decimal number system or base-10 system is the counting method that commonly used daily counting scheme. It relies on ten symbols (digits), namely the digits or numbers from 0 to 9. For instance, number 10 (2 digits), 100 (3 digits, 1000 (4 digits) and so on.

Binary number system is a calculation system that operates with a base of 2. Each individual unit in the system is referred to as a bit, which stands for binary digit. This number system represents values using two distinct symbols: 0 and 1. For example, the decimal number 4 is expressed as 100 three-digit binary or 0100 in four-digit binary or 00100 in five-digit binary. Noted, these leading 0s in binary do not alter the value. There is way to convert binary to decimal. For example, a binary of 10011. The conversion of binary to decimal is as follows. $1*2^4+0*2^3+0*2^2+1*2^1+1*2^0 = 16+0+0+2+1 = 19$. However, a calculation needs to be performed for the reverse conversion from decimal to binary. For instance, for the decimal number 19, the digit is divided by 2, and the remainder is recorded as follows:

- $\frac{19}{2} = 9$, remainder 1
- $\frac{9}{2} = 4$, remainder 1
- $\frac{4}{2} = 2$, remainder 0
- $\frac{2}{2} = 1$, remainder 0
- $\frac{1}{2} = 0$, remainder 1

Hence,the final binary value is 10011.

In contrast, the hexadecimal number system utilizes 16 unique symbols to represent numeric values, which include the ten Arabic numerals (0-9) and six letters (A-F). In the hexadecimal system, each position corresponds to a value from 0 to 15, where A represents 10, B represents 11, C represents 12, D represents 13, E represents 14, and F represents 15. For example, the decimal number 18 is expressed as 12 in hexadecimal. The conversion of hexadecimal to decimal, for instance, a hexadecimal of $6D$. The D is 13. The number 6 is calculated as $6 * 16_1 + 13 * 16_0 = 96$. Hence, the final result is $96 + 13 = 109$. The reverse conversion, from decimal to hexadecimal, is done by dividing the number by 16. For example, when converting the decimal number 109, the number is divided by 16, and the remainder is recorded as follows:

- $\frac{109}{16} = 6$, remainder 13
- $\frac{6}{16} = 0$, remainder 6

The digit 13 is D, hence, the hexadecimal for 109 is equivalent to $6D$.

III. Research Design

Fig. 1 shows the research design. There are four major processes which are proposing the LRSA models, then simulation the encryption and decryption of the proposed LRSAs with the the short messages, long message and result analysis. Firstly, we proposed two types of LRSA which is Gradatim LRSA and Optimized LRSA. Next, the experiment of encryption and decryption the short message using the proposed LRSAs to ensure the LRSAs is work in practice. By using LRSAs to encrypt the message, we can get the ciphertext. We also may obtain the message from the ciphertext by using the decryption process of LRSAs. Secondly, the distribution of the long message characters is counted. Next, the message is encrypted using LRSAs, which resulting the ciphertext. One will compare distributed histogram with the ciphertext.

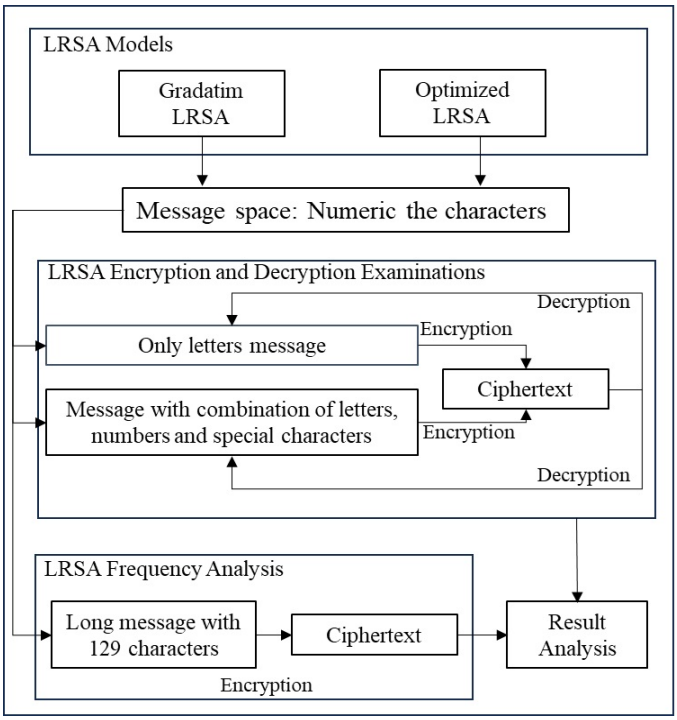


Fig. 1. Research design.

IV. Proposed LRSA

In this section, we present two designs of LRSA, known as Gradatim LRSA and Optimized LRSA. The Gradatim LRSA performs encryption and decryption character by character. The

Optimized LRSA has customized encryption and decryption at the stage of the RSA algorithm. The proposed hybrid encryption and decryption using the linear cipher and RSA algorithm to address the vulnerability of the linear cipher. This hybrid design allows for the implementation of more complex and robust security solutions.

A. Gradatim LRSA

The proposed hybrid encryption method uses both symmetric and asymmetric algorithms. The symmetric algorithm is a linear cipher, while the asymmetric algorithm is the RSA algorithm. We denote it as Gradatim LRSA, which means that the encryption and decryption processes are performed in a gradual and orderly manner.

The proposed hybrid Gradatim encryption as shown in Algorithm 1. By combining the linear cipher with the RSA algorithm, the message is first encoded using the linear cipher and then the resulting ciphertext is further encrypted using the RSA algorithm. This double encryption process prevents the detection of statistical patterns in the message.

Algorithm 1 Gradatim LRSA - Encryption Process

Require: Input: Message, m_{ml}.
1: Chooses the message space M.
2: Chooses the message m with the length of ml.
3: Selects secret keys, a and b, a must be coprime with M.
4: Selects two positive prime numbers, p and q, subjected p, $q > 2$.
5: Calculates $n = p * q$.
6: Calculates $\varphi(n)$.
7: Chooses a positive integer e, where e is coprime with $\varphi(n)$.
8: **for** $i \leftarrow 1$ to ml **do**
9: Calculates ciphertext, $c_i = (a * m_i + b \ mod \ M)^e$ mod n.
10: **end for**
11: **Output:** Ciphertext, c_{ml}.

The proposed hybrid Gradatim decryption as shown in Algorithm 2. The ciphertex is first decrypted using the RSA algorithm and then the resulting output is further decoded using the linear cipher.

Algorithm 2 Gradatim LRSA - Decryption Process

Require: Input: Ciphertext, c_{ml}.
1: Given cipertext, c_{ml}.
2: With existing secret keys, a and b.
3: Calculates private key, $d = e^{-1} \ mod \ \varphi(n)$, gcd(d, e) = 1.
4: **for** $i \leftarrow 1$ to ml **do**
5: Calculates message, $m_i = a^{-1} * ({c_i}^d \text{ mod } n - b) \text{ mod } M$.
6: **end for**
7: **Output:** Message, m_{ml}.

B. Optimized LRSA

The proposed a hybrid Optimized LRSA that uses a symmetric linear cipher and an asymmetric RSA algorithm. The modification occurs at the stage of the RSA algorithm, as shown in Algorithm 3. The message is encoded using the linear cipher. The resulting output is transformed into binary and concatenated. If the length of the message is not an even number, the string is padded with seven zeros. Noted it is the character 'A' as shown in Table I. For every 14 bits, the data is further encrypted with the RSA algorithm.

Algorithm 3 Optimized LRSA - Encryption Process

Require: Input: Message, m_{ml}.
1: Chooses the message space M.
2: Chooses the message m with the length of ml.
3: Selects secret keys, a and b, a must be coprime with M.
4: Selects two positive prime numbers, p and q, subjected p, $q > 2$.
5: Calculates $n = p * q$.
6: Calculates $\varphi(n)$.
7: Chooses a positive integer e, where e is coprime with $\varphi(n)$.
8: **for** $i \leftarrow 1$ to ml **do**
9: Calculates intermediate ciphertext, $k_i = (a * m_i + b) \text{ mod } M$.
10: **end for**
11: **for** $i \leftarrow 1$ to ml **do**
12: Converts intermediate ciphertext, k_i into binary.
13: **end for**
14: **if** ml is even number **then**
15: **for** $i \leftarrow 2$ to ml **do**
16: Concatenates intermediate ciphertext, such that $k_i||k_{i+1}$, we denoted it as K_i.
17: Convert K_i into decimal number, we denoted it as D_i.
18: Calculates ciphertext, $c_i = (D_i)^e$ mod n.
19: **end for**
20: **Output:** Ciphertext, $c_{\frac{ml}{2}}$.
21: **else**
22: Creates a temporary binary in such a way that k_{ml+1} is 0000000. The decimal value is 0. The alphabet is A.
23: **for** $i \leftarrow 2$ to $ml + 1$ **do**
24: Concatenates intermediate ciphertext, such that $k_i||k_{i+1}$, we denoted it as K_i.
25: Convert K_i into decimal number, we denoted it as D_i.
26: Calculates ciphertext, $c_i = (D_i)^e$ mod n.
27: **end for**
28: **Output:** Ciphertext, $c_{\frac{ml+1}{2}}$.
29: **end if**

The proposed hybrid Optimized LRSA decryption is shown in Algorithm 4. The ciphertext is first decrypted using the RSA algorithm. The resulting output is transformed into binary and divided into 7 bits per character. If the length of the message is an odd number, the last 7 bits are discarded. Then, the bit values are converted into decimal; these decimal values are further decoded using the linear cipher.

V. Numeric Character

The character variable with letter or symbol or numeric values is converted into a predefined set of rules numerical value as shown in Table I. For example the alphabet 'A' is equal to 0, 'B' is equal to 1, 'C' is equal to 2, and so on.

Algorithm 4 Optimized LRSA - Decryption Process

Require: Input: Ciphertext, $c_{\frac{ml}{2}}$ or $c_{\frac{ml+1}{2}}$.
With existing secret keys, a and b.
Calculates private key, $d = e^{-1} \mod \varphi(n)$, gcd(d, e) = 1.
if Ciphertext is $c_{\frac{ml}{2}}$ **then**
  for $i \leftarrow 1$ to $\frac{ml}{2}$ **do**
    Calculates intermediate ciphertext, $D_i = {c_i}^d \mod n$.
    Converts D_i into 14 bits binary, we denoted it as K_i.
    Splits the K_i into two 7 bits binary, such that k_{i*2-1} and k_{i*2}.
    Converts k_{i*2-1} and k_{i*2} into decimal number, we denoted it as D'_{i*2-1} and D'_{i*2} respectively.
    Calculates the message, $m_{i*2-1} = a^{-1} * (D'_{i*2-1} - b) \mod M$.
    Calculates the message, $m_{i*2} = a^{-1} * (D'_{i*2} - b) \mod M$.
  end for
Output: Message, m_{ml}.
else
  for $i \leftarrow 1$ to $\frac{ml+1}{2}$ **do**
    Calculates intermediate ciphertext, $D_i = {c_i}^d \mod n$.
    Converts D_i into 14 bits binary, we denoted it as K_i.
    Splits the K_i into two 7 bits binary, such that k_{i*2-1} and k_{i*2}.
    Converts k_{i*2-1} and k_{i*2} into decimal number, we denoted it as D'_{i*2-1} and D'_{i*2} respectively.
    Calculates the message, $m_{i*2-1} = a^{-1} * (D'_{i*2-1} - b) \mod M$.
    Calculates the message, $m_{i*2} = a^{-1} * (D'_{i*2} - b) \mod M$.
  end for
  Discarded m_{ml+1}.
Output: Message, m_{ml}.
end if

We have 26 upper and lower case letters each. There are ten numbers, nice special characters as well as space. For space, we denoted it as as '△'. Noted that this table can be enlarge if needed, which means the set space of message M is not fix.

VI. Simulation Result

This section provides a comprehensive overview of the simulation results obtained from the encryption and decryption processes conducted for the proposed LRSA (Gradatim LRSA and Optimized LRSA). The simulation involved processing messages of both short and long lengths to assess how the LRSA algorithm performs in encryption and decryption.

A. Gradatim LRSA - Encryption and Decryption

Section IV-A presents the Gradatim LRSA algorithm. Here, we show two examinations of encryption and decryption calculations. Both case studies have prime numbers for RSA, with $p = 31$, $q = 3$ and the public exponent e equal to 7. The private exponent d is the modular multiplicative inverse of e mod $(31 - 1)(3 - 1)$, resulting in 43.

TABLE I. Numeric the Alphabets, Numbers and Special Characters

A	0	**B**	1	**C**	2	**D**	3	**E**	4	**F**	5
G	6	**H**	7	**I**	8	**J**	9	**K**	10	**L**	11
M	12	**N**	13	**O**	14	**P**	15	**Q**	16	**R**	17
S	18	**T**	19	**U**	20	**V**	21	**W**	22	**X**	23
Y	24	**Z**	25	**a**	26	**b**	27	**c**	28	**d**	29
e	30	**f**	31	**g**	32	**h**	33	**i**	34	**j**	35
k	36	**l**	37	**m**	38	**n**	39	**o**	40	**p**	41
q	42	**r**	43	**s**	44	**t**	45	**u**	46	**v**	47
w	48	**x**	49	**y**	50	**z**	51	**0**	52	**1**	53
2	54	**3**	55	**4**	56	**5**	57	**6**	58	**7**	59
8	60	**9**	61	**'**	62	**?**	63	**!**	64	**.**	65
△	66	**,**	67	**;**	68	**@**	69	**"**	70	**:**	71

1) Experiment - 1: Assume the message is only capital letter, such that "COMPUTE". Based on Table I, we know the capital letter is from 0 until 25, therefore, the set space, M is equal to 26. Lets, secret keys of linear cipher are $a = 3$ and $b = 10$.

Table II shows the encryption of the text message "COMPUTE" using Gradatim LRSA. The ciphertext is in numeric form, which is "70 0 80 48 9 54", or in hexadecimal "46 00 50 30 09 36 34".

TABLE II. Gradatim LRSA Encryption "COMPUTE"

Message	C	O	M	P	U	T	E
Numeric, m	2	14	12	15	20	19	4
$m' = (3 * m + 10)$ **mod** 26	16	0	20	3	18	15	22
$(m')^7$**mod** 93	70	0	80	48	9	54	52
Ciphertext	70	0	80	48	9	54	52
Hexadecimal	46	00	50	30	09	36	34

Table III shows the decryption of the corresponding ciphertext "70 0 80 48 9 54 52" using Gradatim LRSA. The ciphertext is decrypted using RSA algorithm together with private key d, followed by linear cipher, $(3^{-1} * c - 10)$ mod 26. It is noted that the inverse of 3 mod 26 is based on Extended Euclidean algorithm, resulting in 9.

TABLE III. Gradatim LRSA Decryption Corresponding Ciphertext of "COMPUTE"

Ciphertext	70	0	80	48	9	54	52
$c' = c^{43}$**mod** 93	16	0	20	3	18	15	22
$m = 9(c' - 10)$ **mod** 26	2	14	12	15	20	19	4
Message	C	O	M	P	U	T	E

Table III shows the decryption of the corresponding ciphertext "70 0 80 48 9 54 52" using LRSA. The ciphertext is decrypted using RSA algorithm together with private key d,

followed by linear cipher, $(3^{-1} * c - 10) \bmod 26$. It is noted that the inverse of 3 mod 26 is based on Extended Euclidean algorithm, resulting in 9.

2) Experiment - 2: Assume the message is like a six character of password, such that "C0!fe@". The password is the combination of upper case letter, lower case letter, number and special character as shown in Table I. Therefore, the set space, M is equal to 72. Lets, secret keys of linear cipher are $a = 5$ and $b = 10$.

Table IV shows the encryption of the text message "C0!fe@" using Gradatim LRSA. The ciphertext is in numeric form, which is "80 60 75 42 70 67", or in hexadecimal "50 3C 4B 2A 46 43".

TABLE IV. GRADATIM LRSA ENCRYPTION "C0!FE@"

Message	C	0	!	f	e	@
Numberic, m	2	52	64	31	30	69
$m' = 5 * m + 10$ **mod** 72	20	54	42	21	16	67
$(m')^7$ **mod** 93	80	60	75	42	70	67
Ciphertext	80	60	75	42	70	67
Hexadecimal	50	3C	4B	2A	46	43

Table V shows the decryption of the corresponding ciphertext "80 60 75 42 70 67" using Gradatim LRSA. The ciphertext is decrypted using the RSA algorithm together with private key d, followed by linear cipher, $(5^{-1} * c - 10) \bmod 72$. It is noted that the inverse of 5 mod 72 is based on Extended Euclidean algorithm, resulting in 29.

TABLE V. GRADATIM LRSA DECRYPTION CORRESPONDING CIPHERTEXT OF "C0!FE@"

Ciphertext	80	60	75	42	70	67
$c' = c^{43}$ **mod** 93	20	54	42	21	16	67
$m = 29(c' - 10)$ **mod** 72	2	54	42	31	30	69
Message	C	0	!	f	e	@

Table V shows the decryption of the corresponding ciphertext "80 60 75 42 70 67" using Gradatim LRSA. The ciphertext is decrypted using the RSA algorithm together with private key d, followed by linear cipher, $(5^{-1} * c - 10) \bmod 72$. It is noted that the inverse of 5 mod 72 is based on Extended Euclidean algorithm, resulting in 29.

B. Optimized LRSA - Encryption and Decryption

Section IV-B presents the Optimized LRSA algorithm. Here, we show two examinations of encryption and decryption calculations with the word of "COMPUTE" and "C0!fe@" respectively. Both case studies have prime numbers for RSA, with $p = 127$, $q = 131$ and the public exponent e equal to 19. The private exponent d is the modular multiplicative inverse of $e \bmod (127 - 1)(131 - 1)$, resulting in 7759.

1) Experiment - 1: The experiment message is "COMPUTE". Based on Table I, we know the capital letter is from 0 until 25, therefore, the set space, M is equal to 26. The secret keys of linear cipher are $a = 3$ and $b = 10$.

Table VI shows the encryption of the text message "COMPUTE" using Optimized LRSA. The ciphertext is in numeric form, which is "6541 7480 11085 4721", or in hexadecimal '198D 1D38 2B4D 1271".

Table VII shows the decryption of the corresponding ciphertext "6541 7480 11085 4721" using Optimized LRSA. The ciphertext is decrypted using the RSA algorithm with the private key (d), which is 7759. The decimal output is converted into binary and further divided into 7 bits per character. Since the number of characters is odd, the last 7 bits are discarded. Next, the binary data is converted into decimal and decoded using a linear cipher.

2) Experiment - 2: The experiment 2, the word is a combination of upper case letter, lower case letter, number and special character, which is "C0!fe@". Therefore, the set space, M is equal to 72 as shown in Table I. Lets, secret keys of linear cipher are $a = 5$ and $b = 10$.

Table VIII shows the encryption of the text message "C0!fe@" using Optimized LRSA. The ciphertext is in numeric form, which is "15535 9394 1328", or in hexadecimal "3CAF 24B2 0530".

Table IX shows the decryption of the corresponding ciphertext "15535 9394 1328" using Optimized LRSA. The ciphertext is decrypted using the RSA algorithm along with the private key (d), which is 7759. The decimal output is then converted into binary and further divided into 7 bits per character. Since the number of characters is even, all bits are utilized. Next, the binary data is converted back into decimal and encoded using a linear cipher, such that $(5^{-1} * c - 10) \bmod 72$. It should be noted that the inverse of 5 modulo 72, calculated using the Extended Euclidean algorithm, is 29.

Table IX shows the decryption of the corresponding ciphertext "80 60 75 42 70 67" using LRSA. The ciphertext is decrypted using RSA algorithm together with private key d, followed by linear cipher, such that $5^{-1} * c - 10 \bmod 72$.

VII. FREQUENCY ANALYSIS

Frequency analysis is a technique used in cryptanalysis to determine the frequency of characters in an encrypted text. By analyzing the frequencies of letters in a message, cryptanalysts can make educated guesses about the substitution cipher being used to encrypt the text. The linear cipher is vulnerable to frequency analysis. By determining which characters occur most frequently in encrypted text, one may deduce the original message and crack the code.

For the frequency experiment, the chosen text message contains 129 characters. The message is: 'The linear cipher relies on a linear mathematical operation, such as multiplication and addition to scramble and decode messages.' The distribution of character is shown in Fig. 2. The highest distribution is of the space symbol ($\triangle$), which appears 18 times, followed by character 'a', which appears 14 times. The lowest distribution is of the characters 'T', 'b', 'g', comma symbol, and the full stop symbol, each of which appears once.

Lets examine if the text message is encoded using linear cipher. The set space, M is equal to 72 and the secret keys of linear cipher are $a = 5$ and $b = 10$.

TABLE VI. OPTIMIZED LRSA ENCRYPTION "COMPUTE"

Message, m	C	O	M	P	U	T	E
Numeric, m	2	14	12	15	20	19	4
$k = (3 * m + 10)$ **mod** 26	16	0	20	3	18	15	22
Binary, k	0010000	0000000	0010100	0000011	0010010	0001111	0010110
Concatenation, K	00100000000000		00101000000011		00100100001111		0010110<u>0000000</u>*
Decimal, D	2048		2563		2304		2816
$c = (D)^{19}$**mod** 16637	6541		7480		11085		4721
c **in hexadecimal**	198D		1D38		2B4D		1271

Notes: The underline binary is the concatenation for single character.

TABLE VII. OPTIMIZED LRSA DECRYPTION CORRESPONDING CIPHERTEXT OF "COMPUTE"

Ciphertext, c'	6541		7480		11085		4721
$D = c'^{7759}$**mod** 16637	2048		2563		2304		2816
Binary, K	00100000000000		00101000000011		00100100001111		0010110<u>0000000</u>*
Splitting, k	0010000	0000000	0010100	0000011	0010010	0001111	0010110
c'	16	0	20	3	18	15	22
$m = 9(c' - 10)$ **mod** 26	2	14	12	15	20	19	4
Message, m	C	O	M	P	U	T	E

Notes: The underline binary is the leftover binary, it is discarded.

TABLE VIII. OPTIMIZED LRSA ENCRYPTION "C0!FE@"

Message, m	C	0	!	f	e	@
Numberic, m	2	52	64	31	30	69
$k = 5 * m + 10$ **mod** 72	20	54	42	21	16	67
Binary, k	0010100	0110110	0101010	0010101	0010000	1000011
Concatenation, K	00101000110110		01010100010101		00100001000011	
Decimal, D	2614		5397		2115	
$c = (D)^{19}$ **mod** 16637	15535		9394		1328	
c **in hexadecimal**	3CAF		24B2		0530	

TABLE IX. OPTIMIZED LRSA DECRYPTION CORRESPONDING CIPHERTEXT OF "C0!FE@"

Ciphertext, c'	15535		9394		1328	
$D = c'^{7759}$ **mod** 16637	2614		5397		2115	
Binary, K	00101000110110		01010100010101		00100001000011	
Splitting, k	0010100	0110110	0101010	0010101	0010000	1000011
c'	20	54	42	21	16	67
$m = 29(c' - 10)$ **mod** 72	2	54	42	31	30	69
Message, m	C	0	!	f	e	@

The ciphertext is: 'hfQ0zk9Q;J0Gk:fQJ0JQzkQO0△90 ;0zk9Q;J04;TfQ4;TkG;z0△:QJ;Tk△950OQGf0;O04YzTk:zkG; Tk△ 90;9L0;LLkTk△ 90T△ 0OGJ;9BzQ0;9L0LQG△ LQ04Q OO;aQOv'. The distribution of character ciphertext is shown in Fig. 3. The highest distribution is of the zero, which appears 18 times, followed by semicolon symbol, which appears 14 times. One can conclude that the zero is the ciphertext for the character space symbol (△), while zero is the ciphertext for the character 'a'. Once, we know the ciphertext with the corresponding character, we can form the linear equations and find the secrect key a and b.

Next, we encrypt the text message using Gradatim LRSA and Optimized LRSA respectively. For both simulations, the set space M is equal to 72 and the secret keys of linear cipher are $a = 5$ and $b = 10$. The different only the RSA algorithm parameters.

For the Gradatim LRSA, the RSA two prime numbers are $p = 31$, $q = 3$ and the public exponent e equal to 7. The ciphertext is in hexadecimal form:

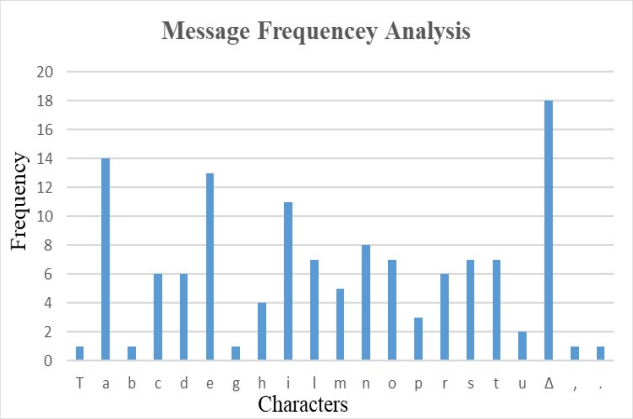


Fig. 2. Message frequency analysis.

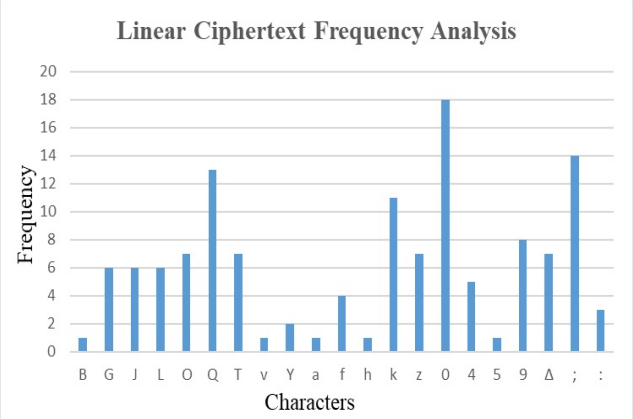


Fig. 3. Linear ciphertext frequency analysis.

‘421F464912243D464448490624291F4648494846122446324
94E3D49444912243D464448493844071F4638440724064412
494E2946484407244E3D39493203061F49443249380312422
4291224064407244E3D49443D2C49442C2C2407244E3D490
74E4932064844380112464944 3D2C492C46064E2C46493846
3232441A463208’.

For the Optimized LRSA, the RSA two prime numbers are $p = 127$, $q = 131$ and the public exponent e equal to 19. The ciphertext is in hexadecimal form: ‘037D03B33D7F0B202271252B261F05B319C20A913D7F2A
F111CB23E738CA3D7F0B2022713F6D15CF05D330130C45
09962A13385FZBCE15CF04D0222A18341DE9033638240B8
A22D4261F3D7F09960C452731033600A1033635AA32F704
D032A90F1706FC2C4507E4364736D6303F1DC02386137B2
3863F6D2AF1382433E212D0’.

Based on the ciphertext generated using Gradatim LRSA and Optimized LRSA, one may not be able to form the frequency distribution as the output ciphertext exceeds the numeric values presented in Table I. For example, when encrypting the character ‘o’ using Gradatim LRSA, the ciphertext value is 78. Therefore, we provide the ciphertext in hexadecimal form. This also indicates that both Gradatim LRSA and Optimized LRSA are not vulnerable to frequency attacks.

VIII. Discussion

Algorithms for encryption and decryption may protect data confidentiality. Encryption scrambles the message into unreadable ciphertext, while decryption is the reverse process of encryption. The proposed Gradatim LRSA and Optimized LRSA include both algorithms for encryption and decryption, as shown in Algorithms 1, 2, 3, and 4, respectively. The experiments in Section III demonstrate that both models effectively perform encryption and decryption.

Based on Table IV and Table VIII, the number of calculations for the second layer of the RSA algorithm shows that the Optimized LRSA is less than the Gradatim LRSA. If the length of the message is ml, the Gradatim LRSA must perform ml operations for the first layer of encryption (linear cipher) and ml operations for the second layer of encryption (RSA algorithm). However, for the Optimized LRSA, the number of calculations is only ml for the first layer (linear cipher) and $\frac{ml}{2}$ for the second layer (RSA algorithm). However, if the ml is a odd number, the Optimized LRSA will perform $\frac{ml+1}{2}$ operations for the second layer encryption. This shows that Optimized LRSA executes faster compared to Gradatim LRSA.

The linear cipher employs a linear mathematical operation to encode a message into unreadable ciphertext, with the frequency of characters in the message remaining the same in the ciphertext but with different characters. Based on the analysis in Section VII, showing that linear cipher is vulnerable to frequency analysis attacks. Hence, the proposed the hybrid encryption method using the linear cipher and RSA algorithm can resist the frequency attacks.

IX. Conclusion and Future Work

In conclusion, this research proposed a secure hybrid encryption method method that combines the strength of a linear cipher with the robust security of the RSA algorithm making it significantly more difficult for attackers to break the encryption. We name it as LRSA. We proposed models: Gradatim LRSA and Optimized LRSA. Optimized LRSA executes fewer rounds compared to Gradatim LRSA. However, both LRSAs can encrypt the message using secret keys from a linear cipher and public keys from the RSA algorithm. The encrypted output is the ciphertext. The LRSAs are also capable of decrypting the ciphertext and recovering the original message without compromising its security.

Existing linear cipher is vulnerable to the frequency attacks where the attackers are able to decipher the messages based on the frequency of occurrence of the characters in the ciphertext. But, the proposed LRSAs are resistance to the frequency attacks. As the proposed LSRAs add an addition layer of complexity to the encryption process, which is RSA algorithm. Hence, LRSAs provide a comprehensive and effective encryption solution that prioritizes the security for protecting sensitive information across different applications. The hybrid encryption method ensure the confidentiality of the messages only available for the authorize parties.

As for the nature of the linear cipher, which only allows for the encryption and decryption of English characters, this presents a major limitation of the proposed design. Therefore,

as future work, one plan is to explore hybrid encryption and decryption methods that can accommodate a broader range of languages, such as Mandarin, Jawi, and Japanese. This work may create a more universal encryption solution that meets the needs of multilingual users.

ACKNOWLEDGMENT

The authors would like to thank Guangdong University of Science & Technology, China, Rabdan Academy, United Arab Emirates.

REFERENCES

[1] C. Paar, J. Pelzl and T. Güneysu, *Introduction to cryptography and data security*, In Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms, pp. 1-35, 2024.

[2] R. Verma, A. Kumari, A. Anand and V.S.S. Yadavalli, *Revisiting shift cipher technique for amplified data security*, Journal of Computational and Cognitive Engineering, 3(1), pp. 8-14, 2024.

[3] S. Yalamati, *Data Privacy, Compliance, and Security in Cloud Computing for Finance*, In Practical Applications of Data Processing, Algorithms, and Modeling, pp 127-144, 2024.

[4] J. Pool, S. Akhlaghpour, F. Fatehi and A. Burton-Jones, *A systematic analysis of failures in protecting personal health data: a scoping review*, International Journal of Information Management, 74, pp. 102719, 2024.

[5] D. O. Ogundipe, *The impact of big data on healthcare product development: A theoretical and analytical review*, International Medical Science Research Journal, 4(3), pp. 341-360, 2024.

[6] S. Agarwal, P. Ghosh, T. Ruan and Y. Zhang, *Transient Customer Response to Data Breaches of Their Information*, Management Science, 2024.

[7] X. Wang, J. Yan, T. P. Munyon and T. R. Crook, *Breached But Not Broken: How Attributional Information Shapes Shareholder Reactions to Firms Following Data Breaches*, Corporate Reputation Review, pp. 1-22, 2024.

[8] Y. Guo, C. Wang and X. Chen, *Functional or financial remedies? The effectiveness of recovery strategies after a data breach*, Journal of Enterprise Information Management, 37(1), pp. 148-169, 2024.

[9] S. Chakraborty, C. Jackson, M. Frazier and K. Clark, *A Study on Password Protection and Encryption in the era of Cyber Attacks*, In SoutheastCon 2024, IEEE, pp. 1-5, 2024.

[10] V. Sasikala and B. S. CH, *Data Leakage Detection and Prevention Using Ciphertext-Policy Attribute Based Encryption Algorithm*, In 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), IEEE, pp. 1460-465, 2024.

[11] N. Ferguson, B. Schneier and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications*, Wiley, 2010.

[12] R. Das and G. Goldsztein, *Mathematics Behind the RSA Algorithm*, Journal of Student Research, 12 (1), 2023.

[13] K. Balasubramanian and M. P. Pitchai, *A survey of fermat factorization algorithms for factoring RSA composite numbers*, Multidisciplinary Science Journal, 6, 2024.

[14] S. Tanwar, R. Balavenu, H. H. Ramesha, M. Tiwari, K. K. Ramachandran and D. K. J. B. Sain, *Applied Cryptography in Banking and Financial Services for Data Protection*, Computer Science Engineering and Emerging Technologies: Proceedings of ICCS, 59, 2024.

[15] A. Desianty and M. I. Imelda, *Systematic Literature Review: Cybersecurity by Utilizing Cryptography Using the Data Encryption Standard (DES) Algorithm*, Jurnal Teknik Informatika, 17(1), pp.30-39, 2024.

[16] J. Schwenk, *Cryptography: Confidentiality. In Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications*, Cham: Springer International Publishing, pp.13-41, 2022.

[17] H. B. Wolfe, *Cryptography: Protecting confidentiality, integrity and availability of data*, In Internet and Intranet Security Management: Risks and Solutions, pp.141-162, 2000.

[18] D. Mahto, D. A. Khan and D. K. Yadav,*Security analysis of elliptic curve cryptography and RSA*, In Proceedings of the world congress on engineering, 1, pp.419-422, 2016.

[19] W. Stallings, *Cryptography and network security:principles and practices*, Pearson Education India, 2006.

[20] B. J. LaMeres, *Number Systems*, In Introduction to Logic Circuits & Logic Design with Verilog, pp. 7-41, 2023.

Enterprise Architecture Framework Selection for Collaborative Freight Transportation Digitalization: A Hybrid FAHP-FTOPSIS Approach

Abdelghani Saoud[1], Adil Bellabdaoui[2], Mohamed Lachgar[3], Mohamed Hanine[4], Imran Ashraf[5]
ITM – Information Technology and Management, ENSIAS, Mohammed V University, Rabat, Morocco[1,2]
L2IS Laboratory, FSTG, Cadi Ayyad University, Marrakesh, Morocco[3]
Higher Normal School, Department of Computer Science, Cadi Ayyad University, Marrakesh, Morocco[3]
LTI, National School of Applied Sciences, Chouaib Doukkali University, El Jadida, Morocco[4]
Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea[5]

***Abstract*—Collaborative freight transportation plays a crucial role for Logistic Service Providers (LSPs) seeking to enhance profitability and service quality, yet it faces challenges at strategic, operational, and technical levels. Digital transformation creates opportunities to overcome these hurdles by extending collaboration beyond physical logistics to encompass information management and digital transformation. Enterprise Architecture Frameworks (EAFs) offer promising solutions by providing a holistic view of various levels within such ecosystems and ensuring alignment between information systems and strategic objectives. However, selecting the right EAF is a complex and critical step. This study introduces an innovative approach for selecting an Enterprise Architecture (EA) framework to support the development of a collaborative freight transportation platform. It emphasizes the importance of adopting a systematic EA methodology in the digitalization of the freight transportation sector. The decision-making process integrates established techniques such as the Analytic Hierarchy Process (AHP) and the Fuzzy Technique for Order of Preference by Similarity to Ideal Solution (F-TOPSIS). Applied to a case study involving a Moroccan logistics company, the approach demonstrates effectiveness in framework selection. The study's findings underscore the method's significance as a valuable tool for organizations embarking on digital transformation through EA, offering adaptability across diverse industries and contexts.**

***Keywords*—Digital transformation; freight transportation; enterprise architecture; multi-criteria decision-making; analytic hierarchy process; fuzzy technique for order of preference by similarity to ideal solution**

I. Introduction

In the evolving landscape of freight transportation, digital transformation is fueled by advancements in Information and Communication Technologies (ICT) and a growing demand for more efficient and sustainable logistics operations [1], [2], [3]. This work is motivated by the imperative to introduce a decision-making method for the meticulous selection of a fitting Enterprise Architecture (EA) framework essential for underpinning the development of a collaborative freight transportation platform. The proposed method integrates two well-known multicriteria decision-making techniques: the Analytic Hierarchy Process (AHP) and the Fuzzy Technique for Order of Preference by Similarity to Ideal Solution (F-TOPSIS). The overarching goal is to aid organizations in the evaluation and ranking of candidate EA frameworks, considering diverse criteria such as functionality, interoperability, scalability, and adaptability.

At the heart of this endeavor lies the challenge of striking a delicate balance amid the conflicting requirements of diverse stakeholders, including IT managers, business analysts, and end-users, in the meticulous selection of an apt EA framework. Moreover, the selection process involves a multitude of criteria often shrouded in subjectivity and resistant to quantification. To surmount these challenges, the authors advocate for a group decision-making approach that actively involves various stakeholders in the selection process. This approach employs a nuanced blend of quantitative and qualitative methods to assess and rank candidate EA frameworks.

The primary contributions of this work are twofold. Firstly, the proposed decision-making method integrates AHP and F-TOPSIS techniques for selecting a suitable EA framework for a collaborative freight transportation platform. Secondly, the application of this method to a case study involving a Moroccan logistics company demonstrates its effectiveness in selecting an appropriate EA framework. The findings from this work can provide valuable insights for other organizations seeking to drive digital transformation through EA.

In the realm of collaborative freight transport, a strategic approach employed by logistics service providers (LSPs) to enhance profitability and service quality, various challenges hinder its effectiveness. These challenges encompass difficulties in finding suitable partners, establishing fair gain-sharing mechanisms, and fostering trust in resource sharing [4]. Simultaneously, the imperative for companies to undertake digital transformation projects to align with innovation trends adds complexity. LSPs are compelled to extend collaboration beyond physical flow, managing information and undergoing digital transformation, further complicating alignment among strategies, business, and systems for multi-stakeholders.

Enterprise architecture frameworks (EAFs) play a pivotal role in addressing such complexity, offering a holistic view of the system and aligning information systems with strategic and business requirements. However, selecting the appropriate EAF is a challenging task due to the plethora of frameworks available, each with its strengths and weaknesses. Existing works on EAF selection often lack specificity to concrete contexts and needs, either proposing abstract evaluation models

or performing global EAF comparisons. This paper addresses these gaps by evaluating EAFs in the context of designing an ongoing digital platform for collaborative freight transportation (DCRFT).

The methodology involves a hybrid Multi-criteria Group Decision Making approach, comprising two phases. In the first phase, criteria are identified through a literature review enriched by expert interviews, and the Analytic Hierarchy Process (AHP) is employed to determine their importance weights. In the second phase, Fuzzy Technique for Order of Preference by Similarity to Ideal Solution (F-TOPSIS) is used to rank the EAF alternatives. Fuzzy set theory is adopted to overcome ambiguity stemming from subjective judgments and incomplete information among decision-makers [5]. Throughout both phases, group decision aggregation techniques are applied and illustrated. The comprehensive approach presented in this work stands as a valuable resource for organizations navigating the intricate landscape of digital transformation in collaborative freight transportation.

The remainder of this paper is organized as follows: Section II introduces the background of Multi-Criteria Decision Making (MCDM) and Enterprise Architecture Framework. Section III provides a literature review related to EAF evaluations. Section IV presents the AHP and F-TOPSIS method, describing the procedural steps of the proposed approach. The results of the case study are discussed in Section V. Section VI presents a sensitivity analysis. Finally, Section VII concludes the article and sheds light on future works.

II. Background

In this section, an in-depth examination of the Enterprise Architecture Framework unfolds, revealing its fundamental principles and practical applications. The focus then shifts towards exploring Digitalizing Freight Transportation: Strategic Solutions with Enterprise Architecture, where the transformative influence of digital technologies on logistics and supply chain management takes center stage. To conclude, attention is directed to the concept of Multi-Criteria Decision Making (MCDM), shedding light on its pertinence within the realm of Driving Digital Transformation in Freight Transportation. Collectively, these sections foster a comprehensive understanding of the study's foundational components, laying the groundwork for a nuanced exploration of their intricate interconnections and implications within the dynamic landscape of freight transportation.

A. Enterprise Architecture Framework

Zachman [6] defines architecture as a set of design elements essential for outlining an object to meet quality requirements and ensure maintenance throughout its utility period. It involves tools for understanding the current state and aiming for a better future state. Enterprise Architecture (EA) provides a holistic organizational view, distinct from technical architecture, and addresses stakeholder concerns [7].

EA acts as a strategic tool, assisting organizations in defining their current (As-is) and desired future (To-be) states regarding infrastructures, processes, and digital capabilities. It aligns strategic and business levels with operational and system implementations, crucial in the current digital landscape for guiding organizational change and facilitating digital transformation [8].

In turbulent environments, sustained competitive advantages require organizational flexibility and resilience [9]. EA can support adaptive capacities and facilitate the progression to higher-level capabilities by re-conceptualizing itself through an enterprise's ecological adaptation perspective.

Moreover, EA provides governance encompassing IT principles, architecture, investment management, and planned strategy, closely tied to organizational business values, yielding benefits in visibility, productivity, and efficiency of business processes and information systems [10].

Numerous studies have linked various advantages to the implementation of enterprise architecture. In a literature review conducted by [11], success factors and benefits of enterprise architecture were identified. These include heightened responsiveness and flexibility to change, enhanced alignment between the business model and IT, reduced IT costs, optimized utilization of IT resources, improved risk management, enhanced integration/interoperability, more favorable outcomes from business and strategic initiatives, refined business processes, and diminished complexity in IT. Notably, these effects are typically indirect, pervasive throughout the entire enterprise, and accrue over an extended period.

B. Digitalizing Freight Transportation: Strategic Solutions with Enterprise Architecture

In the logistics and supply chain management domain, Freight Transportation entails the movement of goods across diverse modes like trucks, trains, ships, and planes [12]. Mode selection considers factors such as distance, urgency, and the nature of goods. Efficient freight transportation is pivotal for seamless goods flow within the supply chain, a critical aspect of the broader logistics network. Driving Digital Transformation in Freight Transportation involves leveraging technological advancements for enhanced efficiency, transparency, and overall effectiveness [13]. This encompasses integrating digital tools, data analytics, and automation to optimize routes, manage inventory, and streamline communication in the freight transportation ecosystem.

The road freight transport sector is witnessing substantial economic growth, playing a crucial role in modern economies and influencing global competitiveness. The surge in e-commerce and globalization has heightened transport demands, urging companies in various modes to enhance associated services. This dynamic presents persistent challenges for road freight transport trucks. Economically, operators must optimize efficiency to maximize profits and minimize empty trips. Environmentally, efforts are required to reduce CO2 emissions, mitigate road congestion, and curb noise pollution. Socially, enhancing accessibility and physical mobility is essential for improving the quality of life for logistics workers and the global population [14], [15], [16], [17].

Trucking companies are compelled to align with "Industry 4.0," emphasizing digital manufacturing and high-level automation [18]. Information exchange and integration of the intelligent logistics chain are critical, with information flow management central in data-driven transportation operations.

In this evolving context, freight transportation demands novel organizational and technological approaches for effective management and adaptation to digital changes [19].

Digital platforms offer productivity in implementing collaborative and intelligent environments, transforming organizational business models through partner discovery, accelerated information sharing, optimization, and tracking of logistical operations [20], [21]. This transition poses technological, organizational, and strategic challenges, requiring a comprehensive methodology. "Enterprise Architecture" (EA) serves as a crucial tool, offering a holistic view of the organization while ensuring alignment between strategic objectives and technical solutions.

In this evolving freight transportation landscape, selecting a tailored Enterprise Architecture Framework (EAF) is paramount. Beyond immediate challenges, the chosen EAF should provide a roadmap for navigating digital transformation, addressing operational complexities and ensuring seamless integration of innovative technologies, efficient processes, and strategic objectives. This approach steers the transformation towards a more agile and responsive freight transportation ecosystem.

C. Multi-Criteria Decision Making (MCDM)

Within the realm of Multi-Criteria Decision Making (MCDM), its application extends beyond traditional problem-solving domains, finding relevance in the context of Driving Digital Transformation in Freight Transportation. MCDM, as a sophisticated evaluation process, serves as a valuable tool for decision-makers facing the intricate challenges of adopting and implementing digital technologies in the freight transportation sector. The inherent complexity of this industry, marked by diverse operational facets and evolving technological landscapes, makes MCDM an ideal approach for navigating the intricacies of decision-making.

In the realm of freight transportation, where uncertainties and risks are inherent, MCDM proves to be an essential mechanism for evaluating digital transformation strategies. By integrating both qualitative and quantitative criteria, decision-makers can systematically assess and compare various alternatives in selecting an Enterprise Architecture Framework (EAF). The decision-maker's active role in expressing preferences and values aligns with the dynamic nature of the freight transportation ecosystem, ensuring that the chosen EAF is not only technologically adept but also aligns with the organization's strategic objectives.

The study conducted by Zavadskas et al. [22] further emphasizes the versatility of MCDM as a structuring tool, providing a systematic method for solving complex problems. As witnessed in various sectors such as project management, urban planning, and supplier selection, MCDM's robust framework for decision-making proves to be adaptable to diverse contexts. In the freight transportation industry, where the stakes are high and the need for informed decision-making paramount, MCDM emerges as a strategic ally in navigating the digital transformation landscape. By incorporating MCDM principles, decision-makers can ensure that the selected Enterprise Architecture Framework aligns cohesively with the multifaceted demands of the industry, contributing to a seamless and effective digital evolution in freight transportation.

The application of Multi-Criteria Decision-Making (MCDM) methodologies, such as AHP and TOPSIS, has proven effective in various technological contexts beyond freight transportation. Recent research has utilized these methods for selecting tools in chatbot development, considering factors like scalability, performance, and maintainability [23]. Similarly, another study applied MCDM techniques to evaluate cross-platform mobile development frameworks, addressing complex decision-making scenarios involving conflicting criteria [24]. These examples highlight the adaptability and utility of MCDM approaches in supporting strategic decision-making across diverse domains.

Building upon earlier applications of MCDM methodologies in freight transportation, recent advancements have extended their utility to simulation-based analytics frameworks and the evaluation of AI-driven tools for predictive and prescriptive decision-making [25]. These methods, including hybrid Intuitionistic Fuzzy-AHP approaches, enable logistics companies to optimize their operations by leveraging real-time data and advanced analytical capabilities. Such integrations facilitate the selection of solutions tailored to complex requirements, bridging traditional decision-making processes with AI-enhanced logistics systems [25].

III. Related Works

Recently, Organizations use EA to maximize their organizational, business and IT project value. It brings multitude benefits over time, from abstract aspect such business–IT alignment and decision-making improvement to measurable advantage such as reducing costs [26], [27]. Now with the continuous and unpredictable market change, EA is needed more than ever.

It has the potential to orchestrate business and digital transformations of an organization in order to act efficiently in the new market environment [28].

However, during the last decades many EA frameworks are developed, which makes the selection of suitable frameworks a difficult decision task. Several works in literature focus on evaluating or comparing some well-known EAF in general basis [29], [30]. Some of them evaluate EAFs on the main architectural components such Metamodel, principles, views and specification documents [31], [32], [33], while others establish comparison based on quality attribute or practice criteria [34], [35], [36], [37], [38]. Table I presents a list of these works. It mentions the studied EAFs, the application domain, and whether the author used process MCDM.

As shown in the Table I, there is a limited collection of popular frameworks chosen by the authors. It is observed also that few studies use MCDM methods to select EAFS. In addition, there is a lack of studies that focus on EAFs comparison according to digital transformation issues.

Moreover, during the literature review we have identified a list of the most chosen criteria that may be useful to compare and select EAFs. Table II presents our classification of these criteria as well as papers that cover them.

TABLE I. EAFs COMPARISON WORKS

Paper	Compared Frameworks	With Selection Process	Use of MCDM Method	Application Domain
[39]	ZF, TEAF, TOGAF, and DODAF	Yes	X	Energy
[40]	ZF, FEAF, TOGAF, SAGA, GEA, MFCNO			Public organization
[36]	ZF, TOGAF, FEAF, DoDAF, and Gartner	Yes		General
[33]	ZF, TOGAF, TEAF, FEAF, DoDAF			General
[41]	ZF, ARIS			General
[31]	DoDAF, GERAM, FEAF, TOGAF, IAF, MIT, Gartner, DYA			General
[32]	ZF, TOGAF, FEAF, DoDAF, TEAF	Yes		General
[34]	ZF, TOGAF, FEAF, DODAF, EAP	Yes		General
[38]	ZF, TEAF, LTGAF, DoDAF, FEAF			General
[42]	ZF, TOGAF, FEAF	Yes	X	Education
[35]	ZF, TOGAF, MODAF, NAF, DODAF, UAF, FEAF	Yes		General
[43]	TOGAF, Zachman, MODAF, FEAF, DoDAF, NAF	Yes		General
[37]	Zachman, TOGAF, DODAF, Gartner, EAP, FEAF, TEAF, LTGAF, GERAM, E2AF	Yes		General
[44]	TOGAF, FEA, Gartner, EAP, DoDAF			General

TABLE II. CLASSIFICATION OF CRITERIA TAKEN FROM LITERATURE

Criteria	Subcriteria	Papers
Modeling	Meta model/Reference model	[34], [32], [35], [43], [45], [46]
	Procedure model	[39], [34], [32], [33],[43], [45], [46]
	Modeling technique/Modeling languages openness/Standardization	[39], [34], [32], [35], [38], [43], [47]
	Viewpoint	[33], [37], [45], [48]
Technical Quality	Alignment	[29], [30], [37], [38], [42], [43], [45], [48]
	Integrity	[29], [30], [32], [38], [43], [49]
	Reusability	[39], [30], [38], [43]
	Security	[30], [38], [43]
	Scalability	[39], [30], [38], [42], [43]
	Reliability	[29], [30], [38]
	Efficiency	[29], [32], [38], [42]
	Adaptability	[34], [30], [42]
Functional Quality	Business drivers	[30], [32], [42], [46]
	Business requirements	[32], [43], [48]
	Architecture knowledge base	[32], [47], [49]
Concepts	Artifacts	[37], [48]
	Governance	[34], [32], [37], [43], [45], [46], [48]
	Repository	[37], [43], [48]
	Strategy	[37], [43], [48]
Usability	Taxonomy	[34], [32], [33], [37], [46], [48]
	Principles practice	[34], [32], [46]
	Understandability from different stakeholders' viewpoints	[32], [33]
	Ease of use	[39], [34], [30], [32], [33], [35], [42], [46]
	Architecture Definition and Understanding	[34], [29], [30], [33], [35], [42], [46]
	Architecture guidelines/documentation	[33], [39], [30], [32], [37], [43], [46], [47], [48]
Technology trends	Cloud	[50]
	Mobile IT and IoT	[50]

Due to the diverse requirements and specifications inherent in various sectors, each use case necessitates a tailored Enterprise Architecture Framework (EAF) that aligns precisely with its unique needs and objectives [51]. Consequently, this article employs advanced Multi-Criteria Decision-Making (MCDM) methods to discern the most suitable EAF for crafting a digital and versatile platform that fosters collaboration in freight transportation (DCRFT). To address this complex system within the realm of digital transformation projects, we advocate for a group decision method, integrating the Analytical Hierarchy Process (AHP) and the Fuzzy Technique for Order Preference by Similarity to Ideal Solution (FTOPSIS). This approach aims to meticulously select an EAF that not only describes but also effectively designs the intricate aspects of the system.

IV. METHODOLOGY

This paper uses two stages method AHP and F-TOPSIS as detailed below (Fig. 1). Firstly, we defined fourteen subcriteria through a literature review enriched by the opinions of four experts. Similarly, four popular EAF were chosen as alternatives to compare. Thereafter, AHP is used to determine the importance weights of criteria. Further, these weights are used in the ranking process based on F-TOPSIS algorithm. The process uses a group decision techniques and fuzzy set theory to overcome the ambiguity due to subjective and imprecise judgments among the decision-makers participating in the evaluation. Fig. 1 illustrates the steps of the two process phases.

A. Problem Definition

This work is an integral part of an ongoing project aimed at developing a digital and versatile platform designed to support collaborative efforts in the transportation of goods. The platform's distinguishing feature is its polymorphic capacity, accommodating a wide range of collaboration forms involving various actors, approaches, rules, and objectives.

Designing a digital project with such richness in terms of complexities necessitates the use of an enterprise architecture framework (EAF). Given the considerable number of available EAFs and the various factors influencing their selection, we have opted to initially employ a Multiple Criteria Decision-Making (MCDM) method. This approach will guide us in

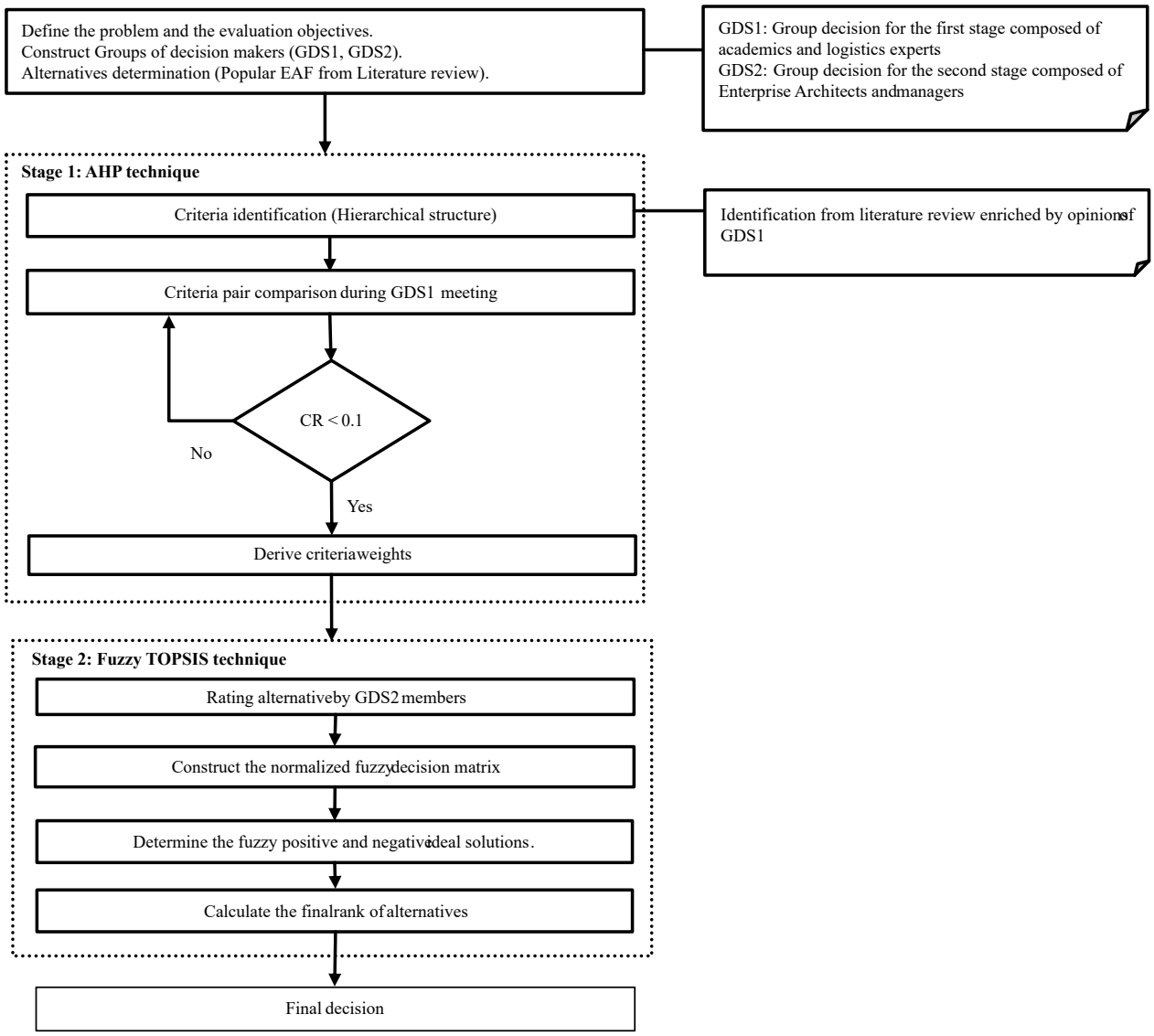


Fig. 1. Proposed integrated methodology for enterprise architecture framework selection.

systematically evaluating and selecting the most appropriate framework to meet the specific requirements of this project.

B. Phase 1: AHP Analytic Hierarchy Process

The Analytic Hierarchy Process (AHP) [52] stands out as one of the most extensively utilized MCDM methods. This method empowers decision makers to break down a complex problem into a more manageable hierarchical structure with a minimum of three levels: the problem objective at the top level, criteria and sub-criteria at the middle level, and alternatives at the bottom level.

Within this process, prioritization of criteria occurs, and each alternative is assigned scores based on these criteria. This evaluation is conducted through pairwise comparisons, employing a predefined Saaty scale (Table III) [53], with a simultaneous check for the consistency of judgments. Ultimately, a weighted score is computed for each alternative, providing a comprehensive and informed basis for decision-making.

TABLE III. SAATY SCALE [53]

Definition	Intensity of importance
Equally important	1
Moderately more important	3
Strongly more important	5
Very strong more important	7
Extremely more important	9
Intermediate more important	2, 4, 6, 8

In this study we have applied AHP only to establish criteria importance weights. The process steps are described below:

Step 1: Considering a set of criteria $C = \{Ci/i = 1, 2, 3 \dots n\}$, we define the matrix $M(n \times n)$ as result of a

TABLE IV. RANDOM INDEX

n	3	4	5	6	7	8	9	11	12	13	14	15
RI	0.52	1.88	1.11	1.25	1.34	1.40	1.48	1.51	1.53	1.55	1.57	1.58

paire-wise comparison for each criterion.

$$M = \begin{bmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{bmatrix}, \quad x_{ii} = 1, \quad x_{ji} = \frac{1}{x_{ij}}, \quad x_{ij} \neq 0 \tag{1}$$

Step 2: calculate the priority vectors and drive Coherence Index (CI) as well as the Coherence Ratio (CR):

$$CI = \frac{\lambda_{\max} - n}{n - 1} \tag{2}$$

where $\lambda_{\max}$ is the largest Eigen value.

$$CR = \frac{CI}{RI} \tag{3}$$

Where *RI (Random Index)* is a value that depends on the number of criteria as illustrated in Table IV.

Step 3: If the Consistency Ratio is less than or equal to 10% establish the criteria weight importance Else back to step 1 and review the paire wise comparison.

C. Phase 2: Fuzzy TOPSIS

TOPSIS stands out as a well-established and widely applied Multiple Criteria Decision-Making (MCDM) method. Its popularity arises from its user-friendly interface, rapid alternative evaluation process, low mathematical complexity, and adaptability for seamless integration with other methods. The computational process of TOPSIS is designed to identify an optimal solution that minimizes the distance to the positive ideal solution (PIS) and maximizes the separation from the negative ideal solution (NIS). The PIS represents a solution composed of the best weights assigned to the criteria, while the NIS is a solution obtained by aggregating the worst values assigned to the criteria [54].

Nevertheless, in many real-world decision problems, the expressions of individuals' opinions often manifest in linguistic terms, introducing vagueness and subjectivity. Consequently, the precision of criteria weights and evaluations for given alternatives becomes challenging. To address imprecise judgments, the MCDM method incorporates a fuzzy theory concept introduced in [55]. In fuzzy theory, instead of assigning a binary "totally true" or "totally false" value to an imprecise decision, a degree of membership is assigned. This degree of membership is typically represented by the interval [0, 1], where 0 signifies "totally false," 1 denotes "totally true," and the intervening values refer to intermediate degrees of truth. In this paper, we utilized the triangular fuzzy number (TFN), defined by the triplet (a, b, c), where a and c are successively the lower and upper bounds, and b is the center where the value is 1 (refer to Fig. 2).

Fig. 3 present the membership function of linguistic terms and Table V shows their correspondence on triangular fuzzy numbers.

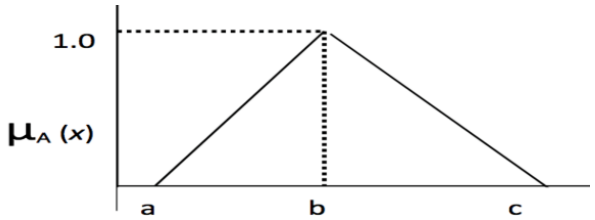


Fig. 2. Triangular fuzzy number.

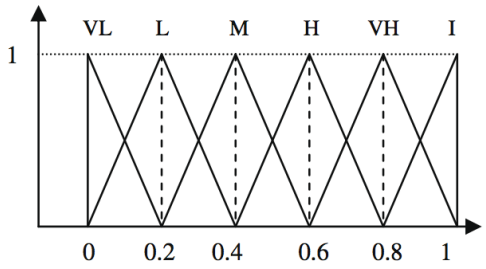


Fig. 3. Membership functions of linguistic terms.

$$\mu_A(x; a, b, c) = \begin{cases} 0, & x \leq a \\ \frac{x-a}{b-a}, & a \leq x \leq b \\ \frac{c-x}{c-b}, & b \leq x \leq c \\ 0, & c \leq x \end{cases} \tag{4}$$

TABLE V. LINGUISTIC VALUES AND CORRESPONDING FUZZY NUMBERS

Linguistic variables	Corresponding Fuzzy numbers
Very low	(0,0,0.2)
Low	(0,0.2,0.4)
Medium	(0.2,0.4,0.6)
High	(0.4,0.6,0.8)
Very high	(0.6,0.8,1)
Excellent	(0.8,1,1)

Considering E the set benefit criteria (greater value is better) and F set of cost criteria (lower value is better) and let $W = (w_1, w_2, \ldots, w_n)$ be the vector of criteria weights concluded from phase 1. The steps of TOPSIS process are as follows [56]:

Step 1: Considering K DMs, define K fuzzy decision matrix $X^k = \left(x_{ij}^k\right)$, where x_{ij}^k is TFN that represent the rating assigned to alternative i for criterion j by decision maker k.

Therefore, the rating of alternatives with respect to each criterion can be calculated as $x_{ij} = \frac{1}{K}\left(x_{ij}^1 + x_{ij}^2 + \cdots + x_{ij}^K\right)$. Each x_{ij}^k is defined by triplet $\left(a_{x_{ij}}, b_{x_{ij}}, c_{x_{ij}}\right)$.

Step 2: By using linear normalization, we build the normalized fuzzy decision matrix $N = (n_{ij})$ as below

$$n_{ij} = \begin{cases} \left(\frac{a_{x_{ij}}}{\max_i c_{x_{ij}}}, \frac{b_{x_{ij}}}{\max_i c_{x_{ij}}}, \frac{c_{x_{ij}}}{\max_i c_{x_{ij}}}\right) & \text{si } j \in E \\ \left(\frac{\min_i a_{x_{ij}}}{c_{x_{ij}}}, \frac{\min_i a_{x_{ij}}}{b_{x_{ij}}}, \frac{\min_i a_{x_{ij}}}{a_{x_{ij}}}\right) & \text{si } j \in F \end{cases} \tag{5}$$

Step 3: The weighted normalized fuzzy matrix V is calculated by multiplying the columns of the normalized fuzzy

decision matrix N and the correspondent weights $w_j \in R$ satisfying $\sum_{j=1}^{n} w_j = 1$. $V = (v_{ij})$

Where $v_{ij} = n_{ij} \cdot w_j = \left(a_{n_{ij}}, b_{n_{ij}}, c_{n_{ij}}\right) \cdot w_j = \left(a_{n_{ij}} \cdot w_j, b_{n_{ij}} \cdot w_j, c_{n_{ij}} \cdot w_j\right)$

Step 4: Deduce the fuzzy positive and negative ideal solution as follows:

$$\text{PIS} = \left(v_1^+, v_2^+, \ldots, v_n^+\right) \tag{6}$$

$$\text{NIS} = \left(v_1^-, v_2^-, \ldots, v_n^-\right) \tag{7}$$

Where $v_j^+ = \max_i v_{ij}$ and $v_j^- = \min_i v_{ij}$

Step 5: determine the distances of each alternative A_i from PIS and NIS

$$d_i^+ = \sum_{j=1}^{n} dd\left(v_{ij}, v_j^+\right) \tag{8}$$

$$d_i^- = \sum_{j=1}^{n} dd\left(v_{ij}, v_j^-\right) \tag{9}$$

By using the formula that calculates the distance dd between two positive TFNs $A = (a_A, b_A, c_A)$ and $B = (a_B, b_B, c_B)$:

$$dd(A, B) = \sqrt{\frac{1}{3}\left[(a_A - a_B)^2 + (b_A - b_B)^2 + (c_A - c_B)^2\right]} \tag{10}$$

Step 6: Deduce the relative closeness of alternative A_i to the ideal solution PIS :

$$RC_i = \frac{d_i^-}{d_i^+ + d_i^-} \tag{11}$$

Step 7: based to the relative group closeness, rank the alternatives A_i and select the best one that have the halue of RC_i.

D. Criteria Identification

During the literature review, it has been noticed that there is no one Enterprise Architecture Framework as all-purpose solution. The choice depends on the requirements and situations being processed. In this perspective, we have focused in the first step to depict the important criteria that will be a keys factor to consider in our situation. Therefore, we have identifying fourteen criteria from literature review enriched by academics and logistics experts' opinions see Table VI.

E. Alternatives

In this section, a brief description is provided for four enterprise architecture frameworks selected as alternatives in this study. These frameworks were chosen based on their frequent inclusion in comparative analyses (refer to Table I).

- **A1: The Zachman Framework** is an enterprise architecture model officially introduced by [6]. It presents a logical structure in a bidimensional matrix format, where the first dimension comprises six columns representing the six fundamental questions: What, How, Where, Who, When, and Why. Each of these questions is then explored through six perspectives. This results in a taxonomy that categorizes the various architectural artifacts necessary for developing and designing an information system to help the organization manage change and ensure alignment between business and IT.
- **A2: TOGAF, The Open Group Architecture Framework**, developed in 1995, has become an industry standard widely adopted for designing, governing, and constructing architectures for organizations. It categorizes enterprise architecture into four domains: Business, Application, Data, and Technology architecture [46]. The TOGAF transformation process is anchored in the Architecture Development Method (ADM) engine, comprising cyclical phases to define, plan, implement, and ultimately manage changes from the current "As-is" architecture to the desired "To-be" architecture [57].
- **A3: DoDAF, The Department of Defense Architecture Framework**, is developed specifically for the United States Department of Defense. While its primary focus is on defense applications, its applicability extends to other domains as well. DoDAF introduces a set of products and a view model designed to serve as tools for visualizing, understanding, and assimilating the broad scope and complexities of an architecture. These products are organized into four views: All View (AV), Operational View (OV), Systems View (SV), and Technical Standards View (TV). Notably, DoDAF is well-suited for large, complex system architectures and stands out for its incorporation of "operational views" [58].
- **A4: The Federal Enterprise Architecture Framework (FEAF)** was developed by the US Federal Chief Information Officers (CIO) Council with the aim of constructing and supporting integrated systems architectures. Its primary objective is to enhance the management and exchange of information within government and federal agencies, facilitating efficient and prompt service delivery to clients and citizens by improving access to information. FEAF is structured around six reference models: performance, business, data, application, infrastructure, and security reference models [58].

V. RESULTS

The evaluation process commences with the establishment of the GDS1 group decision for the initial stage, comprising two academic experts and two logistics experts. During in-depth discussions, the group constructs a hierarchical structure consisting of 14 criteria. Subsequently, they populate the upper and lower triangle elements of the pairwise comparison matrix (refer to Table VII). The comparison ratings are deliberated upon, reaching a consensus within the group.

The consensual weight for each criterion is obtained after establishing the normalized matrix (Table VIII) with (CR= 0,09084).

TABLE VI. CRITERIA DEFINITIONS

Criteria	Description
(C1) Agility challenges	Concern agile design and development of the system in an iterative and flexible manner.
(C2) Requirement taxonomy	Due to the multitude of actors, objectives, and strategies, in addition to the multitude of functionalities between business, operational, and technical: the requirements analysis and design must be granular.
(C3) Focused views	Putting in place appropriate views for each stakeholder to facilitate their understanding, focus, and participation in development.
(C4) Ease of use	The simplicity of the design tool or method.
(C5) Architecture guidelines	Design tool and method guide and documentation.
(C6) Cost	The cost of framework adoption and use.
(C7) Ontology architecture definition	Given the different cultures and vocabularies of the stakeholders, it is better to define an ontology facilitating integration of new keywords.
(C8) Data extensibility and integration	Ability to be extensible in terms of data integration of different types and structures.
(C9) Process and system scalability	Ability to manage and integrate business, operational, or administrative processes.
(C10) Metamodeling and abstractions	The framework level of abstraction to facilitate extensibility during development.
(C11) Artefact interoperability	Facility of interoperability between elements of the solution in terms of data and processes.
(C12) Heterogeneous IoT technology integration	The capabilities of the EAF to handle IoT architecture as an emerging technology widely used in the logistic fields.
(C13) Cloud/Fog cloud implementation	As an emerging technology, Cloud is very practical for this kind of application. This criterion concerns the capabilities of the EAF to implement Cloud architectures.
(C14) Facility to integrate Big data analytics	The capabilities of the EAF to integrate Big data analytics.

TABLE VII. PAIRWISE COMPARISON MATRIX

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14
C1	1	1/5	1/3	5	5	1/3	3	1/2	1/2	2	1/4	1	1/4	¼
C2	5	1	3	7	8	4	7	2	3	4	2	2	3	3
C3	3	1/3	1	5	6	3	5	1/4	1/6	3	1/3	1/4	1/2	1/6
C4	1/5	1/7	1/5	1	2	1/4	3	1/5	1/5	1/4	1/5	1/6	1/7	1/7
C5	1/5	1/8	1/6	1/2	1	1/4	1/2	1/5	1/5	1/4	1/6	1/6	1/7	1/7
C6	3	1/4	1/3	4	4	1	1/2	1/4	1/4	1/2	1/3	1/4	1/6	1/6
C7	1/3	1/7	1/5	1/3	2	2	1	1/3	1/4	1/2	1/4	1/6	1/6	1/6
C8	2	1/2	4	5	5	4	3	1	1	2	1/2	2	1/2	½
C9	2	1/3	6	5	5	4	4	1	1	3	1/2	2	1/2	½
C10	1/2	1/4	1/3	4	4	2	2	1/2	1/3	1	1/3	1/3	1/5	1/5
C11	4	1/2	3	5	6	3	4	2	2	3	1	1/2	1/2	½
C12	1	1/2	4	6	6	4	6	1/2	1/2	3	2	1	1/2	½
C13	4	1/3	2	7	7	6	6	2	2	5	2	2	1	2
C14	4	1/3	2	7	7	6	6	2	2	5	2	2	1/2	1

TABLE VIII. NORMALIZED MATRIX AND PRIORITIES WEIGHTS

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	Eigen weight
C1	0,03	0,04	0,01	0,08	0,07	0,01	0,06	0,04	0,04	0,06	0,02	0,07	0,03	0,03	0,043
C2	0,17	0,20	0,11	0,11	0,12	0,10	0,14	0,16	0,22	0,12	0,17	0,14	0,37	0,32	0,176
C3	0,10	0,07	0,04	0,08	0,09	0,08	0,10	0,02	0,01	0,09	0,03	0,02	0,06	0,02	0,057
C4	0,01	0,03	0,01	0,02	0,03	0,01	0,06	0,02	0,01	0,01	0,02	0,01	0,02	0,02	0,018
C5	0,01	0,03	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,02	0,02	0,012
C6	0,10	0,05	0,01	0,06	0,06	0,03	0,01	0,02	0,02	0,02	0,03	0,02	0,02	0,02	0,033
C7	0,01	0,03	0,01	0,01	0,03	0,05	0,02	0,03	0,02	0,02	0,02	0,01	0,02	0,02	0,020
C8	0,07	0,10	0,15	0,08	0,07	0,10	0,06	0,08	0,07	0,06	0,04	0,14	0,06	0,05	0,082
C9	0,07	0,07	0,23	0,08	0,07	0,10	0,08	0,08	0,07	0,09	0,04	0,14	0,06	0,05	0,089
C10	0,02	0,05	0,01	0,06	0,06	0,05	0,04	0,04	0,02	0,03	0,03	0,02	0,02	0,02	0,035
C11	0,13	0,10	0,11	0,08	0,09	0,08	0,08	0,16	0,15	0,09	0,08	0,04	0,06	0,05	0,093
C12	0,03	0,10	0,15	0,10	0,09	0,10	0,12	0,04	0,04	0,09	0,17	0,07	0,06	0,05	0,087
C13	0,13	0,07	0,08	0,11	0,10	0,15	0,12	0,16	0,15	0,15	0,17	0,14	0,12	0,22	0,134
C14	0,13	0,07	0,08	0,11	0,10	0,15	0,12	0,16	0,15	0,15	0,17	0,14	0,06	0,11	0,122

The next stage consists to scores each alternative against these criterions by EA experts (3 architects), they are asked to rank the four alternatives by using linguistic terms which are transformed to triangular fuzzy number (Tables IX, X, XI). By considering the C6 as cost criteria and the rest of criteria as benefit criteria. We have applied the operations mentioned above (Eq. (5), (6) and (7)) and we obtain the normalized matrix as illustrated in Table XII and Table XIII.

Finally, by applying the Eq. (8), (9) and (11), we have obtained the relative closeness of all alternatives A_i to PIS as depicted in Table XIV, the best rank is assigned to A2- Togaf framework.

TABLE IX. FUZZY RANKING MATRIX : EXPERT 1: CEO, CHIEF ARCHITECT AT EA PRINCIPALS, USA

	A1			A2			A3			A4		
C1	0,00	0,20	0,40	0,20	0,40	0,60	0,20	0,40	0,60	0,20	0,40	0,60
C2	0,80	1,00	1,20	0,20	0,40	0,60	0,20	0,40	0,60	0,20	0,40	0,60
C3	0,60	0,80	1,00	0,20	0,40	0,60	0,20	0,40	0,60	0,20	0,40	0,60
C4	0,60	0,80	1,00	0,60	0,80	1,00	0,60	0,80	1,00	0,60	0,80	1,00
C5	0,80	1,00	1,20	0,60	0,80	1,00	0,60	0,80	1,00	0,60	0,80	1,00
C6	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40
C7	0,80	1,00	1,20	0,20	0,40	0,60	0,20	0,40	0,60	0,20	0,40	0,60
C8	0,20	0,40	0,60	0,20	0,40	0,60	0,20	0,40	0,60	0,20	0,40	0,60
C9	0,60	0,80	1,00	0,60	0,80	1,00	0,60	0,80	1,00	0,60	0,80	1,00
C10	0,20	0,40	0,60	0,20	0,40	0,60	0,20	0,40	0,60	0,20	0,40	0,60
C11	0,60	0,80	1,00	0,60	0,80	1,00	0,20	0,40	0,60	0,20	0,40	0,60
C12	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40
C13	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40
C14	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40

VI. DISCUSSION

The results of the first phase illustrated that the taxonomy of needs and the granularity of details according to the different views of the project stakeholders is the most important criterion to be considered when choosing an EAF adapted to this project. In second place comes the ability to develop emerging cloud, IoT and Big data architectures as they are the indispensable solutions to build powerful, efficient and effective digital platforms. Also, in the same level of importance there are the scalability of the system in terms

TABLE X. FUZZY RANKING MATRIX : EXPERT 2: EXPERIENCED ARCHITECT AND BUILDER OF PROFESSIONAL COMMUNITIES, AUSTRIA

	A1			A2			A3			A4		
C1	0,40	0,60	0,80	0,60	0,80	1,00	0,20	0,40	0,60	0,20	0,40	0,60
C2	0,80	1,00	1,20	0,40	0,60	0,80	0,60	0,80	1,00	0,60	0,80	1,00
C3	0,60	0,80	1,00	0,40	0,60	0,80	0,80	1,00	0,60	0,20	0,40	0,60
C4	0,60	0,80	1,00	0,20	0,40	0,60	0,20	0,40	0,60	0,40	0,60	0,80
C5	0,20	0,40	0,60	0,80	1,00	0,60	0,20	0,40	0,60	0,20	0,40	0,60
C6	0,20	0,40	0,60	0,40	0,60	0,80	0,20	0,40	0,60	0,40	0,60	0,80
C7	0,00	0,20	0,40	0,60	0,80	1,00	0,60	0,80	1,00	0,40	0,60	0,80
C8	0,20	0,40	0,60	0,40	0,60	0,80	0,40	0,60	0,80	0,40	0,60	0,80
C9	0,20	0,40	0,60	0,60	0,80	1,00	0,60	0,80	1,00	0,20	0,40	0,60
C10	0,00	0,20	0,40	0,60	0,80	1,00	0,60	0,80	1,00	0,20	0,40	0,60
C11	0,40	0,60	0,80	0,40	0,60	0,80	0,60	0,80	1,00	0,00	0,20	0,40
C12	0,40	0,60	0,80	0,40	0,60	0,80	0,20	0,40	0,60	0,20	0,40	0,60
C13	0,20	0,40	0,60	0,40	0,60	0,80	0,20	0,40	0,60	0,40	0,60	0,80
C14	0,20	0,40	0,60	0,40	0,60	0,80	0,20	0,40	0,60	0,20	0,40	0,60

TABLE XI. FUZZY RANKING MATRIX : EXPERT 3: ENTERPRISE ARCHITECT, MOROCCO

	A1			A2			A3			A4		
C1	0,00	0,00	0,20	0,00	0,20	0,40	0,00	0,00	0,20	0,00	0,00	0,20
C2	0,60	0,80	1,00	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20
C3	0,40	0,60	0,80	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40
C4	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40
C5	0,00	0,00	0,20	0,20	0,40	0,60	0,20	0,40	0,60	0,20	0,40	0,60
C6	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20
C7	0,40	0,60	0,80	0,20	0,40	0,60	0,20	0,40	0,60	0,20	0,40	0,60
C8	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20
C9	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20
C10	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40
C11	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40	0,00	0,20	0,40
C12	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20	0,20	0,40	0,60
C13	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20
C14	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20	0,00	0,00	0,20

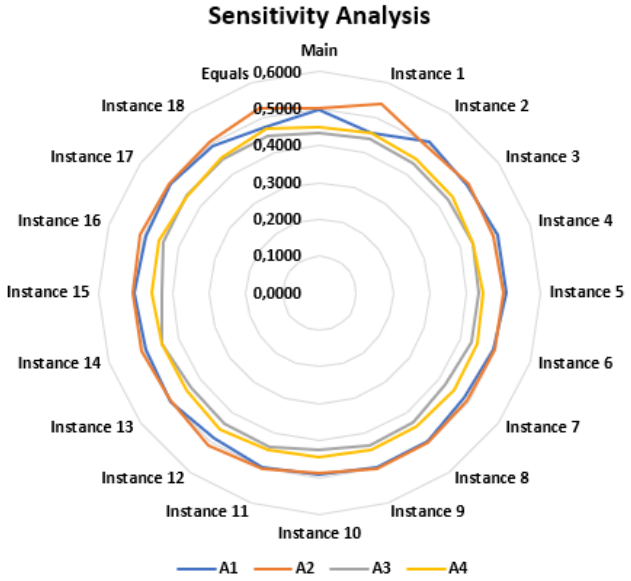


Fig. 4. Sensitivity analysis under different criteria weights.

of data, processes and the interoperability of artefacts.

In the second stage the evaluation of the four frameworks by the Enterprises architects demonstrated that all the frameworks have strengths and weaknesses and puts the Togaf framework as the closest to the context of our need. The decision makers also highlight in all the frameworks a low level of implementation of the new architectures founder of the digital transformation, namely the cloud, Iot and big data. This requires EA must reinvent itself and keep pace with technological evolution and remain a key tool for future business design [59].

To evaluate the current ranking, the Fuzzy VIKOR and Fuzzy Promethee methods are applied to the same problem, and their results are then compared. Details of these methods can be found in [60], [61]. For criterion weighting, the evaluation results obtained by the AHP approach are used. The results of the AHP-fuzzy VIKOR and AHP-fuzzy Promethee approaches are presented in Table XV.

Analysis of Table XV reveals that the ranking of the two best alternatives remains unchanged, while that of the other alternatives varies. This suggests that the proposed methodology produces a solution very similar to the AHP-fuzzy VIKOR and AHP-fuzzy Promethee methodologies, confirming the robustness of the approach.

VII. SENSITIVITY ANALYSIS

In this study, a two-stage decision-making process is employed, integrating both the Analytic Hierarchy Process (AHP) and Fuzzy-TOPSIS methodologies, and subjected to a sensitivity analysis. During this analysis, criteria weights, initially derived using the AHP technique, are exchanged between two criteria while keeping the others constant. For each instance, the resulting values (v+, v-, d+ and d-) are computed to illustrate the updated outcomes. This process is iterated for twenty combinations, maintaining identical weights for specific criteria out of the fourteen, thereby providing a comprehensive evaluation. The details of all instances are succinctly presented in Table XVI, and the resulting rankings of the alternatives are visually depicted in Fig. 4.

Table XVI and Fig. 4 underscore that the initial instance effectively encapsulates the primary findings of the combined AHP-Fuzzy-TOPSIS approach. Notably, among the nineteen instances, Alternative A2 consistently attains the highest score. The sensitivity analysis reveals a significant divergence in the ranking of alternatives when equal weights are assigned to sub-criteria. Despite this, the evaluations suggest that the decision-making process remains generally robust to changes in criteria weights, with Alternative A2 consistently emerging as the preferred choice across various scenarios.

VIII. CONCLUSION

In conclusion, this project has significant implications for logistics and digitalization. By leveraging Enterprise Architecture (EA) as a key tool to address digital transformation challenges, the ongoing project focuses on developing a digital collaboration platform for freight transport. The complexity lies in choosing a suitable Enterprise Architecture Framework (EAF) amid numerous options. The paper introduces a decision-making method that integrates the Analytical Hierarchy Process (AHP) and the Fuzzy Technique for Order Preference by Similarity to Ideal Solution (F-TOPSIS) within a group multi-criteria process to select the most suitable EAF for successful project implementation.

The study's findings offer advantages for projects engaging in digital transformation through EA. A suitable EAF is crucial in providing a comprehensive view of the system and aligning information systems with strategic and business needs. The study identifies the Zachman framework as the closest match among the four EAFs examined, offering valuable insights for modeling complex digital systems through EAFs. Ultimately, implementing an appropriate EA framework can assist Logistics Service Providers (LSPs) in improving profitability and

TABLE XII. PIS END NIS CALCUL

	A1			A2			A3			A4			V-	V+
C1	0,01	0,02	0,03	0,02	0,03	0,04	0,01	0,02	0,03	0,01	0,02	0,03	**0,01**	**0,04**
C2	0,11	0,14	0,18	0,03	0,05	0,08	0,04	0,06	0,09	0,04	0,06	0,09	**0,03**	**0,18**
C3	0,03	0,04	0,06	0,01	0,02	0,04	0,02	0,03	0,03	0,01	0,02	0,03	**0,01**	**0,06**
C4	0,01	0,01	0,02	0,01	0,01	0,02	0,01	0,01	0,02	0,01	0,01	0,02	**0,01**	**0,02**
C5	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	**0,01**	**0,01**
C6	0,03	0,10	0,20	0,07	0,13	0,23	0,03	0,10	0,20	0,07	0,13	0,23	**0,03**	**0,23**
C7	0,01	0,02	0,02	0,01	0,01	0,02	0,01	0,01	0,02	0,01	0,01	0,02	**0,01**	**0,02**
C8	0,02	0,04	0,07	0,03	0,05	0,08	0,03	0,05	0,08	0,03	0,05	0,08	**0,02**	**0,08**
C9	0,03	0,05	0,07	0,05	0,06	0,09	0,05	0,06	0,09	0,03	0,05	0,07	**0,03**	**0,09**
C10	0,00	0,01	0,02	0,01	0,02	0,03	0,01	0,02	0,03	0,01	0,02	0,03	**0,00**	**0,03**
C11	0,04	0,07	0,09	0,04	0,07	0,09	0,03	0,06	0,08	0,01	0,03	0,06	**0,01**	**0,09**
C12	0,02	0,04	0,08	0,02	0,04	0,08	0,01	0,03	0,07	0,02	0,05	0,09	**0,01**	**0,09**
C13	0,02	0,06	0,12	0,04	0,08	0,13	0,02	0,06	0,12	0,04	0,08	0,13	**0,02**	**0,13**
C14	0,02	0,05	0,10	0,03	0,07	0,12	0,02	0,05	0,10	0,02	0,05	0,10	**0,02**	**0,12**

TABLE XIII. THE WEIGHTED NORMALIZED FUZZY MATRIX

	A1			A2			A3			A4			max cji	min aij
C1	0,13	0,27	0,47	0,27	0,47	0,67	0,13	0,27	0,47	0,13	0,27	0,47	0,67	
C2	0,73	0,93	1,13	0,20	0,33	0,53	0,27	0,40	0,60	0,27	0,40	0,60	1,13	
C3	0,53	0,73	0,93	0,20	0,40	0,60	0,33	0,53	0,53	0,13	0,33	0,53	0,93	
C4	0,40	0,60	0,80	0,27	0,47	0,67	0,27	0,47	0,67	0,33	0,53	0,73	0,80	
C5	0,33	0,47	0,67	0,53	0,73	0,73	0,33	0,53	0,73	0,33	0,53	0,73	0,73	
C6	**0,07**	**0,20**	**0,40**	**0,13**	**0,27**	**0,47**	**0,07**	**0,20**	**0,40**	**0,13**	**0,27**	**0,47**		**0,07**
C7	0,40	0,60	0,80	0,33	0,53	0,73	0,33	0,53	0,73	0,27	0,47	0,67	0,80	
C8	0,13	0,27	0,47	0,20	0,33	0,53	0,20	0,33	0,53	0,20	0,33	0,53	0,53	
C9	0,27	0,40	0,60	0,40	0,53	0,73	0,40	0,53	0,73	0,27	0,40	0,60	0,73	
C10	0,07	0,27	0,47	0,27	0,47	0,67	0,27	0,47	0,67	0,13	0,33	0,53	0,67	
C11	0,33	0,53	0,73	0,33	0,53	0,73	0,27	0,47	0,67	0,07	0,27	0,47	0,73	
C12	0,13	0,27	0,47	0,13	0,27	0,47	0,07	0,20	0,40	0,13	0,33	0,53	0,53	
C13	0,07	0,20	0,40	0,13	0,27	0,47	0,07	0,20	0,40	0,13	0,27	0,47	0,47	
C14	0,07	0,20	0,40	0,13	0,27	0,47	0,07	0,20	0,40	0,07	0,20	0,40	0,47	

TABLE XIV. FINAL RANKING

Alternatives	RCI	Ranking
A1	0,4980	2
A2	0,4997	1
A3	0,4341	4
A4	0,4481	3

service quality, ensuring adaptability to innovation trends for competitiveness.

This study introduces a robust method for selecting a pivotal Enterprise Architecture (EA) framework, steering the digital transformation of the freight transportation sector. Leveraging the Analytic Hierarchy Process (AHP) and Fuzzy Technique for Order of Preference by Similarity to Ideal Solution (F-TOPSIS), the approach systematically evaluates and ranks candidate EA frameworks. Application to a case study involving a Moroccan logistics company demonstrated the method's practicality and relevance in real-world scenarios.

Looking ahead, there are exciting opportunities for further research and refinement of the method. The dynamic nature of technology and business environments calls for criteria adaptable to change. Future work could explore the inclusion of dynamic criteria, ensuring selected EA frameworks remain relevant amid evolving technologies. Integrating machine learning techniques into the decision-making process represents another promising avenue for future research. Leveraging historical data and trends, organizations can make informed predictions about the future suitability of EA frameworks.

Further exploration could assess the scalability and adaptability of the proposed EA selection approach across different geographic regions and logistics sectors. Testing its effectiveness in small-to-medium-sized enterprises (SMEs) and large multinational logistics firms would highlight its versatility. The integration of emerging technologies such as blockchain, IoT, and AI could significantly enhance EA frameworks in logistics, improving transparency, efficiency, and security, and driving digital transformation. Future work should also consider including environmental and social criteria in the decision-making process, aligning EA frameworks with green logistics and sustainability objectives. Addressing high-risk factors like geopolitical disruptions, cybersecurity threats, and market volatility through robust risk assessments would further enhance the resilience of EA frameworks. Additionally, exploring hybrid EA frameworks could lead to tailored solutions that promote scalability, flexibility, and adaptability. Finally, expanding this research to other industries, such as healthcare, manufacturing, and energy, would provide valuable comparative insights into the broader application of EA frameworks. Long-term studies that evaluate key performance indicators (KPIs) such as cost reduction, efficiency, and customer satisfaction would help assess the sustainability and effectiveness of these frameworks.

REFERENCES

[1] I. Harris, Y. Wang, and H. Wang, "Ict in multimodal transport and technological trends: Unleashing potential for the future," *International Journal of Production Economics*, vol. 159, pp. 88–103, 2015.

[2] A. Pernestål, A. Engholm, M. Bemler, and G. Gidofalvi, "How will digitalization change road freight transport? scenarios tested in sweden," *Sustainability*, vol. 13, no. 1, p. 304, 2020.

[3] X. Sun, H. Yu, W. D. Solvang, Y. Wang, and K. Wang, "The application of industry 4.0 technologies in sustainable logistics: A systematic literature review (2012–2020) to explore future research opportunities," *Environmental Science and Pollution Research*, pp. 1–32, 2021.

[4] W. Ferrell, K. Ellis, P. Kaminsky, and C. Rainwater, "Horizontal collaboration: opportunities for improved logistics planning," *International Journal of Production Research*, vol. 58, no. 14, pp. 4267–4284, 2020.

[5] M. Hanine, O. Boutkhoum, F. El Barakaz, M. Lachgar, N. Assad, F. Rustam, and I. Ashraf, "An intuitionistic fuzzy approach for smart city development evaluation for developing countries: Moroccan context," *Mathematics*, vol. 9, no. 21, p. 2668, 2021.

TABLE XV. EVALUATION RESULTS VIA AHP-FUZZY VIKOR AND AHP-FUZZY PROMETHEE

Alternatives	Ranking of the present study	AHP-Fuzzy VIKOR		AHP-Fuzzy PROMETHEE	
		VIKOR index Q	Ranking	Net flow	Ranking
A1	2	0.3327	2	-0.0098	2
A2	1	0.2241	1	0.5581	1
A3	3	0.9752	3	-0.2530	3
A4	4	1.0000	4	-0.2954	4

TABLE XVI. RESULTS OF SENSITIVITY ANALYSIS

	Alternatives frameworks				Ranking
	A1	A2	A3	A4	
Instance 1 (Main)	0,4980	0,4997	0,4341	0,4481	A2 - A1 - A4 - A3
Instance 2	0,456034	0,539087	0,441156	0,455069	A2 - A1 - A4 - A3
Instance 3	0,5053	0,4951	0,4357	0,4471	A1 - A2 - A4 - A3
Instance 4	0,495342	0,50159	0,433236	0,446364	A2 - A1 - A4 - A3
Instance 5	0,5077	0,4973	0,4363	0,4357	A1 - A2 - A3 - A4
Instance 6	0,5055	0,4978	0,4317	0,4420	A1 - A2 - A4 - A3
Instance 7	0,495776	0,498447	0,433537	0,449904	A2 - A1 - A4 - A3
Instance 8	0,484433	0,496299	0,423687	0,448482	A2 - A1 - A4 - A3
Instance 9	0,497996	0,499677	0,434062	0,446821	A2 - A1 - A4 - A3
Instance 10	0,497996	0,499677	0,434062	0,446821	A2 - A1 - A4 - A3
Instance 11	0,492556	0,489969	0,425582	0,442957	A1 - A2 - A4 - A3
Instance 12	0,497619	0,500429	0,437678	0,447259	A2 - A1 - A4 - A3
Instance 13	0,4874	0,5104	0,4390	0,4571	A2 - A1 - A4 - A3
Instance 14	0,5011	0,4974	0,4316	0,4472	A1 - A2 - A4 - A3
Instance 15	0,4940	0,5066	0,4499	0,4506	A2 - A1 - A4 - A3
Instance 16	0,5007	0,5059	0,4296	0,4539	A2 - A1 - A4 - A3
Instance 17	0,4967	0,5129	0,4455	0,4565	A2 - A1 - A4 - A3
Instance 18	0,5015	0,5048	0,4477	0,4446	A2 - A1 - A3 - A4
Instnace 19	0,4930	0,5056	0,4488	0,4518	A2 - A1 - A4 - A3
Instance 20 (Equals)	0,4743	0,5267	0,4472	0,4692	A2 - A1 - A4 - A3

[6] J. A. Zachman, "A framework for information systems architecture," *IBM Systems Journal*, vol. 26, no. 3, pp. 276–292, 1987.

[7] R. Perez-Castillo, F. Ruiz-Gonzalez, M. Genero, and M. Piattini, "A systematic mapping study on enterprise architecture mining," *Enterprise Information Systems*, vol. 13, no. 5, pp. 675–718, 2019.

[8] A. Belfadel, E. Amdouni, J. Laval, C. B. Cherifi, and N. Moalla, "Towards software reuse through an enterprise architecture-based software capability profile," *Enterprise Information Systems*, vol. 16, no. 1, pp. 29–70, 2020.

[9] J. F. L. Muñoz and A. E. Esteve, "Executives' role in digital transformation," *International Journal of Information Systems and Project Management*, vol. 10, no. 3, pp. 84–103, 2022.

[10] J. J. Korhonen and M. Halén, "Enterprise architecture for digital transformation," in *2017 IEEE 19th Conference on Business Informatics (CBI)*, vol. 1. IEEE, 2017, pp. 349–358.

[11] M. Hafsi and S. Assar, "What enterprise architecture can bring for digital transformation: an exploratory study," in *2016 IEEE 18th Conference on Business Informatics (CBI)*, vol. 2. IEEE, 2016, pp. 83–89.

[12] G. Prokudin, O. Chupaylenko, V. Lebid, O. Denys, T. Khobotnia, and A. Nazarova, "Logistics of freight transportation and customs service in international transportation," *Chapters of Monographs*, pp. 38–74, 2022.

[13] E. Tijan, M. Jović, S. Aksentijević, and A. Pucihar, "Digital transformation in the maritime transport sector," *Technological Forecasting and Social Change*, vol. 170, p. 120879, 2021.

[14] F. Cruijssen, M. Cools, and W. Dullaert, "Horizontal cooperation in logistics: Opportunities and impediments," *Transportation Research Part E: Logistics and Transportation Review*, vol. 43, no. 2, pp. 129–142, 2007.

[15] O. Ergun, G. Kuyzu, and M. Savelsbergh, "Reducing truckload transportation costs through collaboration," *Transportation Science*, vol. 41, pp. 206–221, 2007.

[16] X. Wang, H. Wang, and H. Kopfer, "Increasing efficiency of freight carriers through collaborative transport planning: Chances and challenges," in *Dynamics and Sustainability in International Logistics and Supply Chain Management-Proceedings of the 6th German-Russian Logistics and SCM Workshop (DR-LOG 2011)*. Göttingen: Cuvillier Verlag, 2011, pp. 41–50.

[17] E. Ballot and F. Fontane, "Reducing transportation co2 emissions through pooling of supply networks: perspectives from a case study in french retail chains," *Production Planning & Control*, vol. 21, no. 6, pp. 640–650, 2010.

[18] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *Journal of industrial information integration*, vol. 6, pp. 1–10, 2017.

[19] A. Saoud and A. Bellabdaoui, "Towards generic platform to support collaboration in freight transportation: taxonomic literature and design based on zachman framework," *Enterprise Information Systems*, vol. 17, no. 2, p. 1939894, 2023.

[20] A. Zutshi and A. Grilo, "The emergence of digital platforms: A conceptual platform architecture and impact on industrial engineering," pp. 546–555, 2019.

[21] A. Saoud and A. Bellabdaoui, "Model of distributed hierarchical framework for carrier collaboration," in *2017 International Colloquium on Logistics and Supply Chain Management (LOGISTIQUA)*. IEEE, 2017, pp. 160–165.

[22] E. K. Zavadskas, Z. Turskis, and S. Kildienė, "State of art surveys of overviews on mcdm/madm methods," *Technological and Economic Development of Economy*, vol. 20, no. 1, pp. 165–179, 2014.

[23] M. Lachgar, H. Hrimech, Y. Ommane, and M. D. Laannaoui, "Holistic approach for selecting chatbot development tools: combining ahp and topsis methodologies," *Journal of Business Analytics*, pp. 1–23, 2024.

[24] M. Lachgar, M. Hanine, H. Benouda, and Y. Ommane, "Decision framework for cross-platform mobile development frameworks using an integrated multi-criteria decision-making methodology," *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, vol. 13, no. 1, pp. 1–22, 2022.

[25] M. A. B. Rabia and A. Bellabdaoui, "Collaborative intuitionistic fuzzy-ahp to evaluate simulation-based analytics for freight transport," *Expert Systems with Applications*, vol. 225, p. 120116, 2023.

[26] E. Niemi and S. Pekkola, "The benefits of enterprise architecture in organizational transformation," *Business and Information Systems Engineering*, vol. 62, no. 6, pp. 585–597, 2020.

[27] G. Shanks, M. Gloet, I. A. Someh, K. Frampton, and T. Tamm, "Achieving benefits with enterprise architecture," *The Journal of Strategic Information Systems*, vol. 27, no. 2, pp. 139–156, 2018.

[28] R. van de Wetering, S. Kurnia, and S. Kotusev, "The role of enterprise architecture for digital transformations," *Sustainability*, vol. 13, no. 4, p. 2237, 2021.

[29] R. Khayami, "Qualitative characteristics of enterprise architecture," *Procedia Computer Science*, vol. 3, pp. 1277–1282, 2011.

[30] S. R. Mirsalari and M. Ranjbarfard, "A model for evaluation of enterprise architecture quality," *Evaluation and Program Planning*, vol. 83, p. 101853, 2020.

[31] Q. Bui, "Evaluating enterprise architecture frameworks using essential elements," *Communications of the Association for Information Systems*, vol. 41, no. 1, p. 6, 2017.

[32] A. O. Odongo, S. Kang, and I.-Y. Ko, "A scheme for systematically selecting an enterprise architecture framework," in *2010 IEEE/ACIS 9th International Conference on Computer and Information Science*, 2010, pp. 665–670.

[33] L. Urbaczewski and S. Mrdalj, "A comparison of enterprise architecture frameworks," *Issues in Information Systems*, vol. 7, no. 2, pp. 18–23, 2006.

[34] P. Hadaya, A. Leshob, P. Marchildon, and I. Matyas-Balassy, "Enterprise architecture framework evaluation criteria: A literature review and artifact development," *Service Oriented Computing and Applications*, vol. 14, no. 3, pp. 203–222, 2020.

[35] J. Bankauskaitė, "Comparative analysis of enterprise architecture frameworks," in *CEUR Workshop Proceedings: IVUS 2019 International Conference on Information Technologies: Proceedings of the International Conference on Information Technologies*, vol. 2470, 2019, pp. 61–64.

[36] B. H. Cameron and E. McMillan, "Analyzing the current trends in enterprise architecture frameworks," *Journal of Enterprise Architecture*, vol. 9, no. 1, pp. 60–71, 2013.

[37] Y. F. Hernández-Julio, W. N. Bernal, and M. Palm, "A comparative analysis of emerging enterprise architecture frameworks," *Journal of Advanced Management Science Vol*, vol. 5, no. 6, 2017.

[38] N. Lim, T. Lee, and S. Park, "A comparative analysis of enterprise architecture frameworks based on ea quality attributes," in *2009 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing*, 2009, pp. 283–288.

[39] F. Zandi and M. Tavana, "A group evidential reasoning approach for enterprise architecture framework selection," *International Journal of Information Technology and Management*, vol. 9, no. 4, pp. 468–483, 2010.

[40] A. Sanchez, R. Basanya, T. Janowski, and A. Ojo, "Enterprise architectures-enabling interoperability between organizations," in *Proceedings of the 36th Argentine Conference on Informatics 8th Argentinean Symposium on Software Engineering, ASSE 2007, Mar del Plata, Argentina*, vol. 1, 2007, pp. 175–184.

[41] M. Kozina, "Evaluation of aris and zachman frameworks as enterprise architectures," *Journal of Information and Organizational Sciences*, vol. 30, no. 1, pp. 115–136, 2006.

[42] S. K. Hildayanti, R. R. Putra, A. S. N. Suhandi, F. Antony, A. Heryati, and R. H. Deviana, "Enterprise architecture framework selection for higher education using topsis method," *International Journal of Engineering and Technology*, vol. 7, no. 4, pp. 5327–5330, 2018.

[43] H. Qazi, Z. Javed, S. Majid, and W. Mahmood, "A detailed examination of the enterprise architecture frameworks being implemented in pakistan," *International Journal of Modern Education and Computer Science*, vol. 11, no. 9, 2019.

[44] B. D. Rouhani, M. N. Mahrin, F. Nikpay, R. B. Ahmad, and P. Nikfard, "A systematic literature review on enterprise architecture implementation methodologies," *Information and Software Technology*, vol. 62, pp. 1–20, 2015.

[45] U. Franke *et al.*, "Eaf2-a framework for categorizing enterprise architecture frameworks," in *2009 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing*, 2009, pp. 327–332.

[46] R. Sessions, "A comparison of the top four enterprise-architecture methodologies," 2007, houston: ObjectWatch Inc.

[47] M. Razavi, F. S. Aliee, and K. Badie, "An ahp-based approach toward enterprise architecture analysis based on enterprise architecture quality attributes," *Knowledge and Information Systems*, vol. 28, no. 2, pp. 449–472, 2011.

[48] F. Nikpay, R. Ahmad, and C. Y. Kia, "A hybrid method for evaluating enterprise architecture implementation," *Evaluation and Program Planning*, vol. 60, pp. 1–16, 2017.

[49] W. F. Boh and D. Yellin, "Using enterprise architecture standards in managing information technology," *Journal of Management Information Systems*, vol. 23, no. 3, pp. 163–207, 2006.

[50] Y. Masuda, "Digital enterprise architecture for global organizations," in *Architecting the Digital Transformation*. Springer, 2021, pp. 265–286.

[51] A. Gorkhali and L. D. Xu, "Enterprise architecture: a literature review," *Journal of Industrial Integration and Management*, vol. 2, no. 02, p. 1750009, 2017.

[52] T. Saaty, *The analytic hierarchy process (AHP) for decision making*, 1980.

[53] T. L. Saaty, "Fundamentals of the analytic hierarchy process," in *The analytic hierarchy process in natural resource and environmental decision making*. Springer, 2001, pp. 15–35.

[54] M. Behzadian, S. K. Otaghsara, M. Yazdani, and J. Ignatius, "A state-of the-art survey of topsis applications," *Expert Systems with Applications*, vol. 39, no. 17, pp. 13 051–13 069, 2012.

[55] L. A. Zadeh, "Fuzzy sets," *Information and control*, vol. 8, no. 3, pp. 338–353, 1965.

[56] D. Kacprzak, "Fuzzy topsis method for group decision making," *Multiple Criteria Decision Making*, vol. 13, pp. 116–132, 2018.

[57] P. A. Ariawan, I. S. Putra, and I. M. Sudarma, "Analysis of enterprise architecture design using togaf framework: A case study at archival unit of faculty of agricultural technology of udayana university," *International Journal of Engineering and Emerging Technology*, vol. 2, no. 2, pp. 52–57, 2018.

[58] M. Sajid and K. Ahsan, "Enterprise architecture for healthcare organizations," *World Applied Sciences Journal*, vol. 30, no. 10, pp. 1330–1333, 2014.

[59] J. Kaidalova, S. Kurt, and S. Ulf, "How digital transformation affects enterprise architecture management–a case study," *International Journal of Information Systems and Project Management*, vol. 6, no. 3, pp. 5–18, 2018.

[60] M. Hanine, O. Boutkhoum, T. Agouti, and A. Tikniouine, "A new integrated methodology using modified delphi-fuzzy ahp-promethee for geospatial business intelligence selection," *Information Systems and e-Business Management*, vol. 15, pp. 897–925, 2017.

[61] K. Peleckis, "Application of the fuzzy vikor method to assess concentration and its effects on competition in the energy sector," *Energies*, vol. 15, no. 4, p. 1349, 2022.

ATG-Net: Improved Feature Pyramid Network for Aerial Object Detection

Junbao Zheng, ChangHui Yang, Jiangsheng Gui*
School of Computer Science and Technology,
Zhejiang Sci-Tech University, Hangzhou, Zhejiang, China

***Abstract*—Object detection in aerial images is gradually gaining wide attention and application. However, given the prevalence of numerous small objects in the Unmanned Aerial Vehicle (UAV) aerial images, the extraction of superior fusion features is critical for the detection of small objects. However, feature fusion in many detectors does not fully consider the specific characteristics of the detection task. To obtain suitable features for the detection task, the paper proposes an improved Feature Pyramid Network (FPN) named ATG-Net, which aims to improve the feature fusion capability. Firstly, we propose an Adaptive Tri-Layer Weighting (ATW) module that adaptively assigns weights to each layer of the feature map according to its size and content complexity. Secondly, a Triple Feature Encoding (TFE) module is implemented, which can fuse feature maps from three different scales. Finally, the paper incorporates the Global Attention Mechanism (GAM) into the network, which includes improved channel attention mechanisms and spatial attention mechanisms. The experiments are conducted on the VisDrone2020 dataset, and the result shows that the network significantly outperforms the baseline detector and a variety of popular object detectors, which significantly improves the feature fusion capability of the network and the detection accuracy of small objects.**

***Keywords*—Object detection; feature pyramid network; adaptive tri-layer weighting; triple feature encoding; global attention mechanism**

I. Introduction

Object detection technology in the UAV capture scene is rapidly advancing, and it plays an important role in the fields of power line inspection, crop analysis, military security [1], [2], [3], and so on. With the development of deep learning, especially convolutional neural networks [4], [5], [6], [7], [8], [9], the performance of object detection has been greatly improved. The detectors contain three main components: backbone, neck, and head. The primary function of the backbone is feature extraction. The mainstream architectures include VGG [10], ResNet [11], DenseNet [12], MobileNet [13], EfficientNet [14], CSPDar-knet53 [15], and SwinTransformer [16], which have been relatively mature. The main function of the neck network is multi-scale feature fusion, feature enhancement, and integration of contextual information. It plays a crucial role in the object detection task. The role of the detection head is to parse the fused feature output from the neck network, including object localization and bounding box regression. The performance of the detection head is largely dependent on the quality of the fused features. Therefore, the design of an effective necking network has a decisive impact on improving the performance of the entire detection system.

*Corresponding author

A widely adopted neck network is to build a feature pyramid network (FPN) [17], which consists of top-down paths and adds lateral connections to the network to achieve the fusion of multi-scale features, enabling the model to better understand and capture the semantic information of the object at different scales. The FPN network usually up-samples the high-level semantic feature maps and combines them with low-level features through simple summation. However, this approach does not adequately address the semantic gaps and dissimilarities between the features, thereby limiting the network's ability to generate highly discriminative features. Furthermore, fusing only high-level and low-level features cannot fully leverage the contextual information of small objects. Such a structure is limited in its ability to capture the fine details of small objects, leading to inaccurate inferences of their locations and categories, which ultimately diminishes overall object detection accuracy.

In recent years, various FPN networks have been proposed to enhance the multi-scale feature fusion capabilities. PANet [18] augmented FPN with a bottom-up path enhancement, allowing information from lower layers to be directly transferred to higher layers, thereby enhancing the flow of information. Bi-FPN [19] proposed a bidirectional cross-scale connectivity structure. This structure enhances feature fusion by adding top-down paths to the FPN. Additionally, it introduces more lateral connections between different levels. These connections improve the fusion of features. Zhang Y et al. [20] proposed a feature pyramid network that combines top-down and bottom-up approaches. By integrating these two architectures, feature maps with richer semantic information and conducive to object detection can be obtained. EFPN [21] designed a feature texture transfer module, which endows the extended feature pyramid with reliable details, extending the original FPN to specialize in small object detection for high-resolution images. SAFPN [22] designed an efficient feature pyramid network for crowded human detection, integrating a refined HS-block into the original FPN to mitigate the effects of scale variations introduced by crowds. With this structure, a single level of features can encompass more receptive fields, accommodating objects at different scales. Although the methods can obtain rich semantic information, they perform a simple summation when fusing low-level and high-level semantics without considering the varying degrees of importance among the features. As a result, they fail to generate highly discriminative features. Additionally, fusing only high-level and low-level semantic features does not fully utilize the contextual information.

Considering cross-layer feature fusion, new design schemes have been proposed. CFPN [23] is a novel cross-layer feature

pyramid network that aggregates multi-scale feature maps and then assigns the aggregated features to the corresponding layers. This enables direct cross-layer communication, improving the asymptotic fusion in salient object detection and yielding better feature maps. However, the method only scales the weights of different feature layers with scaled weights and does not further fuse the feature layers to generate highly discriminative features. ImFPN [24] proposed an improved feature pyramid network based on a similarity fusion module and an attention module, which can fuse different features to accommodate instances of varying sizes. However, the design of the fusion module neglects the differences in the relative importance of the feature maps and, to some extent, increases the computational burden.

In order to solve the above problems, this paper specifically designs a feature pyramid network named ATG-Net for aerial image detection. Firstly, in order to better utilize the contextual information of multi-scale features, a Triple Feature Encoding (TFE) module is proposed to fuse large, medium, and small scale feature maps. Considering that feature maps of different sizes may have different importance in object detection, this paper proposes an Adaptive Tri-Layer Weighting (ATW) module that is able to adaptively predict a set of weights for feature maps of different sizes. Considering that the attention mechanism can make the network more focused on the features of small objects, the Global Attention Mechanism (GAM) [20] is integrated into the network. In the following, Section II outlines the relevant research and studies. Section III details the methodologies of ATW, TFE, and GAM. The detailed comparative experiments and visual analysis are provided in Section IV. Section V concludes with a discussion of the advantages and limitations of the proposed model.

II. Related Work

A. Object Detectors

Contemporary object detectors can be roughly divided into two categories according to the detection process: one-stage and two-stage detectors. One-stage detectors directly predict the class and location of objects within an image. While these detectors offer higher computational efficiency, their accuracy is generally lower compared to alternative approaches. RetinaNet [25] overcomes the obstacle of sample imbalance by introducing focus loss and improves the detection precision. SCA-YOLO [26] proposes a multilayer feature fusion algorithm. In this approach, the single-stage object detection algorithm YOLOv5 is embedded with two newly proposed models and utilizes an adaptive feature fusion network. This enhances the network's feature representation capabilities, significantly improving the detection accuracy of small objects. ASF-YOLO [27] proposes a framework based on attentional scale sequence fusion, which combines both spatial and scale features for accurate and fast cellular instance segmentation. Compared with one-stage detectors, two-stage detectors pursue better detection accuracy at the expense of speed. The R-CNN family of detectors [28], [29] employs a Region Proposal Network (RPN) to generate high-quality candidate anchors, which are then classified and localized. This design enhances the precision of object detection. Double-head R-CNN [30] respectively uses fully connected head and convolutional head for classification and bounding box regression, achieving excellent detection performance.

B. Attention Mechanism

The application of the attention mechanism in object detection has been proven to be extremely effective, which enables the model to focus on the most important areas in the image, thereby improving the accuracy and efficiency of object detection. Squeeze-and-Excitation Networks (SENet) [31] automatically calibrates the responses of feature channels by explicitly modeling the dependencies between the feature channels. By recalibrating the responses of the channels, the model can more effectively leverage the available features. Convolutional block attention module (CBAM) [32] is a straightforward yet effective attention mechanism for feed-forward convolutional neural networks. It generates attention maps independently along the channel and spatial dimensions, thereby enabling adaptive feature refinement. Inspired by CBAM, the Global Attention Mechanism (GAM) [33] enhances the performance of deep neural networks by mitigating information loss and strengthening global interaction representation. Additionally, it incorporates 3D alignment using a multilayer perceptron for channel attention and integrates a convolutional spatial attention submodule. The global attention mechanism is able to amplify the cross-dimensional interactions and capture important features in all three dimensions (channel, spatial width, and spatial height), better preserving the effective information of the original features.

III. Approach

The proposed ATG-Net network (see Fig. 1) consists of a Tri-Layer Weighting Module (ATW), a Triple Feature Encoder Module (TFE), and a Global Attention Mechanism (GAM). ATW enhances the fusion of small, medium, and large-scale features by improving their mechanical properties. It is capable of adaptively predicting a set of weights based on the significance of each feature level for effective aggregation. TFE effectively captures localized fine features of small objects, enabling the integration of local and global information to produce fused features that are better suited for small object recognition. GAM improves the performance of deep neural networks for detecting small objects by reducing information reduction and amplifying the global interaction representation.

A. Adaptive Tri-Layer Weighting Module

Directly fusing feature maps may lead to the loss of important information. Different feature maps may contain distinct types of information, and directly adding or concatenating them can result in certain key features being masked or weakened. Different feature maps may capture distinct features, some of which may be contradictory. Directly fusing these feature maps can lead to feature conflicts, making it difficult for the model to learn effective representations. In order to solve the above problems, the paper proposes an adaptive three-layer weighting (ATW) module that can adaptively predict a set of weights based on the importance of the features for each level. This enables the generation of salient features that are more favorable for small object detection. Fig. 2 illustrates the ATW model structure. Here, C denotes the number of channels, R denotes the feature resolution,

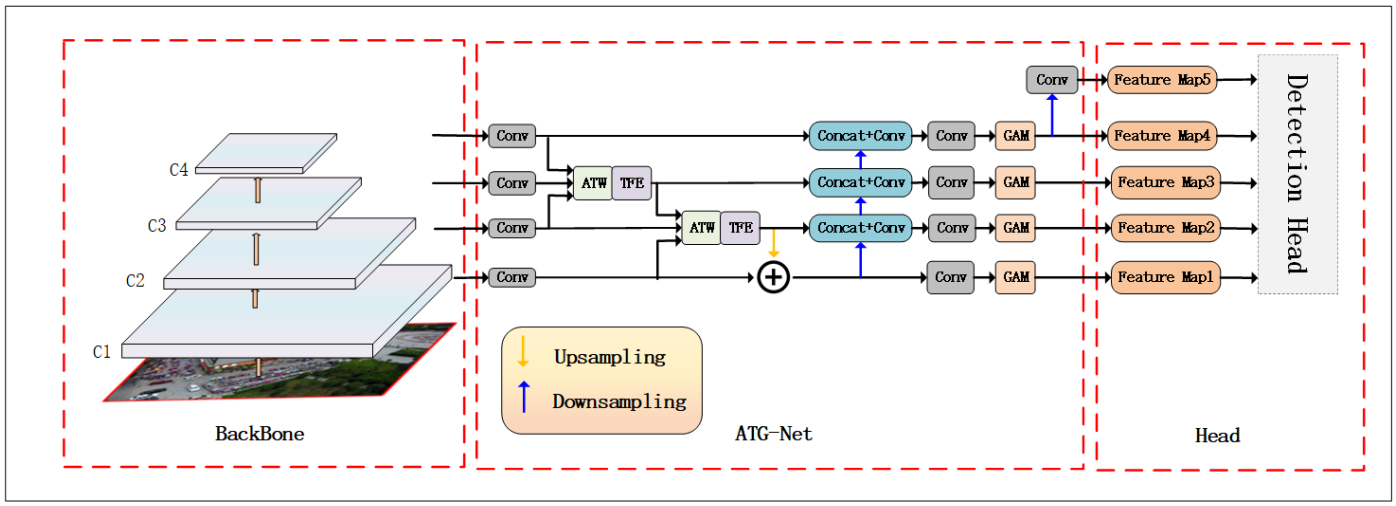


Fig. 1. The framework of ATG-Net. It consists of a backbone network, ATG-Net, and a detection head.

and FC denotes the fully connected layer. Large, Medium, and Small refer to the large-size, medium-size, and small-size feature maps, respectively. First, the features of large, medium, and small sizes are convolved by 1x1 to adjust the number of channels. Secondly, ATW employs global average pooling on each feature map to compress spatial information, resulting in a numerical value for each channel. The channel information is then concat. Finally, the concatenated features are passed through two fully connected layers to generate weight information for the three features. Formally, each layer is characterized by $X_n \in C_n \times R^{H_n \times W_n}$, and ATW computes the channel-wise global representation of $Z \in R^{C \times 1}$ by the following formula:

$$Z = \|_{n=1}^{N} z_n = \|_{n=1}^{N} \left\{ \frac{1}{H_n \times W_n} \sum_{i=1}^{H_n} \sum_{j=1}^{W_n} X_n(i,j) \right\}. \quad (1)$$

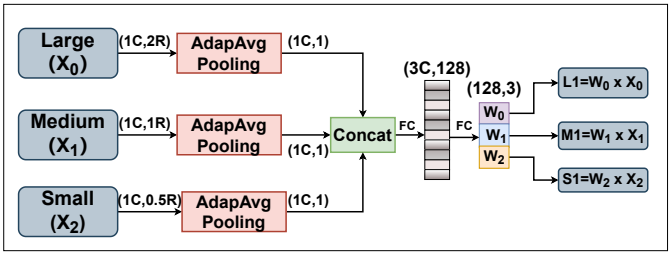


Fig. 2. The structure of the ATW module.

Where $\|$ represents the concatenation function, $C = \sum_{n=1}^{N} C_n$ represents the number of channels represented globally, n ∈ 0,1,2. N represents the number of the feature map, and $X_n(i,j)$ represents represents the feature value at the position (i,j) of the n-th feature map. This paper attempts to make use of aggregate information Z to focus on the features of each level on the significant region rather than the overall feature map. The integrated information Z is passed through two linear transformations to obtain the assigned weight $W \in R^{N \times 1}$.

$$W = FC_2(Relu(FC_1(Z))) \quad (2)$$

As shown in Fig. 2, the symbol W_n represents the nth element of W, and $\times$ denotes the scalar multiplication between X_n and W_n. This approach facilitates the adaptive enhancement of features at each level, thereby promoting precise saliency detection in computer vision applications.

B. Triple Feature Encoder Module

Traditional feature pyramid networks introduce a top-down path to generate multi-scale feature maps by upsampling high-level feature maps and fusing them with low-level feature maps. However, due to the insufficient interaction of semantic information between levels, it is difficult to effectively synergize the low-level detail information with the high-level semantic information, which affects the characterization ability of the fused feature graph. This paper proposes the Triple Feature Encoder Module (TFE) approach, which fuses three scales of feature information to generate high-quality semantic information. The design can not only enhance the characterization ability of features but also improve and refine the feature information.

Fig. 3 shows the structure of the TFE module. Here, C represents the number of channels and R the resolution of feature maps. L1, M1, and S1 denote the large, medium, and small feature maps from the output of the ATW module. The upsample uses nearest neighbor interpolation. For large-size feature maps (L1), a hybrid structure of maximum pooling and average pooling is utilized for down sampling, which is beneficial to preserve the validity and diversity of high-resolution features and small objects. Medium-size feature maps (M1) can be subjected to a convolution operation or without any untransformation. For small-size features (S1), the nearest neighbor interpolation method is used to adjust the resolution to 1R. The three changed features are then subjected to a concat operation, which undergoes a 1*1 convolution operation to modify the output channel. This approach helps to preserve the local feature richness of low-resolution images.

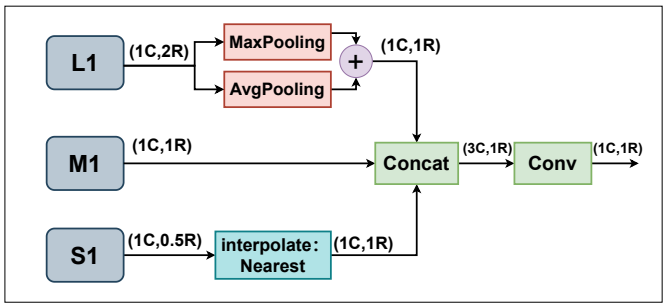


Fig. 3. The structure of the TFE module.

C. Global Attention Mechanism

However, small objects occupy fewer pixels and contain less information in the image, making them more susceptible to being ignored or misclassified during detection. The attention mechanism guides the network to prioritize the features of small objects, thereby enhancing their distinguishability in subsequent processing by improving the representation of their features. By facilitating the capture of long-range dependencies, this mechanism leverages context from surrounding pixels and the broader image, thereby augmenting the network's feature representation capabilities. However, both SENet and CBAM approaches overlook the interactions between channels and spatial dimensions, leading to the loss of cross-dimensional information. The global attention mechanism (GAM) [33] mitigates information loss and amplifies interactions across global dimensions. This enhancement bolsters the features of small objects, mitigates information loss, and thereby elevates the detection performance for such objects.

Fig. 4 shows the overview of the Global Attention Mechanism (GAM), where diagram A represents the overall input-output flow of the GAM, subdiagram B represents the flow of the channel attention mechanism, and subdiagram C represents the flow of spatial attention. Where F_1, F_2 and F_3 represent the input feature map, intermediate state map, and output feature map, respectively. The expressions are as follows:

$$F_2 = M_c(F_1) \otimes F_1 \,. \tag{3}$$

$$F_3 = M_s(F_2) \otimes F_2 \,. \tag{4}$$

where M_c denotes the channel attention mechanism, M_s denotes the spatial attention mechanism, and $\otimes$ denotes element-by-element multiplication.

The channel attention submodule arranges spatial information into 1 dimension and realigns dimensional positions. It subsequently applies a two-layer multi-layer perceptron (MLP) to enhance the interdimensional dependencies between channels and spatial features.

In order to expand the receptive field, the spatial attention mechanism uses 7*7 convolutional layers. To reduce the computational effort, the number of channels is regulated using the channel reduction rate r. Finally, the feature map is passed through a sigmoid activation function, which generates attention weights that indicate the degree of importance of different locations or features.

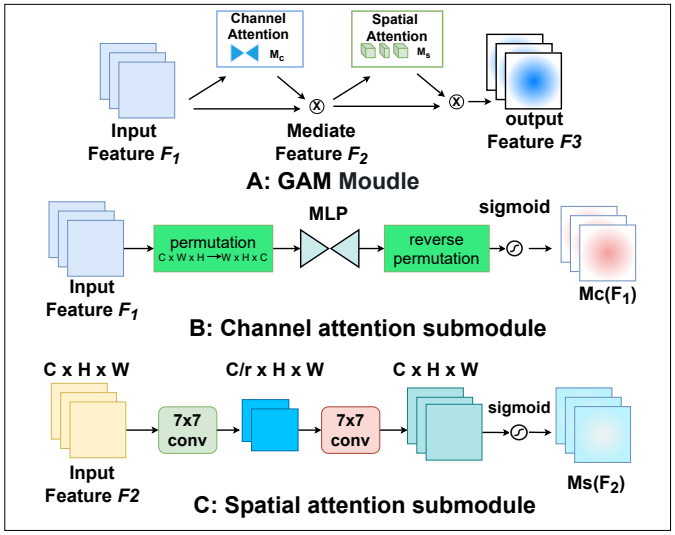


Fig. 4. The overview of the global attention mechanism.

IV. Experiments

To verify the effectiveness of the ATG-Net for small object detection, this paper conducts extensive experiments on the VisDrone2020 [34] dataset, a popular and challenging benchmark for aerial image detection.

1) VisDrone2020: This dataset contains a total of 10,209 images, of which 6471 were used for training, 548 for validation, 1610 for general testing, and 1580 for challenging testing. The image resolution of the dataset is approximately 2000×1500. The dataset encompasses 2.6 million annotations across various categories, primarily focusing on vehicles such as cars, buses, bicycles, tricycles, motorcycles, awning-tricycles, trucks, and vans, along with pedestrians, all captured from drone-based observations. It has extreme category imbalance and scale imbalance, making it an ideal benchmark for studying small object detection problems.

2) Implementation details: RetinaNet (Retina) [25], Faster R-CNN (FRCNN) [29], and Cascade RCNN (CRCNN) [39] are respective representatives of one-stage detectors, two-stage detectors, and cascade detectors. Accordingly, the paper designates them as the baseline detection networks for comparison. For data augmentation, the paper utilizes simple yet effective methods such as random resizing, random cropping, and random flipping. We implement the ATG-Net based on mmdetection on a single Nvidia 3060Ti GPU with 16GB of graphics memory. The optimizer employed is Stochastic Gradient Descent (SGD), initialized with a learning rate of 0.01. The learning rate strategy integrates both linear and cosine annealing schedules, initially employing a linear decay over the first 10 epochs, followed by a cosine decay for the subsequent 20 epochs, thereby encompassing a total training duration of 30 epochs. To assess the network's performance, Average Precision (AP) is utilized as the key metric. $AP_{50:95}$ is the average accuracy calculated over a range of different Intersection over Union (IoU) thresholds. It provides a more comprehensive picture of the model's performance under different IoU thresholds. AP_{50} and AP_{75} are computed at single

TABLE I. DETECTION RESULTS OF DIFFERENT NETWORKS ON THE VISDRONE2020 VALIDATION SET

Method	Backbone	$AP_{50:95}$	AP_{50}	AP_{75}	PED	PER	BC	Car	Van	Truck	TRI	ATRI	Bus	MO
Retina [26]	R50	13.9	27.7	12.7	13.0	7.9	1.4	45.5	19.9	11.5	6.3	4.2	17.8	11.8
FRCNN [26]	R18	21.8	39.2	21.5	18.1	12.9	7.3	50.3	30.5	21.5	15.5	8.1	34.8	18.7
FRCNN [26]	R50	21.7	39.8	21.0	21.4	15.6	6.7	51.7	29.5	19.0	13.1	7.7	31.4	20.7
FRCNN [26]	R101	21.8	40.2	20.9	20.9	14.8	7.3	51.0	29.7	19.5	14.0	8.8	30.5	21.2
CRCNN [26]	R50	23.2	40.7	23.1	22.2	14.8	7.6	54.6	31.5	21.6	14.8	8.6	34.9	21.4
FRCNN+ MMF [35]	R50	22.6	41.7	21.6	21.6	15.3	9.6	51.5	28.5	20.4	15.9	7.5	33.7	21.6
FRCNN+SimCal [36]	R50	20.0	35.8	19.6	18.7	13.8	5.7	51.0	28.4	16.4	13.6	5.9	27.0	19.4
FRCNN+RS+BGS [37]	R50	23.0	43.0	22.0	21.8	16.0	8.1	51.8	31.1	19.8	15.0	8.4	36.1	21.5
FRCNN+DSHNet [38]	R50	24.6	44.4	24.1	22.5	16.5	10.1	52.8	32.6	22.1	17.5	8.8	39.5	23.7
Retina+ATG-Net	R50	18.1	30.6	18.7	13.8	7.7	5.0	48.2	24.7	21.1	10.5	5.5	31.9	12.6
CRCNN+ATG-Net	R50	24.9	40.8	26.3	20.5	12.5	10.2	54.3	34.6	27.4	17.7	11.2	40.2	20.7
FRCNN+ATG-Net	R18	27.2	44.8	28.8	22.5	16.2	12.5	54.9	38.2	27.7	20.4	13.1	42.8	23.6
FRCNN+ATG-Net	R50	**28.9**	**46.8**	**30.9**	**23.7**	**17.2**	**13.8**	**56.2**	**39.7**	**30.4**	**22.6**	**13.9**	**47.1**	**24.9**

IoU thresholds of 0.5 and 0.75 across all categories. AP_s, AP_m and AP_l presents the average precision of the model in detecting small, medium, and large sizes receptively.

A. Experimentation Results

1) Comparison with baseline models: To demonstrate the effectiveness of the ATG-Net algorithm for detecting various types of targets on UAV images, the paper compares the proposed model with three baseline models and various improved FPN methods. The baseline models include Faster RCNN (FRCNN), RetinaNet (Retina), and Cascade RCNN (CRCNN), all evaluated under the same experimental conditions. ResNet18 (R18) and ResNet50 (R50) were chosen as the backbone networks. The evaluation metric for the object category utilizes $AP_{50:95}$. Experimental results with the baseline model and various improved FPN methods are shown in Table I. Where PED stands for pedestrian, PER stands for person, BC stands for bicycle, TRI stands for tricycle, ATRI stands for awning-tricycle, and MO stands for motor.

From Table I, ATG-Net achieves consistent performance improvements across all the detection networks with which it is combined. For Faster R-CNN, this paper uses three backbone architectures for comparative experiments. Notably, the R50 backbone yields the most significant performance boost, enhancing the $AP_{50:95}$ from 21.7% to 28.9%, representing a 7.2% improvement. When compared to the Retina model, there was an AP improvement from 13.9% to 18.4%, marking a 4.5% enhancement. The optimal detection model, Cascade R-CNN, likewise exhibits performance enhancement, with the AP advancing 23.2% to 24.4%. Upon incorporating our proposed ATG-Net module, all three baseline models experienced a significant improvement in detection accuracy across all categories. Notably, in categories like 'bicycle' and 'bus', which are underrepresented in the training data and typically appear very small, our method—employing FRCNN with the R50 backbone—achieves remarkable $AP_{50:95}$ increases of 7.1% and 15.7%, respectively. This highlights the ATG-Net's capability to excel at detecting small objects even when trained on limited data, affirming its robustness in such challenging scenarios.

Table I also presents the detection results of various advanced FPN networks improved upon FRCNN. ATG-Net also achieved the highest average detection precision, surpassing other detectors. In the detection of ten categories, ATG-Net has achieved good results, especially in the category of the bicycle and bus, where it outperforms DSHNet by 3.7% and 7.6%, respectively.

To further demonstrate the effectiveness of the ATG-Net model in detecting small objects, Table II is provided. A comparative analysis of various advanced object detection algorithms on the VisDrone2020 test set is presented. Combining ATG-Net with FRCNN and utilizing R50 as the backbone network, the optimal result was achieved on AP_{50}, with 38.4%. As shown in Table II, categories with a higher proportion of small targets, such as bicycles and buses, exhibit a substantial improvement, with the AP_{50} increasing to 18.2% and 64.4%, respectively.

B. Ablation Experiments

To validate the individual contributions of ATG-Net's feature pyramid components—ATW, TFE, and GAM—to the detection performance, ablation experiments were conducted. Experiments were conducted on the VisDrone2020 validation set using FRCNN as the baseline model and R18 as the backbone network. Table III shows the effect of each component of the ATG-Net on the detection performance.

1) Impact of TFE module: As shown in Table III, the addition of the TFE module increases AP_{50} from 39.0% to 42.4%. The AP_s increases from 14.1% to 16.6%, indicating that the TFE module can effectively improve the precision of small objects. This indicates that the TFE module can well fuse different levels of feature maps, which in turn enhances the model's ability to deal with multi-scale features, enabling the model to obtain better performance in the recognition of small and large objects.

2) Impact of the ATW module: The adaptive triple feature weighting module is able to adaptively predict a set of weights based on the importance of the triple features. ATW and TFE need to be used together. From Table III, when ATW and TFE are fused, AP_s increases from 14.1% to 17.3%. Combining the two modules enhances the model's robustness in detecting small targets. This also demonstrates that the ATW module effectively predicts weights from features of different scales.

3) Impact of GAM module: Although the use of GAM alone did not significantly improve detection performance, combining it with the other two modules enhanced the model's overall object detection capabilities. Compared to the baseline model, AP_{50} improves from 39.0% to 44.8%, an increase of 5.8%. For small objects, the AP increased from 14.1% to

TABLE II. COMPARISON OF EXPERIMENT RESULTS WITH OTHER POPULAR ALGORITHMS ON THE VISDRONE2020 TEST SET

Method	Backbone	AP_{50}	PED	PER	BC	Car	Van	Truck	TRI	ATRI	Bus	MO
CenterNet [40]	R50	26.6	22.6	20.6	14.6	59.7	24.0	21.3	20.1	17.4	37.9	23.7
YOLOv4 [41]	CSPDarknet53	32.5	28.2	15.9	5.8	65.7	25.2	26.1	13.8	8.1	40.2	26.1
YOLOv3-LITE [42]	DarkNet-53	28.5	**34.5**	**23.4**	7.9	70.8	31.3	21.9	15.3	6.2	40.9	32.7
MSA-YOLO [26]	CSPDarknet53	34.7	33.4	17.3	11.2	**76.8**	41.5	41.4	14.8	18.4	60.9	31.0
DINO [43]	Transformer	24.8	15.6	9.4	10.0	47.7	31.1	30.1	17.3	16.8	45.0	17.6
FRCNN+ATG-Net	R18	34.9	26.8	14.4	16.9	72.4	47.8	46.5	24.5	22.3	63.6	31.5
FRCNN+ATG-Net	R50	**38.4**	27.9	15.9	**18.2**	73.7	**50.4**	**49.1**	**24.8**	**25.0**	**64.4**	**34.8**

TABLE III. ABLATION STUDY RESULTS OF THE THREE COMPONENTS OF THE ATG-NET ON VISDRONE2020 VALIDATION SET. ✓ INDICATES THE USE OF THE MODULE

TFE	ATW	GAW	AP_{50}	AP_s	AP_l	param(M)
×	×	×	39.0	14.1	29.0	**121**
✓	×	×	42.4	16.6	33.9	110
×	×	✓	36.1	13.5	30.8	146
✓	✓	×	42.8	17.3	36.1	114
✓	✓	✓	**44.8**	**18.5**	**37.2**	162

18.5%, indicating that the model has excellent small object detection capability.

C. Visualization

In order to more intuitively demonstrate the effectiveness of the proposed method in practical application, some representative images from the Visdrone2020 test challenge dataset were selected for testing. All experiments were conducted by comparing the baseline FRCNN model, using R18 as the backbone network, with the model that combines our proposed ATG-Net with FRCNN.

Fig. 5 compares the visualization results of the highest-resolution feature map generated by the neck network. From left to right, the first column represents the original images, the second column shows the visualization results of the baseline model, and the third column displays the visualization results of our proposed ATG-Net. From the visualization results, it is evident that the feature maps produced by the baseline Faster R-CNN have a limited receptive field. This limitation suggests that the baseline model may struggle to capture detailed information or context over larger areas, leading to inaccuracies in detection. In contrast, the feature maps obtained by our ATG-Net have a global receptive field and focus on relatively smaller regions of interest compared to features of the same level. This characteristic allows our model to capture more detailed information and maintain context across different scales, thereby improving detection precision.

Fig. 6 shows the detect results on representative and more difficult images from the Visdrone2020 test challenge dataset. In this figure, the different categories are represented by different colored boxes, and the numbers on the rectangles indicate the confidence scores. The left column shows the results from the baseline FRCNN model with an R18 backbone. The right column shows the results from both FRCNN and ATG-Net models utilizing the same R18 backbone. Different categories in the detection results are identified using different colored detection boxes. Yellow boxes are used to highlight the detection of small objects, and zoomed-in effects are shown alongside for a more intuitive comparison. From the detection results, it can be seen that the baseline model has misdetections and misses small objects in the presence of occlusion, whereas the proposed model shows no misses and detects more small objects even in the presence of occlusion. In the detection effect image taken from high altitude, the vehicles and pedestrians on the road are very small. In this situation, the model in this paper can also detect them well. In the images of different lighting scenes, the model still has good detection ability in the dim scene.

V. CONCLUSION

In this paper, we proposed ATG-Net, an improved feature pyramid network for boosting UAV aerial image object detection. Firstly, we propose an Adaptive Triple Weighting (ATW) module, which intelligently assigns weights to predictions across diverse scales—large, medium, and small—dynamically emphasizing the significance of each size category. Secondly, we introduce a Triple Feature Encoding (TFE) module to utilize more efficiently on multi-scale contextual information. By applying the derived weights to features across various scales, this module amplifies and integrates multi-resolution features, thereby enhancing the representational capability of small object features. Due to the global attention mechanism (GAM) taking into account global information, it is crucial for enhancing the detection performance of small objects. Extensive experimental results on the VisDrone2020 have demonstrated that ATG-Net can effectively replace existing FPN networks and integrate with various popular detectors. Meanwhile, the proposed model can significantly enhance feature fusion capabilities, thus improving the detection precision of small objects. To enhance ATG-Net's detection capabilities even further, our next goal is to reduce model complexity and build lightweight detection models that can be deployed into edge devices.

REFERENCES

[1] Z. Li, Y. Zhang, H. Wu, S. Suzuki, A. Namiki, and W. Wang, "Design and application of a uav autonomous inspection system for high-voltage power transmission lines," *Remote Sensing*, vol. 15, no. 3, p. 865, 2023.

[2] A. Bouguettaya, H. Zarzour, A. Kechida, and A. M. Taberkit, "A survey on deep learning-based identification of plant and crop diseases from uav-based aerial images," *Cluster Computing*, vol. 26, no. 2, pp. 1297–1317, 2023.

[3] A. Utsav, A. Abhishek, P. Suraj, and R. K. Badhai, "An iot based uav network for military applications," in *2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 2021, pp. 122–125.

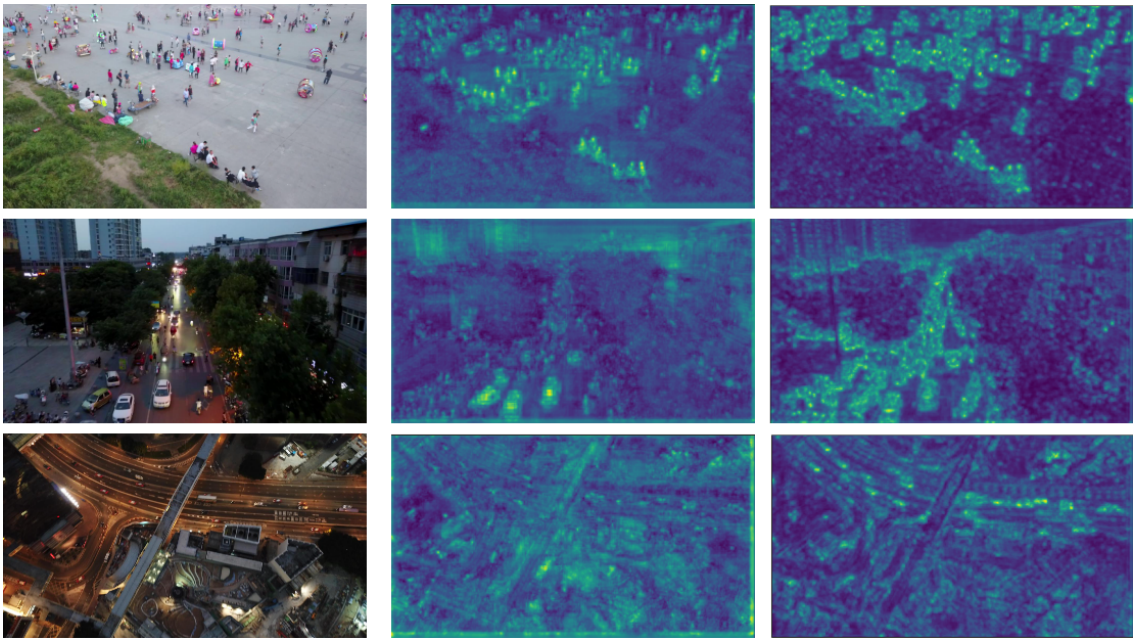


Fig. 5. Feature visualization results. From left to right, the column shows the original input image, the visualization result of the baseline model, and the visualization result of ATG-Net.

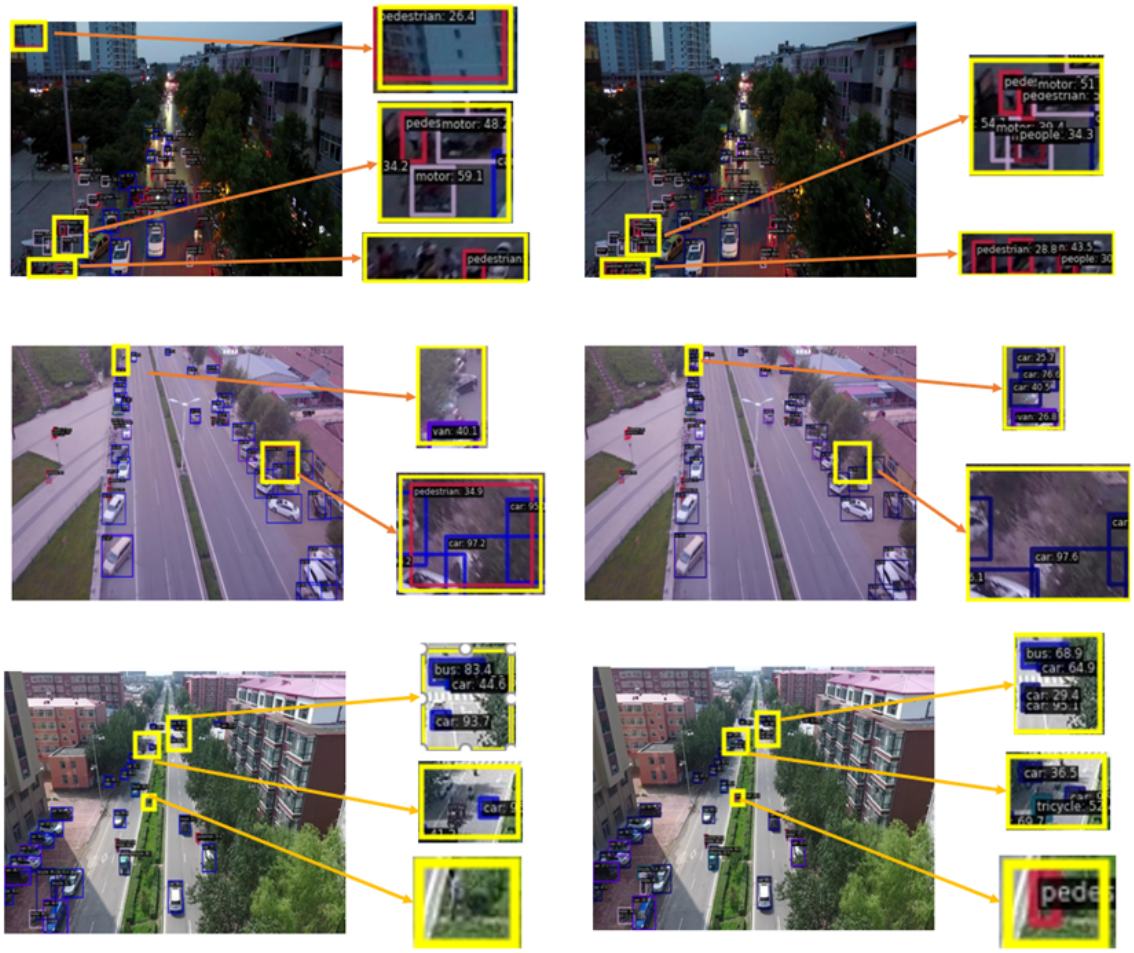


Fig. 6. Visualization results of challenging images on the VisDrone2020 validation dataset.

[4] W. Guettala, A. Sayah, L. Kahloul, and A. Tibermacine, "Real time human detection by unmanned aerial vehicles," in *2022 International Symposium on iNnovative Informatics of Biskra (ISNIB)*. IEEE, 2022, pp. 1–6.

[5] C.-J. Lin and J.-Y. Jhang, "Intelligent traffic-monitoring system based on yolo and convolutional fuzzy neural networks," *IEEE Access*, vol. 10, pp. 14 120–14 133, 2022.

[6] M. S. Mia, A. A. B. Voban, A. B. H. Arnob, A. Naim, M. K. Ahmed, and M. S. Islam, "Danet: Enhancing small object detection through an efficient deformable attention network," in *2023 International Conference on the Cognitive Computing and Complex Data (ICCD)*. IEEE, 2023, pp. 51–62.

[7] Y. Mo, J. Huang, and G. Qian, "Deep learning approach to uav detection and classification by using compressively sensed rf signal," *Sensors*, vol. 22, no. 8, p. 3072, 2022.

[8] P. Sun, R. Zhang, Y. Jiang, T. Kong, C. Xu, W. Zhan, M. Tomizuka, L. Li, Z. Yuan, C. Wang *et al.*, "Sparse r-cnn: End-to-end object detection with learnable proposals," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2021, pp. 14 454–14 463.

[9] G. Wang, Y. Chen, P. An, H. Hong, J. Hu, and T. Huang, "Uav-yolov8: a small-object-detection model based on improved yolov8 for uav aerial photography scenarios," *Sensors*, vol. 23, no. 16, p. 7190, 2023.

[10] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.

[11] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 770–778.

[12] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 4700–4708.

[13] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, "Mobilenets: Efficient convolutional neural networks for mobile vision applications," *arXiv preprint arXiv:1704.04861*, 2017.

[14] M. Tan and Q. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," in *International conference on machine learning*. PMLR, 2019, pp. 6105–6114.

[15] C.-Y. Wang, H.-Y. M. Liao, Y.-H. Wu, P.-Y. Chen, J.-W. Hsieh, and I.-H. Yeh, "Cspnet: A new backbone that can enhance learning capability of cnn," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops*, 2020, pp. 390–391.

[16] Z. Liu, Y. Lin, Y. Cao, H. Hu, Y. Wei, Z. Zhang, S. Lin, and B. Guo, "Swin transformer: Hierarchical vision transformer using shifted windows," in *Proceedings of the IEEE/CVF international conference on computer vision*, 2021, pp. 10 012–10 022.

[17] T.-Y. Lin, P. Dollár, R. Girshick, K. He, B. Hariharan, and S. Belongie, "Feature pyramid networks for object detection," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 2117–2125.

[18] S. Liu, L. Qi, H. Qin, J. Shi, and J. Jia, "Path aggregation network for instance segmentation," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 8759–8768.

[19] M. Tan, R. Pang, and Q. V. Le, "Efficientdet: Scalable and efficient object detection," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 10 781–10 790.

[20] Y. Zhang, J. H. Han, Y. W. Kwon, and Y. S. Moon, "A new architecture of feature pyramid network for object detection," in *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*. IEEE, 2020, pp. 1224–1228.

[21] C. Deng, M. Wang, L. Liu, Y. Liu, and Y. Jiang, "Extended feature pyramid network for small object detection," *IEEE Transactions on Multimedia*, vol. 24, pp. 1968–1979, 2021.

[22] X. Zhou and L. Zhang, "Sa-fpn: An effective feature pyramid network for crowded human detection," *Applied Intelligence*, vol. 52, no. 11, pp. 12 556–12 568, 2022.

[23] Z. Li, C. Lang, J. H. Liew, Y. Li, Q. Hou, and J. Feng, "Cross-layer feature pyramid network for salient object detection," *IEEE Transactions on Image Processing*, vol. 30, pp. 4587–4598, 2021.

[24] L. Zhu, F. Lee, J. Cai, H. Yu, and Q. Chen, "An improved feature pyramid network for object detection," *Neurocomputing*, vol. 483, pp. 127–139, 2022.

[25] T.-Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollár, "Focal loss for dense object detection," in *Proceedings of the IEEE international conference on computer vision*, 2017, pp. 2980–2988.

[26] S. Zeng, W. Yang, Y. Jiao, L. Geng, and X. Chen, "Sca-yolo: A new small object detection model for uav images," *The Visual Computer*, vol. 40, no. 3, pp. 1787–1803, 2024.

[27] M. Kang, C.-M. Ting, F. F. Ting, and R. C.-W. Phan, "Asf-yolo: A novel yolo model with attentional scale sequence fusion for cell instance segmentation," *Image and Vision Computing*, vol. 147, p. 105057, 2024.

[28] R. Girshick, "Fast r-cnn," in *Proceedings of the IEEE international conference on computer vision*, 2015, pp. 1440–1448.

[29] S. Ren, K. He, R. Girshick, and J. Sun, "Faster r-cnn: Towards real-time object detection with region proposal networks," *IEEE transactions on pattern analysis and machine intelligence*, vol. 39, no. 6, pp. 1137–1149, 2016.

[30] Y. Wu, Y. Chen, L. Yuan, Z. Liu, L. Wang, H. Li, and Y. Fu, "Rethinking classification and localization for object detection," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 10 186–10 195.

[31] J. Hu, L. Shen, and G. Sun, "Squeeze-and-excitation networks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 7132–7141.

[32] S. Woo, J. Park, J.-Y. Lee, and I. S. Kweon, "Cbam: Convolutional block attention module," in *Proceedings of the European conference on computer vision (ECCV)*, 2018, pp. 3–19.

[33] Y. Liu, Z. Shao, and N. Hoffmann, "Global attention mechanism: Retain information to enhance channel-spatial interactions," *arXiv preprint arXiv:2112.05561*, 2021.

[34] P. Zhu, L. Wen, D. Du, X. Bian, H. Fan, Q. Hu, and H. Ling, "Detection and tracking meet drones challenge," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 11, pp. 7380–7399, 2021.

[35] X. Zhang, E. Izquierdo, and K. Chandramouli, "Dense and small object detection in uav vision based on cascade network," in *Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops*, 2019, pp. 118–126.

[36] T. Wang, Y. Li, B. Kang, J. Li, J. Liew, S. Tang, S. Hoi, and J. Feng, "The devil is in classification: A simple framework for long-tail instance segmentation," in *Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part XIV 16*. Springer, 2020, pp. 728–744.

[37] Y. Li, T. Wang, B. Kang, S. Tang, C. Wang, J. Li, and J. Feng, "Overcoming classifier imbalance for long-tail object detection with balanced group softmax," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 10 991–11 000.

[38] W. Yu, T. Yang, and C. Chen, "Towards resolving the challenge of long-tail distribution in uav images for object detection," in *Proceedings of the IEEE/CVF winter conference on applications of computer vision*, 2021, pp. 3258–3267.

[39] Z. Cai and N. Vasconcelos, "Cascade r-cnn: Delving into high quality object detection," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 6154–6162.

[40] B. M. Albaba and S. Ozer, "Synet: An ensemble network for object detection in uav images," in *2020 25th International conference on pattern recognition (ICPR)*. IEEE, 2021, pp. 10 227–10 234.

[41] S. Ali, A. Siddique, H. F. Ateş, and B. K. Güntürk, "Improved yolov4 for aerial object detection," in *2021 29th Signal Processing and Communications Applications Conference (SIU)*. IEEE, 2021, pp. 1–4.

[42] H. Zhao, Y. Zhou, L. Zhang, Y. Peng, X. Hu, H. Peng, and X. Cai, "Mixed yolov3-lite: A lightweight real-time object detection method," *Sensors*, vol. 20, no. 7, p. 1861, 2020.

[43] N. D. Vo, N. Le, G. Ngo, D. Doan, D. Le, and K. Nguyen, "Transformer-based end-to-end object detection in aerial images," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 10, 2023. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2023.01410113

Deep Learning Classification of Gait Disorders in Neurodegenerative Diseases Among Older Adults Using ResNet-50

K.A. Rahman[1], E.F. Shair*[2], A.R. Abdullah[3], T.H. Lee[4], N.H. Nazmi[5]
Rehabilitation and Assistive Technology Research Group,
Faculty of Electrical Technology and Engineering, Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia[1,2,3,4]
Malaysia-Japan International Institute of Technology, Universiti Teknologi Malaysia,
Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia[5]

***Abstract*—Gait disorders in older adults, particularly those associated with neurodegenerative diseases such as Parkinson's Disease, Huntington's Disease, and Amyotrophic Lateral Sclerosis , present significant diagnostic challenges. Since these NDDs primarily affect older adults, it is crucial to focus on this population to improve early detection and intervention. This study aimed to classify these gait disorders in individuals aged 50 and above using vertical ground reaction force (vGRF) data. A deep learning model was developed, employing Continuous Wavelet Transform (CWT) for feature extraction, with data augmentation techniques applied to enhance dataset variability and improve model performance. ResNet-50, a deep residual network, was utilized for classification. The model achieved a validation accuracy of 95.06% overall, with class-wise accuracies of 97.14% for ALS vs CO, 92.11% for HD vs CO, and 93.48% for PD vs CO. These findings underscore the potential of combining vGRF data with advanced deep-learning techniques, specifically ResNet-50, to classify gait disorders in older adults accurately, a demographic critically affected by these diseases.**

***Keywords*—Gait disorders; neurodegenerative diseases; deep learning; vertical Ground Reaction Force (vGRF); ResNet-50**

I. Introduction

Gait, the manner of walking, is a fundamental human activity involving the intricate coordination of the brain, nerves, and muscles. Globally, gait problems have significantly increased, leading to approximately 646,000 fatal falls annually, particularly among individuals aged 50 years and above [1]. These disorders are the second most common cause of accidental deaths worldwide and contribute substantially to healthcare costs. For instance, Norton et al. [2] estimated that gait disorders account for approximately 0.85% to 1.5% of global healthcare expenses. Jia et al. [3] highlighted the rising prevalence of gait-related falls, emphasizing the need for early detection and intervention to mitigate these issues. Particularly among older adults, gait problems significantly impact mobility, quality of life, and mortality [4].

Neurodegenerative diseases (NDDs) are one of the most significant contributors to gait disorders. These diseases result from the progressive loss of neurons, leading to impaired communication between the brain and muscles. Parkinson's disease (PD), Huntington's disease (HD), and Amyotrophic Lateral Sclerosis (ALS) are among the most prevalent NDDs, each profoundly affecting gait patterns in distinct ways. For instance, Hoff et al. [5] observed that ALS patients typically exhibit slower walking speeds and longer stride durations, while Hausdorff et al. [6] reported increased gait variability in individuals with HD and PD. These conditions impair patients' motor functions, further complicating their management.

Advanced research techniques have illuminated the complex dynamics of gait in NDDs. For example, detrended fluctuation analysis has been used to identify specific gait patterns in neurodegenerative conditions [7], while multi-resolution entropy analysis has revealed disorder-specific gait dynamics [8]. Additionally, platforms like PhysioNet have been instrumental in providing benchmark datasets for studying these disorders [9]. Despite these advancements, Setiawan et al. [10] noted that accurately diagnosing specific NDDs through gait analysis remains challenging due to overlapping symptoms across conditions. Ye et al. [11] and Zhao et al. [12] emphasized the need for more robust multi-class classification techniques to distinguish PD, HD, and ALS effectively.

Existing methods have achieved varying levels of success. For instance, Baratin et al. [13] reported 85% accuracy using Discrete Wavelet Transform (DWT) with entropy and coherence features. Similarly, Zhao et al. [12] achieved 95.6% accuracy with dual-channel LSTM networks. However, many studies, such as those by Faisal et al. [14], have struggled to distinguish closely related gait disorders in mixed cohorts. Approaches employing convolutional neural networks (CNNs) have shown higher classification rates than traditional methods [15], but Fraiwan et al. [16] noted that ensemble classifiers can significantly enhance accuracy. Nevertheless, methods like these often face overfitting challenges due to limited data variability [17].

Hybrid approaches combining CNNs with Long Short-Term Memory (LSTM) networks have also shown promise. For example, Elziaat et al. [18] achieved 92.4% accuracy in predicting freezing of gait in PD patients by integrating spatial and temporal features. Deterministic learning theory with radial basis function (RBF) neural networks demonstrated 93.75% accuracy in classifying ALS, PD, and HD [19]. Amin and Singhal [20] emphasized the importance of dimensionality reduction techniques, achieving 93% accuracy for HD and 89% for PD. Furthermore, Mehra et al. [21] utilized IoT-based

sensors to achieve an accuracy of 98.8% in early PD detection. Ensemble methods like AdaBoost, which analyze features such as vertical ground reaction force (vGRF), have also proven effective, achieving 99.17 percent.

Recent studies have explored novel methods for improving classification accuracy. For instance, Penage et al. [22] transformed vGRF signals into recurrence plots, achieving high accuracy in multi-class classifications using CNNs. Erdas et al. [23] utilized convolutional LSTM networks combined with 3D CNNs, reaching a detection accuracy of 96.33% for NDDs, with specific accuracies of 97.68% for ALS, 94.69% for HD, and 95.05% for PD. These methods demonstrate the potential of advanced deep learning techniques but also highlight gaps in addressing the unique challenges faced by older adults [24].

Despite these advancements, most studies have focused on binary classifications or younger populations, leaving older adults—who are particularly susceptible to NDDs—understudied. To address this gap, this study employs Continuous Wavelet Transform (CWT) to transform vGRF signals into time-frequency spectrograms, enabling the extraction of both temporal and frequency-domain features. Unlike DWT, which may overlook transient signal features, CWT captures subtle gait abnormalities crucial for diagnosis. The ResNet-50 deep learning model, known for its robust feature extraction capabilities, is employed for classification. Data augmentation techniques are applied to enhance model generalizability and mitigate overfitting [25]. These advancements make the proposed method uniquely suited to addressing the challenges of accurately diagnosing neurodegenerative gait disorders in older adults.

The remainder of this article is organized as follows. Section II details the materials and methods, Section III presents the results, and Section IV discusses the findings. Finally, Section V concludes the study, summarizing key contributions and future research directions.

II. Methodology

The methodology of this study is summarised in Fig. 1. The study aimed to develop a machine-learning model for classifying gait disorders in older adults. The process involved three main steps: Data Collection, Data Preprocessing, Feature Extraction, ML Model Training and testing

A. Dataset

In this study, the "Gait in Neurodegenerative Diseases Dataset" provided by Hausdorff et al.[26] was employed. Fig. 2 illustrates the gait data collection procedure. Raw data were collected from vGRF sensors using force-sensitive resistors placed under the foot inside the shoes. During the experiment, each subject walked along a 77-meter-long hallway for five minutes at their normal pace.

The dataset includes recordings from 64 subjects, comprising 13 patients with ALS, 15 patients with PD, 20 patients with HD, and 16 CO. Since this study focuses on older adults, only data from subjects aged 50 and above were selected for analysis.

The gait parameters recorded for each subject include stance, swing, double support interval, and stride for both the left and right foot. For this study, only the right foot force data were analysed. On average, each subject contributed approximately 277 gait cycles, depending on their walking speed during the 5-minute data recording period [27].

TABLE I. Information of Gait Data Participants

Statistical Parameter	CO	HUNT	PARK	ALS
Age (Year)	62.6 ± 8.63	57.2 ± 6.24	66.5 ± 9.06	61.75 ± 7.07
Height (m)	1.84 ± 0.10	1.78 ± 0.14	1.99 ± 0.12	1.797 ± 0.34
Weight (kg)	74.6 ± 13.02	64 ± 10.8	87.38 ± 13.68	89.04 ± 13.91
Gait Speed (m/s)	1.29 ± 0.21	1.10 ± 0.14	1.34 ± 0.27	1.23 ± 0.19

The final dataset used in the model includes data from five healthy controls (average age: 62.6 years), seven patients with PD (average age: 66.5 years), five patients with HD (average age: 57.2 years), and four patients with ALS is (average age: 61.75 years). The breakdown of the dataset is shown in Table I. Detailed information about the participants, including their age, height, weight, and gait speed, is presented. The dataset was split for training and validation purposes, the dataset was split, with 70% of the data used for training and 30%.

B. Data Pre-processing

A five-minute gait force signal was captured and filtered using a digital band-pass filter, with the filtered signal $y(t)$ computed as the convolution of the raw signal $x(t)$ and the filter's impulse response $h(t)$, as shown in Eq. (1).

$$y(t) = h(t) \times x(t) \tag{1}$$

Wavelet denoising was then applied to further clean the signal, transforming $y(t)$ into the wavelet domain, thresholding the coefficients, and reconstructing the denoised signal $z(t)$, as expressed in Eq. (2).

$$z(t) = W^{-1}\left(T\left(W(y(t))\right)\right) \tag{2}$$

To optimize temporal and frequency resolution, wavelet transforms were applied using window durations of 10, 30, and 60 seconds. The 10-second window was selected for the final analysis, providing the best balance for capturing relevant gait features [28].

C. Data Augmentation

To enhance model performance and prevent overfitting, various data augmentation techniques were applied to the gait signals, which were transformed into the frequency-time domain for analysis by the ResNet-50 model. Horizontal flipping, mathematically represented as $f(x, y) \rightarrow f(-x, y)$, and random rotations between -10 and 10 degrees [Eq. (1)] were used to introduce variability.

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{1}$$

Random translations along the x and y axes [Eq. (2)] were applied to simulate different positions.

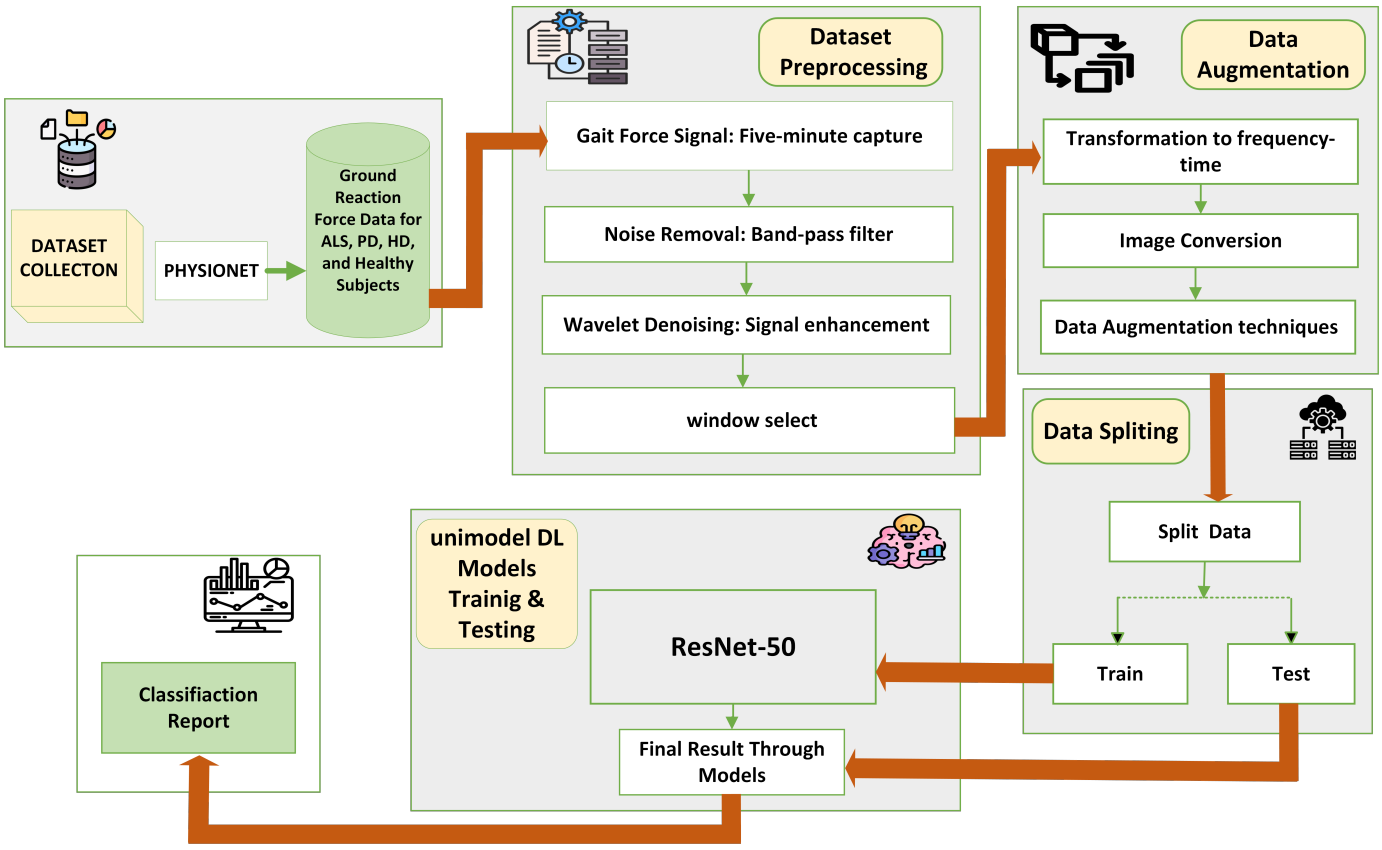


Fig. 1. Diagram of the proposed method.

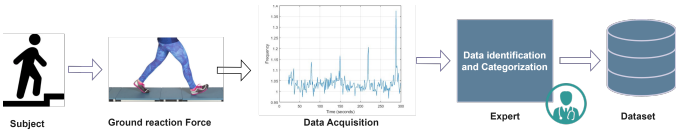


Fig. 2. Data collecting procedure.

$$(x, y) \rightarrow (x + \Delta x, y + \Delta y) \tag{2}$$

Brightness and contrast adjustments [Eq. (3)], scaling [Eq. (4)], and Gaussian blur [Eq. (5)] were also implemented to increase dataset diversity.

$$I' = \alpha I + \beta \tag{3}$$

$$(x, y) \rightarrow (sx, sy) \tag{4}$$

$$G(x, y) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{x^2 + y^2}{2\sigma^2}\right) \tag{5}$$

Each transformation introduced new variations in the dataset, improving model robustness by simulating different object sizes, perspectives, and noise levels, which helped the model generalize better in classification tasks.

D. Classification Model: ResNet-50

The proposed ResNet-50 model was employed to classify gait disorders using gait data transformed into the frequency-time domain via Continuous Wavelet Transform (CWT). The model architecture and data preprocessing steps are depicted in Fig. 3. The architecture consists of several key components aimed at extracting hierarchical features and classifying the four target gait disorder classes: CO, HD, PD, and ALS.

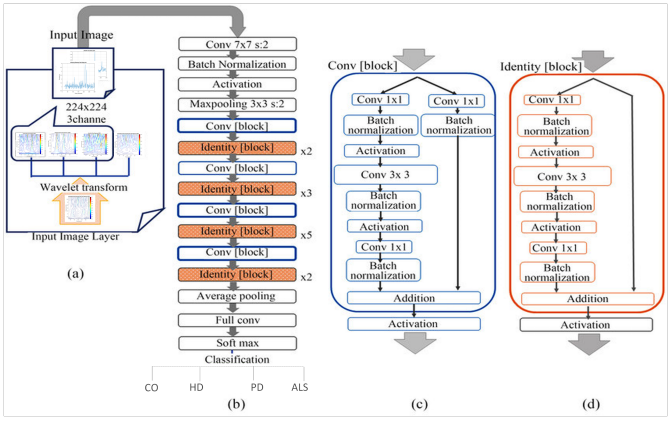


Fig. 3. Overview of the ResNet-50 architecture.

1) Model Architecture Overview: The architecture begins with the input image, processed through several convolutional

layers [Fig. (3b)], each followed by batch normalization and ReLU activation to capture local patterns. The convolutional layers are organized into residual blocks, as shown in Fig. 3(c) and 3(d), where identity and convolutional shortcuts allow the network to retain information and mitigate the vanishing gradient problem, enabling the training of deeper networks.

The convolutional operation for any layer l is mathematically expressed as:

$$O_l = f(W_l * I_{l-1} + b_l) \tag{6}$$

where O_l is the output feature map, W_l is the convolutional filter applied to the input I_{l-1}, and $f(x) = \max(0, x)$ is the ReLU activation function. After each convolutional block, pooling layers reduce the spatial dimensions of the feature maps to prevent overfitting and reduce computational load, as described by:

$$P_l = \text{pool}(O_l) \tag{7}$$

As the network deepens, feature complexity increases through the five stages of the network, eventually resulting in global average pooling, which reduces the spatial dimensions of each feature map to a single value:

$$y_k = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} O_{i,j}^k \tag{8}$$

Finally, the pooled features are passed through a fully connected layer, followed by the softmax activation function to produce a probability distribution across the gait disorder classes. The softmax is expressed as:

$$P(y = k|x) = \frac{\exp(z_k)}{\sum_{j=1}^{K} \exp(z_j)} \tag{9}$$

2) Training and Optimization: The model was trained using the Adam optimizer, with an initial learning rate of 0.001 and a mini-batch size of 32. Training was conducted over 30 epochs, with 70% of the dataset used for training and 30% for validation. The network minimized the categorical cross-entropy loss function:

$$L = -\sum_{k=1}^{K} y_k \log(P(y = k|x)) \tag{10}$$

The architecture was fine-tuned by replacing the fully connected and classification layers of the pre-trained ResNet-50 model to adapt it for the specific task of gait disorder classification. The training showed consistent improvement in accuracy, with a final validation accuracy of 95.06%.

This architecture, shown in Fig. 3, highlights the model's ability to learn intricate gait features effectively, addressing the reviewer's request for details on the number of layers, optimization method, and training parameters.

E. Performance Evaluation

To evaluate the effectiveness of the Gait Neurodegenerative Disorders classification model, key performance metrics including accuracy, sensitivity, specificity, precision, recall, and F1 score were calculated. These metrics were derived from the confusion matrix, which tracks the true positives (TPs), false positives (FPs), false negatives (FNs), and true negatives (TNs) for each class. Specificity, defined as the proportion of true negatives out of the total actual negatives, is calculated using Eq. (9). Sensitivity, also known as recall, measures the proportion of true positives out of the total actual positives and is given by Eq. (10). Accuracy, indicating the overall correctness of the model, is computed as per Eq. (11). Precision, reflecting the proportion of true positive predictions among the total predicted positives, is calculated in Eq. (12).Lastly, the F1 score, which balances precision and recall, is provided by Eq. (13). Together, these metrics offer a comprehensive assessment of the model's performance in classifying neurodegenerative disorders based on gait data.

$$\text{Specificity} = \frac{\sum_{i=1}^{n} \text{TN}_i}{\sum_{i=1}^{n} (\text{TN}_i + \text{FP}_i)} \tag{9}$$

$$\text{Sensitivity} = \frac{\sum_{i=1}^{n} \text{TP}_i}{\sum_{i=1}^{n} (\text{TP}_i + \text{FN}_i)} \tag{10}$$

$$\text{Accuracy} = \frac{\sum_{i=1}^{n} (\text{TP}_i + \text{TN}_i)}{\sum_{i=1}^{n} (\text{TP}_i + \text{TN}_i + \text{FP}_i + \text{FN}_i)} \tag{11}$$

$$\text{Precision} = \frac{\sum \text{TP}}{\sum (\text{TP} + \text{FP})} \tag{12}$$

$$\text{F1 score} = \frac{2 \times (\text{Precision} \times \text{Sensitivity})}{\text{Precision} + \text{Sensitivity}} \tag{13}$$

III. Result

In this study, MATLAB 2022b was used for data preprocessing, augmenting data, and training the Deep learning model for classification.

A. Statistical Analysis

Fig. 4 illustrates the time-domain frequency plots for the gait data of Control (CO) subjects and patients with Huntington's disease (HD), Parkinson's disease (PD), and Amyotrophic Lateral Sclerosis (ALS). The CO group (A) displays stable and consistent gait frequencies, while HD (B) shows erratic patterns, indicative of severe gait disturbances. PD (C) presents a mix of stable and fluctuating frequencies, whereas ALS (D) shows moderate variability in step frequency.

Fig. 5 provides the time-frequency spectrograms generated using Continuous Wavelet Transform (CWT) for each group. ALS (D) shows stable walking patterns with tightly packed contours, while HD (B) reflects irregular and erratic gait frequencies. PD (C) exhibits mixed contours, and the control group (A) maintains consistent patterns.

These findings are consistent with [29], offering further insight into the distinct gait characteristics of each condition.

Fig. 6 presents box plots that compare key gait features across ALS, PD, HD, and control groups. The mean gait

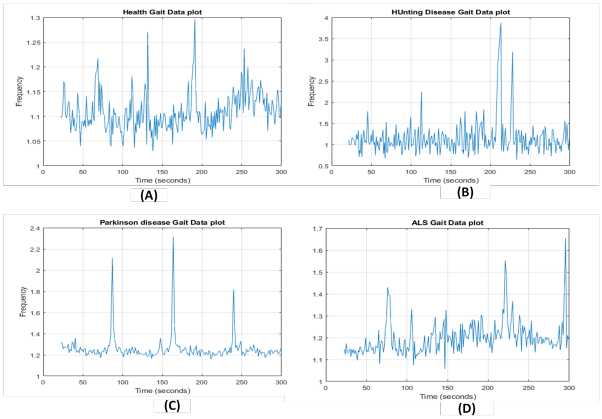


Fig. 4. Gait Time-Domain Patterns: (A) Control, (B) Huntington Disease, (C) Parkinson Disease, (D) ALS.

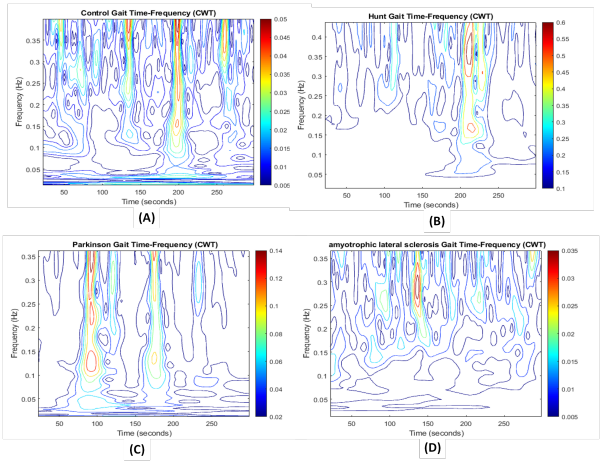


Fig. 5. Gait Time-Frequency Patterns (CWT): (A) Control, (B) Huntington Disease, (C) Parkinson Disease, (D) ALS.

values show that ALS patients have a lower median, reflecting their slower gait. The interquartile range (IQR) is wider for HD, indicating more variable gait patterns, characteristic of Huntington's disease.

The standard deviation and variance for PD suggest moderate variability, indicating motor fluctuations, while RMS and instantaneous RMS reveal greater dispersion in the neurodegenerative groups compared to controls, highlighting reduced gait control.

The gait speed box plot shows a significant decrease in ALS patients, emphasizing their slower walking patterns. These features will be key inputs for training deep learning models to accurately classify gait disorders, facilitating early detection and intervention. By integrating these insights with machine learning techniques, we can effectively monitor and classify gait abnormalities associated with neurodegenerative diseases.

B. ResNet-50 Model Training Progress

Fig. 7 shows the training and validation accuracy, as well as the training and validation loss, across iterations. The accuracy plot indicates steady improvement, with validation accuracy peaking around 95% and training accuracy reaching near 100%, demonstrating the model's effective learning of the data patterns.

The loss plot reveals a consistent decrease in both training and validation losses over time, with the training loss stabilizing at a low value. Although the validation loss shows some fluctuations, the overall trend suggests that the model generalizes well to unseen data.

C. Confusion Matrix for the ResNet-50 Model

Fig. 8 illustrates the confusion matrix for the ResNet-50 model, demonstrating its performance in classifying the four gait disorder classes. The model exhibits high classification accuracy, particularly for the CO and PARK classes, with minimal misclassification across classes. The ALS and HUNT classes show strong sensitivity and specificity, indicating effective distinction among the different gait disorders.

D. Classification Results

The performance of the ResNet-50 model in classifying gait disorders was evaluated using key metrics such as Validation Accuracy, Precision, Sensitivity, Specificity, and F1 Score, as shown in Table II. The model achieved a high validation accuracy of 95.06% for distinguishing between neurodegenerative diseases and healthy controls, indicating strong overall performance across all classifications.

TABLE II. VALIDATION PERFORMANCE METRICS FOR THE RESNET-50 MODEL

Evaluation Parameter	ALS vs CO	HD vs CO	PD vs CO	NDD vs CO
Validation Accuracy	97.14%	92.11%	93.48%	95.06%
Precision	96.88%	94.50%	92.88%	94.04%
Sensitivity	89.50%	98.90%	93.65%	91.68%
Specificity	96.30%	98.40%	92.90%	98.85%
F1 Score	97.11%	98.70%	93.22%	92.94%

Precision scores were also robust, with ALS vs CO achieving 96.88%, HD vs CO at 94.50%, PD vs CO at 92.88%, and NDD vs CO at 94.04%, reflecting the model's capacity to correctly identify relevant instances. Sensitivity varied across the conditions, with HD vs CO attaining the highest sensitivity at 98.90%, followed by PD vs CO at 93.65%, NDD vs CO at 91.68%, and ALS vs CO at 89.50%.

Specificity, a measure of the model's ability to correctly identify negative cases, was consistently high across all classifications: ALS vs CO at 96.30%, HD vs CO at 98.40%, PD vs CO at 92.90%, and NDD vs CO at 98.85%. These values demonstrate the model's strong ability to distinguish between diseased and control cases effectively.

The F1 Score, which balances precision and sensitivity, also confirmed the model's robust classification performance. ALS vs CO achieved an F1 Score of 97.11%, HD vs CO at 98.70%, PD vs CO at 93.22%, and NDD vs CO at 92.94%, highlighting the model's consistency in both detecting true positives and avoiding false positives.

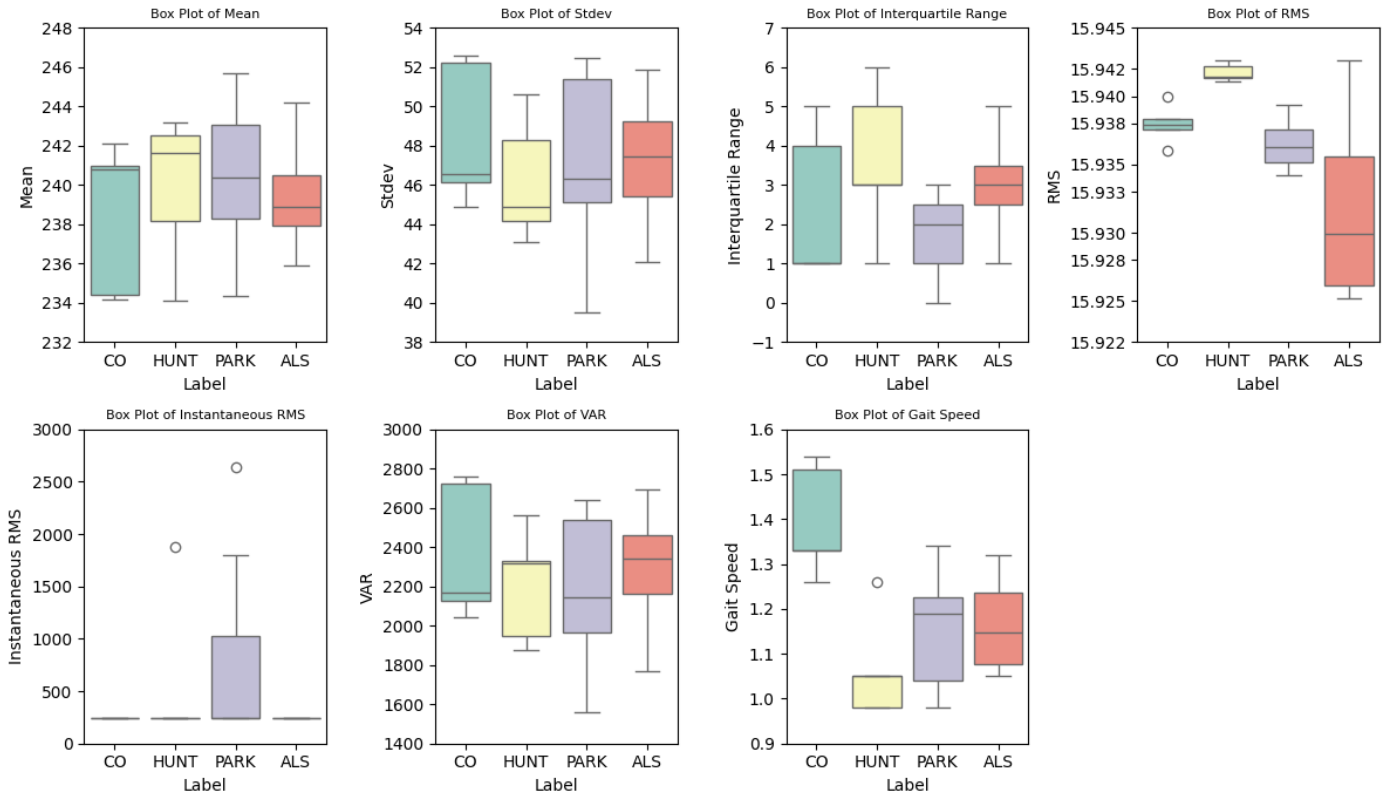


Fig. 6. Box plot analysis of gait features.

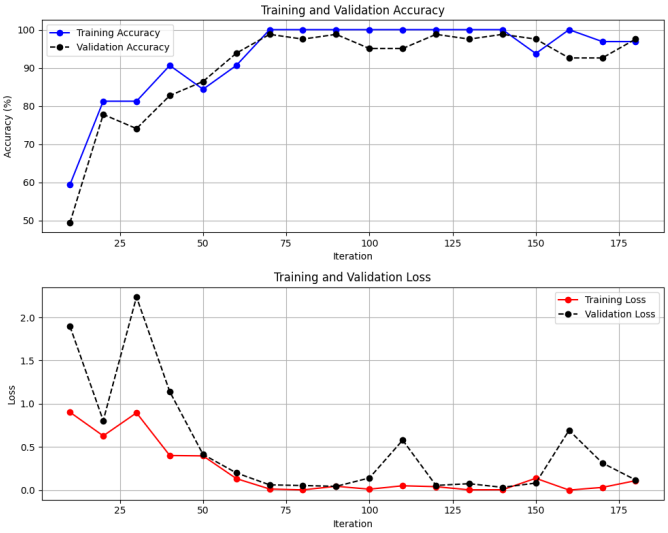


Fig. 7. Training and validation accuracy and loss over iterations.

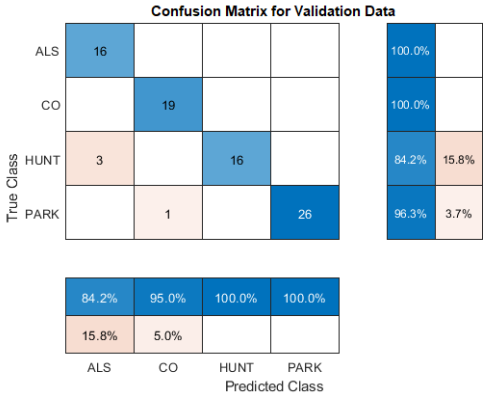


Fig. 8. Validation confusion matrix for the ResNet-50 model.

IV. Discussion and Comparison

This study specifically focused on classifying gait disorders in older adults, a demographic that is critically understudied despite being highly susceptible to neurodegenerative diseases (NDDs) such as Parkinson's Disease (PD), Huntington's Disease (HD), and Amyotrophic Lateral Sclerosis (ALS). Utilizing vertical Ground Reaction Force (vGRF) data and advanced deep learning techniques (ResNet-50), this research provides a more targeted approach, focusing on individuals aged 50 and above, whereas previous studies often included a broader age range or did not account for the unique characteristics of older adults.

Table III compares the classification accuracy of various models across studies. Our model, using ResNet-50 and vGRF data, achieved a high validation accuracy of 95.06% for distinguishing between different neurodegenerative conditions. This performance is competitive with previous efforts that utilized a variety of techniques and features. For example, Hong et al. [30] used a combination of stride, swing, and stance intervals

TABLE III. CLASSIFICATION ACCURACY OF DIFFERENT MODELS

Study	Signal	Methodology	ALS vs CO	PD vs CO	HD vs CO	NDD vs CO
[30]	Str. Int, Sw. Int, Sta. Int, DS. Int	Statistical Features (Min, Max, Avg, Std)	96.79%	89.33%	90.28%	90.63%
[19]	Sw. Int, Sta. Int	Deterministic Learning, RBF Neural Networks	93.1%	100%	100%	93.75%
[20]	Str. Int, Sw. Int, Sta. Int, DS. Int	Statistical Features (Mean, Std, Variance, Skewness, Kurtosis)	85%	89%	93%	85%
[31]	VGRF	Statistical Features (RMS, Variance, Kurtosis)	-	-	-	99.17%
[10]	VGRF	Time-Frequency Spectrogram	100%	97.42%	100%	98.44%
[24]	VGRF, Str. Int, Sw. Int, Sta. Int	Classical Nonlinear Features	95.72%	91.68%	91.71%	92.87%
[23]	VGRF	Recurrence Plot	100%	100%	97.56%	98.93%
[22]	VGRF	Raw VGRF	92%	81%	79%	78%
This Study	**VGRF**	**Time-Frequency Spectrogram,ResNet-50**	**97.14%**	**92.11%**	**93.48%**	**95.06%**

along with statistical features, achieving 96.79% accuracy for ALS vs CO, which is comparable to our study's 97.14%. However, their study did not focus specifically on older adults, making the results of our study particularly significant for this vulnerable population.

Other studies such as Zeng et al. [19] employed deterministic learning theory and RBF neural networks, achieving 93.1% for ALS vs CO. While this is a strong result, our study surpassed it by integrating Time-Frequency Spectrograms with ResNet-50, reflecting the effectiveness of deep learning models in capturing complex gait patterns, particularly in an older demographic. Furthermore, Zeng's study targeted a broader population, while our focus on older adults emphasizes the applicability of our model to clinical settings where early detection is critical.Similarly, the approach by Amin et al. [20] used stride and swing intervals with statistical features such as mean, standard deviation, and kurtosis, achieving lower accuracy rates (85% for ALS vs CO). This indicates that traditional machine learning techniques, even when combined with well-known gait metrics, may not be as effective as deep learning-based models in identifying subtle gait differences in older adults.

In contrast, Fraiwan et al. [31] achieved an impressive accuracy of 99.17% using ensemble decision tree classifiers with vGRF data. While their accuracy is slightly higher than ours, their study focused on a general population, whereas our model's 95.06% accuracy for older adults demonstrates strong performance in a more challenging demographic. The use of ensemble methods can be further explored in future studies for enhanced model performance in older populations.Setiawan et al. [10] reported a similar performance using vGRF data and time-frequency spectrograms, achieving 97.42% for PD vs CO and 100% for HD vs CO. Our model's results for these two conditions (93.48% and 92.11%, respectively) are slightly lower, which could be attributed to the increased complexity of gait patterns in older adults, especially those aged 50 and above. However, the overall performance of our model across all NDDs remains strong and consistent.

Moreover, studies such as Zhao et al. [24] and Lin et al. [23] utilized recurrence plot features and classical nonlinear analysis methods to classify gait disorders. They achieved high accuracies for individual tasks (100% for ALS and HD), but their methodologies did not specifically target the older population. Our study not only achieved comparable performance but also focused on older adults, where gait variability and complexity are more pronounced.

V. CONCLUSION

This study utilized Continuous Wavelet Transform (CWT) for feature extraction and ResNet-50 for classification, yielding a competitive validation accuracy of 95.06%, which aligns with or exceeds results from previous studies. The model achieved class-wise accuracies of 97.14% for ALS vs CO, 92.11% for HD vs CO, and 93.48% for PD vs CO. A key distinction of our work is the focus on older adults aged 50 and above, which, combined with data augmentation techniques, enhances model generalization. This differentiates our study from prior research that typically focused on younger populations or broader age ranges. The integration of vGRF data with advanced deep learning techniques provides a robust framework for accurately classifying gait disorders, particularly in the context of early diagnosis for older adults. Future studies could expand upon these findings by incorporating additional data modalities, such as medical history or multimodal sensor inputs, to further improve diagnostic accuracy and enable comprehensive monitoring of neurodegenerative disease progression in older adults.

ACKNOWLEDGMENT

This research was supported by the Fundamental Research Grant Scheme from the Ministry of Higher Education Malaysia, grant FRGS/1/2023/SKK06/UTEM/02/1, and Support from the Kesidang scholarship.

REFERENCES

[1] S. Raghu, M. Raghu, A. P. Marla, S. S. Kotian, and N. Kumari, "Fall-related injuries and their prevention strategies of in-patient population in tertiary health care setup," *QAI Journal for Healthcare Quality and Patient Safety*, vol. 3, no. 1, pp. 1–7, 2022.

[2] R. Norton, R. B. Ahuja, C. Hoe, *et al.*, "Nontransport unintentional injuries," in *Injury Prevention and Environmental Health* (C. N. Mock, R. Nugent, O. Kobusingye, *et al.*, eds.), ch. 4, Washington, DC: The International Bank for Reconstruction and Development / The World Bank, 3rd ed., 2017.

[3] H. Jia, E. I. Lubetkin, K. DeMichele, D. S. Stark, M. M. Zack, and W. W. Thompson, "Prevalence, risk factors, and burden of disease for falls and balance or walking problems among older adults in the u.s.," *Preventive Medicine (Baltimore)*, vol. 126, p. 105025, 2019.

[4] ACTRN, "Fall risk assessment and effectiveness of home based exercise on turning ability, balance and functional mobility among older malaysian adults aged 50 years and above." http://www.who.int/trialsearch/Trial2.aspx?TrialID=ACTRN12613000855729, 2013. No. April, 2013.

[5] J. I. Hoff, A. A. Plas, E. A. H. Wagemans, and J. J. van Hilten, "Accelerometric assessment of levodopa-induced dyskinesias in parkinson's disease," *Movement Disorders*, vol. 16, no. 1, pp. 58–63, 2001.

[6] J. M. Hausdorff *et al.*, "Dynamic markers of altered gait rhythm in amyotrophic lateral sclerosis," *Journal of Applied Physiology*, 2000. Accessed: Mar. 20, 2024. [Online]. Available: http://www.jap.org.

[7] F. Setiawan, A. B. Liu, and C. W. Lin, "Development of neurodegenerative diseases' gait classification algorithm using convolutional neural network and wavelet coherence spectrogram of gait synchronization," *IEEE Access*, vol. 10, pp. 38137–38153, 2022.

[8] E. F. Shair, S. A. Ahmad, A. R. Abdullah, M. H. Marhaban, and S. B. M. Tamrin, "Selection of spectrogram's best window size in emg signal during core lifting task," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 16, no. 4, pp. 1650–1658, 2018.

[9] G. B. Moody, "Physionet: Research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, 2000.

[10] F. Setiawan and C. W. Lin, "Identification of neurodegenerative diseases based on vertical ground reaction force classification using time–frequency spectrogram and deep learning neural network features," *Brain Sciences*, vol. 11, no. 7, 2021.

[11] Q. Ye, Y. Xia, and Z. Yao, "Classification of gait patterns in patients with neurodegenerative disease using adaptive neuro-fuzzy inference system," *Computational and Mathematical Methods in Medicine*, vol. 2018, 2018.

[12] A. Zhao, L. Qi, J. Dong, and H. Yu, "Dual channel lstm based multi-feature extraction in gait for diagnosis of neurodegenerative diseases," *Knowledge-Based Systems*, vol. 145, pp. 91–97, 2018.

[13] E. Baratin, L. Sugavaneswaran, K. Umapathy, C. Ioana, and S. Krishnan, "Wavelet-based characterization of gait signal for neurological abnormalities," *Gait & Posture*, vol. 41, no. 2, pp. 634–639, 2015.

[14] M. A. A. Faisal *et al.*, "Nddnet: a deep learning model for predicting neurodegenerative diseases from gait pattern," *Applied Intelligence*, vol. 53, no. 17, 2023.

[15] C. W. Lin, T. C. Wen, and F. Setiawan, "Evaluation of vertical ground reaction forces pattern visualization in neurodegenerative diseases identification using deep learning and recurrence plot image feature extraction," *Sensors (Switzerland)*, vol. 20, no. 14, pp. 1–22, 2020.

[16] L. Fraiwan and O. Hassanin, "Computer-aided identification of degenerative neuromuscular diseases based on gait dynamics and ensemble decision tree classifiers," *PLoS One*, vol. 16, no. 6, 2021.

[17] H. Zhao, J. Xie, Y. Chen, J. Cao, W. H. Liao, and H. Cao, "Diagnosis of neurodegenerative diseases with a refined lempel–ziv complexity," *Cognitive Neurodynamics*, vol. 18, no. 3, 2024.

[18] N. E.-B. Hadeer El-ziaat and R. Moawad, "A hybrid deep learning approach for freezing of gait prediction in patients with parkinson's disease," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 13, no. 4, pp. 766–775, 2022.

[19] W. Zeng and C. Wang, "Classification of neurodegenerative diseases using gait dynamics via deterministic learning," *Information Sciences*, vol. 317, pp. 246–258, 2015.

[20] S. Amin and A. Singhal, "Identification and classification of neurodegenerative diseases using feature selection through pca-lda," in *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON)*, pp. 578–586, IEEE, 2017.

[21] N. Mehra and P. Mittal, "Design and implementation of ml model for early diagnosis of parkinson's disease using gait data analysis in iot environment," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 13, no. 7, pp. 578–586, 2022.

[22] C. W. Lin, T. C. Wen, and F. Setiawan, "Evaluation of vertical ground reaction forces pattern visualization in neurodegenerative diseases identification using deep learning and recurrence plot image feature extraction," *Sensors (Switzerland)*, vol. 20, pp. 1–22, Jul. 2020.

[23] C. B. Erdaş, E. Sumer, and S. Kibaroglu, "Neurodegenerative disease detection and severity prediction using deep learning approaches," *Biomed Signal Process Control*, vol. 70, p. 103069, Sep. 2021.

[24] Ç. B. Erdaş, E. Sümer, and S. Kibaroglu, "Neurodegenerative disease detection and severity prediction using deep learning approaches," *Biomed Signal Process Control*, vol. 70, p. 103069, Sep. 2021.

[25] Ç. B. Erdaş, E. Sümer, and S. Kibaroglu, "Neurodegenerative diseases detection and grading using gait dynamics," *Multimed Tools Appl*, vol. 82, pp. 22925–22942, Jun. 2023.

[26] PhysioNet, "Gait in neurodegenerative disease database." https://doi.org/10.13026/C27G6C, 2024. Accessed: Aug. 23, 2024.

[27] R. W. Bohannon and A. W. Andrews, "Normal walking speed: A descriptive meta-analysis," *Physiotherapy*, vol. 97, no. 3, pp. 182–189, 2011.

[28] E. F. Shair, S. A. Ahmad, A. R. Abdullah, M. H. Marhaban, and S. B. M. Tamrin, "Determining best window size for an improved gabor transform in emg signal analysis," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 16, no. 4, pp. 1650–1658, 2018.

[29] K. A. Rahman, E. F. Shair, and A. R. Abdullah, "Analysis of gait patterns in neurodegenerative disorders among older adults: A ground reaction force data approach," in *Proceedings of the 10th World Congress on Electrical Engineering and Computer Systems and Sciences (EECSS'24)*, 2024. doi: 10.11159/icbes24.131.

[30] S. Hong and E. Kim, "Sensitivity analysis of width representation for gait recognition," *The International Journal of Fuzzy Logic and Intelligent Systems*, vol. 16, no. 2, 2016.

[31] L. Fraiwan and O. Hassanin, "Computer-aided identification of degenerative neuromuscular diseases based on gait dynamics and ensemble decision tree classifiers," *PLOS ONE*, vol. 16, pp. 1–22, 06 2021.

How Predictable are Fitness Landscapes with Machine Learning? A Traveling Salesman Ruggedness Study

Mohammed El Amrani[1], Khaoula Bouanane[2], Youssef Benadada[3]
ANISSE Team-Faculty of Sciences, Mohammed V University in Rabat, Rabat, Morocco[1]
Smart Systems Laboratory, ENSIAS, Mohammed V University in Rabat, Rabat, Morocco[2,3]

***Abstract*—The notion of fitness landscape (FL) has shown promise in terms of optimization. In this paper we propose a machine learning (ML) prediction approach to quantify FL ruggedness by computing the entropy. The approach aims to build a model that could reveal information about the ruggedness of unseen instances. Its contribution is attractive in many cases like black-box optimization and in case we can rely on the information of small instances to discover the features of larger and time-consuming ones. The experiment consists in evaluating multiple ML models for the prediction of the ruggedness of the traveling salesman problem (TSP). The results show that ML can provide, for instances of a similar problem, acceptable predictions and that it can help to estimate ruggedness of large instances in that case. However, the inclusion of several features is necessary to have a more predictable landscape, especially when dealing with different TSP instances.**

Keywords*—Fitness landscape analysis; optimization algorithms; machine learning; landscape ruggedness; traveling salesman problem

I. Introduction

Over the last few decades, work on optimization algorithms has mainly focused on the algorithmic side, while the analysis of the problem itself has received relatively little attention. That is, most of the research published on this topic does not provide a sufficient analysis of the problem, why the algorithm works well and under which conditions [34]. Therefore, characterizing a problem should lead to a deeper understanding of it and better choices of algorithms and, hence, have an increased chance of producing better solutions. For this purpose, the concept of fitness landscape (FL) analysis was proposed with the aim of designing a generic approach that characterizes optimization problems. The concept was first introduced to illustrate the dynamics of biological evolutionary optimization [28], but it has also proved useful in understanding the behavior of optimization algorithms in both binary and continuous optimization problems. Thus, FL analysis is relevant both to predict the performance of algorithms and to improve their design. The interested reader is referred to [19] for more details on the transition from modeling real processes to modeling optimization problems. The issue of predictability of the FL was studied in biology (e.g. [4]) and in this paper, we aim to show a case in which it can be helpful for combinatorial optimization.

The integration of machine learning (ML) in operations research is increasingly crucial in light of recent advances [12], especially for the study of fitness landscapes in optimization problems such as the traveling salesman problem (TSP). ML can aid in characterizing ruggedness, thereby enhancing decision-making with predictive insights. This paper investigates the ruggedness of TSP landscapes using entropy as a key measure and introduces a novel ML-based approach for predictive analysis. The study addresses challenges in landscape characterization, extending traditional methods to unseen problem instances.

In general, the aim of FL analysis is to improve knowledge about the properties of a problem. Malan et al. [4] highlighted several characteristics of the FL as well as the measurements used for them. In particular, ruggedness is a property that often depends on the number and distribution of local optima and is related to the level of variation in fitness values in a FL. A number of measurements have been proposed to measure the landscape ruggedness. These measurements are the subject of the paper, and our aim is to deepen our understanding of this property, leveraging the great advances in data-driven approaches that have been carried out in recent years. More specifically, our approach consists of proposing a machine learning (ML)-based approach that extends existing methods for quantifying landscape ruggedness for unseen instances, in which its calculation can be time consuming.

This paper has three main objectives: (1) to evaluate the ability of ML to predict the robustness of TSP fitness landscapes, (2) to explore the role of entropy as a key metric in landscape analysis, and (3) to assess the generalization ability of ML to unseen problem instances. In pursuing these objectives, the paper makes the following contributions:

- It extends previous work by applying ML techniques to analyze TSP robustness, leveraging entropy to improve fitness landscape characterization.
- To the best of our knowledge, this is the first study to use ML to understand a TSP-specific fitness landscape feature, providing new insights into its structure and complexity.

The rest of paper is organized as follows. In Section II, we present the concept of ruggedness of the landscape and the measures proposed to quantify it. Section III is devoted to the description and discussion of the integration of ML in this problem. Both sections are interleaved with a brief literature review of the topic. Section IV presents the experiments.

Finally, the conclusion and the perspectives are depicted in Section V.

II. Background and Literature Review

The use of machine learning to understand the robustness of FL in combinatorial optimization problems, such as the TSP, is gaining increasing attention. A similar goal is explored in [30], where the authors examine the generalization ability of a machine learning model for problem reduction on the classical TSP. This paper shares a similar goal, aiming to explore the ability of ML to model landscape robustness, but distinguishes itself by focusing on entropy-based measures and their predictive potential.

A. Ruggedness of the Fitness Landscape

An important issue that may arise for FL analysis concerns to which extent we are able to generate generic FL measures. Although there are a number of independent measures such as the number of global optima, it is widely accepted that in many problems it is not possible to fully characterize the landscape using independent features [19]. Indeed, what is difficult to solve for a randomized hill climbing is not necessarily difficult for a genetic algorithm (GA) or when using a GA with different mutation operators. We can also note that many of the adopted measures depend on the definition of a neighborhood relation (e.g. the size of a basin of attraction). Based on this remark, the most well-known definition of a FL was proposed in [18] and consists of the triplet (X, N, ϕ), where:

- X is a set of candidate solutions (search space)
- N is a neighborhood relation
- $\phi\colon X \to \mathbb{R}$ is the fitness function

We can see from this definition that the FL not only depends on the problem but is also strongly related to the choice of an algorithm's operator. Therefore, as pointed out in [10], the concept of landscape could only be fully characterized in the context of an associated neighborhood structure and a specific operator. In what follows, we are interested in the ruggedness feature which also depends on the operator.

The issue of fitness ruggedness has been addressed in the literature from a number of perspectives. For instance, Vassilev et al. [10] defined three properties to characterize the FL, which are neutrality, smoothness and ruggedness. Most often the difficult and problematic case concerns the rugged landscape. This case is considered the most challenging and several works have been adopted to treat it (although neutral and smooth FLs have also been examined in the literature).

Concerning measurements, the auto-correlation function (ACF) proposed by Weinberger [11] is the most classic one for measuring it. The idea shown in that paper consists of performing random walks using a specific operator to study the correlation structure of a landscape. More precisely, the author, by considering the case of mutation as an operator, carried out random walks starting from a point chosen at random; then at each step, a bit of the vector chosen at random is flipped. We note that in this case, the ACF could be considered as a time series [35]. However, the ACF measure has been criticized in some works, which have pointed out its weakness in the characterization of the FL (e.g. [7]). Moreover, [16] pointed out that the importance of autocorrelation is often overplayed in fitness landscapes studies. Thus, the measure proposed in [32] to study ruggedness, which is described below, has become the most common over the last decade. We refer to [32] for a detailed description of the approach based on ruggedness.

It should also be noted that ruggedness has been primarily studied for continuous optimization problems [33], but was extended to combinatorial optimization [17]. Another measurement of ruggedness has been proposed, which is information content [23], and is beyond the scope of this paper.

The ruggedness has been studied for some optimization problems. The study in [16] investigated the similarities and difference between four combinatorial optimization problems, including the traveling salesman problem (TSP) and the quadratic assignment problem (QAP). In particular, their study showed that the four problems have similar ruggedness. Furthermore, Tayarani and Bennett [31] studied the impact of the ruggedness among other measures for the graph-coloring problem. In addition, Kallel et al. [10] reviewed some mathematical properties of the ruggedness.

Although ML has not been used yet to predict the ruggedness; an approach to predict it was proposed using time series analysis. In fact, Hordijk [35] proposed an extension of [11] using the Box–Jenkins method [1]. The author's idea consists of exploring the landscape structure by studying the corresponding autoregressive moving average (ARMA) model [1] which, according to the author, characterizes the landscape ruggedness much more precisely; its contribution consists in providing a stochastic model which could be used to make predictions for fitness values of distant points in the landscape.

We can notice, in this section, that entropy is an important measure used to characterize landscape ruggedness in certain works. In this paper, we aim to bridge the gap between them and advancements in data-driven approaches. Therefore, in Section III, we highlight works focused on understanding the TSP landscape and main approaches using ML for FL analysis, then introduce our approach and the adopted ML algorithms.

B. Understanding of the Traveling Salesman Problem Landscape

There are multiple papers which studied the FL of the TSP. For example, Boese et al. [2] asserted that the search space of TSP instances (under 2-opt moves) has a big-valley structure, in which local optima are clustered around one central global optimum. However, this statement has been questioned in multiple papers (e.g. [5]) and its generalization is also an issue of discussion [24]. Indeed, as noted in study [25], the TSP structure is not yet fully understood. On the other hand, ML was used for the TSP but not to analyze its landscape. We refer to study [21] for more information on the topic. In particular, in study [36], the authors investigated the generalization error of a ML model when the training and test instances have different instance characteristics, sizes or are from different TSP variants. The authors have a goal similar to our paper, namely to test the generalization capacity of ML algorithms to large instances, but using a different approach. Another analysis technique, notably the principal component analysis, was used in study [35] to analyse several features of

the TSP FL. The authors provided several conclusions which can mainly be summarized as follows: the difficulty of the instance (e.g. the number of local optima, the probability of reaching a global optimum) increases with the size of the problem and the level of the increase depends on the type of problem.

C. Machine Learning for Fitness Landscape Analysis

ML has been adopted in the context of FL in most cases with the aim of selecting the best algorithm based on the prediction of its performance, by adopting the information included in the computed features of the landscape. By analyzing the literature, we note that one of the first papers which paved the way for the emergence of such research is [15]. It introduced the concept of empirical hardness of optimization, showing how to build empirical hardness models which, given a new problem instance, predict an algorithm's runtime. Moreover, awareness of the importance of such approaches were reinforced with the appearance of the concept of exploratory landscape analysis (ELA) [13], shifting attention to this topic over the past decade.

However, we can notice that most of these researches are empirical-based and try to add features or to compute them in a less expensive way (e.g. [9]), without clearly contributing to the improvement of the problem understanding. The aim of these works is to build automatic tools for the selection or design of algorithms. Therefore, a number of tools have been proposed to extract FL features (e.g. Flacco package [14]).

In fact, we can see that such frameworks, even if useful in practice, cannot help to improve our knowledge on the problem which is of the utmost importance. That is, in most of these ML approaches, the authors try to use or define a large number of features, which could be in the hundreds, that may affect the performance of the algorithms. For instance, Mirshekarian et al. [22] proposed 380 features for the job-shop scheduling problem. But, many of the defined features might not be appropriate [37]. Hence, a typical phase is feature selection, which aims to select the most relevant ones. The ultimate goal of these approaches is to select the most suitable algorithms without providing an explanation for that selection. We note that we are aware that with the appearance of deep learning, the features could be computed automatically as investigated, for example, in [8]. However, deep learning is also unable to provide an explanation of the different selections.

The literature review elucidates the challenge of quantifying the ruggedness of fitness landscapes, emphasizing its dependence on problem characteristics and algorithmic operators. It surveys various methods for ruggedness characterization, with a focus on entropic measures, highlighting their significance in optimization studies. Moreover, it positions the current study as pioneering in utilizing machine learning to predict ruggedness, aiming to enhance understanding and inform algorithmic selection strategies.

Therefore, in this paper, our adoption of ML is different. In fact, we are interested in predicting the values of a specific and crucial feature (ruggedness). Although it is necessary to inclusion of several features for a better FL analysis, this work can be considered as a first and crucial work in this respect. To the best of our knowledge, despite its importance, this is the first investigation of the use of ML for predicting the ruggedness of FL. Ruggedness has been considered instead as a feature for most data-driven approaches for algorithm selection based on ELA. In the following, we describe our proposed approach.

III. The Proposed Approach

Our approach consists of two steps. The first concerns TSP optimization. In this step, the data necessary for the experiments is collected by running an optimization algorithm which consists of successive random walks. The number of iterations is fixed at 100. We choose (2-opt) as the neighborhood to implement the random walk for the TSP. Using this, we can calculate the entropy values of different problem instances as in Eq. (4). For each instance, we performed 30 executions of the random walk and computed the entropy for each instance and run. We are then able to obtain a sufficient sample size for the three experiments, which is 360, 300 and 240, respectively. As described below, in the first experiment, we generate random instances with different sizes. In the second, we analyze different TSPLIB instances while the third one is about a prediction for a specific TSPLIB instance family.

The second step consists of ML prediction. The target variable to be predicted (y) is the entropy. Two features (X) are used, which are the number of cities and the execution number, in addition to the instance family for TSPLIB instances. Based on the accuracy of predictions on unseen instances, we evaluate our approach. Below, we highlight the adopted ML algorithms and define the different steps of our approach.

Algorithm 1: Data Generation for ML Algorithms

```
Data: TSP instance
Random generation of distances for random instances
for k = 1 to 30 do
    for l = 1 to 100 do
        Perform a random walk
    Compute the entropy corresponding to execution k
Result: Entropy values in addition to TSP
  instances-related information
```

In Algorithm 1, we present the adopted ML algorithm and outline the key steps of our approach. Additionally, the flowchart (Fig. 1) provides a visual representation of the methodology, illustrating the process from data generation to ruggedness prediction for TSP instances using ML models.

In this paper, we have adopted a number of ML methods that yield satisfactory results for regression (continuous) problems such as gradient boosting (GR), random forest (RF) and support vector machines (SVM). These approaches, which are among the most adopted ones for regression problems, are the methods used to predict ruggedness. For more information about them, we refer to [20], [3] and [29], respectively.

IV. Experiments

In this section, a series of numerical experiments are carried out to evaluate the ML prediction of landscape ruggedness. The objective is twofold: first, we illustrate how ML can be adopted for this problem. Second, we seek to see what

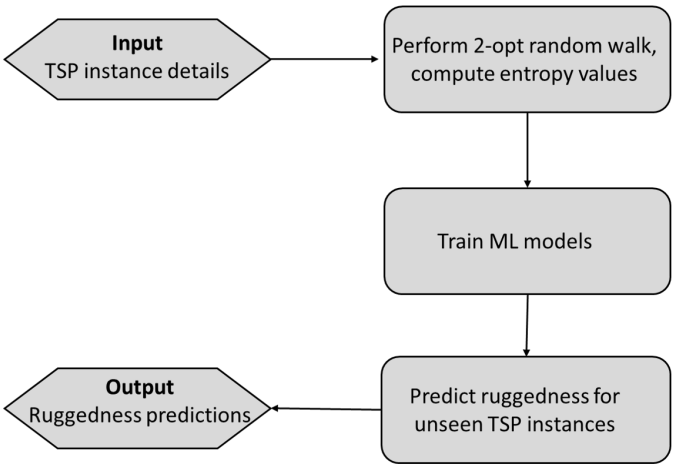


Fig. 1. Flowchart illustrating the proposed system for ruggedness prediction of TSP fitness landscapes.

this prediction can reveal about the structure of landscapes of unseen instances. More specifically, as mentioned above, our experiment first consists of running an algorithm, which is made up of consecutive randomized moves, on instances of classical combinatorial optimization problems while computing the ruggedness entropy value and second, of examining the ML predictive capacity of the entropy on these and other unseen instances by comparing the predicted values with the actual ones.

A. Experimentation Setup

In this paper, we consider the TSP, which is one of the most studied problems in combinatorial optimization. The Mlrose package [6] is adapted to implement the random walk with 2-opt neighborhood. First, we start the experiments with randomly generated TSP instances (the distances are generated randomly). Then, we experiment the approach on TSPLIB instances.

As mentioned earlier, the three ML algorithms chosen in this study are RF, GB and SVM. To implement them, we utilize the Scikit-learn library [27]. We optimize the parameters for RF and GB. Specifically, the number of trees in RF is set to 200, and the loss function to be optimized for GB is set to 'least absolute deviation' for better regression performance. For the other RF and GB parameters, we adopt the default parameters. Regarding SVM, the parameter γ (kernel coefficient) is automatically trained while the values of C (regularization factor) and ϵ are set to 1 and 0.01, respectively. We have chosen these values to enable a balance between overfitting and underfitting.

All experiments are conducted on a computer equipped with an Intel i7-9750H and 16GB of RAM. The measures adopted in this paper are: R^2 (coefficient of determination), mean absolute error (MAE) and mean square error (MSE).

To evaluate ML algorithms, there are two typical methods, notably training-test split or division and cross validation. In this paper, we have used the two methods depending on our objective. First, for random experiments and TSPLIB instances of a similar problem, we adopted the training-test split. More precisely, the first 75% of the data is used for training and 25% is used as test data. Our goal is to see if we can accurately predict the ruggedness of large TSP instances without needing to compute them and simply by examining small instances. Second, for different TSPLIB instances, we adopted 5-fold cross validation [36] to have a robust assessment of the ML predictions. In this case, the testing is performed across instances.

We have uploaded the used code for more details on our approach. The corresponding information is available in the Github repository (blinded for refereeing).

B. Random Instances

As a first experiment, we consider randomly generated TSP instances.

First, in our experiment, we choose nine instances for training and three for testing, depending on the number of cities. For training, we used the values (10, 20, 50, 100, 200, 500, 1000, 2000, 5000) and for testing, we adopted the values (6500, 8000 and 10000). As we have performed 30 runs for each instance, the training set size is 270 and the test set size is 90.

Second, for each of the three ML algorithms (RF and GB and SVM), we display in Table I a comparison of the prediction capabilities of the three algorithms in both training and test sets. That is, we show in Table I the R^2, MAE and MSE values obtained by comparing RF, GB and SVM predictions in training and test sets. The results of the test sets are those which are really necessary for evaluation but those of the training are given as additional information on the structure of the landscape.

TABLE I. COMPARISON OF ENTROPY PREDICTIONS FOR RANDOM TSP INSTANCES

		R2	MAE	MSE
RF	Test acc.	0.7108	0.0202	0.0006
	Training acc.	0.9347	0.0180	0.0005
GB	Test acc.	0.6907	0.0214	0.0007
	Training acc.	0.7337	0.0190	0.0005
SVM	Test acc.	0.2137	0.0380	0.0020
	Training acc.	0.0498	0.0322	0.0016
NN	Test acc.	0.1641	0.6570	0.1300
	Training acc.	0.9630	0.2500	0.1023

Both RF and GB gave acceptable results on the test set. SVM, as trained, seems not to be suitable for this case. The best results are given by RF. That is, RF provided the best results on the test sets, which are the needed for unseen predictions. We can conclude that RF is the most suitable for this case study, with the proposed parameters.

Third, to give a better overview of the RF predictions, we depict in Fig. 2 and Fig. 3 the prediction given by RF in both test and training sets along with the real values.

We can notice from the Fig. 2 and Fig. 3 that the entropies are overall slightly positively correlated with the number of cities. In other words, the entropy in general increases slightly with the number of cities. This can be seen as the values in the

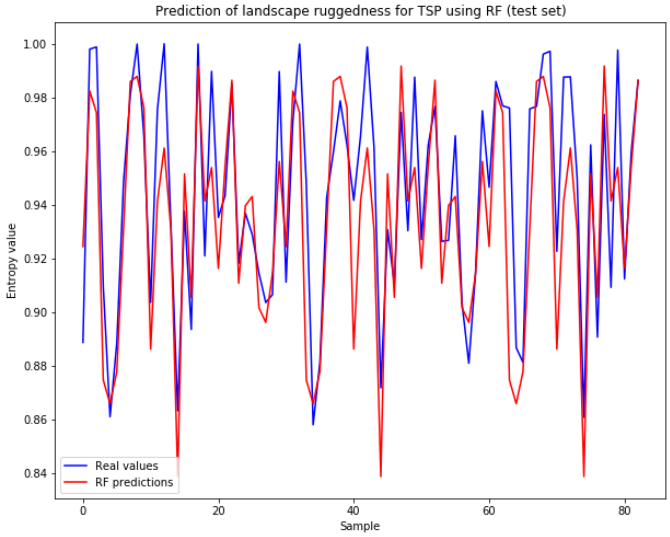


Fig. 2. RF prediction on the test set.

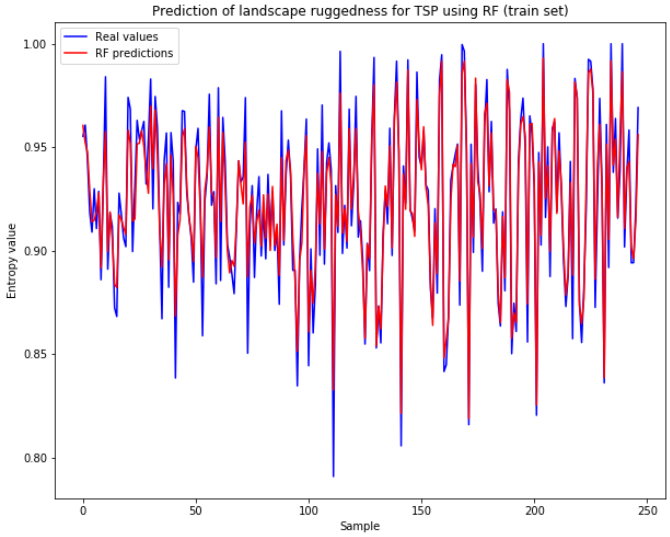


Fig. 3. RF prediction on the training set.

test sets are slightly, which corresponds to higher cities, are slightly higher than of the training set and there is a very weak increasing trend of the value in function of the sample (and then of the cities). Although ML prediction is not extremely accurate, it can detect patterns in the data and provide a fairly good ruggedness prediction.

C. Instances of Different TSPLIB Problems

After looking at the randomly generated TSP instances (Table II), we aim to study several TSPLIB instances.[1] Below we show the names of the instances with the corresponding number of cities.

Our goal in this part is to see how well we can predict ruggedness for problem instances, using the information from other instances, regardless of the instance family. To answer this issue, cross validation is more appropriate than training-test split. In this experiment, we conducted the 5-fold cross validation. In total, we get 300 sample and we use them for this purpose. In Table III, we display the results of the mean of the R^2, negative MAE[2] and MSE factors, which are used in the 5-fold cross validation.

TABLE II. TSPLIB INSTANCES

Instance	Number of cities
Bays	29
Berlin	52
Brazil	58
Eil	51, 76, 101
Ch	130, 150
TSP	225
Fl	417

TABLE III. COMPARISON OF ENTROPY PREDICTIONS FOR INSTANCES OF DIFFERENT TSPLIB PROBLEM INSTANCES

	R^2	Negative MAE	Negative MSE
RF	-0.8797	-0.0385	-0.1525
GB	-0.7478	-0.0352	-0.1422
SVM	-0.7514	-0.0550	-0.2057
NN	0.2660	-15877.1021	-102.0534

It is clear from Table III (e.g. the R^2 values) that the results are not good and the algorithms are not able to provide acceptable predictions. The reason for these unsatisfactory results compared to the previous case is due to the fact that ruggedness appears unpredictable if combined with other factors. It is necessary to combine several features to expect to have an accurate prediction. We note that the results are also not satisfactory when adopting the training-test split in the same way as in the first study.

D. Instances of a Similar TSPLIB Problem

In this section, we focus specifically on instances of a particular TSPLIB instance family and examine the evolution of ruggedness as a function of only the number of cities and, importantly, our ability to predict large unseen instances. More precisely, we consider the instance studied in [26]. In this case study, we consider the instances with cities of 76, 107, 124, 136, 144 and 152 as a training test (75%). The instances with 226 and 264 (25%) are the test set. All instances are executed 30 times. As mentioned before, the reason is that we aim to see if we can predict the ruggedness of instances with higher cities by simply getting information from lower cities, and cross validation is not needed in this case.

We can notice from Table IV, that GB gave the best results in the test set. (We note that the RF predictions are better in the training set but the GB results are more promising in our context.) In Fig. 4 and Fig. 5, we provide the prediction given by GB in the test and training sets with the actual values.

We can notice from Fig. 4 and Fig. 5 that entropy does not globally have a very significant variation in function of the

[1]The instances can be found in http://elib.zib.de/pub/mp-testdata/tsp/tsplib/tsp/index.html

[2]For cross validation, scikit-learn uses negative MAE and MSE. More information about them can be found in https://community.dataquest.io/t/why-is-scoring-equal-to-neg-mean-squared-error/547283

TABLE IV. COMPARISON OF ENTROPY PREDICTIONS FOR INSTANCES OF A SIMILAR TSPLIB PROBLEM

		R2	MAE	MSE
RF	Test acc.	0.3088	0.0220	0.0015
	Training acc.	0.7829	0.0100	0.0002
GB	Test acc.	0.2102	0.0250	0.0020
	Training acc.	0.4651	0.0150	0.0006
SVM	Test acc.	-0.0078	0.0174	0.0009
	Training acc.	-0.0092	0.0203	0.0011
NN	Test acc.	0.1641	0.1150	0.1314
	Training acc.	0.9630	0.9066	0.2023

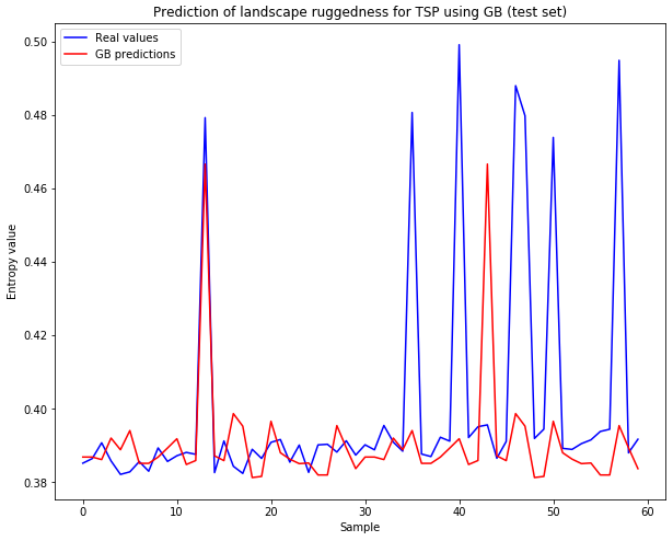


Fig. 4. GB prediction on the test set.

number of cities. The GB predictions are in general consistent with the actual values, and it can then be considered that ML can be useful in this situation.

The results for the three cases can be summarized as follows:

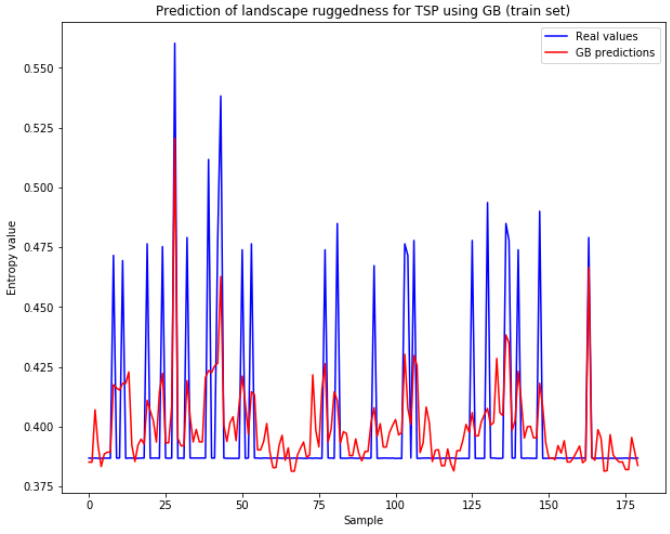


Fig. 5. GB prediction on the training set.

- For random TSP instances, the computed ruggedness factor seems to increase globally. ML can detect this pattern and then provide satisfactory predictions.
- ML algorithms failed to detect patterns in different TSPLIB instances. The reason seems that other factors than size must be included to be able to use ML in this case.
- For a specific TSPLIB instance, there is no significant increase in the factor. ML can also be useful in this case by giving a satisfactory prediction for the same unseen instance with a higher number of cities (although the increase in the size is not the same as for the first experiment).

V. CONCLUSION

Fitness landscape analysis has shown promise for better understanding the functionality of optimization algorithms and reducing their unpredictability. In this paper, we proposed a new ML design to predict the FL ruggedness of unseen large instances based on the values of historical small instances. This work, to the best of our knowledge, is the first attempt to take advantage of recent advances in data-driven approaches to analyze and estimate a feature of FL.

This work can be considered as the first step aimed at predicting the characteristics of problem instances in which their calculation is time-consuming. A practical exploitation of any optimization problem is to run the algorithms in the smallest instances, build the machine learning model, and then predict the features on the very large instances. Estimating the characteristics of a very large instance without needing to run the algorithms can be useful, e.g., to choose the appropriate algorithm to solve these instances.

In this paper, the experiment consists in evaluating the predictive capacity of 3 ML algorithms. The data sets in the three experiments are collected by running the 2-opt random walk 30 times on several instances. In our case, random forest was the best suited for the random TSP instances. For the different TSPLIB instances, no algorithm could find satisfactory results. When focusing on a specific TSPLIB problem, the results found by the gradient boosting are the best. We can conclude that machine learning prediction can be useful when we have identical or similar problem instances with difference mainly in number of cities. The contributions are summarized as follows:

- Our study reveals that machine learning models perform better on random TSP instances than on specific TSPLIB instances. This finding suggests that ML can effectively capture patterns in less complex, more uniform problem structures.
- The results highlight the importance of incorporating additional problem-specific features to improve prediction accuracy for TSP instances of different families. Our work lays the groundwork for future studies to explore more sophisticated models and feature sets, advancing the field's understanding of fitness landscape predictability.

These results are consistent with established findings, demonstrating the correlation between robustness and performance, as well as the difference of ML performance depending on the nature of TSP instances. This paper builds on this knowledge by providing significant new findings and results.

As the Concorde solver is able to easily solve many TSP instances of quite large size to optimality, another approach that may be investigated in the study of ruggedness is target analysis, i.e., giving an optimal solution and checking to which extent, possibly using ML, this can be found from a given starting solution and allowing to learn from the path between those solutions. Finally, even if the practical contribution is not well apparent in the above-mentioned data instances, this work can be considered as a first step that can be extended to much larger instances and problems in which the calculation of the factor can be very time-consuming. The exploitation of information of small instances can be much helpful. Further research should then focus on this issue. Indeed, it is of utmost importance to concretely show the practical impact of our approach (e.g. in black-box optimization). Moreover, it is important to further study the practical application of ML by finding the needed sample (number of instances) to have an accurate prediction on the different problem instances. Further research can also focus on applying the approach to other similar problems such as the family TSP or to integrate into other types of metaheuristics. The reason for the poor results seems to be that the three ruggedness prediction models considered are known to yield satisfactory results in continuous domains. In fact, the advancement in ML prediction is an outstanding area of research that could hold promise in estimating the FL features of unresolved instances and studying the links between these features.

The results of this study highlight the significant impact of robustness and landscape structure on algorithm performance. Building on these insights, future research could focus on designing ML-based adaptive optimization algorithms that can dynamically adjust strategies based on landscape features. Furthermore, leveraging ML to efficiently manage large-scale TSP instances could advance the field, especially in real-world applications requiring scalable solutions.

REFERENCES

[1] Random Forests. In Claude Sammut and Geoffrey I. Webb, editors, *Encyclopedia of Machine Learning and Data Mining*, pages 1054–1054. Springer US, Boston, MA, 2017.

[2] Kenneth D. Boese, Andrew B. Kahng, and Sudhakar Muddu. A new adaptive multi-start technique for combinatorial global optimizations. *Operations Research Letters*, 16(2):101–113, September 1994.

[3] Leo Breiman. Random forests. *Machine Learning*, 45(1):5–32, 2001.

[4] J. Arjan G. M. de Visser and Joachim Krug. Empirical fitness landscapes and the predictability of evolution. *Nature Reviews Genetics*, 15(7):480–490, July 2014. Publisher: Nature Publishing Group.

[5] D R Hains, L D Whitley, and A E Howe. Revisiting the big valley search space structure in the TSP. *Journal of the Operational Research Society*, 62(2):305–312, February 2011. Publisher: Taylor & Francis _eprint: https://doi.org/10.1057/jors.2010.116.

[6] Dr Genevieve Hayes. gkhayes/mlrose, March 2024. original-date: 2018-10-20T19:48:34Z.

[7] Wim Hordijk. A Measure of Landscapes. *Evolutionary Computation*, 4(4):335–360, December 1996.

[8] André Hottung, Shunji Tanaka, and Kevin Tierney. Deep Learning Assisted Heuristic Tree Search for the Container Pre-marshalling Problem. *Computers & Operations Research*, September 2019.

[9] Frank Hutter, Lin Xu, Holger H. Hoos, and Kevin Leyton-Brown. Algorithm runtime prediction: Methods & evaluation. *Artificial Intelligence*, 206:79–111, January 2014.

[10] T Jones. *Evolutionary algorithms, fitness landscapes and search.* Thesis, The University of New Mexico, 1995.

[11] L. Kallel, B. Naudts, and C. R. Reeves. Properties of Fitness Functions and Search Landscapes. In Leila Kallel, Bart Naudts, and Alex Rogers, editors, *Theoretical Aspects of Evolutionary Computing*, pages 175–206. Springer, Berlin, Heidelberg, 2001.

[12] Maryam Karimi-Mamaghan, Mehrdad Mohammadi, Patrick Meyer, Amir Mohammad Karimi-Mamaghan, and El-Ghazali Talbi. Machine learning at the service of meta-heuristics for solving combinatorial optimization problems: A state-of-the-art. *European Journal of Operational Research*, 296(2):393–422, January 2022.

[13] Pascal Kerschke and Mike Preuss. Exploratory landscape analysis. In *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, GECCO '19, pages 1137–1155, New York, NY, USA, July 2019. Association for Computing Machinery.

[14] Pascal Kerschke and Heike Trautmann. Comprehensive Feature-Based Landscape Analysis of Continuous and Constrained Optimization Problems Using the R-Package Flacco. In Nadja Bauer, Katja Ickstadt, Karsten Lübke, Gero Szepannek, Heike Trautmann, and Maurizio Vichi, editors, *Applications in Statistical Computing: From Music Data Analysis to Industrial Quality Improvement*, pages 93–123. Springer International Publishing, Cham, 2019.

[15] Kevin Leyton-Brown, Nudelman Eugene, and Yoav Shoham. Empirical Hardness Models for Combinatorial Auctions. In Peter Cramton, Yoav Shoham, and Richard Steinberg, editors, *Combinatorial Auctions*, page 0. The MIT Press, December 2005.

[16] Arnaud Liefooghe, Fabio Daolio, Sébastien Verel, Bilel Derbel, Hernán Aguirre, and Kiyoshi Tanaka. Landscape-Aware Performance Prediction for Evolutionary Multiobjective Optimization. *IEEE Transactions on Evolutionary Computation*, 24(6):1063–1077, December 2020. Conference Name: IEEE Transactions on Evolutionary Computation.

[17] Katherine M. Malan and Andries P. Engelbrecht. Quantifying ruggedness of continuous landscapes using entropy. In *2009 IEEE Congress on Evolutionary Computation*, pages 1440–1447, May 2009. ISSN: 1941-0026.

[18] Katherine M. Malan and Andries P. Engelbrecht. A survey of techniques for characterising fitness landscapes and some possible ways forward. *Information Sciences*, 241:148–163, August 2013.

[19] Katherine M. Malan and Andries P. Engelbrecht. Fitness Landscape Analysis for Metaheuristic Performance Prediction. In Hendrik Richter and Andries Engelbrecht, editors, *Recent Advances in the Theory and Application of Fitness Landscapes*, pages 103–132. Springer, Berlin, Heidelberg, 2014.

[20] Llew Mason, Jonathan Baxter, Peter Bartlett, and Marcus Frean. Boosting algorithms as gradient descent. *Advances in neural information processing systems*, 12, 1999.

[21] Umberto Mele, Luca Maria Gambardella, and Roberto Montemanni. Machine Learning Approaches for the Traveling Salesman Problem: A Survey. pages 182–186, January 2021.

[22] Sadegh Mirshekarian and Dušan N. Šormaz. Correlation of job-shop scheduling problem features with scheduling efficiency. *Expert Systems with Applications*, 62:131–147, November 2016.

[23] Mario A. Muñoz, Michael Kirley, and Saman K. Halgamuge. Exploratory Landscape Analysis of Continuous Space Optimization Problems Using Information Content. *IEEE Transactions on Evolutionary Computation*, 19(1):74–87, February 2015. Conference Name: IEEE Transactions on Evolutionary Computation.

[24] Gabriela Ochoa and Nadarajen Veerapen. Additional Dimensions to the Study of Funnels in Combinatorial Landscapes. In *Proceedings of the Genetic and Evolutionary Computation Conference 2016*, GECCO '16, pages 373–380, New York, NY, USA, July 2016. Association for Computing Machinery.

[25] Gabriela Ochoa and Nadarajen Veerapen. Mapping the global structure of TSP fitness landscapes. *Journal of Heuristics*, 24(3):265–294, June 2018.

[26] Manfred Padberg and Giovanni Rinaldi. Optimization of a 532-city symmetric traveling salesman problem by branch and cut. *Operations Research Letters*, 9(5):353, September 1990.

[27] Fabian Pedregosa, Gaël Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Vincent Dubourg, Jake Vanderplas, Alexandre Passos, David Cournapeau, Matthieu Brucher, Matthieu Perrot, and Édouard Duchesnay. Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*, 12(85):2825–2830, 2011.

[28] Jr. Skipper, Robert A. The Heuristic Role of Sewall Wright's 1932 Adaptive Landscape Diagram. *Philosophy of Science*, 71(5):1176–1188, 2004. Publisher: [The University of Chicago Press, Philosophy of Science Association].

[29] Alex J. Smola and Bernhard Schölkopf. A tutorial on support vector regression. *Statistics and Computing*, 14(3):199–222, August 2004.

[30] Yuan Sun, Andreas Ernst, Xiaodong Li, and Jake Weiner. Generalization of machine learning for problem reduction: a case study on travelling salesman problems. *OR Spectrum*, 43(3):607–633, September 2021.

[31] M. H. Tayarani-N. and Adam Prügel-Bennett. Anatomy of the fitness landscape for dense graph-colouring problem. *Swarm and Evolutionary Computation*, 22:47–65, June 2015.

[32] Mohammad-H. Tayarani-N. and Adam Prügel-Bennett. On the Landscape of Combinatorial Optimization Problems. *IEEE Transactions on Evolutionary Computation*, 18(3):420–434, June 2014. Conference Name: IEEE Transactions on Evolutionary Computation.

[33] Vesselin K. Vassilev, Terence C. Fogarty, and Julian F. Miller. Smoothness, Ruggedness and Neutrality of Fitness Landscapes: from Theory to Application. In Ashish Ghosh and Shigeyoshi Tsutsui, editors, *Advances in Evolutionary Computing: Theory and Applications*, pages 3–44. Springer, Berlin, Heidelberg, 2003.

[34] Jean-Paul Watson. An Introduction to Fitness Landscape Analysis and Cost Models for Local Search. In Michel Gendreau and Jean-Yves Potvin, editors, *Handbook of Metaheuristics*, pages 599–623. Springer US, Boston, MA, 2010.

[35] E. Weinberger. Correlated and uncorrelated fitness landscapes and how to tell the difference. *Biological Cybernetics*, 63(5):325–336, September 1990.

[36] Tzu-Tsung Wong and Po-Yang Yeh. Reliable Accuracy Estimates from k-Fold Cross Validation. *IEEE Transactions on Knowledge and Data Engineering*, 32(8):1586–1594, August 2020. Conference Name: IEEE Transactions on Knowledge and Data Engineering.

[37] Urban Škvorc, Tome Eftimov, and Peter Korošec. Understanding the problem space in single-objective numerical optimization using exploratory landscape analysis. *Applied Soft Computing*, 90:106138, May 2020.

Analyzing EEG Patterns in Functional Food Consumption: The Role of PCA in Decision-Making Processes

Mauro Daniel Castillo Pérez[1], Jesús Jaime Moreno Escobar[2], Verónica de Jesús Pérez Franco[3],
Ana Lilia Coria Paéz[4], Oswaldo Morales Matamoros[5]
Escuela Superior de Ingeniería Mecánica y Eléctrica, Zacatenco, Instituto Politécnico Nacional, México[1]
Centro de Investigación en Computación, Instituto Politécnico Nacional, México[2,5]
Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas, Instituto Politécnico Nacional, México[3]
Escuela Superior de Comercio y Admistración, Tepepan, Instituto Politécnico Nacional, México[4]

***Abstract*—The impact of obesity and diabetes are two central reasons for the high rate of developing cardiovascular diseases in this country, which is largely due to their ultra-processed, diet-rich foods. Supervised Learning for Decision Making: A Case Study of Functional Food Taste Perceptions In this experiment, we trained ordinary consumers to estimate the taste preferences of a unique group from which no ratings were available(11) and established that decision making can be performed through supervision. A deep learning neural network architecture according to the present disclosure is designed to model the decision-making behavior of consumers consuming functional products. The efficiency of the model can be increased upto 1.23% making use of proper values for the rest of the hyperparameters as explained in experiments carried out where we set the optimal configuration so that nurturing it gives the best results.**

***Keywords*—EEG analysis; functional foods; decision-making; deep learning; Principal Component Analysis (PCA)**

I. Introduction

By 2023, decision-making has become essential and complex due to the vast amount of information and uncertainty present today. Additionally, various factors such as the fear of failure can negatively affect decision-making. This also impacts health, specifically obesity and overweight, which are linked to dietary decisions. In Latin America, obesity has increased by 55%, and in Mexico, it affects 76.4% of adults and 35.6% of children between the ages of 5 and 11, [1].

Some of these factors could be:

- Deceptive Advertising: Unhealthy food products are promoted as healthy, making informed decisions difficult (for example, whole grain bread labeled as "light"), [2].
- Social Pressure: The discrediting of people with obesity influences their dietary choices and self-image, sometimes leading them to consume unhealthy foods to cope with stress, [3].

Decision-making affects not only at a personal level but also in governmental and corporate spheres, where incorrect decisions can cause significant damage.

Some examples where a wrong decision could have an impact are:

- Policy: Lack of transparency and corruption can have devastating consequences.
- Environment: Disputes and short-term economic decisions harm the planet.
- Social Justice: Decisions about economic and social policies can influence inequality.
- Education: Decisions about curricula and funding affect the quality of education.

Principal Component Analysis (PCA) and Artificial Intelligence (AI), including Deep Convolutional Neural Networks (DCNN), [4], can help analyze complex data and improve decision-making. These technologies can identify patterns in health data and predict diseases by organizing large datasets and providing more accurate and predictive analyses. In the context of overweight and obesity, they can enhance dietary decision-making by providing a deeper understanding of the factors influencing these conditions. On the other hand, four main deficiencies of PCA can be stated: i) Assumes linear relationships: PCA can only capture linear relationships between variables. If the relationships between the data are nonlinear, PCA will not be able to model them adequately; ii) Loss of interpretability: Although PCA reduces dimensionality, the principal components do not have a clear interpretation in terms of the original variables, which can make the results difficult to interpret; iii) Sensitivity to noise: If the data contains noise, it can influence the computation of the principal components, affecting the results; and iv) Computationally expensive for large datasets: For very large or high-dimensional datasets, the computation of the covariance matrix and its significant vectors can be computationally expensive.

The design of an intelligent system using deep learning networks makes it possible to classify a person's like/dislike choices with an efficiency of 80%.

This work is based on EEG Analysis, a technique that uses electroencephalographic signals to study brain activity, being useful in the analysis of brain patterns.

The analysis of EEG is important for various reasons, primarily due to its ability to provide information about the brain's electrical activity, allowing the study and understanding of a variety of cognitive, emotional, and physiological processes. It also has several key study reasons, such as:

- Study of brain activity in real time: EEG provides a real-time window into brain activity, allowing the direct observation of changes in brain wave patterns related to different mental states, such as attention, relaxation, sleep, or decision-making [5].
- Study of decision-making: EEG is also used to investigate how the brain makes decisions by detecting neuronal responses to external stimuli [6].
- Interaction between emotions and decisions: EEG is used to measure brain activity, providing information about how emotions influence decision-making [7].

It also incorporates the use of Functional Foods, which are foods that, in addition to their nutritional value, offer additional health benefits, such as disease prevention or improving a person's health. The philosophy of Decision-Making is applied, which is a cognitive process through which a person evaluates options and selects the most appropriate one to make an informed decision. This process is complemented by the tool of Deep Learning, a branch of artificial intelligence based on artificial neural networks that allows analyzing complex data, identifying patterns, and making accurate predictions and the tool Principal Component Analysis (PCA) is a statistical technique that reduces the dimensionality of complex data sets while preserving the most relevant characteristics. The combination of these concepts enables efficient classification in decision-making.

This work consists of a total of five sections, starting with the introduction, which provides the context of the work. Similarly, related work is given in Section II, presenting an analysis of studies directly related to the proposed one. This is followed by the theoretical framework in Section III, which explains the mathematical and theoretical foundations used in the work. The methodology in Section IV explains how the network operates, leading to the experiment in Section V, where the functionality of the proposed method is tested, and finally, the conclusions in Section VI is presented, where the obtained results are discussed.

II. Related Works

A search was conducted in the databases of IEEE Xplore and Hindawi; this research was carried out with the purpose of finding works that have a similar relationship with the approach followed in the preparation of this document. A total of 13 works were found, which relate to the fundamental topics for the development of this study. From these 13 works, 4 works were derived, whose focus provides a greater contribution to the research.

Fig. 1 is a PRISMA flow diagram, which includes the systematic review of citations, where less relevant works to the objective are discarded, and where these citations were searched in the aforementioned search sites. In this way, 13 articles were found, for example, there is one titled Development of AI model to analyze customer behavior by decision

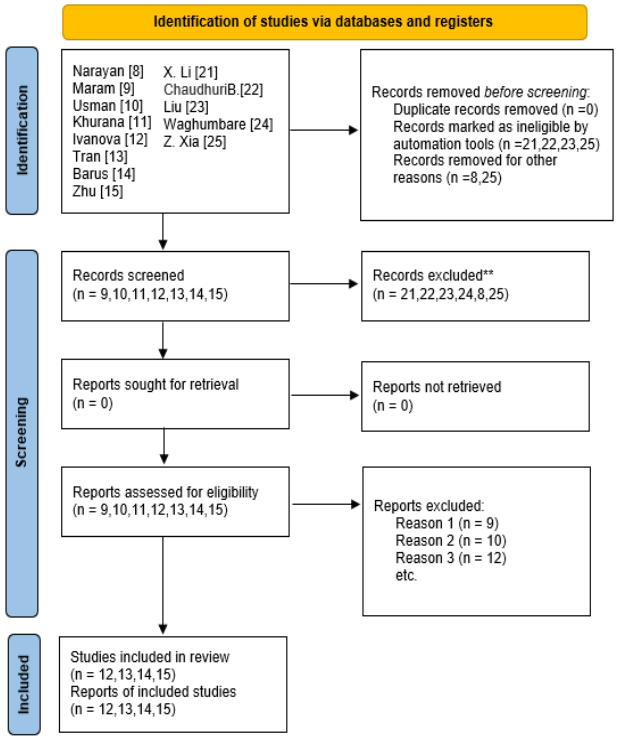


Fig. 1. Identification of related works via research databases such as IEEE Xplore and Hindawi.

making system, written by L. Rong, Y. Ding, M. Wang, M.S. Hossain et al. in [8], which discusses a model that uses artificial intelligence for facial recognition and deep neural networks to analyze customer behavior. It investigates how the consumer's mental process influences the purchasing process. Another example is the paper titled Analysis of Consumer Coffee Brand Preferences Using Brain-Computer Interface and Deep Learning, written by M. Maram, M.A. Khalil, K. George et al. in [9]. This work focuses on the acquisition and analysis of EEG signals using a wireless device, where tools like MATLAB and Python in Google Colab are used to design an interface aimed at identifying coffee brand preferences through brain activity. A different case is the paper titled A Deep Learning Model for Classification of EEG written by S.M. Usman, S.M.A. Shah, O.C. Edo, J. Emakhu et al. in [10], where the study focuses on the use of EEG signals to classify product preferences by observing their packaging. Brain signals from 25 volunteers were monitored while they viewed different packages, using data analysis tools and machine learning models to automatically identify consumer preferences. Finally, there is the paper titled A Survey on Neuromarketing Using EEG Signals, written by V. Khurana, M. Gahalawat, P. Kumar, P.P. Roy, D.P. Dogra, E. Scheme, M. Soleymani et al. in [11], which explains how neuroscience uses tools like EEG. This technique is used to analyze brain activity during the consumer decision-making process. Electrodes are employed to measure brain waves, and analysis software is used to interpret the collected data, thus enabling an understanding of consumer preferences.

Once some relevant works are presented, the following section will present those that are most directly related to this

work, fulfilling similar objectives and/or analyses, these are:

i) *Motor Learning and Decision Making in Volatile Environment in Bipolar Disorder*,
ii) *On a Development of Sparse PCA Method for Face Recognition Problem*,
iii)*Prediction Using Support Vector Machine and Logistic Regression Model with Combination of PCA and SMOTE*,
iv)*Continuous Speech Recognition Based on DCNN-LSTM*.

A. Motor Learning and Decision Making in Volatile Environment in Bipolar Disorder

This study by M. Ivanova and M. H. Ruiz in [12] investigates how motor learning and decision-making in a volatile environment affect individuals with bipolar disorder. The hypothesis is that disruptions in learning in volatile environments may play a crucial role in the development and manifestation of bipolar disorder. The study compares patients with bipolar disorder to a control group of healthy individuals, using psychological tests and experimental tasks that simulate conditions of uncertainty. A neural network model is employed to analyze the data and seek patterns that relate motor learning to neurophysiological markers, aiming to improve the diagnosis and treatment of bipolar disorder. The diagram of this study can be seen in Fig. 2.

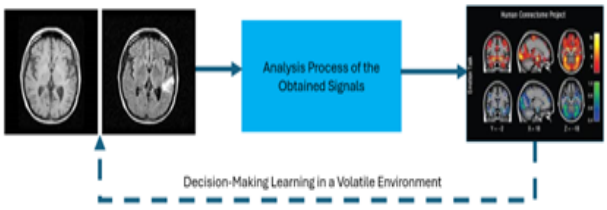


Fig. 2. Model diagram, motor learning and decision making in a volatile environment in bipolar disorder.

B. On a Development of Sparse PCA Method for Face Recognition Problem

This work by L. Tran and colleagues in [13], proposes an innovative semi-supervised learning method based on the unnormalized p-Laplacian graph for speech recognition. The method aims to improve the accuracy and performance of speech recognition through machine learning techniques and signal processing. A semi-supervised learning model is constructed using voice samples, and experiments are conducted to evaluate its effectiveness compared to other methods, achieving significant improvements in accuracy and performance, Fig. 3.

C. Prediction Using Support Vector Machine and Logistic Regression Model with Combination of PCA and SMOTE

This study conducted by O. P. Barus and colleagues in [14], focuses on the use of machine learning for liver disease prediction and facial recognition. In the first study, Logistic Regression (LR) and Support Vector Machine (SVM) algorithms are employed, along with PCA and SMOTE, to improve early and accurate detection of liver diseases. In the second study, advanced versions of sparse PCA are used to improve the accuracy of facial recognition, applying methods such as

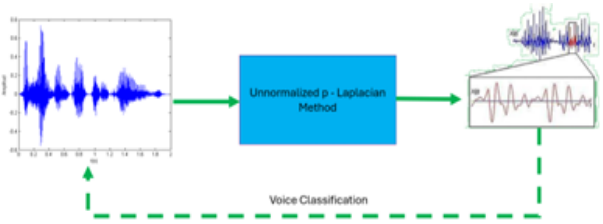


Fig. 3. Model diagram, on a development of sparse PCA method for face recognition problem.

Proximal Gradient Sparse PCA and Fast Iterative Shrinkage-Thresholding Algorithm Sparse PCA. Fig. 4 shows both studies combing clinical and facial data to achieve accurate and effective predictions.

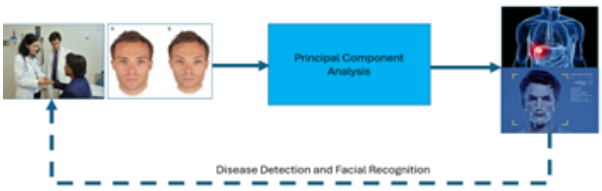


Fig. 4. Model diagram, prediction using support vector machine and logistic regression model with combination of PCA and SMOTE.

D. Continuous Speech Recognition Based on DCNN-LSTM

This work by Y. Zhu and Q. Zeng in [15], compares different acoustic features and network structures in automatic speech recognition. Using Mandarin datasets (THCHS-30 and ST-CMDS), the study extracts acoustic features such as the spectrogram and Mel cepstral coefficient (MFCC). Deep Convolutional Neural Networks (DCNN) and Long Short-Term Memory Neural Networks (LSTM) are evaluated, concluding that the spectrogram is the most effective feature and that LSTM networks significantly improve speech recognition accuracy compared to DCNNs. Fig. 5 depicts the combination of DCNN and LSTM results in a remarkable improvement in speech-to-text conversion.

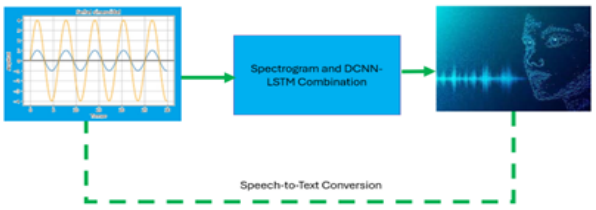


Fig. 5. Model diagram, continuous speech recognition based on DCNN-LSTM.

III. Theoretical Framework

A. Principal Component Analysis PCA

Principal Component Analysis (PCA) is a fundamental statistical technique used in multivariate data analysis. Its

objective is to transform a set of P correlated data into a new set of fewer and uncorrelated variables. PCA reduces the complexity of the original data, facilitating its interpretation and analysis, and allows for the identification of hidden patterns and structures within the data. The PCA method takes data described by k variables in an $n \times k$ matrix X, representing n subjects in a k-dimensional space, Eq. (1):

$$\mathbf{X} = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1k} \\ x_{21} & x_{22} & \dots & x_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nk} \end{bmatrix} \quad (1)$$

The new variables, or principal components, are generated through linear combinations of the original variables. The aim is for the first principal component to contain the maximum possible variance, while restricting the magnitude of its elements to avoid excessive variance. This process is repeated to find the subsequent principal components, ensuring that each new component is uncorrelated with the previous ones.

B. Electroencephalogram (EEG)

The Electroencephalogram (EEG) is a study that detects and records the electrical activity of the brain under different conditions, including the basal state and through activation methods such as hyperventilation and photostimulation. The electrical signal collected is amplified and represented in the form of lines that show the activity of various brain areas over time, a representation of this can be seen in the Fig. 6.

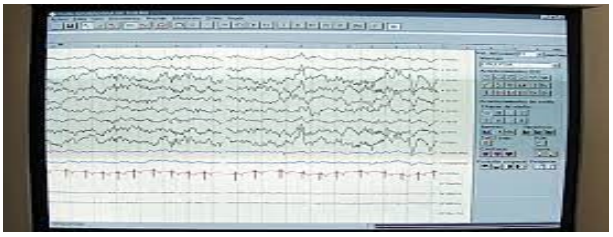


Fig. 6. Brain electrical signal.

The EEG monitors the electrical functioning of the brain and can detect both global alterations and changes in specific areas. It is useful for identifying various lesions such as tumors, hemorrhages, encephalitis, and trauma, Fig. 7.

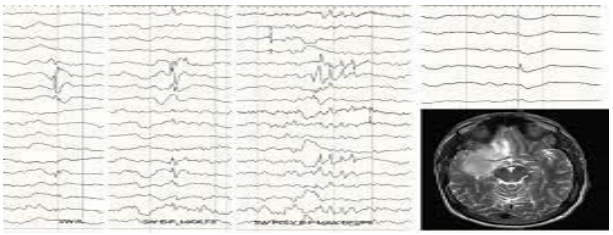


Fig. 7. EEG of a brain tumor.

C. Deep Learning Neural Networks

1) VGG16 Neural Network: The VGG16, Fig. 8, neural network is a deep convolutional network architecture developed by the Visual Geometry Group (VGG) at the University of Oxford. Used in computer vision tasks such as image recognition and classification, VGG16 is characterized by its 16-layer depth, divided into 13 convolutional layers and 3 fully connected layers.

a) Main features:

- Convolution Filters: Uses 3x3 filters with a fixed depth of 64 and 128 in its initial layers, followed by additional layers with more filters.
- Pooling Layers: Employs pooling layers with a 2x2 window to reduce dimensionality and extract prominent features.

The training of VGG16 follows the standard supervised learning approach, using labeled datasets and adjusting the network weights through backpropagation and optimization with stochastic gradient descent (SGD).

This is a complex architecture due to the fact that it consists of 16 training layers, where 13 are convolutional layers, using a 3x3 matrix for feature extraction, and 3 fully connected layers at the end, to reduce the dimensionality it has max pooling layers. At the input, it receives images of 224x224 pixels with three channels (RGB), and in the end, it has a softmax layer that allows for image classification.

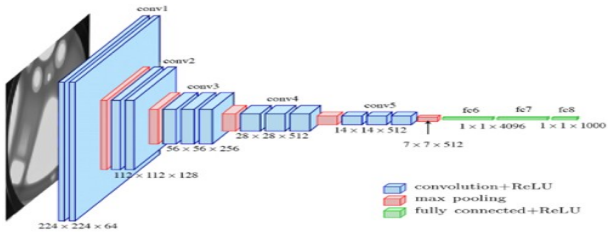


Fig. 8. VGG16 neural network architecture.

2) Inception Neural Network: The Inception neural network was created by Google Brain in 2014 to address the challenges of image classification in large and complex datasets. Its modular structure uses multiple convolutional layers and Inception modules, allowing the network to learn and extract features at different spatial scales within an image.

a) Main features:

- Inception Modules: They combine parallel convolutional operations with different filter sizes to capture information at different scales.
- Efficiency and Accuracy: The modular structure enables more efficient and accurate image classification.
- Text Recognition and Classification:Adapted for text processing tasks such as classification and sentiment analysis.

The training of the Inception network uses large labeled datasets and deep learning techniques, with a focus on optimization through stochastic gradient descent.

This architecture is composed of modules, meaning that instead of using a single convolutional operation, this architecture uses filters of different matrix types, which allows capturing various features at different scales within the same block. These results are combined, resulting in better characterization. Additionally, it uses dimensionality reduction layers to maintain efficiency, which makes it effective in applications with images.

3) AlexNet Neural Network: The AlexNet neural network, Fig. 9, is an architecture that marked a significant shift in the field of deep learning by significantly outperforming other architectures in image classification. Developed by Alex Krizhevsky, Ilya Sutskever, and Geoffrey Hinton, AlexNet consists of 5 convolutional layers and 3 fully connected layers.

a) Main features:

- Pooling Layers: It uses pooling layers to reduce dimensionality and prevent overfitting.
- Non-linear Activation Functions: It employs non-linear activation functions to accelerate training and prevent the vanishing gradient.

The training of AlexNet follows the supervised learning paradigm, using backpropagation and stochastic gradient descent on large datasets such as ImageNet.

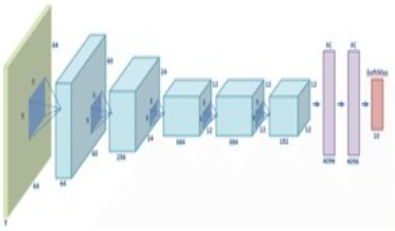


Fig. 9. AlexNet neural network architecture.

AlexNet is composed of a set of layers designed to extract spatial features at different levels. This architecture consists of 5 convolutional layers with large kernels that capture broad spatial patterns, followed by 3 fully connected layers that process and classify the learned features. Similarly, it incorporates max-pooling layers to reduce dimensionality and uses ReLU activation functions. Additionally, it includes mechanisms such as dropout to prevent overfitting during training.

4) ResNet Neural Network: The ResNet neural network was developed by Microsoft Research in 2015 to address the vanishing gradient problem and enable the training of much deeper models without performance degradation.

a) Main features:

- Residual Blocks: They include connections that allow information to flow directly through the layers, making it easier to train deep networks.

ResNet, Fig. 10, training follows the principles of supervised deep learning, using large labeled datasets and optimization via stochastic gradient descent.

The ResNet50 architecture is composed of residual blocks, meaning that instead of learning features directly, the layers

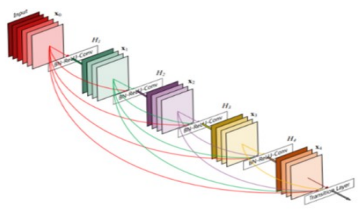


Fig. 10. ResNet neural network architecture.

focus on capturing the differences between the input and the output within each block. This is achieved through shortcut connections, which allow data to pass directly through the network without going through all intermediate layers. This architecture not only facilitates network training but also avoids issues like gradient vanishing. Thanks to this, it is widely used for processing images with high precision.

5) EfficientNet Neural Network: The EfficientNet neural network was developed by Google in 2019 to optimize the balance between accuracy and computational efficiency in image processing.

a) Main features:

- Compound Scaling: It optimizes the width, depth, and resolution of the network in a balanced manner using a method called Compound Scaling.

The training of EfficientNet uses labeled datasets and supervised learning techniques, adjusting the weights of the network through optimization algorithms such as stochastic gradient descent.

The EfficientNet architecture is designed to optimize efficiency in computer vision tasks, focusing on a single aspect. This architecture uses a compound scaling approach to uniformly scale the depth, width, and input resolution dimensions of the model, achieving a more comprehensive characterization of image features. It is based on modules that combine convolutional operations with dimensionality reduction techniques, achieving a balance between accuracy and computational efficiency.

6) You Only Look Once (YOLO) Algorithm: The YOLO algorithm stands out for its ability to detect objects in images quickly and accurately. Developed in 2016, YOLO approaches object detection as a simultaneous classification and bounding box regression problem.

a) Main features:

- Single-Pass Detection: It performs object detection in a single pass through the convolutional neural network.
- Multi-object predictions: It can detect multiple objects in an image, assigning a class probability to each bounding box.
- Real-Time: Its ability to perform real-time object detection makes it suitable for applications requiring rapid response.

The training of YOLO, Fig. 11, involves using labeled datasets and applying supervised learning techniques. The network is trained to recognize patterns and features of objects, adjusting the weights through backpropagation and optimization techniques.

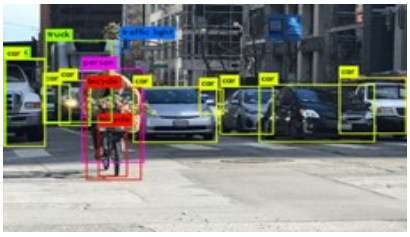


Fig. 11. Example of object detection with YOLO.

The YOLO architecture is designed for real-time object detection through the use of modules organized into blocks, where each block includes convolutional operations of various matrix sizes, allowing it to capture features at different scales within the same structure. These layers consist of max-pooling operations to reduce dimensions and preserve relevant features.

7) Data Augmentation: Data augmentation is a fundamental technique in machine learning and data processing. It involves creating new data samples by applying transformations to existing data while preserving the original information and label.

a) Applications and techniques:

- Image Augmentation: Rotations, flips, crops, changes in lighting, brightness and zoom, Fig. 12.

Fig. 12. Example of data augmentation on an image.

- Text Augmentation: Change of word order, synonyms, punctuation, and sentence structure, Fig. 13.

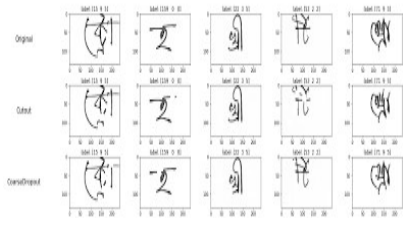


Fig. 13. Example of data augmentation in text.

- Audio Augmentation: Change of pitch, addition of noise, and variation of speed.

Data augmentation is applied before training the model to increase data variety and improve the model's predictive capability and robustness. There are various libraries in Python such as TensorFlow, Keras, PyTorch, and Augmentor that facilitate the implementation of these techniques.

IV. Method

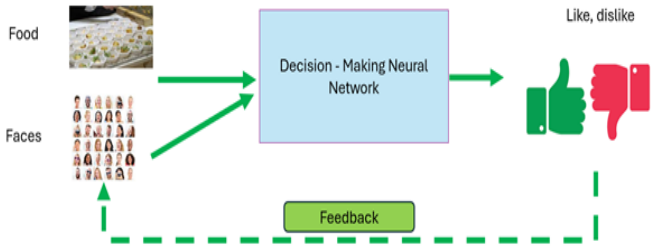


Fig. 14. General model of the system.

The decision-making system, Fig. 14, uses a neural network that analyzes images of food and the faces of consumers. This data enters a model that interprets the images to determine whether the food is considered "like" or "dislike" by the person. The model is self-correcting: if the interpretation does not match the expected outcome, it learns and adjusts its response.

A. Acquisition of the EEG Signal

The EEG signal measures the electrical activity during the excitation of pyramidal neurons in the cerebral cortex. This activity generates an electric and magnetic field, measurable with EEG systems through the skull and scalp, which attenuate the signal and add noise. The electrodes used to capture the EEG signal can be superficial, basal, or surgical. For this research, superficial electrodes are used, placed on the scalp following the International 10-20 Positioning System, based on anatomical points such as the inion, nasion, and lobes of the ears, this configuration does not generate any bias in decision-making.

For signal capture, the ThinkGear TGAM1 is used, which collects neural signals and processes them into usable data, filtering out interference. The NeuroSky ThinkGear module is a non-invasive interface with a 98% confidence level. However, due to noise levels, the device applies a reliable notch filter of 50Hz or 60Hz to reduce such noise. If not adequately filtered, it can affect the values of attention, meditation, and raw EEG data [16]. Additionally, signal loss through the scalp can impact the device's reliability. To address this, the module uses the poor quality code [16], which monitors electrode quality. If the connection with the scalp is suboptimal, this value increases to 200, indicating issues in signal acquisition, such as contact losses due to movement or incorrect placement.

The device is positioned at Fp1, as shown in Fig. 15, which measures electrical activity in the left frontal part of the brain, making it important for neurological diagnostics and scientific studies. Due to the fact that the Fp1 position is more directly associated with the person's emotional activity and attention,

it makes it a more relevant indicator for assessing emotional preferences in decision-making. On the other hand, the Fp2 position is not considered suitable for this study, as it is not as directly linked to the person's emotional regulation and attention, which would affect the result [17], therefore the Fp1 position is the most suitable for the study of decision-making.

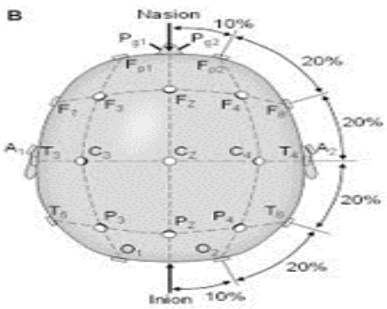


Fig. 15. Fp1 position.

B. The internal Model of the System

Internally, the model uses data reception from the products and the participants' faces to output classified and useful data. This helps to reduce dimensionality using Principal Component Analysis. Once reduced, we move to the next block where we extract data samples to send to the training model block. At the end of this process, the proposed model will indicate "like" or "dislike.", Fig. 16.

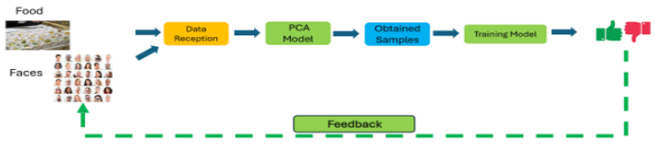


Fig. 16. Internal model of the system.

V. Experimental Results

A. Initial Configuration

The minimum requirements to run the model are as follows:

- Windows 10
- Intel Core i5
- 8.00 GB
- NeuroSky ThinkGear
- Google Colab
- Test Subjects

B. Results

C. Functionality Test

The functionality test is designed to demonstrate the use of the model, where the experiment is divided into faces and products.

1) Functionality Test of Products: As a first step, the file containing the images of the products and faces must be downloaded to train and test the model. In this case, the folder is named flavor.zip, Fig. 17. Additionally, the test image is loaded to verify that the data has been loaded correctly.

Fig. 17. Samples folder.

Once it is verified that the data has been loaded correctly, we proceed to build and train the neural network, thus providing the following model, which shows the convolutional and pooling layers, one example of this can be see in the Fig. 18.

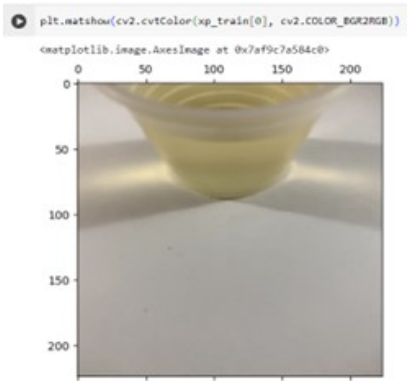


Fig. 18. Example of product samples.

For the case of the product experiment, we have the following inference matrix, which, as can be seen, classifies "like" and "dislike.", Fig. 19.

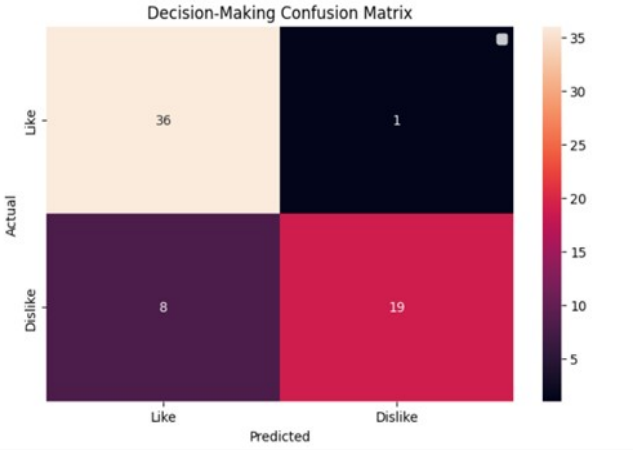


Fig. 19. Product inference matrix.

Similarly, for the case of the face experiment, we have the following inference matrix, which, as can be seen, classifies "like" and "dislike", Fig. 20.

As the final step, the inference matrix is shown with the combination of both experiments, resulting in the following outcome, Fig. 21.

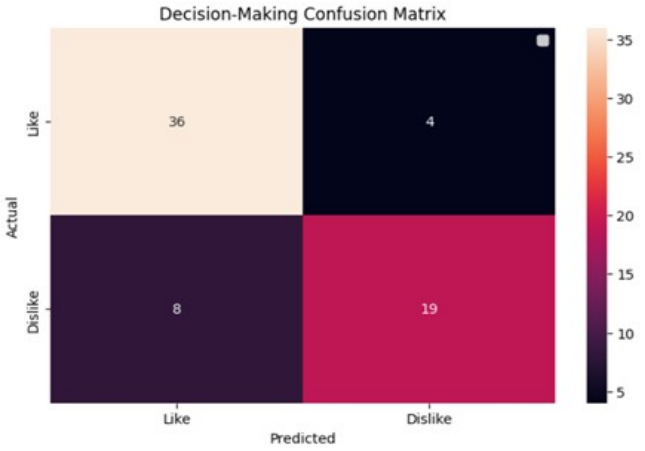


Fig. 20. Face inference matrix.

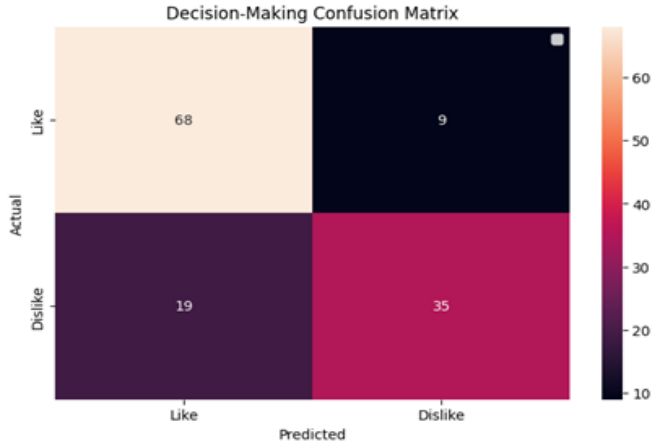


Fig. 21. Inference matrix of both experiments.

D. Experiment

To improve or observe changes in the percentage of effectiveness of the model, a series of experiments were implemented, using 5 variables that are part of the model. These are:

- Activation fuction of the model (A).
- Early Stopping during model training (B).
- Optimizer of the model (C).
- Sample size of images when entering the model (D).
- Amount of training data for the model (E).

The following the Table I, shows the aforementioned variables, along with their high and low values (or zero and one). It is worth noting that combinations of these variables were made to conduct possible tests, both in the Product model and in the Face model, resulting in two experiments.

Since both experiments use the same variables, the following hypothesis can be proposed:

TABLE I. VALUES OF THE VARIABLES TO ANALYZE

Variable	Low (0)	High (1)
Activation Fuction	ReLU	Leaky ReLU
Patience	5	10
Optimizer	ADAM	NADAM
Image Size	48	224
Batch Size	32	64

$$H_0: \quad A_i = 0; \quad B_i = 0; \quad C_i = 0; \quad D_i = 0; \quad E_i = 0;$$
$$H_1: \quad A_i \neq 0; \quad B_i \neq 0; \quad C_i \neq 0; \quad D_i \neq 0; \quad E_i \neq 0;$$

$$A_j \quad B_j \quad C_j \quad D_j \quad E_j$$

The results of both experiments are shown below

1) Product Experiment: The experiment is conducted using analysis of variance (ANOVA) for multiple factors on the F1 Score, Table II. Several tests and graphs are performed to determine which variables have a statistically significant effect on the F1 Score. It also evaluates the significance of interactions between variables, as long as sufficient data is available. Once the experiment is conducted, combining the variables to measure the outcome, the following results are obtained.

F1 SCORE HACER LO MISMO, duda en la pregunta

TABLE II. VARIANCE ANALYSIS F1 SCORE – TYPE III SUM OF SQUARES VALUES OF PRODUCTS

Source	P-Value
MAIN EFFECTS	
A: Activation Fuction	0.1560
B: Patience	0.0000
C: Optimizer	0.9295
D: Image Size	0.0038
E: Batch Size	0.0004

In the previous table, the results of the variance analysis are shown through a Type III sum of squares. The results indicate that both hypotheses A and C do not contribute to the outcome, and therefore, they are discarded.

$$H_0: \quad A_i = 0$$
$$H_0: \quad C_i = 0$$

Once the previous hypotheses are eliminated, the experiment is recalculated, where the following result is obtained, in the Table III.

TABLE III. VARIANCE ANALYSIS F1 SCORE – TYPE III SUM OF SQUARES OF SIGNIFICANT VARIABLES FOR PRODUCTS, SECOND EXPERIMENT

Source	P-Value
MAIN EFFECTS	
A: Patience	0.0000
B: Image Size	0.0038
C: Batch Size	0.0004

As can be seen in the table above, the remaining hypotheses do influence the experiment, which is why they are considered important. Once obtained, through the comparison of means, the value that effectively influences the percentage of effectiveness of the model can be observed, thus having the following results.

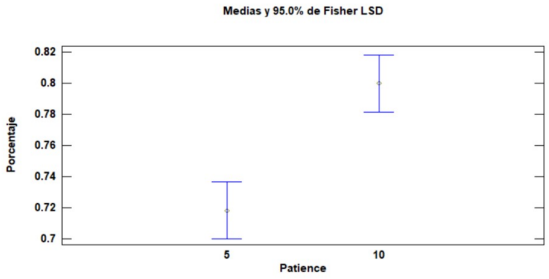


Fig. 22. Fisher LSD mean of the `Patience` variable for products.

This graph, Fig. 22, shows that the `patience` variable has a higher degree of confidence when its value is 10, as its representation is shifted to the right and separated from the other function.

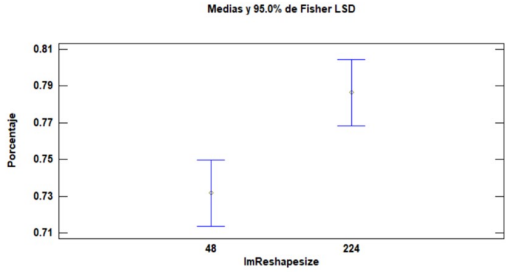


Fig. 23. Fisher LSD mean of the `ImReshapeSize` variable for products.

The previous graph, Fig. 23, shows that the `ImReshapeSize` variable has an effect on the experiment, with an image size of 224 being the most optimal.

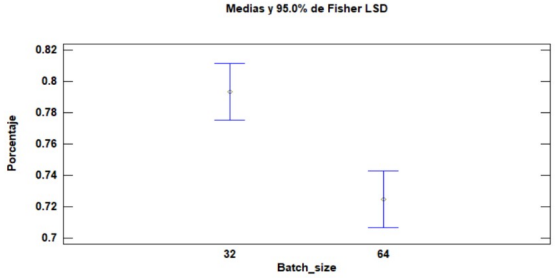


Fig. 24. Fisher LSD mean of the `Batch Size` variable for products.

Fig. 24 shows that the `BatchSize` variable has an effect on the experiment, with a value of 32 being the most optimal. This is because it is separated from the other value and is the first to represent the best option. The model uses a `Batchsize` of 32 and 64. With the applied statistical analysis, it is concluded that the value of 32 influences the model's performance more, particularly in the *Low-Beta*() and *Low-Gamma ()* frequency bands, while the value of 64 decreases the model's performance. As shown in Fig. 24, the value of 32 is above 64.

2) Faces Experiment: For this experiment, the same procedure is carried out as in the previous case, with the same variables and hypotheses.

TABLE IV. VARIANCE ANALYSIS F1 SCORE – TYPE III SUM OF SQUARES FOR FACES

Source	P-Value
MAIN EFFECTS	
A: Activation Fuction	0.0042
B: Patience	0.0019
C: Optimizer	0.4491
D: Image Size	0.8359
E: Batch Size	0.0012

In previous table, Table IV, the results of the analysis of variance are shown, through a Type III sum of squares, the results show that both hypothesis C and D do not contribute to the result, so they are discarded.

$$H_0: \quad C_i = 0$$
$$H_0: \quad D_i = 0$$

Once the previous hypotheses are eliminated, the experiment is recalculated, where the following result is obtained.

TABLE V. VARIANCE ANALYSIS F1 SCORE – TYPE III SUM OF SQUARES OF SIGNIFICANT VARIABLES FOR FACES.

Source	P-Value
MAIN EFFCETS	
A: Activation Fuction	0.0038
B: Patience	0.0017
C: Batch Size	0.0010

As seen in the previous table, Table V, the remaining hypotheses do influence the experiment, making them important. Once the results are obtained through the comparison of means, we can observe which value effectively impacts the model's effectiveness percentage, leading to the following outcomes.

The graph, Fig. 25,indicates that the ReLU `activation function` has a higher degree of confidence, as its representation is shifted to the right and separated from the other function.

The graph, Fig. 26, shows that the value of the `patience` variable has a higher degree of confidence when set to 10. This is because its representation is shifted to the right and separated from the other function.

The graph, shows that the `Batch Size` variable has an effect on the experiment, with a value of 32 being the most optimal, Fig. 27,this is because it is separated from the other value and is the first to represent the best option.

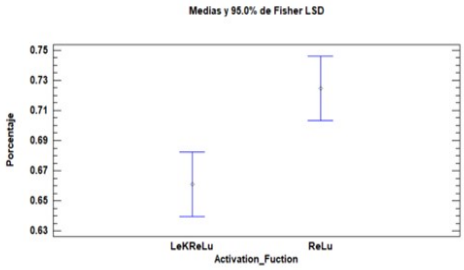


Fig. 25. Fisher LSD mean of the `Activation function` variable for faces.

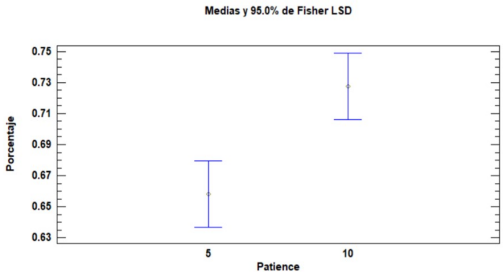


Fig. 26. Fisher LSD mean of the `Patience` variable for faces.

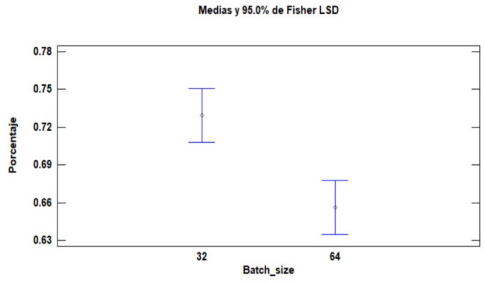


Fig. 27. Fisher LSD mean of the `Batch size` variable for faces.

E. Discussion

The two experiments have different training methods. One tests Products consumed by the subject, and the other tests the subject's Face. Both experiments use the same independent variables, but vary in the dependent variable. Using Statgraphics software, it was determined which variables influence each experiment. The following table, Table VI,shows these variables and their highest confidence values.

TABLE VI. VALUES OF THE VARIABLES FOR EACH EXPERIMENT

Products	Value	Faces	Value
Patience	10	Patience	10
ImReshapesize	224	Activation_Fuction	ReLu
Batch_size	32	Batch_size	32

The table indicates that both experiments share two variables with the same values: `Patience` (10) and `Batch_size` (32). `Patience` determines how many epochs the model can worsen before stopping, preventing overfitting. `Batch_size` is the number of training examples used by the network to update its weights, affecting the training process. In both cases, these values are essential for achieving 95% effectiveness.

Each experiment has a unique variable. In the Products experiment, `ImReshapesize` refers to the size of the image (224) input into the network. In the Faces experiment, `Activation_Fuction` is the mathematical function that determines the output of a neuron, with ReLU being the function used, which returns zero for negative values.

With the adjustment of hyperparameters such as the `ReLU` activation function, the `ADAM` optimizer, a `batchsize` of 32, and a `patience` of 10, while increasing the image size to 224, the model's accuracy was optimized. Additionally, the *Kolmogorov* complexity was reduced, which refers to the concept of algorithmic complexity that measures the amount of information required to describe or generate a dataset [18]. In other words, it is the length of the code used in the shortest program that can produce a given sequence of data as output, streamlining the model and decreasing its computational process [19]. By adjusting the hyperparameters and simplifying the data, the neural network was able to learn more efficiently, reducing the amount of information and the number of input data, thus becoming more agile in analyzing the image and EEG signals.

VI. CONCLUSIONS

In this work, 13 related studies were found concerning the use of decision-making, principal component analysis (PCA), and convolutional neural networks, of which 4 studies were selected for in-depth analysis. These studies were chosen for their connection to the use of convolutional neural networks and the methods they employ, with the main differences being in the decision-making aspect and target audience.

Furthermore, the theoretical foundations of the project were defined, integrating various convolutional neural networks used for different tasks, as well as knowledge about EEG, and lastly, techniques for more optimal data analysis were studied.

Additionally, the processes and subprocesses necessary for developing the decision-making model of whether I like it or not were presented. The three main processes were: i) Data collection through EEG and photographs, ii) Training the neural network with the collected data, and iii) Model functioning.

To verify the model's functionality, a series of experiments were designed with the interaction of 5 variables: a) ImReashepesize, b) Optimizer, c) Patience, d) Activation function, e) Batch size; experimentation was repeated with products and faces. The generated values for F1 Score and their combinations were examined through a Multifactorial Analysis of Variance. This analysis highlights that the two main variables influencing this model are patience and batch size, making the model more efficient.

Moreover, regarding the project's profitability, it is concluded that it is rejected, as the investment made for this project is not recovered, indicating that when not considering inflation, profitability decreases.

Therefore, this work contributes to the design of a neural network focused on decision-making in young people aged 18 to 20, contributing to the food and health sector by indicating whether a person likes what they consume, thus preventing overweight among these individuals.

As future work or derivations of this proposal, the following should be considered:

- Expand the target audience to include older adults and children of different ages.
- Improve the database by increasing its size with the participation of specialists.
- Design a new series of experiments that take into account other variables, such as Dropout, Epochs, etc.
- Implement the model in an IoT (Internet of Things) system.
- Combining Fp1, Fp2, O1, and O2 to create a brain mapping or qEEG analysis, which is an assessment tool used to measure electrical activity in the cerebral cortex. This map is then used to help diagnose mental health conditions by providing a statistical means of evaluating electrical activity in the cortex, [20].
- Expand the context of assistance to diseases such as diabetes or hypertension.

ACKNOWLEDGMENT

The Instituto Politécnico Nacional of Mexico, through the Comisión de Operación y Fomento de Actividades Académicas (COFAA) and SIP-projects No. *20241623* and *20241762*, has provided funding for this work. The research was carried out at the Escuela Superior de Ingeniera Mecánica y Eléctrica, Campus Zacatenco. It should be mentioned that this study is a crucial component of the doctoral dissertation titled *Modelo integral de Neuromarketing para innovar en las empresas del sector alimentario* supported by *Verónica Pérez*, under the supervision of Dr. Ana Coria and Dr. Jaime Moreno. Moreover, this research is also part of the master's thesis titled *Modelo sistémico para explicar el comportamiento de los consumidores durante la toma de decisiones, basado en inteligencia artificial*, guided by Dr. Oswaldo Morales and Dr. Jaime Moreno, and supported by Mauro Castillo.

REFERENCES

[1] C. Oropeza Abúndez, Ed., *Encuesta Nacional de Salud y Nutrición 2018-19: Resultados Nacionales*, primera edición ed. Cuernavaca, Morelos, México: Instituto Nacional de Salud Pública, 2020.

[2] O. C. E. Posible. 5 enganos alimentarios. ¡que no te la cuelen! Accedido el 20 de noviembre de 2024. [Online]. Available: https://www.otroconsumoposible.es/5-enganos-alimentarios-que-no-te-cuelen/

[3] C. Mitchell, "Ops-oms: Sobrepeso afecta a casi la mitad de la población de todos los países de américa latina y el caribe salvo por haití," *Journal of Embedded Systems*, vol. 15, no. 4, pp. 123–145, 2017.

[4] CASADOMO. El mit diseña un sistema de red neuronal de aprendizaje profundo para dispositivos iot. Accedido el 20 de noviembre de 2024. [Online]. Available: https://www.casadomo.com/2020/11/20/mit-disena-sistema-red-neuronal-aprendizaje-profundo-dispositivos-iot

[5] E. Niedermeyer and F. L. da Silva, *Electroencephalography: Basic Principles, Clinical Applications, and Related Fields*. Lippincott Williams & Wilkins, 2004.

[6] T. H. Lee and K. S. Lee, "A new method for analyzing the decision-making process using eeg signals," *Neuroscience Letters*, vol. 639, pp. 18–24, 2017.

[7] L. I. Aftanas and S. A. Golocheikine, "Human anterior and frontal midline theta and lower alpha reflect emotionally positive state and were related to self-regulation of emotion," *Neuroscience Letters*, vol. 310, no. 1, pp. 57–60, 2001.

[8] Y. Narayan, M. A. Tripathi, P. P. Singh, D. A. Vidhate, R. Singh, and M. M. S. Rao, "Development of ai model to analyze the customer behavior by decision making system," in *2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS)*, vol. 1, 2023, pp. 1–5.

[9] M. Maram, M. A. Khalil, and K. George, "Analysis of consumer coffee brand preferences using brain-computer interface and deep learning," in *2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 2023, pp. 227–232.

[10] S. M. Usman, S. M. Ali Shah, O. C. Edo, and J. Emakhu, "A deep learning model for classification of eeg signals for neuromarketing," in *2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD)*, 2023, pp. 1–6.

[11] V. Khurana, M. Gahalawat, P. Kumar, P. P. Roy, D. P. Dogra, E. Scheme, and M. Soleymani, "A survey on neuromarketing using eeg signals," *IEEE Transactions on Cognitive and Developmental Systems*, vol. 13, no. 4, pp. 732–749, 2021.

[12] M. Ivanova and M. H. Ruiz, "Motor learning and decision making in volatile environment in bipolar disorder," in *2022 Fourth International Conference Neurotechnologies and Neurointerfaces (CNN)*, Kaliningrad, Russian Federation, 2022, pp. 55–58.

[13] L. Tran, B. Ngo, T. Tran, L. Pham, and A. Mai, "On a development of sparse pca method for face recognition problem," in *2021 International Conference on Advanced Technologies for Communications (ATC)*, Ho Chi Minh City, Vietnam, 2021, pp. 265–269.

[14] O. P. Barus, J. Happy, Jusin, J. J. Pangaribuan, S. Z. H, and F. Nadjar, "Liver disease prediction using support vector machine and logistic regression model with combination of pca and smote," in *2022 1st International Conference on Technology Innovation and Its Applications (ICTIIA)*, Tangerang, Indonesia, 2022, pp. 1–6.

[15] Y. Zhu and Q. Zeng, "Continuous speech recognition based on dcnn-lstm," in *2023 5th International Conference on Intelligent Control, Measurement and Signal Processing (ICMSP)*, Chengdu, China, 2023, pp. 1247–1250.

[16] I. NeuroSky, "Neurosky eeg brainwave chip and board TGAM1," http://www.neurosky.com, San Jose, CA, USA, 2010, technical Specifications Document.

[17] D. G. Chávez, "Toma de decisiones guiada por emociones detectadas en señales de electroencefalograma mediante redes convolucionales," Ph.D. dissertation, Universidad Autónoma Metropolitana, 2023.

[18] H. Kabir and N. Garg, "Machine learning enabled orthogonal camera goniometry for accurate and robust contact angle measurements," *Scientific Reports*, vol. 13, p. 1497, 2023. [Online]. Available: https://doi.org/10.1038/s41598-023-28763-1

[19] V. Bolón-Canedo and B. Remeseiro, "Feature selection in image analysis: a survey," *Artificial Intelligence Review*, vol. 53, pp. 2905–2931, 2020. [Online]. Available: https://doi.org/10.1007/s10462-019-09750-3

[20] M. Das and M. Mahadevappa, "Enhancing asd cognitive assessment with p300 classification using emd-based qeeg wavelet features," in *2023 7th International Conference on Computer Applications in Electrical Engineering-Recent Advances (CERA)*, 2023, pp. 1–6.

Learning Local Reconstruction Errors for Face Forgery Detection

Haoyu Wu, Lingyun Leng, Peipeng Yu
College of Cyberspace Security, Jinan University, Guangzhou, China

***Abstract*—Although several deepfake detection technologies have achieved great detection accuracy inside the data domain in recent years, there are still limitations in cross-domain generalization. This is due to the model's ease of fitting the data sample distribution in the training data domain and its tendency to detect a specific forgery trace in order to reach a judgment rather than catching generalized forgery traces. In this paper, we propose to learn Local Reconstruction Errors for face forgery detection. The local anomaly traces of the fake face are often mapped using the original real face as a reference; however, the original real face of the fake face cannot be acquired in the real scenario. Therefore, this solution designs a local reconstruction autoencoder trained with real samples. By masking key areas of the face, the original real face can be reconstructed. Because the autoencoder only learns how to restore the essential parts of the real face using local patches of real samples, it cannot recover the forging traces or target face information in the fake face. Therefore, the reconstructed image forms a reconstructed difference with the original image. This solution aids the model in detecting local differences in fake faces by producing feature-level local difference attention mappings in the network's middle layer. A series of experiments demonstrate that this solution has good detection and generalization performance.**

***Keywords*—Face forgery; deepfake detection; local anomalies; generalized detection**

I. Introduction

With the rapid development of deep learning technology, deepfake technology has found widespread applications. By manipulating or replacing images or videos of faces, deepfake technology can alter visual content in subtle ways, posing significant threats to privacy, public opinion, and information security[1], [2], [3], [4]. Consequently, effectively detecting forged faces has become a crucial research topic in the field of computer vision.

Currently, there have been significant advancements in deepfake detection, with many methods performing well on forged data similar to their training datasets [5], [6], [7]. However, these methods often lack generalization when faced with unknown types of forgeries. Enhancing the generalization of detection models across various forgery methods is an urgent challenge. Our primary motivation is that there are notable differences between forged faces and their authentic counterparts (in terms of identity, artifacts, etc.). By leveraging these differences, we can accurately identify key areas of forgery rather than merely learning a single forgery pattern. Traditional methods either require reference images of the original faces or use self-attention mechanisms to predict key areas, both of which have significant limitations.

With the above considerations in mind, in this paper, we propose a local reconstruction-based deepfake detection method. By designing a local reconstruction autoencoder trained on real samples, we can mask and reconstruct critical regions of the face. The model generates a reconstruction difference map between the forged and real faces. Since the autoencoder cannot reconstruct the forgery traces in the forged face, this reconstruction difference map provides new discriminative information for forgery detection. Furthermore, we introduce a feature-level local difference attention map within the model to enhance the focus on forged regions. A series of experimental results demonstrate that this approach exhibits excellent detection performance and generalization capability across multiple datasets.In brief, our contributions are summarized as follows:

- We propose a novel detection framework based on local reconstruction for restoring genuine faces, which can eliminate artifacts in forged faces and guide the model to learn key regions.
- We introduce a local reconstruction autoencoder framework based on a key region masking algorithm, capable of restoring the original genuine face from local genuine patches.
- We present a method that uses local feature attention maps based on reconstructed image comparison to guide the detection model to focus on key regions and learn highly generalizable features.
- Our approach effectively enhances the generalization ability of the detection model on unknown datasets and against unknown forgery methods.

II. Related Work

A. Face Forgery Algorithms

Recent face forgery methods benefit from advances in deep learning. It can be classified into three categories based on the target of manipulation: face swapping, face editing, and face generation. In the early stages, researchers [3] viewed face swapping as a style transfer problem. Guided by facial landmark points, convolutional neural networks (CNNs) could transform one facial image into another, adopting the style of a face with a specific identity. However, with the rapid advancement of deep learning, several novel face swapping algorithms have emerged, significantly reducing the difficulty of face swapping [8], [9]. The progress of Generative Adversarial Networks (GANs) has further enhanced the realism of forged faces [10], [11], [12].

B. Face Forgery Detection Algorithms

Deepfake technology often produces noticeable artifacts when synthesizing or distorting facial features, such as unreasonable distortions of facial elements, edge artifacts, and missing details. Matern *et al.* [13] observed that certain Deepfake and Face2Face forgeries resulted in visual anomalies like differences in eye color, distorted facial contours, and missing tooth details. They aimed to detect these inconsistencies, but such artifacts only appear in lower-quality deepfake products, lacking universality. Nirkin *et al.* [14] proposed a method that segments detection images into internal (eyes, nose, mouth) and external (ears, hair) facial regions to train separate vectors for feature extraction. However, this approach does not adapt well to forgeries affecting external facial areas, resulting in limited generalization. Liu *et al.* [15] identified fundamental statistical differences in texture data between forged and real faces, leading to the development of a novel architecture for global texture representation to enhance the robustness of forgery detection. Chen *et al.* [16] used facial masking to detect whether images had undergone interference, reconstructing affected images to check for artifacts in the cleaned results. Dong *et al.*[17] approached this through image matching, proposing that forged images contain artifacts unrelated to the features of the original and target images. They designed a training set of matching images (forged, original, and target) to implicitly guide model learning, achieving good performance against compression. Wang *et al.* [18] developed a deepfake detection model focused on identifying potential noise traces, extracting features from both facial and background segments. They employed a novel multi-head contrastive interaction method to assess the similarity between facial and background noise features for image authenticity detection. Huang *et al.* [19] highlighted the differences between explicit and implicit identities in swapped images, introducing explicit identity contrast loss and implicit identity exploration loss to increase the distance between the explicit and implicit identities of fake faces, using this information for authenticity determination. However, Dong *et al.* [20] argued that focusing on identity information hinders the generalization of classification models, leading to a breakthrough with a method that prioritizes local features while ignoring overall identity information.

In summary, deepfake detection algorithms are designed to guide models in capturing specific artifact features, thereby identifying manipulated images by responding to these artifacts. Nevertheless, a common limitation of these methods is their often inadequate generalization capability when encountering previously unseen types of forgeries.

III. Methodology

A. Overview

The distribution of real human faces is consistent and uniform [21], while it is difficult for forged faces to completely eliminate all traces of artifacts, leading to a lack of continuity in the distribution of fake faces. Therefore this paper explores whether it is possible to design a method that constrains the model to learn key difference areas. A promising approach is to use the local differences between forged faces and their original faces, employing the original face to create an attention mask for the forged face. However, in most cases, the detection side cannot obtain the original face corresponding to the forged face. Thus, this paper attempts to reconstruct the distribution of the real face from the forged face to assist in detecting authenticity.

Based on the above concept, this paper proposes a deepfake detection scheme based on local reconstruction. As shown in Fig. 1, the scheme consists of two stages: (1) Training stage based on masked reconstruction of real samples. The content of a forged face typically originates from a source image and a target image, corresponding to its internal and external face, whereas a real image has a unified internal and external face. Therefore, this scheme pre-trains an encoder and decoder based on a Vision Transformer (ViT) using real face images. By randomly masking most facial features during face reconstruction, the encoder and decoder learn the distribution of real faces, acquiring the ability to recover the original real face information from partially masked real faces. (2) Training stage based on local difference attention map constraints. After training the encoder and decoder, their weights are fixed, and the to-be-detected image is masked and reconstructed to obtain a reconstructed image. Both the reconstructed image and the to-be-detected image are input into a fixed-weight feature extraction network to calculate multiple feature-level local difference attention maps. These attention maps are used to guide the model to learn key regional features for generalized detection.

B. Training Stage Based on Masked Reconstruction of Real Samples

The purpose of the training stage based on masked reconstruction of real samples is to train the encoder and decoder to learn the distribution of real face data, enabling the reconstruction of a complete real face image from local real face regions. Inspired by the MAE method, this scheme trains a ViT-based encoder and decoder structure using real faces with masked key facial regions. First, a face image of size $C \times H \times H$ is divided into N patches, each of size $C \times P \times P$, where $N = \frac{H^2}{P^2}$, and C, H, and P represent the number of image channels, the image's side length, and the patch's side length, respectively. Then, the proposed key region masking algorithm randomly masks patches in key facial regions, and the model learns to reconstruct the masked patches based on the remaining parts of the face image. The trained encoder and decoder learn the ability to recover the original real face information from local real face regions, allowing for effective reconstruction of the masked parts of a real face. When the encoder and decoder, trained solely on real face data, are used to perform masked reconstruction on a forged face, they can reconstruct the original real face from the genuine local regions of the forged face, but they will not restore the local forged artifacts in the fake face.

1) Key Region Masking Algorithm: Typically, the facial features, such as the eyes, nose, and mouth, are the key areas in forged faces. To ensure that the encoder and decoder learn to reconstruct the original face from real facial regions, and avoid reconstructing forged areas during fake face testing, this scheme defines a key region that includes facial features. As shown in Fig. 2, the proposed method first uses a landmark algorithm to extract the coordinates of 68 key facial points for all faces in the dataset. From these, it selects the coordinates

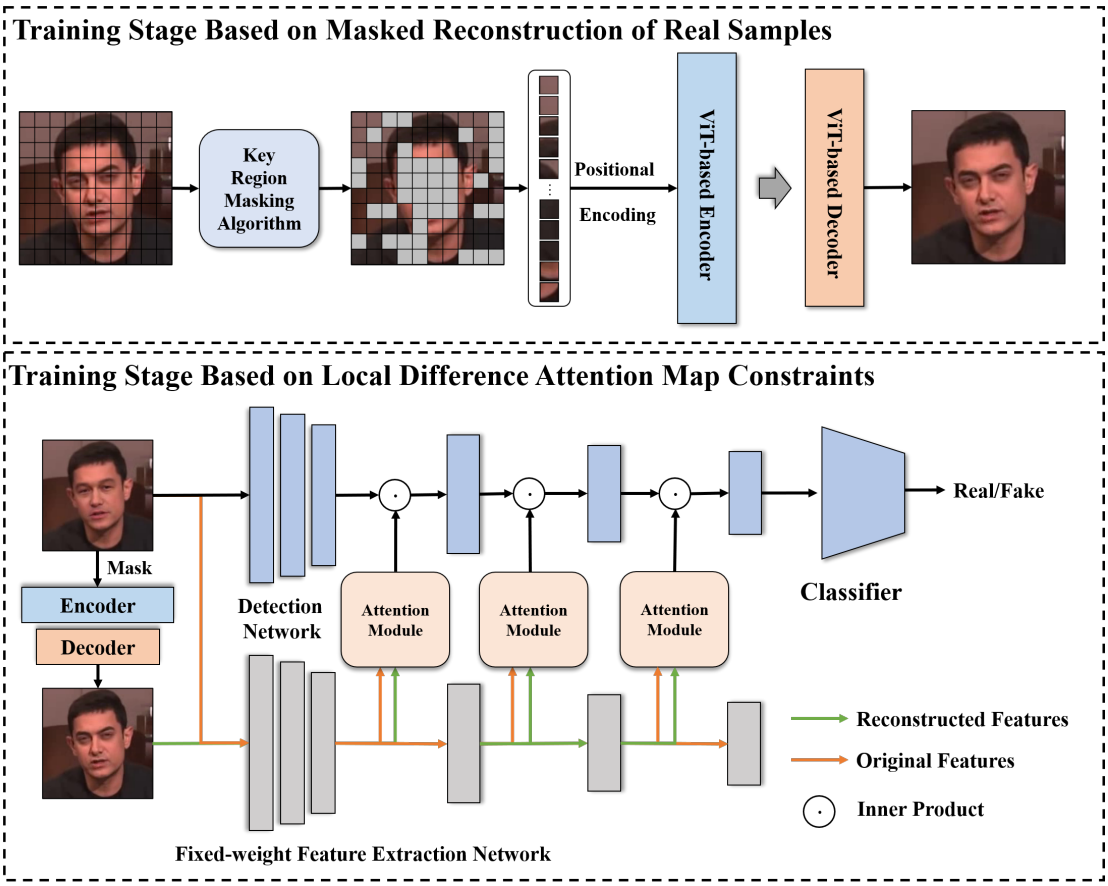


Fig. 1. Framework of local reconstruction-based deepfake detection algorithm.

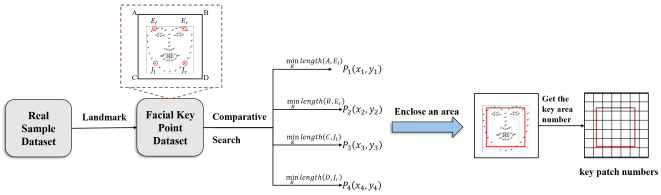


Fig. 2. Key area masking algorithm flowchart.

of the left eyebrow, right eyebrow, left jaw, and right jaw that are closest to the image vertices, denoted as P_1 , P_2, P_3, and P_4. The area enclosed by these points can cover the facial features of most faces in the dataset. Next, the four coordinates are expanded outward to form a rectangular region, which is defined as the key facial region. The face image is then divided into patches, where each small patch is assigned a number i, where $i \in \{1, 2, \ldots, N\}$. Based on the pixel coordinates of the key region, a set of key patch numbers, denoted as $T = \{45, 46 \ldots\}$, can be calculated, representing the patches included in the key region. Finally, random masking is applied to the image at a proportion of p, ensuring that most patches in the key patch set are masked. The sequence of unmasked patches is then fed into the encoder to reconstruct the original face image.

2) Face Reconstruction via Encoder and Decoder: The ViT-based encoder first receives the input sequence of unmasked patches and assigns a positional index to each unmasked patch. These patches are then passed through a series of Transformer blocks to learn the deep features of the real patch regions, which are used for subsequent face reconstruction. After undergoing a series of encoding processes, the encoder outputs the features of the unmasked patches. At this stage, the decoder takes these unmasked patch features as input and adds mask tokens to the masked areas to form a complete image, then applies positional encoding to all patch features. The mask tokens are shared, learnable vectors used to represent the masked patches that need to be reconstructed. Through a series of reconstruction processes within the decoder, the final linear layer of the decoder outputs a linear projection of the reconstructed image. After adjusting the dimensions and size, the reconstructed image is obtained. The reconstruction loss is then calculated only for the masked patches using mean squared error (MSE), with the loss expression as follows:

$$L_{rec} = \frac{1}{N} \sum_{i=1}^{n} (y_i - x_i)^2 \tag{1}$$

where x represents the reconstructed masked patches, and y represents the actual masked patches. By leveraging the information of masked patch indexes and calculating the reconstruction loss only for the masked patches, the computation is reduced, significantly improving the training efficiency of the

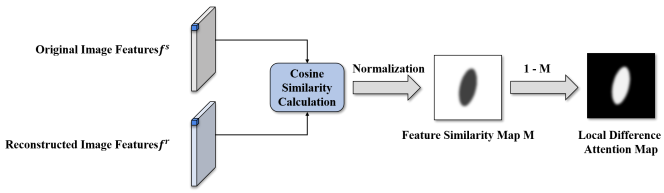


Fig. 3. Feature-Level local difference attention map calculation flowchart.

encoder and decoder.

C. Training Stage Based on Local Difference Attention Map Constraints

The training stage based on local difference attention map constraints aims to guide the model to learn the local differences in forged face images by calculating feature-level local difference attention maps between the reconstructed and original images. After the ViT-based encoder and decoder are trained on real face data, they have only acquired the knowledge of reconstructing local real facial regions. Therefore, this scheme fixes the parameters of the encoder and decoder and applies them during the training phase of the detection task. First, after dividing the face image into patches and masking the key regions, the unmasked patch sequence is input into the encoder-decoder framework to obtain the reconstructed face image. Next, a pre-trained feature extraction network with fixed parameters is used to extract a series of feature maps from the middle layers of the network for both the reconstructed face and the original face. Using similarity calculations, feature-level local difference attention maps are obtained. To ensure that the size of the feature-level local difference attention maps matches the feature maps in the middle layers of the detection network, both the feature extraction network and the detection network adopt the Xception architecture. The method for calculating the local difference attention map is shown in Fig. 3. This scheme uses cosine similarity to compute the similarity at each location between the original image features and the reconstructed image features. After normalizing the results, by subtracting the feature similarity map M from 1 to emphasize the difference regions, the final local difference attention map is obtained. The calculation expression is as follows:

$$AttentionMap_i = 1 - \frac{1 + CosineSimilarity(f_i^s, f_i^r)}{2} \quad (2)$$

where f^s and f^r represent the features of the original image and the reconstructed image, respectively, and $CosineSimilarity$ represents the cosine similarity calculation, which ranges from $[-1, 1]$. The higher the value, the more similar the two features are.

In the final classification prediction, this scheme uses the same network model as the feature extraction network described above as the basic framework, allowing the local difference attention map to guide the model in learning the key regional difference features. As shown in Fig. 1, the proposed method performs an inner product between the multiple feature maps of the original face image from the middle layers of the network and the local difference attention map, thereby constraining the model's learning process. Finally, the features extracted by the model are input into the classifier for real/fake classification, and binary cross-entropy (BCE) loss is used to constrain the training. The loss function is as follows:

$$L_{cls} = -\frac{1}{N}\sum_{k=1}^{n} y_k \log(x_k) + (1 - y_k)\log(1 - x_k) \quad (3)$$

where x represents the real/fake prediction, and y represents the real/fake label.

TABLE I. RESULTS OF IN-DATASET EVALUATIONS

Methods	FF++(C23)		FF++(C40)	
	Acc	AUC	Acc	AUC
Face-X-ray[22]	—	87.4	—	61.6
MesoNet[5]	83.1	84.3	70.47	72.62
Multi-task[6]	85.65	85.43	81.3	75.59
XceptionELA[23]	93.86	94.8	79.63	82.9
SPSL[24]	91.5	95.32	81.57	82.82
CFFs[25]	—	97.21	—	86.56
M2TR[26]	91.86	96.75	83.89	87.15
Two-branch[27]	96.43	98.7	86.34	86.59
HFI-Net[28]	91.87	97.07	58.69	88.4
RFM[29]	**95.69**	**98.79**	**87.06**	89.83
Ours	91.78	97.4	80.75	**90.12**

IV. EXPERIMENTS

A. Datasets

The experiments in this study utilize the following three datasets for testing and evaluation: FaceForensics++[30], Celeb-DF-v2[31], and the DFD dataset[32]. FaceForensics++ is a large public dataset for facial forgery detection, containing 1,000 real videos and 4,000 forged videos generated using four manipulation methods: Deepfakes, Face2Face, FaceSwap, and NeuralTextures. Additionally, FaceForensics++ includes three compression levels: the original version (C0), a high-quality version (C23), and a low-quality version (C40). Celeb-DF-v2 is a challenging dataset composed of 569 real videos and 5,639 forged videos extracted from YouTube. The DFD dataset is another large-scale dataset containing 363 real videos and 3,068 forged videos across various scenarios.

B. Experimental Setup

The experiments in this study are implemented using the PyTorch framework, with programming conducted in Python. The datasets are divided for training, validation, and testing of the detection model. OpenCV is used to extract a series of continuous, non-repeating video frames from videos at fixed intervals. The RetinaFace face recognition algorithm is employed to locate the face regions in the video frames, align these regions, and crop them appropriately. All face images are resized to a uniform dimension of 224×224 pixels. All experiments utilize the Adam optimizer for training, with a learning rate set to 0.0001 and a batch size of 32. The ViT-based encoder and decoder are trained for 300 epochs, with a masking ratio of 75%. The Xception-based feature extraction network and classifier are trained for 30 epochs, with 200 iterations per epoch. The training is conducted on

TABLE II. RESULTS OF CROSS-MANIPULATION EVALUATIONS ON FF++C23(AUC)

Methods	Train	DF	F2F	FS	NT	Avg
En-b4[33]	DF	99.65	**73.6**	40.73	**73.94**	71.98
SimMIM[34]		99.64	62.43	66.74	62.74	**72.89**
FDFL[34]		98.91	58.9	**66.87**	63.61	72.07
Ours		**99.85**	70	41.38	71.42	70.66
En-b4[33]	F2F	**87.15**	99.26	51.6	66.85	**76.22**
SimMIM[34]		84.27	**99.28**	53.49	53.87	72.73
FDFL[34]		67.55	93.06	55.35	66.66	70.66
Ours		78.99	99.01	**55.53**	**70.45**	75.92
En-b4[33]	FS	61.44	68.96	**99.57**	49.83	69.95
SimMIM[34]		**88.12**	58.88	99.19	**52.55**	**74.67**
FDFL[34]		75.9	54.64	98.37	49.72	69.66
Ours		63.4	**70.79**	99.53	51.48	71.3
En-b4[33]	NT	83.98	69.08	46.32	**97.59**	74.24
SimMIM[34]		**85.26**	64.38	46.62	69.95	73.38
FDFL[34]		79.09	74.21	**53.99**	88.54	73.96
Ours		84.14	**76.4**	50.88	96.51	**76.98**

an NVIDIA GTX GeForce 3090 Ti platform with 24 GB of VRAM. Additionally, binary classification accuracy (Acc) and the area under the ROC curve (AUC) are used as performance evaluation metrics for the model.

C. In-Dataset Evaluation

This section tests the in-dataset detection performance of the proposed method on the FaceForensics++ (FF++) datasets, and compares it with other state-of-the-art methods. The proposed method is independently trained on and validated using the test sets of FF++(C23) and FF++(C40) datasets. The results are shown in Table I. It can be observed that, the proposed method achieves high test accuracy on the FF++(C23) datasets. The lower AUC performance on FF++(C40) may be attributed to the inconsistent quality of the original compressed images. During the training phase with real samples, the encoder and decoder did not incorporate lower-quality images for training, resulting in deviations and quality issues when reconstructing low-quality images.

D. Cross-Dataset Evaluation

1) Cross-Manipulation Method Evaluation: Cross-manipulation method evaluation is a significant approach to assess the generalization capability of detection methods, with important practical implications. This section conducts cross-testing of the proposed method across four different manipulation methods on the FF++(C23) dataset, with the results shown in Table II. It can be observed that the average performance across the four cross-tests exceeds 70%. In comparison with other advanced methods, the proposed approach, trained on the NT dataset, achieves a higher average AUC performance of 76.98% across the four manipulation methods, representing an improvement of 2% in detection performance. Additionally, the average test results from training on F2F reach 75.92%, with a gap of less than 1% compared to the higher performance of En-b4. The experimental data in the table demonstrate that the proposed method exhibits effective generalization across single-source manipulation methods, confirming the feasibility of this approach.

The aforementioned experiments demonstrate the generalization evaluation from a single manipulation domain to other domains. Additionally, there exists a method for evaluating generalization in multi-source forgery detection. This experiment utilizes three training sets from FF++ (excluding DF) for joint training and tests on DF, defined in the table as GID-DF. Similarly, the experiment trains on three other manipulation sets (excluding F2F) and tests on F2F. All test results are presented in Table III. For the DF tests, existing methods have reached a high performance level, with the proposed method closely following, showing an AUC performance difference of less than 7% from the state-of-the-art methods. Although there is a gap in AUC performance for GID-DF(C23) compared to the leading methods, the accuracy performance and results on the C40 version dataset remain outstanding, surpassing other existing advanced methods. Regarding the F2F tests, mainstream methods show subpar performance, while the proposed method achieves the best results, exceeding current advanced methods by 1% in AUC performance and 2% in accuracy performance, demonstrating improvements across different compression levels of F2F images. These experimental data strongly affirm the superiority of the proposed method in multi-source forgery detection.

2) Cross-Dataset Evaluation: This section evaluates the performance of the proposed method across different datasets. The method was trained on the FF++(C23) dataset and tested on the FF++(C23) library, Celeb-DF-v2, and DFD. The experimental results, as shown in Table IV, indicate that the method achieved the best AUC performance on the DFD dataset and demonstrated highly competitive performance on Celeb-DF-v2, surpassing most advanced methods with a gap of less than 5% compared to the state-of-the-art methods. This suggests that the proposed method exhibits good generalization capabilities across unknown datasets.

E. Ablation Study

As the proposed method is an integrated detection framework, it is not possible to conduct an ablation study on individual components or stages. Here, we present the comparative experimental results between the proposed method and the Xception-based classification baseline model. The baseline model was trained on FF++(C23) and tested for AUC performance on Celeb-DF-v2 and DFD. The testing results, as shown in Table V, indicate that the proposed method outperforms the baseline model on both Celeb-DF-v2 and DFD, demonstrating its effectiveness.

F. Visualization of Results

This section further demonstrates the reconstructed images generated by the autoencoder framework trained on real samples. As shown in Fig. 4, the similarity between the real image and the reconstructed image is very high for real face images. However, for forged images, which contain artifacts not present in real samples, reconstructing the forged images with masked key facial regions results in reconstructed images that do not retain the original forged information, leading to significant local differences compared to the original forged images. Additionally, since the encoder and decoder are capable of reconstructing real samples, the reconstructed facial features of the forged images tend to resemble those of the original

TABLE III. RESULTS OF MULTI-SOURCE MANIPULATION EVALUATIONS ON FF++

Methods	GID-DF(C23)		GID-DF(C40)		GID-F2F(C23)		GID-F2F(C40)	
	Acc	AUC	Acc	AUC	Acc	AUC	Acc	AUC
EfficientNet[33]	82.4	91.11	67.6	75.3	63.32	80.1	61.41	67.4
Focalloss[35]	81.33	90.31	67.47	74.95	60.8	79.8	64	67.21
ForensicTransfer[36]	72.01	—	68.2	—	64.5	—	55	—
Multi-task[6]	70.3	—	66.76	—	58.74	—	56.5	—
MLDG[37]	84.21	91.82	67.15	73.12	63.46	77.1	58.12	61.7
LTW[38]	85.6	92.7	69.15	75.6	65.6	80.2	65.7	72.4
DCL[39]	**87.7**	**94.9**	**75.9**	**83.82**	68.4	82.93	67.85	75.07
Ours	79.28	87.9	70.22	78.67	**73.62**	**84.29**	**69.25**	**76.5**

TABLE IV. RESULTS OF CROSS-DATASET EVALUATIONS ON FF++C23(AUC)

Methods	FF++(C23)	Celeb-DF-v2	DFD
TI2Net[40]	**99.95**	68.22	72.03
FRLM[41]	99.5	70.58	68.17
F3Net[42]	98.1	71.21	86.1
Face-X-ray[22]	87.4	74.2	85.6
MLDG[37]	98.99	74.56	88.14
GFF[43]	98.36	75.31	85.51
SFDG[44]	99.53	75.83	88
SOLA[45]	99.25	76.02	—
MultiAtt[46]	99.27	76.65	87.58
BIG-Arts[47]	99.39	77.04	89.92
LTW[38]	99.17	77.14	88.56
FAAFF[48]	99.27	77.59	—
Local-Relation[49]	99.46	78.26	89.24
DCL[39]	99.3	**82.3**	91.66
Ours	97.24	77.47	**95.23**

TABLE V. RESULTS OF ABLATION STUDY

Methods	FF++(C23)	Celeb-DF-v2	DFD
Baseline	**99.09**	72.15	87.86
Ours	97.24	**77.47**	**95.23**

real faces, which is influenced by the training effect of the encoder and decoder on large amounts of real face data.

V. CONCLUSION

This paper proposes a deepfake detection algorithm based on local reconstruction, comprising two stages: the training stage based on masked reconstruction of real samples and the training stage based on local difference attention map constraints. There are local differences between forged faces and the original real faces, and attention maps generated from these local differences can guide the model to learn key forgery regions, shifting the model's focus from global to local features to improve detection performance. Previous methods either require the original real image as a reference or use self-attention mechanisms to predict key regions, both of which have significant limitations. In contrast, this method enhances practical applicability by using a local reconstruction approach to recover the original real face from local regions of real faces, aligning better with real-world scenarios. By

Fig. 4. Reconstruction results of real and forged images.

calculating feature-level local difference attention maps between the reconstructed and original images, the model is effectively constrained to learn the features of key forgery regions, further enhancing its ability to extract difference features. Extensive experiments demonstrate the effectiveness and reliability of this method in improving generalization performance. However, our local reconstruction method does not fully exploit the information available in forged faces and struggles with reconstructing low-quality faces. In future research, we aim to develop new algorithms that incorporate the identity information in forged faces to better recover the original real faces. In the future, leveraging local masking and reconstruction to restore real faces holds significant potential and valuable research implications for both generalized detection and proactive forensic analysis.

REFERENCES

[1] T. Karras, "Progressive growing of gans for improved quality, stability, and variation," *arXiv preprint arXiv:1710.10196*, 2017.

[2] T. Karras, S. Laine, and T. Aila, "A style-based generator architecture for generative adversarial networks," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2019, pp. 4401–4410.

[3] I. Korshunova, W. Shi, J. Dambre, and L. Theis, "Fast face-swap using convolutional neural networks," in *Proceedings of the IEEE international conference on computer vision*, 2017, pp. 3677–3685.

[4] J. Thies, M. Zollhofer, M. Stamminger, C. Theobalt, and M. Nießner, "Face2face: Real-time face capture and reenactment of rgb videos," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 2387–2395.

[5] D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, "Mesonet: a compact facial video forgery detection network," in *2018 IEEE international*

workshop on information forensics and security (WIFS). IEEE, 2018, pp. 1–7.

[6] H. H. Nguyen, F. Fang, J. Yamagishi, and I. Echizen, "Multi-task learning for detecting and segmenting manipulated facial images and videos," in *2019 IEEE 10th international conference on biometrics theory, applications and systems (BTAS)*. IEEE, 2019, pp. 1–8.

[7] H. H. Nguyen, J. Yamagishi, and I. Echizen, "Capsule-forensics: Using capsule networks to detect forged images and videos," in *ICASSP 2019-2019 IEEE international conference on acoustics, speech and signal processing (ICASSP)*. IEEE, 2019, pp. 2307–2311.

[8] R. Natsume, T. Yatagawa, and S. Morishima, "Fsnet: An identity-aware generative model for image-based face swapping," in *Computer Vision–ACCV 2018: 14th Asian Conference on Computer Vision, Perth, Australia, December 2–6, 2018, Revised Selected Papers, Part VI 14*. Springer, 2019, pp. 117–132.

[9] Y. Nirkin, Y. Keller, and T. Hassner, "Fsgan: Subject agnostic face swapping and reenactment," in *Proceedings of the IEEE/CVF international conference on computer vision*, 2019, pp. 7184–7193.

[10] Z. He, W. Zuo, M. Kan, S. Shan, and X. Chen, "Attgan: Facial attribute editing by only changing what you want," *IEEE transactions on image processing*, vol. 28, no. 11, pp. 5464–5478, 2019.

[11] H. Tang, D. Xu, N. Sebe, and Y. Yan, "Attention-guided generative adversarial networks for unsupervised image-to-image translation," in *2019 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2019, pp. 1–8.

[12] X. Li, S. Zhang, J. Hu, L. Cao, X. Hong, X. Mao, F. Huang, Y. Wu, and R. Ji, "Image-to-image translation via hierarchical style disentanglement," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2021, pp. 8639–8648.

[13] F. Matern, C. Riess, and M. Stamminger, "Exploiting visual artifacts to expose deepfakes and face manipulations," in *2019 IEEE Winter Applications of Computer Vision Workshops (WACVW)*. IEEE, 2019, pp. 83–92.

[14] Y. Nirkin, L. Wolf, Y. Keller, and T. Hassner, "Deepfake detection based on discrepancies between faces and their context," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 10, pp. 6111–6121, 2021.

[15] Z. Liu, X. Qi, and P. H. Torr, "Global texture enhancement for fake face detection in the wild," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 8060–8069.

[16] Z. Chen, L. Xie, S. Pang, Y. He, and B. Zhang, "Magdr: Mask-guided detection and reconstruction for defending deepfakes," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 9014–9023.

[17] S. Dong, J. Wang, J. Liang, H. Fan, and R. Ji, "Explaining deepfake detection by analysing image matching," in *European conference on computer vision*. Springer, 2022, pp. 18–35.

[18] T. Wang and K. P. Chow, "Noise based deepfake detection via multi-head relative-interaction," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, no. 12, 2023, pp. 14 548–14 556.

[19] B. Huang, Z. Wang, J. Yang, J. Ai, Q. Zou, Q. Wang, and D. Ye, "Implicit identity driven deepfake face swapping detection," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2023, pp. 4490–4499.

[20] S. Dong, J. Wang, R. Ji, J. Liang, H. Fan, and Z. Ge, "Implicit identity leakage: The stumbling block to improving deepfake detection generalization," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2023, pp. 3994–4004.

[21] Z. Shang, H. Xie, Z. Zha, L. Yu, Y. Li, and Y. Zhang, "Prrnet: Pixel-region relation network for face forgery detection," *Pattern Recognition*, vol. 116, p. 107950, 2021.

[22] L. Li, J. Bao, T. Zhang, H. Yang, D. Chen, F. Wen, and B. Guo, "Face x-ray for more general face forgery detection," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 5001–5010.

[23] T. S. Gunawan, S. A. M. Hanafiah, M. Kartiwi, N. Ismail, N. F. Za'bah, and A. N. Nordin, "Development of photo forensics algorithm by detecting photoshop manipulation using error level analysis," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 7, no. 1, pp. 131–137, 2017.

[24] H. Liu, X. Li, W. Zhou, Y. Chen, Y. He, H. Xue, W. Zhang, and N. Yu, "Spatial-phase shallow learning: rethinking face forgery detection in frequency domain," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2021, pp. 772–781.

[25] P. Yu, J. Fei, Z. Xia, Z. Zhou, and J. Weng, "Improving generalization by commonality learning in face forgery detection," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 547–558, 2022.

[26] J. Wang, Z. Wu, W. Ouyang, X. Han, J. Chen, Y.-G. Jiang, and S.-N. Li, "M2tr: Multi-modal multi-scale transformers for deepfake detection," in *Proceedings of the 2022 international conference on multimedia retrieval*, 2022, pp. 615–623.

[27] I. Masi, A. Killekar, R. M. Mascarenhas, S. P. Gurudatt, and W. AbdAlmageed, "Two-branch recurrent network for isolating deepfakes in videos," in *Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part VII 16*. Springer, 2020, pp. 667–684.

[28] C. Miao, Z. Tan, Q. Chu, N. Yu, and G. Guo, "Hierarchical frequency-assisted interactive networks for face manipulation detection," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3008–3021, 2022.

[29] C. Wang and W. Deng, "Representative forgery mining for fake face detection," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2021, pp. 14 923–14 932.

[30] A. Rossler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "Faceforensics++: Learning to detect manipulated facial images," in *Proceedings of the IEEE/CVF international conference on computer vision*, 2019, pp. 1–11.

[31] Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, "Celeb-df: A large-scale challenging dataset for deepfake forensics," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 3207–3216.

[32] N. Dufour and A. Gully, "Contributing data to deepfake detection research," *Google AI Blog*, vol. 1, no. 2, p. 3, 2019.

[33] M. Tan and Q. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," in *International conference on machine learning*. PMLR, 2019, pp. 6105–6114.

[34] H. Chen, Y. Lin, B. Li, and S. Tan, "Learning features of intra-consistency and inter-diversity: Keys toward generalizable deepfake detection," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 3, pp. 1468–1480, 2022.

[35] T.-Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollar, "Focal loss for dense object detection," in *Proceedings of the IEEE International Conference on Computer Vision*, 2017, pp. 2980–2988.

[36] D. Cozzolino, J. Thies, A. Rössler, C. Riess, M. Nießner, and L. Verdoliva, "Forensictransfer: Weakly-supervised domain adaptation for forgery detection," *arXiv preprint arXiv:1812.02510*, 2018.

[37] D. Li, Y. Yang, Y.-Z. Song, and T. Hospedales, "Learning to generalize: Meta-learning for domain generalization," in *Proceedings of the AAAI conference on artificial intelligence*, vol. 32, no. 1, 2018.

[38] K. Sun, H. Liu, Q. Ye, Y. Gao, J. Liu, L. Shao, and R. Ji, "Domain general face forgery detection by learning to weight," in *Proceedings of the AAAI conference on artificial intelligence*, vol. 35, no. 3, 2021, pp. 2638–2646.

[39] K. Sun, T. Yao, S. Chen, S. Ding, J. Li, and R. Ji, "Dual contrastive learning for general face forgery detection," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, no. 2, 2022, pp. 2316–2324.

[40] B. Liu, B. Liu, M. Ding, T. Zhu, and X. Yu, "Ti2net: temporal identity inconsistency network for deepfake detection," in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 2023, pp. 4691–4700.

[41] C. Miao, Q. Chu, W. Li, S. Li, Z. Tan, W. Zhuang, and N. Yu, "Learning forgery region-aware and id-independent features for face manipulation detection," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 4, no. 1, pp. 71–84, 2021.

[42] Y. Qian, G. Yin, L. Sheng, Z. Chen, and J. Shao, "Thinking in frequency: Face forgery detection by mining frequency-aware clues," in *European conference on computer vision*. Springer, 2020, pp. 86–103.

[43] Y. Luo, Y. Zhang, J. Yan, and W. Liu, "Generalizing face forgery detection with high-frequency features," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2021, pp. 16 317–16 326.

[44] Y. Wang, K. Yu, C. Chen, X. Hu, and S. Peng, "Dynamic graph learning with content-guided spatial-frequency relation reasoning for deepfake detection," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2023, pp. 7278–7287.

[45] J. Fei, Y. Dai, P. Yu, T. Shen, Z. Xia, and J. Weng, "Learning second order local anomaly for general face forgery detection," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022, pp. 20 270–20 280.

[46] H. Zhao, W. Zhou, D. Chen, T. Wei, W. Zhang, and N. Yu, "Multi-attentional deepfake detection," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2021, pp. 2185–2194.

[47] H. Chen, Y. Li, D. Lin, B. Li, and J. Wu, "Watching the big artifacts: Exposing deepfake videos via bi-granularity artifacts," *Pattern Recognition*, vol. 135, p. 109179, 2023.

[48] C. Tian, Z. Luo, G. Shi, and S. Li, "Frequency-aware attentional feature fusion for deepfake detection," in *ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2023, pp. 1–5.

[49] S. Chen, T. Yao, Y. Chen, S. Ding, J. Li, and R. Ji, "Local relation learning for face forgery detection," in *Proceedings of the AAAI conference on artificial intelligence*, vol. 35, no. 2, 2021, pp. 1081–1088.

Integrated Detection and Tracking Framework for 3D Multi-Object Tracking in Vehicle-Infrastructure Cooperation

Tao Hu, Ping Wang, Xinhong Wang
College of Electronic and Information Engineering
Tongji University, Shanghai, China

***Abstract*—Vehicle-infrastructure cooperative perception has emerged as a promising approach to enhance 3D multi-object tracking by leveraging complementary data from vehicle and infrastructure sensors. However, existing methods face significant challenges, including difficulty in handling occlusions, suboptimal identity association, and inefficiencies in trajectory management, limiting their performance in real-world scenarios. In this paper, we propose a novel vehicle-infrastructure cooperative 3D multi-object tracking framework that addresses these challenges through three key innovations. First, an integrated detection-tracking framework jointly optimizes object detection and tracking, enhancing temporal consistency and reducing errors caused by separately handling the two tasks. Second, the XIOU identity association metric leverages 3D spatial and geometric relationships, ensuring robust object matching even under occlusions. Third, a four-stage cascade matching (FSCM) strategy adaptively manages trajectories by leveraging detection and prediction confidences, enabling accurate tracking in complex environments. Evaluated on the V2X-Seq dataset, our method achieves a MOTA of 57.23 and a MOTP of 74.64, significantly reducing identity switches while ensuring low bandwidth consumption and reliable tracking, highlighting its effectiveness and suitability for real-world deployment.**

***Keywords*—Vehicle-infrastructure cooperative perception; 3D multi-object tracking; XIOU metric; four-stage cascade matching; integrated detection-tracking framework**

I. Introduction

In recent years, while single-vehicle perception for autonomous driving has achieved notable advancements, *vehicle-infrastructure cooperative perception* has emerged as a transformative alternative. By integrating data from infrastructure-side sensors, this approach overcomes the inherent limitations of vehicle-only systems, such as limited perception range, blind spots, and lower detection confidence. It extends perception capabilities, enhances detection accuracy, and improves system reliability, positioning itself as a critical research focus in modern autonomous driving.

A cornerstone of vehicle-infrastructure cooperative perception is *3D multi-object tracking (MOT)*, which ensures temporal consistency by tracking objects across consecutive frames. Accurate 3D MOT is pivotal for downstream tasks like trajectory prediction and collision avoidance, directly contributing to the safety and effectiveness of autonomous driving systems. The objective is to accurately localize objects in 3D space while consistently maintaining their identities over time.

However, despite advancements in cooperative perception, 3D MOT methods still encounter significant challenges:

1) Insufficient Interaction Between Detection and Tracking: Many existing methods treat detection and tracking as separate processes, often relying on the *Tracking-by-Detection* paradigm. This limits the mutual enhancement between detection and tracking, as detection results are primarily optimized for tracking while failing to incorporate the valuable priors that tracking can provide for detection—an essential aspect for temporal consistency in dynamic environments.
2) Insufficient Utilization of 3D Spatial Information: Current methods often adapt 2D identity association techniques to 3D scenarios without fully harnessing the spatial richness of 3D point clouds. This limitation is particularly pronounced in vehicle-infrastructure cooperative contexts, where precise spatial alignment and 3D pose estimation are key for robust identity association.
3) Challenges in Occlusion Handling: Occlusion is a common occurrence in real-world autonomous driving scenarios, yet existing methods struggle to maintain consistent object identities when visibility is compromised. Effective mechanisms to handle occlusion and manage identity switches during visibility transitions remain underdeveloped.

These limitations underscore the need for more integrated, adaptive, and robust approaches to 3D MOT in vehicle-infrastructure cooperative scenarios. To address these challenges, we propose a novel *vehicle-infrastructure cooperative 3D multi-object tracking algorithm* based on an integrated detection and tracking architecture. By leveraging LiDAR point cloud data from both vehicle and infrastructure sources, our method provides a more accurate and real-time solution for 3D object detection and tracking. Specifically, it introduces the following key innovations:

1) Integrated Detection and Tracking Framework: We propose a fully integrated architecture that processes detection and tracking in a unified manner. By employing position encoding and cross-attention mechanisms, the framework seamlessly combines appearance and motion cues. Additionally, a temporal prior enhancement module is introduced, allowing tracking results to inform the detection process, leveraging

temporal priors to improve detection accuracy.

2) 3D-Task Adaptive Identity Association: Our method takes full advantage of 3D spatial pose information from LiDAR point clouds. We introduce a new identity association metric that accounts for spatial overlap, positional similarity, and orientation alignment, enabling robust object matching over time in 3D space.
3) Occlusion-Adaptive Matching Algorithm: We present a four-stage cascade matching algorithm that dynamically adjusts the tracking process based on the confidence levels of detection and prediction results. This strategy ensures robust tracking during occlusion events, effectively maintaining object identities even when objects are partially or fully hidden from view.

The remainder of this paper is organized as follows: Section II reviews related work, discussing existing approaches to vehicle-infrastructure cooperative 3D perception. Section III describes the proposed integrated detection and tracking framework in detail. Section IV outlines the experimental setup and results, covering datasets, evaluation metrics, and comprehensive analyses. Section V concludes the paper with final remarks and future research directions.

II. Related Work

This section discusses recent developments in *vehicle-infrastructure cooperative perception* and *multi-object tracking (MOT)*, both critical for improving autonomous driving systems.

A. Vehicle-Infrastructure Cooperative Perception

Cooperative perception enhances the perception capabilities of individual vehicles by integrating data from infrastructure-based sensors. It can be categorized into three main types based on the shared data:

1) Data-Level Cooperation: In data-level cooperation, raw sensor data such as LiDAR point clouds are directly shared between vehicles and infrastructure [1], [14], [29]. This approach allows vehicles to expand their perception range significantly by receiving unprocessed sensor data from other sources. However, the substantial data transmission requirements place a significant burden on network bandwidth.

2) Feature-Level Cooperation: Feature-level cooperation involves sharing pre-processed feature data, reducing the transmission load while retaining more information than object-level cooperation [17], [6], [5]. The performance of feature-level cooperation depends heavily on the feature fusion strategies employed, balancing between bandwidth savings and the amount of retained information.

3) Object-Level Cooperation: In object-level cooperation, only the final detection results are shared, minimizing the data transmission burden but potentially leading to information loss [24]. This method relies heavily on the accuracy and robustness of the individual perception models used on each vehicle and infrastructure component.

The emergence of large-scale cooperative perception datasets, both in simulation and real-world environments, has greatly advanced research in this domain. Notable examples include *V2X-Sim* [10], *DAIR-V2X-C* [24], and *V2X-Seq* [25], with *V2X-Seq* standing out as the first real-world dataset for vehicle-infrastructure sequential perception. These datasets provide comprehensive data for 3D object detection and tracking tasks, offering a foundation for further research in cooperative perception.

B. Multi-Object Tracking

In cooperative perception, *multi-object tracking (MOT)* plays a critical role in maintaining object identities over time by associating detected objects across frames, forming a temporal understanding of their movement. MOT is crucial for downstream tasks such as trajectory prediction and collision avoidance in autonomous driving. The process typically involves three main stages: object detection and feature representation, identity association, and trajectory management.

1) Object Detection and Feature Representation: This stage handles the initial detection and feature extraction from sensory data, which is critical for tracking objects across time. Traditionally, these tasks have been performed separately, with detection followed by feature extraction. One prominent example of this approach is *DeepSort* [19], which uses a Kalman filter for motion modeling and a deep learning-based appearance descriptor for object re-identification, offering a robust solution for tracking objects across frames while maintaining their identities. Recent methods, such as *OmniTracker* [16], focus on exploring the interplay between detection and tracking and transferring this relationship to various tracking tasks. This separation allows for independent optimization of detection and tracking, but it may lead to redundant computations.

Joint detection and feature representation, on the other hand, combines detection and tracking into a single network, improving the efficiency of multi-object tracking. Popular methods like *FairMOT* [27] and *TransTrack* [15] employ joint architectures where object detection and feature extraction are performed simultaneously, reducing the computational overhead while improving feature consistency. *TransMOT* [4] introduces a spatio-temporal graph transformer for encoding short trajectories and matching them across frames using a spatial graph decoder. Additionally, *UTM* [23] simultaneously enhances object detection and feature representation using identity-sensitive knowledge. Despite these advancements, challenges remain, especially in 3D multi-object tracking, where integrating motion cues and spatial information from point cloud data requires sophisticated handling of dynamic environments.

2) Identity Association: Identity association is critical for tracking objects across multiple frames and ensuring that each object maintains a consistent identity. Various metrics have been proposed to perform this association. Early works such as *AB3DMOT* [18] rely on simple intersection-over-union (IoU) metrics to associate objects between frames. However, this method struggles with occlusions and complex 3D environments. Recent researches such as Chiu et al. [3] and *CenterPoint* [22] improve identity association by replacing traditional IoU with more sophisticated metrics like Mahalanobis and L2 distance. These metrics help capture both spatial overlap and the underlying distribution of data points, enhancing tracking accuracy, especially in complex 3D environments where simple IoU metrics may struggle.

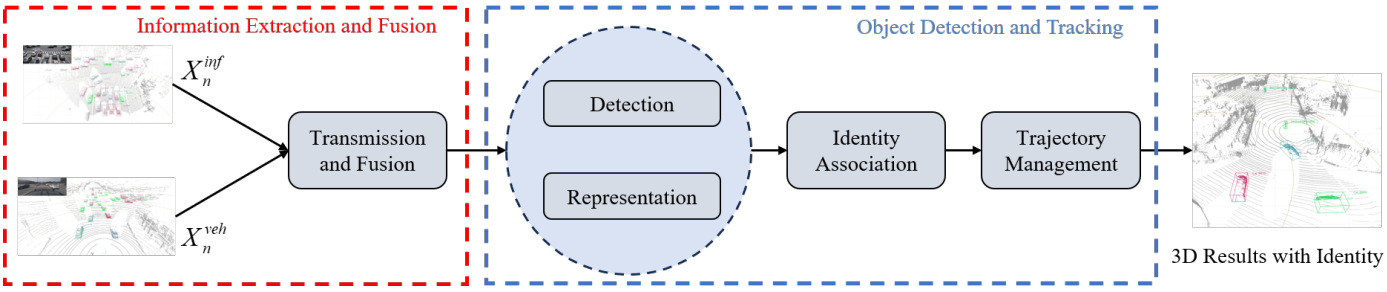


Fig. 1. The temporal perception process in vehicle-infrastructure cooperative sensing: The process comprises two main parts: data fusion and object detection-tracking, producing a 3D perception output with identity information.

Advanced association methods have been developed to handle more complex scenarios. *C-BIoU* [21] improves traditional IoU-based matching by introducing a buffer region around the bounding boxes, enhancing matching accuracy under occlusion. *EagerMOT* [7] incorporates velocity and directionality into the association process, leveraging motion cues to improve association reliability. Another advanced metric, *DIoU* [28], introduces distance and aspect ratio terms into the IoU calculation, improving matching accuracy in 2D scenarios. These identity association techniques aim to reduce false positives and increase the robustness of tracking in dynamic environments where objects may be occluded or exhibit erratic movement.

3) Trajectory Management: The final stage of MOT involves managing the trajectories of objects across frames. The goal is to maintain accurate object tracks while adding, updating, or removing object trajectories as necessary. Early methods such as *SORT* [2] use a simple bipartite graph matching approach to link detected objects between consecutive frames. This method provides a fast and efficient solution but is limited in handling occlusions and long-term tracking.

More advanced techniques, such as *DeepSort* [19], use a cascade matching strategy where recently updated trajectories are prioritized during the matching process, allowing for better handling of short-term occlusions. *ByteTrack* [26] takes this approach further by splitting detections into high and low-confidence categories, first matching high-confidence detections with tracked objects, and then using low-confidence detections to match occluded objects. This technique improves the continuity of object trajectories during occlusions. Recent methods like *SimpleTrack* [12] adapt ByteTrack's methodology to 3D tracking tasks, introducing confidence-based updates to better handle occlusion in real-world environments. Another recent method, *SimTrack* [11], criticizes the heuristic matching approach of earlier methods, arguing that it relies too heavily on manual tuning. Instead, *SimTrack* proposes using a confidence-weighted matching strategy between the predicted object locations and the detected objects, simplifying the tracking process while improving robustness. These trajectory management strategies aim to maintain object continuity across time, especially when objects undergo occlusions or disappear from the field of view temporarily.

Despite the progress made, several challenges remain in multi-object tracking, especially in 3D environments where spatial and temporal dynamics are more complex. One major limitation is the failure to fully integrate the strengths of both object detection and tracking, which are often treated as independent tasks. Furthermore, current 3D identity association metrics do not make full use of the precise pose information available in point clouds, hindering matching accuracy. Moreover, cross-frame matching strategies fail to leverage both detection and prediction dimensions to fully explore and maintain object identity, particularly in complex and dynamic environments. These gaps highlight areas for further research and improvement.

III. Methodology

In the case where the vehicle and infrastructure sensors collect data at consistent frequencies, the input for the vehicle-infrastructure cooperative 3D multi-object tracking task can be described in two parts:

1. The infrastructure-side sensor data sequence $\mathbf{S}^{\text{inf}}$, as shown in Eq. (1), where $\mathbf{X}_n^{\text{inf}}$ represents the infrastructure sensor data from the n-th pair of vehicle-infrastructure matched data. The corresponding timestamp sequence for the infrastructure data is denoted as $\mathbf{T}^{\text{inf}}$, as shown in Eq. (2).

$$\mathbf{S}^{\text{inf}} = \{\mathbf{X}_n^{\text{inf}}\}_{n=1}^{N} \tag{1}$$

$$\mathbf{T}^{\text{inf}} = \{t_n^{\text{inf}}\}_{n=1}^{N} \tag{2}$$

2. The vehicle-side sensor data sequence $\mathbf{S}^{\text{veh}}$, as shown in Eq. (3), where $\mathbf{X}_n^{\text{veh}}$ represents the vehicle sensor data from the n-th pair of vehicle-infrastructure matched data. The corresponding timestamp sequence for the vehicle data is denoted as $\mathbf{T}^{\text{veh}}$, as shown in Eq. (4).

$$\mathbf{S}^{\text{veh}} = \{\mathbf{X}_n^{\text{veh}}\}_{n=1}^{N} \tag{3}$$

$$\mathbf{T}^{\text{veh}} = \{t_n^{\text{veh}}\}_{n=1}^{N} \tag{4}$$

As shown in Fig. 1, the vehicle-infrastructure cooperative 3D multi-object tracking process is composed of two main parts: information extraction and fusion, and object detection and tracking. These are further divided into four stages:

- Data Transmission and Fusion: This stage involves pre-processing vehicle and infrastructure point cloud data. The data is transmitted over limited bandwidth

to the vehicle side, where it is fused with the vehicle's sensor data.

- Object Detection and Feature Representation: This stage detects 3D objects from the fused sensor data and represents the temporal variations in the object features.
- Identity Association: The system builds a unified identity association benchmark for objects across frames based on their features. A cost matrix is generated to match objects across frames.
- Trajectory Management: Based on the cost matrix from identity association, the system performs matching between detected objects and existing tracks. It also handles adding, deleting, and updating tracks, ultimately producing a unified 3D spatiotemporal perception result with identity information.

A. Data Transmission and Fusion Using the FF-Tracking Framework

This section leverages the FF-Tracking [25] framework as outlined in *V2X-Seq*. The **Data Transmission and Fusion** process, as illustrated in Fig. 2, is designed to facilitate sensor data exchange between the vehicle and infrastructure under limited bandwidth conditions.

1) Infrastructure Side: On the infrastructure side, sensor data at timestamp t_n^{inf} is processed through the Pillar Feature Network (PFNet) [9] to extract BEV (Bird's Eye View) features. The extracted BEV feature map is represented as:

$$\mathbf{F}_n^{\text{inf}} = \text{PFNet}(\mathbf{X}_n^{\text{inf}}), \tag{5}$$

where $\mathbf{X}_n^{\text{inf}}$ is the raw point cloud data from the infrastructure sensors, and $\mathbf{F}_n^{\text{inf}}$ is the BEV feature extracted at time t_n^{inf}.

Next, a Feature Flow Generator is employed to capture the temporal dynamics between consecutive infrastructure frames. Given the BEV feature map from the current timestamp t_n^{inf} and the previous timestamp t_{n-1}^{inf}, the feature flow $\mathbf{F}_n^{\text{flow}}$ is computed as:

$$\mathbf{F}_n^{\text{flow}} = \text{FlowGenerator}(\mathbf{F}_n^{\text{inf}}, \mathbf{F}_{n-1}^{\text{inf}}), \tag{6}$$

where the *FlowGenerator* module is built with two Backbone-FPN structures, one branch generates static features $\mathbf{F}^{\text{static}}$, and the other branch generates the feature derivative $\mathbf{F}^{\text{deriv}}$. This module computes the temporal differences between the two frames, capturing how the scene evolves over time. The feature flow is compressed using a convolutional layer to reduce bandwidth requirements:

$$\mathbf{F}_n^{\text{comp}} = \text{Conv}(\mathbf{F}_n^{\text{flow}}), \tag{7}$$

where $\mathbf{F}_n^{\text{comp}}$ represents the compressed feature flow ready for transmission.

2) Vehicle Side: Once the infrastructure-side compressed feature flow $\mathbf{F}_n^{\text{comp}}$ is transmitted to the vehicle side, it undergoes Deconvolution to reconstruct the infrastructure features at the vehicle's side:

$$\mathbf{F}_n^{\text{rec}} = \text{Deconv}(\mathbf{F}_n^{\text{comp}}), \tag{8}$$

where $\mathbf{F}_n^{\text{rec}}$ denotes the reconstructed feature map, which can be divided into two parts: one part represents the static feature $\mathbf{F}_n^{\text{static}}$, and the other part represents the feature derivative $\mathbf{F}_n^{\text{deriv}}$.

Next, the vehicle aligns the reconstructed infrastructure features to its own current timestamp t_n^{veh} using the Prediction and Affine Transform module. This module compensates for temporal misalignment between the infrastructure and vehicle data:

$$\mathbf{F}_n^{\text{align}} = \text{AffineTransform}(\mathbf{F}_n^{\text{static}} + (t_n^{\text{veh}} - t_n^{\text{inf}}) \cdot \mathbf{F}_n^{\text{deriv}}), \tag{9}$$

where $\mathbf{F}_n^{\text{align}}$ represents the aligned infrastructure features in the vehicle's frame of reference.

Simultaneously, the vehicle extracts its own features $\mathbf{F}_n^{\text{veh}}$ from its sensor data $\mathbf{X}_n^{\text{veh}}$:

$$\mathbf{F}_n^{\text{veh}} = \text{FeatureExtractor}(\mathbf{X}_n^{\text{veh}}). \tag{10}$$

Finally, the vehicle-side features and the aligned infrastructure features are concatenated and convolved to form the fused feature map $\mathbf{F}_n^{\text{fused}}$:

$$\mathbf{F}_n^{\text{fused}} = \text{Conv}(\text{Concat}(\mathbf{F}_n^{\text{veh}}, \mathbf{F}_n^{\text{align}})). \tag{11}$$

This fused feature map, containing both vehicle-side and infrastructure-side data, is passed to the detection and tracking modules for further processing.

B. Integrated Object Detection and Tracking

In this section, we describe the proposed integrated object detection and tracking framework, utilizing a Deformable DETR-based architecture for both encoding and decoding stages, as shown in Fig. 3. The architecture is composed of the following core components: **Temporal Prior Enhancement**, **Encoder**, and two parallel branches for **Object Detection** and **Object Prediction**.

1) Temporal Prior Enhancement: The input to the Temporal Prior Enhancement module consists of the fused feature maps from two consecutive frames, $\mathbf{F}_n^{\text{fused}}$ and $\mathbf{F}_{n-1}^{\text{fused}}$. To save computational resources, the fused feature map from the previous frame is stored and used in the next frame for prior enhancement. The previous frame's fused feature map, $\mathbf{F}_{n-1}^{\text{fused}}$, is downsampled and serves as the keys ($\mathbf{K}$) and values ($\mathbf{V}$) for the cross-attention mechanism. The current frame's fused feature map, $\mathbf{F}_n^{\text{fused}}$, is used as the queries ($\mathbf{Q}$).

The cross-attention mechanism computes the weighted combination of the features as follows:

$$\text{Attention}(\mathbf{Q}, \mathbf{K}, \mathbf{V}) = \text{softmax}\left(\frac{\mathbf{Q}\mathbf{K}^T}{\sqrt{d_k}}\right)\mathbf{V}, \tag{12}$$

where $\mathbf{Q} = \mathbf{F}_n^{\text{fused}}$ is the query from the current frame, and $\mathbf{K}$, $\mathbf{V} = \mathbf{F}_{n-1}^{\text{fused}}$ are the key and value from the previous frame. The term d_k represents the dimension of the key, which is used to scale the dot product between the query and key to prevent the result from becoming too large. After cross-attention, the resulting feature map undergoes further refinement through a Multilayer Perceptron (MLP) for introducing non-linearity and enhancing the model's capacity to capture complex relationships in the data:

$$\mathbf{F}_n^{\text{enhanced}} = \text{MLP}(\text{Attention}(\mathbf{F}_n^{\text{fused}}, \mathbf{F}_{n-1}^{\text{fused}})). \tag{13}$$

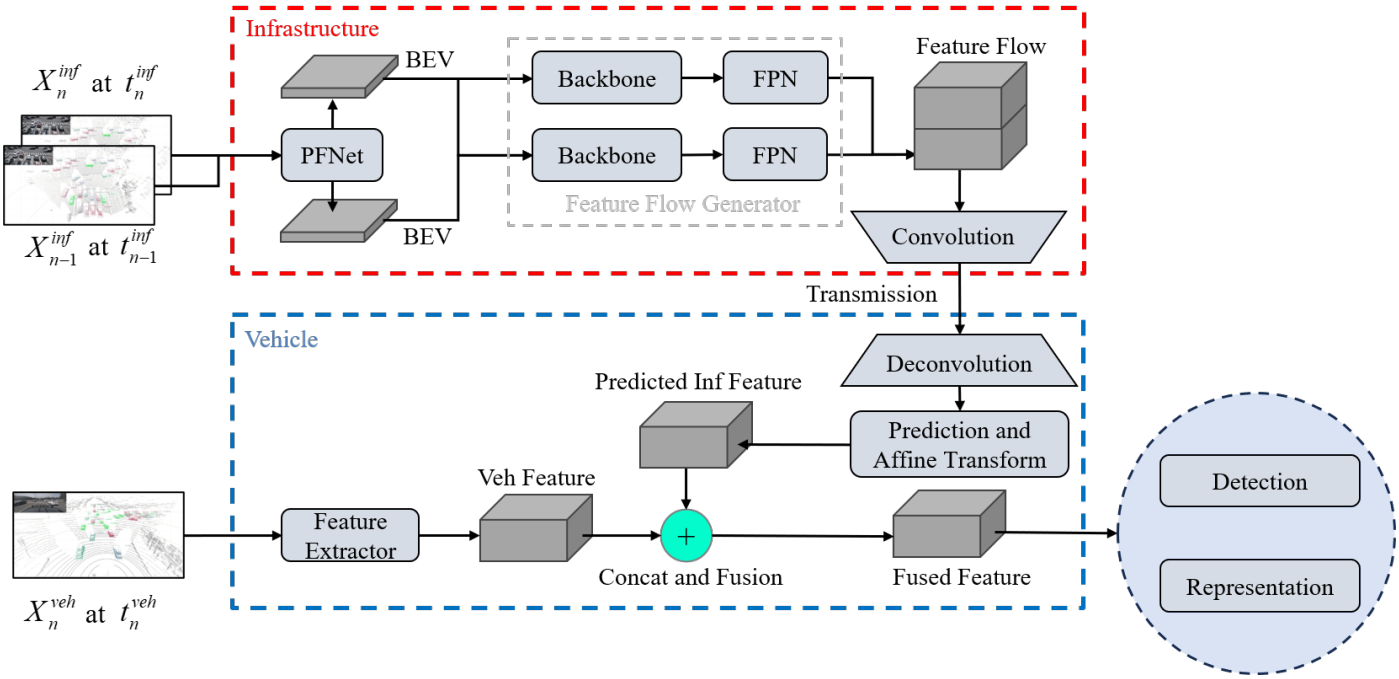


Fig. 2. The architecture of the data transmission and fusion module using the FF-Tracking framework. Infrastructure-side features are compressed and transmitted to the vehicle, where they are deconvolved, temporally and spatially aligned, and fused with vehicle-side data.

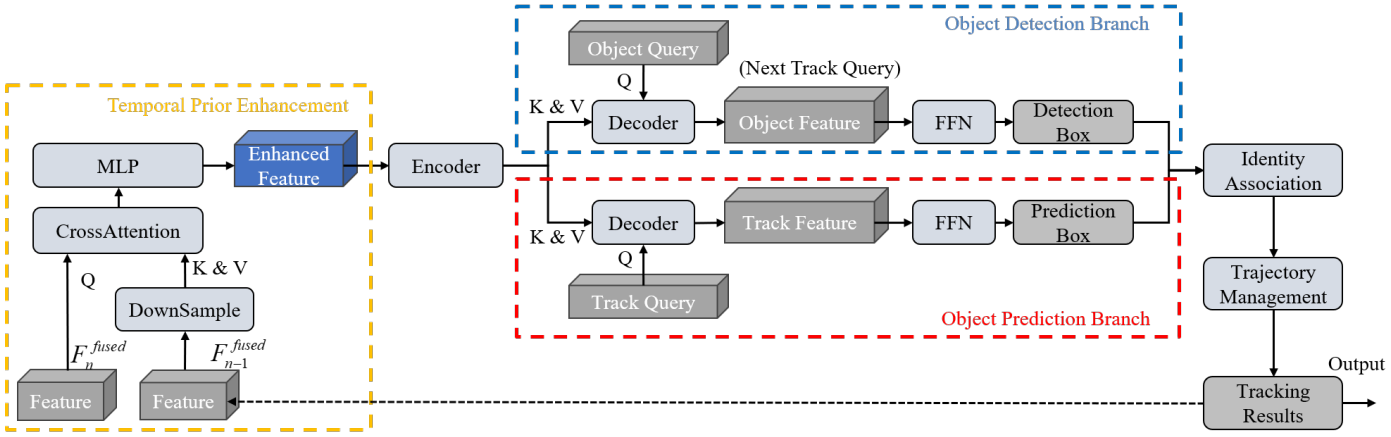


Fig. 3. The overall architecture for integrated object detection and tracking using deformable DETR. The process includes temporal prior enhancement, encoding, and two parallel branches for object detection and prediction, which jointly contribute to tracking results.

The output is the enhanced feature map $\mathbf{F}_n^{\text{enhanced}}$, which integrates temporal information from the previous frame to improve the accuracy and stability of detection and tracking in the current frame.

2) Encoder: The enhanced feature $\mathbf{F}_n^{\text{enhanced}}$ is passed to a Deformable DETR Encoder [30], which applies deformable attention over a set of reference points $\mathbf{P}$ distributed across the feature map. These reference points guide the attention mechanism, allowing it to focus on relevant regions, which is particularly suitable for sparse input data like point clouds:

$$\mathbf{Z}_n^{\text{enc}} = \text{DeformableAttention}(\mathbf{F}_n^{\text{enhanced}}, \mathbf{K}, \mathbf{V}, \mathbf{P}), \quad (14)$$

where $\mathbf{Z}_n^{\text{enc}}$ is the output of the encoder, and $\mathbf{K}$, $\mathbf{V}$ are derived from the same enhanced feature map $\mathbf{F}_n^{\text{enhanced}}$.

3) Object Detection Branch: The Object Detection Branch uses the encoded feature $\mathbf{Z}_n^{\text{enc}}$ and processes it through a Deformable DETR decoder to detect objects within the current frame. The decoder utilizes a set of learnable object queries $\mathbf{Q}^{\text{obj}}$ to retrieve object features:

$$\mathbf{F}_n^{\text{obj}} = \text{Decoder}(\mathbf{Q}^{\text{obj}}, \mathbf{Z}_n^{\text{enc}}), \quad (15)$$

where $\mathbf{F}_n^{\text{obj}}$ represents the detected object features. These features are passed to a feedforward neural network (FFN) to generate detection bounding boxes $\mathbf{B}_n^{\text{det}}$:

$$\mathbf{B}_n^{\text{det}} = \text{FFN}(\mathbf{F}_n^{\text{obj}}). \quad (16)$$

4) Object Prediction Branch: Simultaneously, the Object Prediction Branch tracks objects by predicting their locations

in the next frame based on past tracking information. The encoded feature $\mathbf{Z}_n^{\text{enc}}$ is processed with the track query $\mathbf{Q}^{\text{track}}$ which is the object features $\mathbf{F}_{n-1}^{\text{obj}}$ in the previous frame, retrieving the tracking features $\mathbf{F}_n^{\text{track}}$:

$$\mathbf{F}_n^{\text{track}} = \text{Decoder}(\mathbf{Q}^{\text{track}}, \mathbf{Z}_n^{\text{enc}}). \tag{17}$$

These features are processed through another FFN to predict the locations of objects from the previous frame in the current frame, providing the propagated positions for the tracked objects $\mathbf{B}_n^{\text{pred}}$:

$$\mathbf{B}_n^{\text{pred}} = \text{FFN}(\mathbf{F}_n^{\text{track}}). \tag{18}$$

5) Identity Association and Trajectory Management: The detected objects and predicted objects are matched using an identity association module, which computes a cost matrix between detection and prediction bounding boxes. This cost matrix is used to associate objects between frames. The tracking results are then managed in the trajectory management module, which updates existing trajectories, adds new trajectories, and deletes lost trajectories.

6) Advantages of Integrated Design: The integrated design of this architecture, based on Deformable DETR, allows simultaneous object detection and tracking within the same pipeline. By sharing the same enhanced features and attention mechanisms between detection and prediction branches, the architecture efficiently combines object detection and tracking tasks. This integration fully leverages the complementary relationship between detection and tracking, as the temporal prior information enhances the consistency of the features, allowing detection and tracking to mutually benefit from each other's information.

C. Identity Association Using XIOU Metric

In our approach, we propose a novel **XIOU** metric for identity association between detected and predicted objects. This metric incorporates three key factors: Intersection over Union (IOU), center point distance, and yaw angle difference between the two bounding boxes (as shown in Fig. 4).

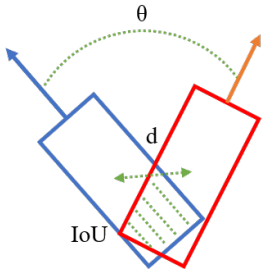


Fig. 4. Visualization of XIOU elements: IOU, center point distance, and yaw angle difference.

First, the basic IOU is calculated between the detection bounding box $\mathbf{B}^{\text{det}}$ and the prediction bounding box $\mathbf{B}^{\text{pred}}$, which measures the overlap between the two boxes:

$$\text{IOU}(\mathbf{B}^{\text{det}}, \mathbf{B}^{\text{pred}}) = \frac{V_{\text{I}}}{V_{\text{U}}}, \tag{19}$$

where V_{I} is the intersection volume of the two 3D bounding boxes, and V_{U} is their union volume.

To improve upon the limitations of IOU in cases where there is no overlap between the two boxes, the Generalized IOU (GIOU) [13] metric is used:

$$\text{GIOU}(\mathbf{B}^{\text{det}}, \mathbf{B}^{\text{pred}}) = \frac{V_{\text{I}}}{V_{\text{U}}} - \frac{V_{\text{C}} - V_{\text{U}}}{V_{\text{C}}}, \tag{20}$$

where V_{C} is the volume of the smallest convex shape enclosing both $\mathbf{B}^{\text{det}}$ and $\mathbf{B}^{\text{pred}}$. GIOU extends IOU by adding a distance-based penalty term, addressing cases where IOU is zero due to non-overlapping boxes.

Building on GIOU, our **XIOU** metric further integrates orientation and distance between the center points of the two boxes:

$$G_{\cos}(\theta_{\mathbf{B}^{\text{det}}}, \theta_{\mathbf{B}^{\text{pred}}}) = \cos(\theta_{\mathbf{B}^{\text{det}}} - \theta_{\mathbf{B}^{\text{pred}}}) + 1, \tag{21}$$

$$G_{\text{iou}}(\mathbf{B}^{\text{det}}, \mathbf{B}^{\text{pred}}) = \text{GIOU}(\mathbf{B}^{\text{det}}, \mathbf{B}^{\text{pred}}) + 1, \tag{22}$$

$$\text{XIOU}(\mathbf{B}^{\text{det}}, \mathbf{B}^{\text{pred}}) = \frac{G_{\text{iou}} \times G_{\cos}}{4}, \tag{23}$$

where $\theta_{\mathbf{B}^{\text{det}}}$ and $\theta_{\mathbf{B}^{\text{pred}}}$ represent the yaw angles (orientations) of the detection and prediction bounding boxes, respectively. This term captures the orientation difference between the boxes, while the GIOU term handles their spatial relationship.

Our **XIOU** metric offers improved performance in 3D environments by taking into account the spatial overlap, orientation similarity, and distance between objects. This makes it particularly well-suited for 3D object tracking tasks, where precise alignment of object positions and orientations is crucial for maintaining consistent identities across frames.

D. Trajectory Management with Cascade Matching

Trajectory management plays a critical role in maintaining accurate object tracking over time. This step involves matching detected objects with existing trajectories, updating object tracks, and handling the creation or deletion of tracks as necessary. Traditional approaches, such as ByteTrack, employ a two-stage matching process, starting with high-confidence detections followed by low-confidence ones. However, this approach struggles in occlusion scenarios. As shown in Fig. 5(a), object detection confidence gradually decreases during occlusion, while Fig. 5(b) shows how confidence slowly recovers when occlusion fades.

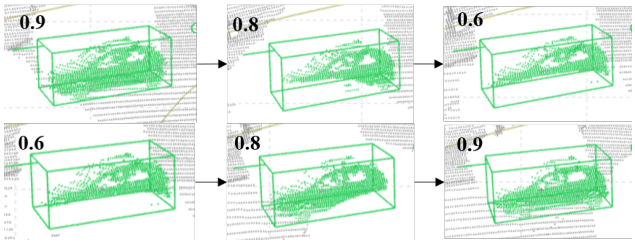


Fig. 5. (a) Confidence decline during occlusion. (b) Confidence recovery after occlusion. The figures illustrate how detection confidence changes when objects are occluded and when occlusion diminishes.

To address the challenges of tracking objects under occlusion, we introduce a **Four-Stage Cascade Matching (FSCM)** algorithm. This method improves upon previous approaches by dividing detection results and track predictions

into high-confidence and low-confidence categories, handling them across four stages. Each stage applies the Hungarian algorithm to perform the matching based on the XIOU similarity metric, which considers object overlap, orientation, and spatial alignment.

1) Stage 1: High-confidence Detection and High-confidence Track Matching: In the first stage, detections and tracks are divided into high-confidence and low-confidence sets based on predefined thresholds. A detection is considered high-confidence if its detection score s_d exceeds the detection threshold m_d, and similarly, a track is considered high-confidence if its tracking confidence score s_t exceeds the tracking threshold m_t. High-confidence detections $\mathbf{D}^{\text{high}}$ are matched with high-confidence tracks $\mathbf{T}^{\text{high}}$. The cost matrix is computed as:

$$\mathbf{C}^{\text{high}} = \mathbf{1} - \text{XIOU}(\mathbf{D}^{\text{high}}, \mathbf{T}^{\text{high}}). \tag{24}$$

The Hungarian [8] algorithm is applied to minimize the cost matrix $\mathbf{C}^{\text{high}}$. The matched detections and tracks are processed, while the unmatched ones are passed to the next stage.

2) Stage 2: Low-confidence Detection and High-confidence Track Matching: Low-confidence detections ($s_d < m_d$), denoted as $\mathbf{D}^{\text{low}}$, are matched with the high-confidence tracks ($s_t \geq m_t$) that remained unmatched from the previous stage. This is useful for handling partially occluded objects whose detection scores have decreased, while their tracking predictions remain reliable. The cost matrix is calculated as:

$$\mathbf{C}^{\text{low-high}} = \mathbf{1} - \text{XIOU}(\mathbf{D}^{\text{low}}, \mathbf{T}^{\text{high}}), \tag{25}$$

and the Hungarian algorithm matches the remaining high-confidence tracks with low-confidence detections.

3) Stage 3: High-confidence Detection and Low-confidence Track Matching: In this stage, high-confidence detections $\mathbf{D}^{\text{high}}$ are matched with low-confidence tracks $\mathbf{T}^{\text{low}}$, which were not matched in the previous stages. This helps recover objects that were previously occluded but are now detected with high confidence:

$$\mathbf{C}^{\text{high-low}} = \mathbf{1} - \text{XIOU}(\mathbf{D}^{\text{high}}, \mathbf{T}^{\text{low}}). \tag{26}$$

Again, the Hungarian algorithm is used to assign detections to tracks, updating the trajectories for reappearing objects.

4) Stage 4: Low-confidence Detection and Low-confidence Track Matching: Finally, low-confidence detections $\mathbf{D}^{\text{low}}$ are matched with low-confidence tracks $\mathbf{T}^{\text{low}}$. This step manages prolonged occlusion or potential false detections:

$$\mathbf{C}^{\text{low}} = \mathbf{1} - \text{XIOU}(\mathbf{D}^{\text{low}}, \mathbf{T}^{\text{low}}). \tag{27}$$

The Hungarian algorithm minimizes the cost matrix, and matched detections and tracks are processed.

5) Unmatched Detections and Tracks: If any high-confidence detections remain unmatched, they are used to initialize new tracks. Unmatched low-confidence detections are discarded as background noise. Tracks that remain unmatched are retained for N frames. If tracks remain unmatched beyond the threshold, they are deleted from the system.

6) Summary of FSCM Algorithm: This four-stage cascade matching algorithm divides both detections and predictions into high-confidence and low-confidence categories, leveraging the XIOU metric at each stage. The Hungarian algorithm is employed in all stages to ensure optimal matching. By progressively refining the matching process, this method ensures robust tracking, even under occlusion, and takes full advantage of detection and prediction confidences.

IV. Experiments

The primary goal of our experiments is to validate the effectiveness and robustness of the proposed method for vehicle-infrastructure cooperative 3D multi-object tracking. We conduct a series of experiments on the V2X-Seq dataset to evaluate the tracking performance under varying latency conditions and compare it with several state-of-the-art methods. Additionally, we perform an ablation study to investigate the contributions of the key modules in our architecture, including the integrated detection-tracking framework, XIOU identity association, and four-stage cascade matching (FSCM).

A. Dataset and Evaluation Metrics

Our experiments are conducted on the V2X-Seq dataset, the first large-scale real-world dataset specifically designed for vehicle-infrastructure cooperative 3D multi-object tracking. It contains over 15,000 pairs of synchronized vehicle-side and infrastructure-side frames, with each pair including 3D LiDAR point clouds and annotations with tracking IDs. All vehicle and infrastructure data in V2X-Seq are time-synchronized and spatially aligned, making it ideal for evaluating cooperative tracking performance in real-world scenarios. With over 150,000 frames across more than 200 sequences, V2X-Seq provides diverse traffic environments and object dynamics, offering a comprehensive benchmark for assessing tracking accuracy and robustness, especially under challenging conditions such as occlusions and communication delays. We use the following evaluation metrics to compare the performance of different methods:

- MOTA (Multi-Object Tracking Accuracy): MOTA reflects the overall tracking accuracy by considering three factors: false positives, missed targets, and identity switches. Higher values indicate better performance.

$$\text{MOTA} = 1 - \frac{\sum_t (\text{FN}_t + \text{FP}_t + \text{IDSW}_t)}{\sum_t \text{GT}_t}, \tag{28}$$

  where FN_t, FP_t, and IDSW_t are the false negatives, false positives, and identity switches at time t, and GT_t is the number of ground truth objects.

- MOTP (Multi-Object Tracking Precision): MOTP evaluates the localization precision of the tracked objects by computing the average distance between the predicted and ground-truth object locations.

$$\text{MOTP} = \frac{\sum_t \sum_i d_t^i}{\sum_t c_t}, \tag{29}$$

  where d_t^i is the distance between the predicted and ground-truth locations for object i at time t, and c_t is the number of matched object pairs at time t.

TABLE I. COMPARISON OF TRACKING PERFORMANCE ON THE V2X-SEQ DATASET UNDER DIFFERENT LATENCY CONDITIONS

Latency(ms)	Fusion Type	Method	MOTA↑	MOTP↑	IDS↓	BPS↓(Byte/s)
0	Object-Level	Hungarian [8]	53.18	72.35	273	3.3×10^3
	Data-Level	Concat [25]	56.03	70.17	296	1.3×10^7
	Feature-Level	FF-Tracking [25]	54.75	69.76	222	6.2×10^5
	Feature-Level	**Ours**	**57.23**	**74.64**	**206**	6.2×10^5
200	Object-Level	Hungarian [8]	50.32	71.58	260	3.3×10^3
	Data-Level	Concat [25]	51.27	69.67	234	1.3×10^7
	Feature-Level	FF-Tracking [25]	52.26	69.64	225	1.2×10^6
	Feature-Level	**Ours**	**55.76**	**74.15**	**219**	1.2×10^6

- IDS (Identity Switches): This metric tracks identity changes during tracking, with lower values indicating better performance.
- BPS (Bytes Per Second): This metric measures the bandwidth for vehicle-infrastructure communication, defined as the data exchanged per second in bytes.

B. Implementation Details

Our model employs a backbone network and FPN structure similar to that used in SECOND [20], optimized using the AdamW optimizer. The initial learning rate is set to 1×10^{-4}, and we use 500 queries during training. Both decoders are trained with identical loss functions, incorporating a classification loss and XIOU loss as the final objective. For the tracking process, we set the detection score threshold m_d to 0.5, tracking score threshold m_t to 0.4, and retain unmatched trajectories for $N = 20$ frames. The network is implemented in Pytorch and trained on an NVIDIA GeForce RTX 3090 GPU.

In the inference phase, the first frame's feature map serves as the prior frame's feature for downsampling and temporal prior enhancement. Simultaneously, the track query initializes with the object features from the first frame. From the second frame onward, the point cloud feature sequence is processed following the methodology described, outputting tracking results across all frames.

C. Comparison with State-of-the-Art Methods

We compare the performance of our method against several approaches in the V2X-Seq dataset under two latency conditions: 0 ms and 200 ms. The methods include data-level, object-level, and feature-level fusion techniques, specifically:

- Concat (Data-Level) [25]: In this method, the infrastructure point cloud is transformed to the vehicle's coordinate system, where pseudo-images from both vehicle and infrastructure are concatenated. This approach uses the PointPillars detector and follows AB3DMOT's TBD (tracking-by-detection) paradigm for multi-object tracking.
- Hungarian (Object-Level) [8]: In this approach, vehicle and infrastructure detections are performed independently. Detected object sets from both vehicle and infrastructure are transmitted and matched using the Hungarian algorithm to fuse results.
- FF-Tracking (Feature-Level) [25]: This method transmits the feature flow between consecutive frames from the infrastructure to the vehicle, reducing data transmission while maintaining accuracy.

As shown in Table I, our method consistently outperforms others across key metrics, particularly in **MOTA**, achieving 57.23 at 0 ms latency—**1.2 points** higher than Concat (56.03) and **4.05 points** higher than Hungarian (53.18). This improvement reflects the combined contributions of our integrated detection-tracking framework, XIOU identity association, and four-stage cascade matching (FSCM). In terms of **MOTP**, our method achieves 74.64, surpassing Concat's 70.17 and Hungarian's 72.35, highlighting its effective use of 3D positional and orientational information. Additionally, with the lowest **IDS** score of 206, it demonstrates robust identity association and trajectory management.

Under the 200 ms delay condition, our method maintains high tracking accuracy with a **MOTA** of 55.76, outperforming Concat (51.27) and Hungarian (50.32). The **MOTP** remains at 74.15, the highest among all methods, while the **IDS** count remains low at 219. These results demonstrate the resilience of our approach to communication delays, inheriting the robustness of the FF-Tracking framework. By preserving temporal consistency in feature flow and leveraging efficient identity association, the proposed framework effectively mitigates the negative impact of delayed data transmission.

In terms of data transmission efficiency, our method achieves a transmission rate of 6.2×10^5 Byte/s, which is over **20 times** lower than Concat (1.3×10^7 Byte/s). This substantial reduction is achieved through feature-level fusion, which transmits compressed feature flows. Despite this lower bandwidth usage, our method provides a **4%** higher MOTA, highlighting its ability to optimize communication resources while improving tracking accuracy.

D. Ablation Study

We conduct an ablation study to quantify the contributions of our three key modules: the integrated detection-tracking framework, XIOU identity association, and the four-stage cascade matching (FSCM) algorithm. The baseline method, AB3DMOT, is used for comparison by systematically replacing each module in our framework with the corresponding component from AB3DMOT. The results are presented in Table II.

1) Impact of the Integrated Detection-Tracking Framework: Replacing our integrated detection-tracking framework with AB3DMOT's tracking-by-detection (TBD) paradigm results in a **2.1-point decrease in MOTA** (from 57.23 to 55.13). This indicates the unified framework's critical role in bridging detection and tracking, enabling the detection branch to benefit from tracking priors while allowing the tracking branch to leverage enhanced detection results. The observed drop in

TABLE II. ABLATION STUDY ON THE V2X-SEQ DATASET

Method	Tracking Framework	Identity Association	Trajectory Management	MOTA↑	MOTP↑	IDS↓
AB3DMOT	TBD	IOU	Single Matching	54.75	69.76	222
Ours	**Integrated**	**XIOU**	**FSCM**	**57.23**	**74.64**	**206**
1	TBD	XIOU	FSCM	55.13	72.43	208
2	Integrated	IOU	FSCM	56.72	73.58	214
3	Integrated	XIOU	Single Matching	55.38	74.16	215

MOTA demonstrates that separating detection and tracking increases errors, for example, in scenarios involving fast-moving or partially occluded objects. By integrating detection and tracking within the same pipeline, our framework effectively reduces identity switches and improves object recall, ensuring robust performance in dynamic traffic environments.

2) Impact of XIOU Identity Association: When XIOU is replaced with AB3DMOT's IOU, **MOTA drops by 0.51 points** (from 57.23 to 56.72), and **IDS increases by 3.9%** (from 206 to 214). This demonstrates XIOU's ability to capture spatial and orientation consistency, which is particularly beneficial in occlusion-heavy environments. XIOU effectively resolves ambiguous matches between detection and prediction bounding boxes by incorporating yaw angle and center-point distance, leading to improved identity consistency and reduced errors during complex interactions between vehicles. In contrast, IOU struggles to maintain identity consistency when objects overlap or move in close proximity, leading to more identity switches and reduced tracking accuracy.

3) Impact of the Four-Stage Cascade Matching (FSCM): Replacing our four-stage cascade matching (FSCM) algorithm with AB3DMOT's single matching strategy increases **IDS by 4.3%** (from 206 to 215) and reduces **MOTA by 1.85 points** (from 57.23 to 55.38). These results highlight FSCM's ability to manage trajectory updates effectively, particularly in handling occlusions and reappearing objects. FSCM dynamically adapts to the confidence levels of both detections and tracks, ensuring robust identity associations across frames. Single matching, on the other hand, lacks this flexibility, resulting in higher identity switches and degraded tracking performance, particularly in challenging scenarios with frequent occlusions or sudden object reappearances. By incorporating FSCM, our method achieves lower IDS and higher MOTA, demonstrating its importance for maintaining accurate and consistent trajectories under complex real-world conditions.

4) Module Contribution Analysis: Among the three modules, the integrated detection-tracking framework contributes the largest MOTA gain (**2.1 points**), highlighting its significant impact on overall tracking accuracy. FSCM provides the second-highest gain (**1.85 points in MOTA**), underscoring its importance in trajectory management under challenging conditions. XIOU, while contributing a relatively smaller MOTA improvement (**0.51 points**), plays a crucial role in reducing IDS, demonstrating its effectiveness in identity association tasks. Collectively, these modules form a robust system that achieves superior performance compared to traditional methods.

E. Challenges and Future Directions

1) Bandwidth Efficiency: Although our method significantly reduces data transmission compared to data-level fusion methods, the bandwidth requirement (6.2×10^5 Byte/s) remains relatively high compared to object-level methods like Hungarian. This poses challenges for large-scale deployment in real-world bandwidth-constrained environments. Future work should focus on optimizing feature extraction and compression strategies to further reduce transmission overhead while maintaining tracking accuracy.

2) Handling Long Occlusions and Disappearances: While the proposed framework effectively addresses moderate occlusions and identity switches, it struggles in scenarios involving long-term occlusions or complete object disappearances. For instance, re-associating objects after prolonged absence remains challenging. Future efforts could focus on incorporating adaptive temporal modeling techniques and improved motion prediction strategies to enhance the system's robustness in such complex and dynamic environments.

V. CONCLUSION

In this work, we proposed an innovative framework for vehicle-infrastructure cooperative 3D multi-object tracking, emphasizing three key contributions: an integrated detection-tracking framework, the XIOU identity association metric, and a four-stage cascade matching (FSCM) strategy. The integrated framework enhances both detection accuracy and tracking consistency by jointly leveraging detection and tracking information. The XIOU metric improves identity association by effectively incorporating 3D spatial information, while FSCM provides robust tracking continuity in occlusion scenarios. Experimental results on the V2X-Seq dataset validate the effectiveness of these innovations, with our method demonstrating superior tracking accuracy, reduced identity switches, and low bandwidth usage even under delayed communication conditions. These results underscore the potential of feature-level fusion and temporal prior enhancement in real-world V2X applications. Future work will focus on optimizing bandwidth efficiency through improved feature extraction and compression, and enhancing robustness in handling long-term occlusions and dynamic scenarios with adaptive temporal modeling and motion prediction, paving the way for more reliable and efficient V2X applications.

ACKNOWLEDGMENTS

This work was supported in part by the International Strategic Innovative Project of the National Key R&D Program of China (2023YFE0112500) and the Fundamental Research Funds for the Central Universities (22120230311).

REFERENCES

[1] Eduardo Arnold, Mehrdad Dianati, Robert de Temple, and Saber Fallah. Cooperative perception for 3d object detection in driving scenarios using infrastructure sensors. *IEEE Transactions on Intelligent Transportation Systems*, 23(3):1852–1864, 2020.

[2] Alex Bewley, Zongyuan Ge, Lionel Ott, Fabio Ramos, and Ben Upcroft. Simple online and realtime tracking. In *2016 IEEE international conference on image processing (ICIP)*, pages 3464–3468. IEEE, 2016.

[3] Hsu-kuang Chiu, Jie Li, Rareş Ambruş, and Jeannette Bohg. Probabilistic 3d multi-modal, multi-object tracking for autonomous driving. In *2021 IEEE international conference on robotics and automation (ICRA)*, pages 14227–14233. IEEE, 2021.

[4] Peng Chu, Jiang Wang, Quanzeng You, Haibin Ling, and Zicheng Liu. Transmot: Spatial-temporal graph transformer for multiple object tracking. In *Proceedings of the IEEE/CVF Winter Conference on applications of computer vision*, pages 4870–4880, 2023.

[5] Siqi Fan, Haibao Yu, Wenxian Yang, Jirui Yuan, and Zaiqing Nie. Quest: Query stream for practical cooperative perception. In *2024 IEEE International Conference on Robotics and Automation (ICRA)*, pages 18436–18442. IEEE, 2024.

[6] Yue Hu, Shaoheng Fang, Zixing Lei, Yiqi Zhong, and Siheng Chen. Where2comm: Communication-efficient collaborative perception via spatial confidence maps. *Advances in neural information processing systems*, 35:4874–4886, 2022.

[7] Aleksandr Kim, Aljoša Ošep, and Laura Leal-Taixé. Eagermot: 3d multi-object tracking via sensor fusion. In *2021 IEEE International conference on Robotics and Automation (ICRA)*, pages 11315–11321. IEEE, 2021.

[8] Harold W Kuhn. The hungarian method for the assignment problem. *Naval Research Logistics (NRL)*, 52(1):7–21, 2004.

[9] Alex H Lang, Sourabh Vora, Holger Caesar, Lubing Zhou, Jiong Yang, and Oscar Beijbom. Pointpillars: Fast encoders for object detection from point clouds. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 12697–12705, 2019.

[10] Yiming Li, Dekun Ma, Ziyan An, Zixun Wang, Yiqi Zhong, Siheng Chen, and Chen Feng. V2x-sim: Multi-agent collaborative perception dataset and benchmark for autonomous driving. *IEEE Robotics and Automation Letters*, 7(4):10914–10921, 2022.

[11] Chenxu Luo, Xiaodong Yang, and Alan Yuille. Exploring simple 3d multi-object tracking for autonomous driving. In *Proceedings of the IEEE/CVF international conference on computer vision*, pages 10488–10497, 2021.

[12] Ziqi Pang, Zhichao Li, and Naiyan Wang. Simpletrack: Understanding and rethinking 3d multi-object tracking. In *European Conference on Computer Vision*, pages 680–696. Springer, 2022.

[13] Hamid Rezatofighi, Nathan Tsoi, JunYoung Gwak, Amir Sadeghian, Ian Reid, and Silvio Savarese. Generalized intersection over union: A metric and a loss for bounding box regression. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 658–666, 2019.

[14] Sanbao Su, Yiming Li, Sihong He, Songyang Han, Chen Feng, Caiwen Ding, and Fei Miao. Uncertainty quantification of collaborative detection for self-driving. In *2023 IEEE International Conference on Robotics and Automation (ICRA)*, pages 5588–5594. IEEE, 2023.

[15] Peize Sun, Jinkun Cao, Yi Jiang, Rufeng Zhang, Enze Xie, Zehuan Yuan, Changhu Wang, and Ping Luo. Transtrack: Multiple object tracking with transformer. *arXiv preprint arXiv:2012.15460*, 2020.

[16] Junke Wang, Dongdong Chen, Zuxuan Wu, Chong Luo, Xiyang Dai, Lu Yuan, and Yu-Gang Jiang. Omnitracker: Unifying object tracking by tracking-with-detection. *arXiv preprint arXiv:2303.12079*, 2023.

[17] Tsun-Hsuan Wang, Sivabalan Manivasagam, Ming Liang, Bin Yang, Wenyuan Zeng, and Raquel Urtasun. V2vnet: Vehicle-to-vehicle communication for joint perception and prediction. In *Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part II 16*, pages 605–621. Springer, 2020.

[18] Xinshuo Weng, Jianren Wang, David Held, and Kris Kitani. 3d multi-object tracking: A baseline and new evaluation metrics. In *2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pages 10359–10366. IEEE, 2020.

[19] Nicolai Wojke, Alex Bewley, and Dietrich Paulus. Simple online and realtime tracking with a deep association metric. In *2017 IEEE international conference on image processing (ICIP)*, pages 3645–3649. IEEE, 2017.

[20] Yan Yan, Yuxing Mao, and Bo Li. Second: Sparsely embedded convolutional detection. *Sensors*, 18(10):3337, 2018.

[21] Fan Yang, Shigeyuki Odashima, Shoichi Masui, and Shan Jiang. Hard to track objects with irregular motions and similar appearances? make it easier by buffering the matching space. In *Proceedings of the IEEE/CVF winter conference on applications of computer vision*, pages 4799–4808, 2023.

[22] Tianwei Yin, Xingyi Zhou, and Philipp Krahenbuhl. Center-based 3d object detection and tracking. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 11784–11793, 2021.

[23] Sisi You, Hantao Yao, Bing-Kun Bao, and Changsheng Xu. Utm: A unified multiple object tracking model with identity-aware feature enhancement. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 21876–21886, 2023.

[24] Haibao Yu, Yizhen Luo, Mao Shu, Yiyi Huo, Zebang Yang, Yifeng Shi, Zhenglong Guo, Hanyu Li, Xing Hu, Jirui Yuan, et al. Dair-v2x: A large-scale dataset for vehicle-infrastructure cooperative 3d object detection. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 21361–21370, 2022.

[25] Haibao Yu, Wenxian Yang, Hongzhi Ruan, Zhenwei Yang, Yingjuan Tang, Xu Gao, Xin Hao, Yifeng Shi, Yifeng Pan, Ning Sun, et al. V2x-seq: A large-scale sequential dataset for vehicle-infrastructure cooperative perception and forecasting. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 5486–5495, 2023.

[26] Yifu Zhang, Peize Sun, Yi Jiang, Dongdong Yu, Fucheng Weng, Zehuan Yuan, Ping Luo, Wenyu Liu, and Xinggang Wang. Bytetrack: Multi-object tracking by associating every detection box. In *European conference on computer vision*, pages 1–21. Springer, 2022.

[27] Yifu Zhang, Chunyu Wang, Xinggang Wang, Wenjun Zeng, and Wenyu Liu. Fairmot: On the fairness of detection and re-identification in multiple object tracking. *International journal of computer vision*, 129:3069–3087, 2021.

[28] Zhaohui Zheng, Ping Wang, Wei Liu, Jinze Li, Rongguang Ye, and Dongwei Ren. Distance-iou loss: Faster and better learning for bounding box regression. In *Proceedings of the AAAI conference on artificial intelligence*, volume 34, pages 12993–13000, 2020.

[29] Yang Zhou, Cai Yang, Ping Wang, Chao Wang, Xinhong Wang, and Nguyen Ngoc Van. Vit-fusenet: Multimodal fusion of vision transformer for vehicle-infrastructure cooperative perception. *IEEE Access*, 2024.

[30] Xizhou Zhu, Weijie Su, Lewei Lu, Bin Li, Xiaogang Wang, and Jifeng Dai. Deformable detr: Deformable transformers for end-to-end object detection. *arXiv preprint arXiv:2010.04159*, 2020.

A Robust Model for a Healthcare System with Chunk Based RAID Encryption in a Multitenant Blockchain Network

Bharath Babu S, Jothi K R*
School of Computer Science and Engineering
Vellore Institute of Technology
Vellore, TamilNadu, India 632014

***Abstract*—Healthcare informatics has revolutionized data extraction from large datasets. However, using analytics while protecting sensitive healthcare data is a major challenge. A novel methodology for Privacy-Preserving Analytics in Healthcare Records addresses this essential issue in this study. The multi-tenant Blockchain framework uses chunk-based RAID encryption. For the healthcare business, chunk-based RAID encryption in a multi-tenant blockchain architecture creates a durable, safe, and efficient solution for processing confidential healthcare information. This solution improves data security, integrity, availability, performance, regulatory compliance, and scalability by combining RAID and blockchain technology. Contemporary healthcare systems need these qualities to work well. This approach was done in Python, and the libraries used the VSCode tool. To maintain data security, integrity, and accessibility, a strong healthcare system architecture with chunk-based RAID encryption in a multi-tenant blockchain network requires various advanced technologies.**

Keywords*—Multi-tenant; chunk-based; RAID; blockchain; healthcare records

I. Introduction

The quick progress in the internet of things (IoT) concept has transformed healthcare businesses by introducing significant enhancements in e-health/medical records drug prescription data, and insurance information. The rapid advancement of the internet of things (IoT) has revolutionized healthcare industries by offering substantial improvements in e-health/medical records, drug prescription data, and insurance information. IoT devices enable real-time monitoring of patients. Additionally, they have the potential to decrease the necessity of hospital visits for regular health examinations. Home health monitoring systems that are connected can effectively decrease the duration of hospital visits and lower the expenses associated with readmission. The Internet of Things (IoT)-enabled medical devices have the capability to aid in the process of diagnosing medical conditions by providing alerts and triggering notifications prior to the onset of symptoms. Numerous software as a service applications make advantage of multi-tenant data storage, which involves the sharing of resources and the layout of the data-store across multiple tenants. The fact that each user or tenant is given their own instance of a single tenant application, on the other hand, results in increased expenses for servicing and maintenance for both the tenants and the suppliers. When resources are shared across multiple tenants in a multi-tenancy setting, those costs are reduced for all of the parties involved [1, 2]. Despite this, multitenant architectures pose data security risks. When multiple tenants share a storage area, data infringement is more likely if their data is not properly isolated. A hostile tenant can assault other tenants' data by sending harmful information, making unauthorized transactions, or interrupting exchanges. This can be done several ways. Therefore, a robust system is essential to ensure that multi-tenant data cannot be altered without authority. Flexibility and data segregation are crucial in multi-tenant applications [3].

Blockchain technology is a recent invention that allows secure data storage in multi-user applications. In addition to bitcoin, blockchain technology is becoming a powerful tool for secure and immutable storage systems [3]. Blockchains or Distributed Ledgers prevent data tampering by decentralizing and cryptographic hashing. Blockchain storage is designed to securely and permanently store data and transactions, preventing tampering. Access to private or permissioned blockchains is limited to identifiable members [4]. Blockchains offer an unchangeable ledger that lets authorized network participants see stored data in real time.

Blockchain is a highly promising technology that has the potential to greatly improve the efficiency of healthcare data management operations. It achieves this by offering unparalleled data efficiency and ensuring trust in the system. The platform provides a diverse array of notable and inherent characteristics, including distributed storage, visibility, permanence, verification, adaptability in data access, interlinking, and safeguarding, thereby facilitating extensive adoption of blockchain technology for healthcare data management [5].

Blockchain employs smart contracts to establish mutually agreed upon terms and conditions among all healthcare partners in the network, eliminating the need for intermediaries [6,7]. It minimizes superfluous administrative expenses. Blockchain primarily depends on three fundamental concepts: peer-to-peer networks, public key cryptography, and consensus procedures [8]. Blockchain is categorized into three types based on permission management: public, private, and consortium blockchains [9]. Any individual with internet access can participate in the consensus procedure of public blockchains.

*Corresponding authors

Public blockchains incorporate incentives and employ proof-of-work or proof-of-stake techniques to ensure encrypted digital verification. The public blockchain system is completely visible, meaning that the identity of each participant is kept pseudo-anonymous. In a private blockchain, network control is exclusively held by a single company. Thus, this particular type of blockchain necessitates a reliable intermediary to achieve consensus. The consortium blockchain integrates the benefits of public and private blockchain networks. This solution is specifically ideal for select enterprises who have the objective of optimizing communication within their own network. Healthcare businesses have the flexibility to choose any sort of blockchain network based on their individual requirements or use case scenarios, as each network has its own advantages and disadvantages.

The framework laid out in this article aims to enhance other related blockchain-based systems for storage in the following aspects: The aim of chunk-based RAID encryption in a multi-tenant blockchain model for the healthcare sector is to provide a robust, secure, and efficient framework for managing sensitive healthcare data. By leveraging the strengths of both RAID and blockchain technologies, this approach ensures enhanced data security, integrity, availability, performance, regulatory compliance, and scalability, which are crucial for the effective operation of modern healthcare systems. Utilize separate ledgers or channels to ensure that the data of different tenants remains isolated and inaccessible to others. This approach is commonly employed in permissioned blockchain networks such as Hyper-ledger Fabric. Implement strong access control mechanisms to restrict access to each tenant's data, ensuring only authorised individuals can view or interact with it. Deploy resilient authentication techniques to bolster security for users accessing the blockchain network. One such solution is to use multi-factor authentication (MFA) in order to improve security measures. Role-Based Access Control (RBAC) is a mechanism for controlling access to resources in a methodical manner. Administrators can utilize this feature to allocate roles to users, thereby specifying the permissions and privileges they possess. RBAC enables companies to enforce access controls that limit users to only the information and functionality essential for their specific position. This enhances security and minimizes the likelihood of unauthorized access. It is crucial to assign responsibilities to users and establish permissions depending on their duties in order to ensure efficient management. This enhances the administration of resource and operation authorization within the network.

Section II investigates existing approaches and discusses the issues of protecting medical records in multi-tenant systems. Section III discusses the proposed solutions along with the block chain technology with chunk-based RAID encryption to address the existing problems. Section IV explains the analytical and technological implementation of the cryptographic methods, RAID setups and data transfer protocols. Section V evaluates the proposed method over other existing techniques. Section VI examines the model's limitations, applications and further scopes.

A. Literature Review

Extensive research is being conducted in various interdisciplinary fields using blockchain technology. The research conducted in [10] has aimed to tackle the issue of internet piracy in the movie business by the creation of a blockchain-powered anti-piracy system called "Vanguard". This system replaces the traditional method of registering intellectual property (IP) and monitors the ownership of IP rights to prevent unauthorised distribution of data. The utilisation of blockchain technology and certificateless cryptography has been employed in [11] to create a data storage system that effectively manages and safeguards vast quantities of IoT data.

The authors of [12] have employed blockchain technology to develop methods for sharing data in smart cities. In [13], a proposal was made for a Blockchain Tree to store information from smart ID cards. This method enhances security by incorporating blockchain technology at a lower level and extending it to a higher level.

The research in [14] centres on the utilisation of blockchain technology for several applications in the food business, such as food tracing, land registrations, customer awareness programmes, and farm insurance. The proposed system has been implemented by authors using the open-source platform Multi-Chain. An important benefit of utilising blockchain technology is its ability to effectively deter forgery and fraud due to its inherent immutability and transparency. In a study referenced as [15], a blockchain-based solution is proposed to avoid property fraud, including fraud related to bank loans.

Ping end-to-end Reporting (PingER) is a framework created by the SLAC National Accelerator Laboratory in the United States for measuring internet performance across the globe. The proposal suggests implementing a distributed blockchain technology to store data for PingER in a decentralised manner. Instead of storing data in a centralised location, this system distributes the data files across various sites using Distributed Hash Tables (DHT). Only the metadata of these files is saved on the blockchain.

The study [16] discusses a novel concept called Blockchain-as-a-Service (BaaS), which is comparable to Software-as-a-Service (SaaS). This is a cloud-based service that simplifies the process of setting up a blockchain. It also offers a platform for running apps and provides security and other essential elements of blockchain technology.

The authors of [17] have suggested a system based on blockchain technology for a multitenant architecture. Each tenant possesses an independent blockchain with certain permissions, which is then linked to a central chain. The collaboration for this project was conducted with Laava ID Pty Ltd (Laava), and the execution was accomplished using the Ethereum platform. This study examines the healthcare sector as a prominent field for the implementation of blockchain technology. Extensive research and documentation have been dedicated to studying the application of blockchain in the healthcare industry. Researchers in [18] have integrated blockchain technology into digital services, such as online consultations. They have successfully implemented a decentralised system to ensure utmost security in the healthcare industry. Blockchain technology has improved transparency in communication between users and clients, particularly in the context of doctor-patient interactions. Furthermore, the authors have included three separate case studies in this specific field: Telemedicine, Patientory, and Medblock.

The study [19] provides a thorough examination of the research conducted on electronic health record (EHR) systems that utilise blockchain technology. Several consensus algorithms have been explored by researchers for implementation in public blockchains. These include the Practical Byzantine Fault Tolerance replication algorithm (PBFT), RAFT, Proof of Authority (PoA), Proof of Capacity (PoC), and Proof of Elapsed Time (PoET). An innovative solution called MediBchain has been developed in [20] to ensure the security and privacy of healthcare data by leveraging blockchain technology. They have utilised Elliptic Curve Cryptography (ECC) to secure sensitive information.

A mobile application has been created utilising blockchain technology to store data related to cognitive behavioural therapy for patients with insomnia [21]. The data is stored in the Hyperledger Fabric blockchain network using JSON format. This system utilises blockchain technology to ensure data transparency and accessibility while eliminating the risk of data tampering. Blockchain technology has been successfully integrated with artificial intelligence systems to develop a predictive system for managing the clinical risks associated with COVID-19 infection [22-25]. This integration has shown promising results in improving clinical risk management.

B. Challenges Faced in the Existing Techniques

1) Single database, shared schema: In the healthcare industry, a single database with a shared schema shown in Fig. 1 presents many challenges, especially when considering security, confidentiality, data consistency, and expandability. These are the main issues with this approach. A unified database with a shared schema can attract attackers. A compromise could disclose all patient data from numerous departments or institutions. It's difficult to restrict access to specific data in a shared schema to authorized users. Data segmentation to protect sensitive patient data is tough. Multiple users updating the database at once might cause data conflicts and overwrites, compromising data integrity. Single-database uniformity is key. Inconsistencies can cause serious medical errors. Data leaking is a prominent concern in a shared schema architecture, when multiple tenants utilize the same schema. These factors can result in security breaches, and impairments in performance [26]. Access control is intricate, and conflicts over resources can have a negative influence on performance. Increasing the number of renters may lead to scalability concerns. Optimizing searches across several tenants is a challenging task that requires the construction of efficient indexing and caching solutions to prevent performance issues. Handling schema changes poses difficulties, and data migration carries a high chance of errors. Insufficient options for personalization and adaptability are further obstacles. Tenant management include the effective process of bringing new tenants on board, removing tenants when necessary, ensuring equitable distribution of resources, and implementing security measures at the individual row level. By implementing resource quotas, automatic monitoring tools, and conducting frequent audits, it is possible to reduce these issues and enhance the management of a single database common schema.

2) Single database, separate schema: Implementing a solitary database with distinct schemas for individual tenants in the healthcare sector poses numerous difficulties. These difficulties

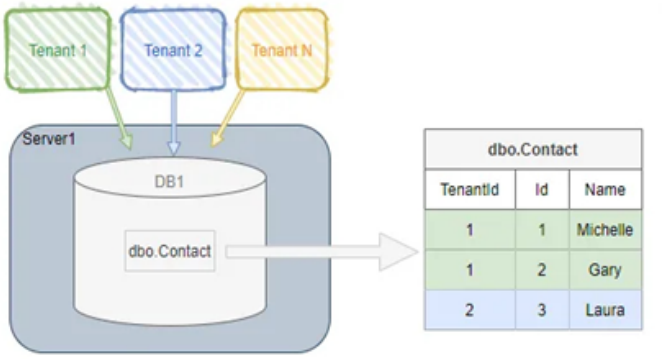


Fig. 1. Single database, shared schema model.

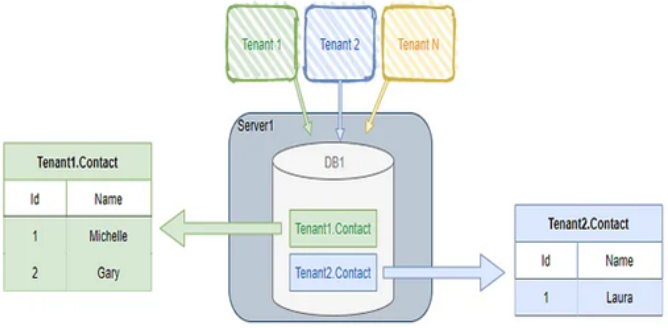


Fig. 2. Single database, separate schema model.

can have an impact on performance, security, maintainability, and compliance [27]. The system Restoring data for a single tenant is not a simple task, although it is slightly easier than the technique of using a single database with a shared schema (Fig. 2), because the tenant data is kept separate. As the tenant count increases, a significant number of database objects will be generated to handle and uphold. Schema modifications require a more complex process, as they need to be distributed to several tenants.

C. Database per Tenant

Drawbacks to using a Database per tenant (Fig. 3) approach include the need for additional server maintenance and security measures, an increase in the number of database objects to manage and maintain as the number of tenants rises, and the complexity of creating new schemas when adding new tenants [28].

1) Multiple databases, multiple tenants per database, shared schema: The disadvantages of having numerous databases, multiple tenants per database, and a shared schema (Fig. 4) are as follows: Tenants persist in employing a shared database and schema alongside other folks. Further maintenance is required. Those in charge of managing many databases face complex operational challenges, the risk of data breaches, the necessity for efficient performance monitoring, obstacles in attaining scalability, increased maintenance responsibilities, and concerns over security [29]. Enforcing compliance with regulations like GDPR and HIPAA can be challenging in shared schema setups. Operational complexity

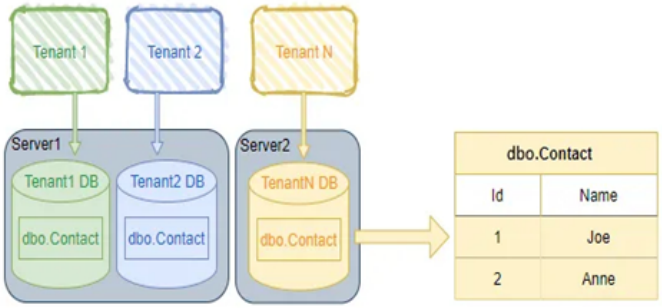


Fig. 3. Database per tenant model.

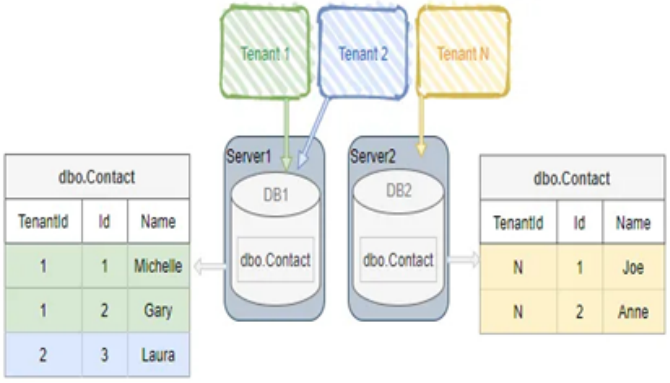


Fig. 4. Multiple databases, multiple tenants per database, shared schema model.

refers to the range of duties involved in managing a system, including backup and recovery methods, monitoring, problem-solving, and limitations on modification. Efficiently managing economic issues, including infrastructure expenses, is essential for properly allocating resources and ensuring compliance.

II. Research Method

This research takes a methodical approach to tackle the identified challenges. Researcher thoroughly examine and incorporates insights from various sources such as academic papers, industrial blogs, and related research initiatives. The proposed approach efficiently combines the benefits of blockchain technology and chunk-based RAID encryption to address important difficulties in healthcare data management, such as security, fault tolerance, scalability, performance, and regulatory compliance. Its sturdy design protects sensitive medical information while retaining high efficiency and adaptability, making it a great option for the changing demands of modern healthcare organizations.

A. Proposed System

To address the difficulties presented by current multi-tenancy database systems, we suggest an innovative method that utilizes the dynamic arrangement of tenant connections and incorporates blockchain technology to overcome the stated issues. Our goal is to establish a flexible and scalable environment by implementing a dynamic topology in healthcare organizations which can create a robust, scalable, and flexible environment that supports their evolving needs while maintaining high standards of performance and security. This will enable tenants to communicate with each other smoothly, without being limited by a predefined schema. This dynamic connectivity facilitates improved data isolation, which enables quick restoration of individual tenant data without the complications associated with a single shared schema. In addition, we implement blockchain technology to securely handle the relationships between renters. The decentralized and tamper-resistant characteristics of blockchain guarantee the reliability and safety of tenant connections, effectively resolving problems regarding High Availability, Disaster Recovery, and Monitoring techniques. This novel method reduces the requirement for extensive maintenance and schema modifications, offering a strong basis for a scalable, secure, and easily controllable multi-tenancy database structure. Through the use of blockchain technology, we address the difficulties associated with existing models by decentralizing connectivity and ensuring security. This provides a revolutionary solution for a dynamic and safe database environment that can accommodate multiple users. Healthcare businesses have the ability to establish a strong, adaptable, and versatile infrastructure that caters to their changing requirements while upholding exceptional levels of performance and security.

B. Secured Data Transaction of Tenants using Blockchain Technology

Implementing secure data transactions for healthcare tenants using blockchain technology entails utilizing the inherent characteristics of blockchain, like decentralization,immutability, and transparency, to guarantee the integrity,security, and privacy of data. Our proposed system incorporates Blockchain Technology to guarantee the secure transfer of data between clients. Blockchain, being a distributed and tamper-proof ledger, offers an unchangeable record of all transactions. Data transactions are cryptographically encrypted to guarantee data integrity and prevent unauthorized access. This not only improves the overall security of healthcare data but also establishes a clear and responsible framework for data transfers inside the multi-tenant environment. The model of multi-tenant blockchain network for the health sector is illustrated in the Fig. 5.

C. A Mathematical Framework for Enhancing Data Security in Multi-Tenant Blockchain Technology

Securing data in multi-tenant blockchain technology requires utilizing a mathematical framework that integrates different cryptographic techniques and consensus mechanisms. This framework is designed to guarantee the security and reliability of healthcare data, while also ensuring the smooth operation and effectiveness of the blockchain network. Here is a comprehensive approach to developing such a framework.

1) Cryptographic Hash Functions: Cryptography uses mathematical hash functions. Hash functions usually take variable-length inputs and output fixedlength outputs. Computing systems depend on hash functions for message integrity and data validation. Though “weak” cryptographically due to their polynomial-time solvability, these algorithms are not easily decipherable. By using cryptographic hash functions, ordinary hash functions become more secure, making it harder

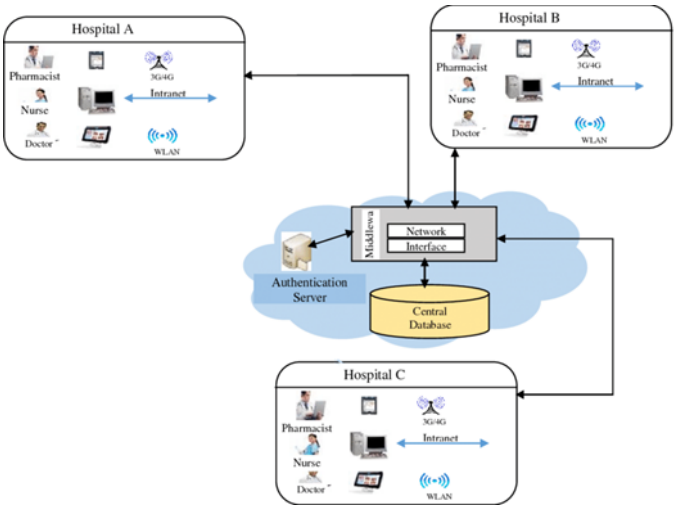


Fig. 5. Multitenant blockchain model for healthcare sector.

to decrypt communications or find their originators. Cryptographic hash functions have three traits: They never meet. It is vital that each input provides a unique output hash. Can hide. It should be difficult to discern a hash function's input from its output [30]. They should help solve riddles. A specified output can make selecting an input difficult. Therefore, input must come from a variety of sources. Cryptographic hash functions are employed in a chunk-based RAID encryption system to guarantee the integrity of each individual chunk of data. The procedure is dividing the data into pieces, applying a hashing function to each chunk, encrypting each chunk, and subsequently dispersing the encrypted chunks throughout the RAID array. This method aids in safeguarding against data corruption and guarantees the ability to identify any modifications made to the data Table I.

TABLE I. CHUNK-BASED RAID ENCRYPTION

Mathematical Approach for Hashing in Chunk-Based RAID Encryption	
Step1	**Data Chunking** Let D be the data to be stored in the RAID. Divide the data D into n chunks Ci Where i = 1,2,3.... n as shown in the equation D=C_1C_2C_n.
Step2	**Hashing Each Chunk** Compute the hash of each chunk using a cryptographic hash function H. $H_i = H(C_i)$ Where Ci is the ith chunk of data Hi is the hash value of the ith chunk H is the cryptographic hash function. Apply SHA-256 to each chunk Ci, and obtain in the equation, $H_i = SHA - 256(C_i)$.
Step3	**Encrypting Each Chunk** Encrypt each chunk using an encryptional algorithm E with a key K as shown in below equation. $E_i = E(K, C_i)$ Where E is the Encryption Function K is the encryption Key Ei is the encrypted chunk. Encrypt each chunk Ci with AES and key K, and obtain the equation below. $E_i = AES(K, C_i)$.
Step4	**Storing Hashes and Encrypted Chunks** EStore the hash values Hi and the encrypted chunks Ei in the RAID array. Distribute Ei across the RAID disks according to the chosen RAID configuration.

2) Password Verification: Most websites store passwords as hashes because text files are unsafe. Passwords are hashed when entered. The company's servers' hashed values are compared to the outcome. Hackers have created rainbow tables, databases containing common passwords and their hashes, to gain unauthorized access to accounts.

A chunk-based RAID encryption system can employ cryptographic hash functions and password-based key derivation functions (PBKDFs) to verify passwords. The objective is to securely authenticate the password utilized for the encryption and decryption of data chunks. Belowis a comprehensive formula and step-by-step process for verifying passwords in a system.

The user has provided a confidential pass code, denoted as P. To prevent precompiled attacks, a distinct salt value S is appended to the password prior to hashing. The process of generating a cryptographic key K from a password and salt is referred to as a key derivation function (KDF). In order to authenticate the password during the decryption process, the system must verify that the entered password is capable of generating the accurate encryption key. The mathematical function to derive the key K using the provided password P and the stored salt S is given in Eq. (1):

$$K = KDF(P, S) \tag{1}$$

Decrypt each encrypted chunk E_i using the derived key K using Eq. (2):

$$C_i = Decrypt(K, E_i) \tag{2}$$

Compute the hash H' of each decrypted chunk Ci by Eq. (3):

$$H' = Hash(C_i) \tag{3}$$

Verify the computed hash H' matches the stored hash H_i, if $H' == H_i$ for all i, then the passcode is verified.

3) Signature Generation and Verification: Signature creation plays a vital role in ensuring the validity and integrity of data pieces in chunk-based RAID encryption solutions. Signature generation commonly entails the utilization of cryptographic methods to generate a distinct identifier (signature) for every chunk.

Mathematical signature verification verifies digital documents and messages. When all conditions are met, a valid digital signature proves to the recipient that the communication was sent by a known sender and was not tampered with. Use the private key privK and a digital signature algorithm DSA to sign the hash Hi by the Eq. (4) and (5):

$$SignPrivatekey(x) = SignatureSignprivatekey(x) = Signature \tag{4}$$

$$Sign_i = DSA_{sign}(priv_K, H_i) \tag{5}$$

The equation depicts the process of generating a digital signature using a private key, ensuring data authenticity and non-repudiation within the blockchain. The average digital signature technique has three algorithms. The key generation algorithm creates keys first. Signing algorithms use messages and private keys to create signatures. Finally, the signature verifying method verifies signatures.

To verify the signature, recalculate the hash Hi of the received chunk Ci using Eq. (6):

$$H^{'} = SHA - 256(C_i) \tag{6}$$

To validate the signature, utilize the public key pubk that corresponds to the private key privK and employ the same digital signature procedure, DSA as in Eq. (7) and (8):

$$Verif = DSA_{Verif}(pub_K, H^{'}, Sign_i) \tag{7}$$

$$Verifypublickey(Signature, Data, Blockchain) = \{True, False\} \tag{8}$$

This equation represents the verification process, ensuring that data transactions are authentic and valid through the use of public key verification. If the verification process is successful, then the Signi, is considered legitimate, and it is confirmed that the data chunk Ci has not been altered or tampered with.

4) Verifying File and Message Integrity: Hashes ensure the integrity of transmitted messages and information by preventing unauthorized alterations. The practice establishes a "chain of trust". Users have the ability to release a hashed representation of their data together with the corresponding key. This allows recipients to verify the integrity of their data by comparing the hash value they compute with the published value.

5) Advanced Smart Contract Implementations for Transactions: Smart Contracts are essential for automating and ensuring compliance with the conditions of agreements between renters. Our system integrates sophisticated Smart Contract implementations to simplify and automate intricate transaction procedures. Smart Contracts enforce predetermined norms and conditions, guaranteeing the smooth, secure, and compliant execution of data transactions. This not only decreases the requirement for human intervention but also improves the effectiveness and dependability of transactions inside the multi-tenant system. A smart contract SCi is created for each transaction through Eq. (9) as follows:

$$SC_i = \{H_i, Sign_i, \sigma, \gamma, Term_i\} \tag{9}$$

Where σ and γ are the security and compliance parameters and Termi is the terms and conditions specified for the data transaction. Now deploy this SCi in the blockchain through the following Eq. (15):

$$B \leftarrow B \cup \{SC_i\} \tag{10}$$

6) Dynamic Network Creation: In order to overcome the difficulties related to fixed network structures, we suggest the adoption of a Dynamic Network Creation technique. Tenants have the opportunity to connect and disconnect from the network as required, offering adaptability and scalability. The process of creating a dynamic network allows tenants to easily adjust to changing needs, resulting in a flexible and responsive multi-tenant environment. This strategy addresses the problems associated with inflexible network setups, enhancing the system's ability to adapt to the changing requirements of tenants.

Establishing a dynamic network in a multi-tenant blockchain system entails overseeing numerous autonomous tenants, such as distinct businesses or users, and enabling them secure and scalable interaction within the blockchain network. This can be accomplished through the utilization of a synergistic integration of intelligent agreements, dynamic node allocation, and robust communication protocols. Presented here is a mathematical framework for such a system:

During dynamic node allocation, Nodes Nm is allocated to tenants Tm depending upon several criteria like load, requirement, etc. This is done by Eq. (11):

$$N_{T_m} = \{N_m | N_m is assigned to T_m\} \tag{11}$$

To prevent bottlenecks, it is important to evenly distribute nodes among tenants. This is done by Eq. (12):

$$\sum\nolimits_{m=1}^{i} = \frac{load(N_m)}{i} \approx \frac{Totalload}{m} \tag{12}$$

Then deploy the created smart contract to the multitenant blockchain model Bm. Then the Tenants submit transactions TXm which are validated by smart contracts by the following Eq. (13) and (14):

$$TX_m = \{Sender = T_m, Receiver, data, signature\} \tag{13}$$

$$Valid(TX_m) \Leftrightarrow Verif(TX_m, SC_i) \tag{14}$$

Finally, the network graph g (Tm, Nm) is adjusted to the changing load and new tenants through the Eq. (15):

$$g(T_m, N_m) \rightarrow g(T_m^{'}, N_m^{'}) \tag{15}$$

This mathematical framework supports the creation of a flexible, scalable, and secure dynamic network for multi-tenant blockchain applications in healthcare or other sectors.

D. Data Transaction Architecture

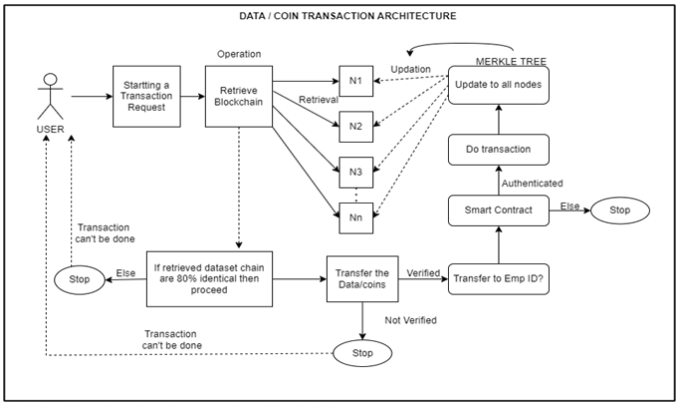


Fig. 6. Data transaction architectures block diagram.

For the purpose of ensuring redundancy and mirrored storage, data is consistently stored in RAID 1 sets. RAID 0 striping is a method that enhances speed by distributing data in an equitable manner across many drives. It is the Monitoring AI that oversees the whole system, ensuring that it operates at its highest possible level. Significant occurrences are gathered and encrypted by the log storage system in a safe manner for the purpose of subsequent reference and analysis. The block diagram of the data transaction architecture of the proposed model is shown in the Fig. 6.

1) Data Transaction and Protocols of Key Generation: The proposed technology integrates data transactions with methods for key generation to bolster the security and privacy of data transactions. Every transaction is linked to a cryptographic currency, and the key generation procedures guarantee secure communication among users. This not only enhances security but also enables the tracking and responsibility of data flows. The utilization of cryptographic coins and resilient key generation procedures enhances the overall security stance of the multi-tenant system.

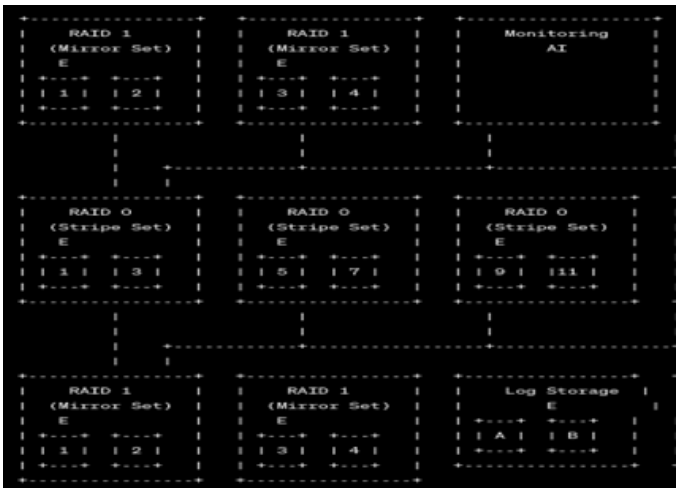


Fig. 7. Chunks with RAID encryption model.

2) Chunks with Raid Concept Encryption: When setting up a chunk-based RAID system, it is standard practice to follow the procedures outlined below: Split the data into i number of Chunks. Choose an appropriate chunk size based on the workload and characteristics of the data. Select the RAID level that optimally meets the requirements for both performance and redundancy. Ensure the disks are ready for use in the RAID array by properly formatting and initializing them. Use RAID management software or hardware to create the RAID array, specifying the appropriate chunk size and RAID level as shown in the Fig. 7. When data is written to the RAID array, it is divided into smaller segments and distributed among the disks according to the chosen RAID level.

Our solution utilizes the concept of Chunks with RAID (Redundant Array of Independent Disks) for encrypting and managing a huge number of database items. This strategy maximizes storage economy while ensuring fault tolerance. Data is divided into smaller segments called chunks, and the RAID idea guarantees both redundancy and reliability. Data security is enhanced by encrypting each piece separately. This approach not only streamlines the administration of an increasing number of tenants but also guarantees the security and accessibility of data through duplication and encryption. Our system utilizes Blockchain Technology, Smart Contracts, dynamic network formation, coin transactions with key generation protocols, and chunks with RAID concept encryption to transform the multi-tenant database design. This comprehensive method tackles issues related to security, scalability, and adaptability, offering a strong basis for a contemporary and effective multi-tenant system.

RAID 1 (Mirror Sets): There are several RAID 1 (mirror) sets indicated by the first and second rows. Each RAID 1 set comprises two drives that replicate each other, ensuring redundancy. Each RAID 1 block contains a "E" which signifies encryption, suggesting that the data saved on these mirrored sets is encrypted.

RAID 0 (Stripe Sets): The third row comprises RAID 0 (stripe) sets, which enhance performance by striping data across the RAID 1 sets. Each RAID 0 set comprises two drives, and the "E" denotes encryption for the striped data.

Monitoring AI: The central "Monitoring AI" block symbolizes an artificial intelligence system that oversees the entire RAID arrangement. This AI system has the responsibility of monitoring and managing the health, performance, and security of the storage system.

Log Storage: There are two "Log Storage" blocks in the last row, each containing its own pair of mirrored drives. Each log storage block is encrypted, as shown by the "E". Storing logs is essential for documenting events, faults, and activities in the storage system, which helps with diagnosing and resolving issues.

3) Advantages of chunk-based raid encryption:

- **Enhanced Efficiency:** By dividing data chunks across many drives, read and write operations may be executed simultaneously, resulting in improved overall performance.
- **Data Redundancy:** Chunk-based RAID offers different levels of data redundancy, which helps guard against disk failures.
- **Scalability:** RAID systems can be extended by including more disks into the array, augmenting storage capacity and perhaps enhancing performance.

III. Results and Discussion

We assess the efficacy of the chunk-based RAID Encryption scheme in the context of a sole data owner, specifically focusing on the operations of data encryption, token generation, query generation, search, decryption, and verification. This is implemented using the VSCode $(Version 1.89.1)$.

A. Data Encryption Assessment

With this encryption system, the data is broken down into smaller parts and each piece is securely encrypted before being sent, guaranteeing that transactions are protected and cannot be intercepted. By analyzing this technique, it becomes clear that the effectiveness of chunk-based RAID encryption is impacted by the size of the chunks and the total number of chunks. The encryption process duration Te can be affected by factors such as the data size D, the number of chunks Ci, and the computational complexity CXe as shown in the Eq. (16):

$$T_e = CX_e. \mid D \mid \tag{16}$$

Thus the encryption time for each block is calculated as follows:

$$T_{(e,block)} = CX_e.B \tag{17}$$

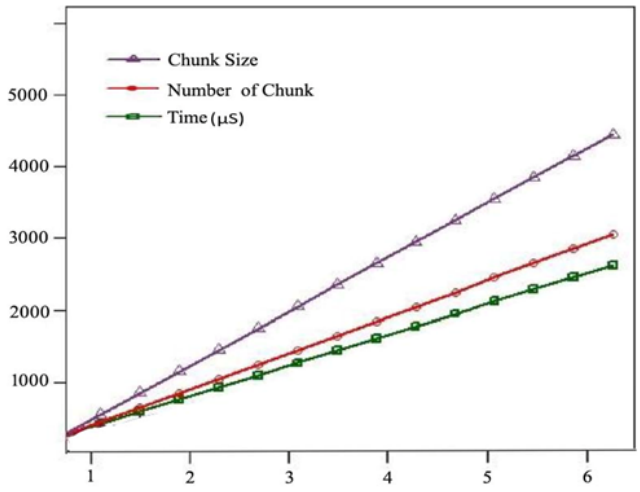


Fig. 8. Data encryption assessment graph.

It is evident from the graph shown in Fig. 8, the encryption progressively grows as the quantity of the data increases and stays within the lowest number that is feasible.

B. Decryption Assessment

The decryption phase consists of two distinct phases. The first stage entails deciphering the encrypted identities of the papers, while the following step concentrates on decrypting the encrypted documents themselves. The encrypted document identities and documents are decrypted with a symmetric decryption technique. After examining the data, it is clear that the size of the obtained result is directly related to the size of the dataset. The decryption process duration Td can be affected by factors such as the data size D, the number of chunks Ci, and the computational complexity CXd as shown in the Eq. (18):

$$T_d = CX_d. \mid D \mid \tag{18}$$

Thus the decryption time for each block is calculated as follows:

$$T_{(d,block)} = CX_d.B \tag{19}$$

Thus the decryption increases gradually with the increased data size and sticks to the minimum possible value within the limits.

C. Assessing the Verification Process

The verification process is utilized to ascertain the accuracy and entirety of the recovered papers. Based on the results, we can see that the verification performance is minimally impacted by the amount of the received result. The verification technique takes around 0.0001 seconds to complete because to the high efficiency of SHA-256 [41].

D. Explorations Involving Multiple Data Owners

Blockchain facilitates the involvement of multiple data owners. In this study, we evaluated the efficacy of the recommended technique, which only involved a single data owner. When multiple individuals or entities possess data, there is a notable discrepancy in the processes of generating encryption keys and performing encryption. The time required for key generation remains the same, regardless of the number of data owners. To perform a search across data owners, the client must obtain authorization from each individual data owner. This results in the creation of a large number.

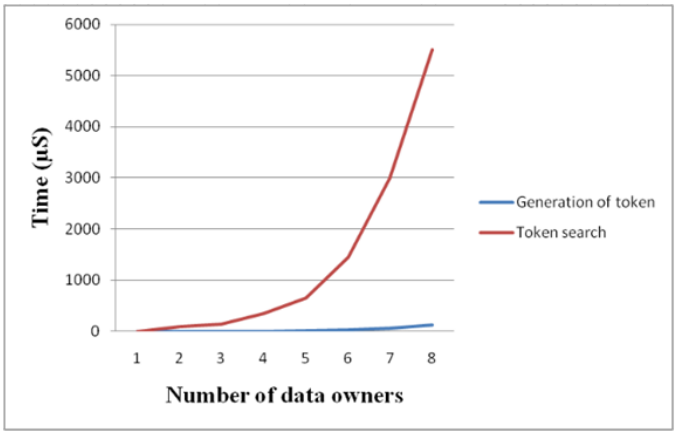


Fig. 9. Performance of multi owners in terms of generation and search tokens.

of tokens. Utilizing tokens enables a focused search operation on data that has been granted authorized access, as opposed to looking over the entirety of the data. To evaluate the effectiveness of the token generation and search algorithm, we execute them on 2, 4, 8, 16, and 32 data owners who authorize a client to access their data. Every data owner has a dataset containing 3125 keywords and 412,477 documents. The results are depicted in Fig. 9. The figure clearly demonstrates that as the number of data owners increases, both the time needed for token production and search both increase in a rather linear fashion. However, the time needed for token manufacturing is small in comparison to the time spent on the search process.

E. Latency

Chunk-based RAID encryption causes slowness owing to inherent factors in data processing and protection. Every segment of data must undergo encryption before being written to the RAID array, and decryption before being read. The intricacy and processing requirements of the encryption technique, such as AES, have a direct impact on the latency. RAID levels that employ parity, such as RAID 5 or RAID 6, necessitate extra computations to determine and confirm parity information. This procedure has the potential to cause delays, particularly when used in conjunction with encryption. Concurrency in disk operations can lead to increased latency, especially when the RAID controller is required to handle numerous simultaneous tasks across multiple disks. The delay can be influenced by the size of the data chunks utilized in the RAID arrangement. Using smaller chunks can result in more frequent encryption and parity calculations, while larger chunks may decrease these additional tasks but could introduce other inefficiencies. The efficiency of the RAID controller in handling encryption and parity computations has a considerable impact on total delay. In Network attached

storage systems, network latency can impact the performance, especially when data needs to be transmitted across a network and then encrypted before being stored in the RAID array.

The latency in encryption, specifically in the context of chunk-based RAID encryption, can be determined by taking into account multiple factors: data splitting and distribution, encryption processing, disk I/O operations, and possibly network delays. Below is a universal equation for determining the overall latency:

$$L_{Total} = L_{Split} + L_{Encrypt} + L_{(Disk_{io})} + L_{Network} \quad (20)$$

Where: L_{Split} = Latency due to data splitting and distribution
$L_{Encrypt}$ = Latency due to encryption processing
L_{diskio}= Latency due to disk I/O operations
$L_{Network}$ = Latency due to network transmission.

Latency caused by data splitting and distribution refers to the duration required to partition the data into segments and disperse them among many drives. The outcome is contingent upon the size of the data chunks (C), the quantity of disks (Dn), and the efficacy of the RAID controller. This is given by the Eq. (21):

$$L_{Split} = f(C, D_n) \quad (21)$$

Latency caused by encryption processing encompasses the duration required to encrypt individual portions of data. The time required for encryption depends on factors such as the specific encryption technique employed (AES-256), the size of the data chunk (C), and the processing capacity (CPU speed). This is given by the Eq. (22):

$$L_{Encrypt} = \sum_{(i=1)}^{n} (\frac{c_i}{B_{encrypt}}) + O_{Encrypt} \quad (22)$$

Where: n = Number of chunks
C_i = Size of the ith chunk
$B_{Encrypt}$ = Encryption bandwidth (throughput, e.g., MB/s)
$O_{Encrypt}$ = Overhead associated with the encryption process (initialization, padding, etc.)

Latency caused by disk I/O activities refers to the duration required for read and write operations on the physical disks. This latency is influenced by factors such as the kind of disk (HDD or SSD), the RAID level, and the read/write speed of the disks. This is given by the Eq. (23):

$$L_{diskio} = \sum_{i=1}^{n} (\frac{C_i}{B(disk_{io}} + O_{diskio} \quad (23)$$

Where: B_{diskio} = Disk I/O bandwidth (throughput, e.g. MB/s)

$O_{disk_{io}}$= Overhead associated with disk I/O operations (seek time, rotational latency, etc.)

Latency due to network transmission includes the time taken to transmit data over a network and depends on the network bandwidth and latency. This is denoted by the Eq. (24).

$$L_{network} = \sum_{i=1}^{n} (\frac{C_i}{B_{network}}) + O_{network} \quad (24)$$

Where $O_{network}$ = Overhead associated with network transmission (latency, packet loss, etc.)

The data size is 1 MB, divided into 10 pieces. The encryption bandwidth is 50 MBpS, the disk I/O bandwidth is 100 MBpS, and the network bandwidth is 100 MBpS. Assuming LSplit is negligible or already included in other components The assumed overhead is 0.01S. The calculated total loss is

$$LTotal = 0.21 + 0.11 + 0.11 = 0.43s$$

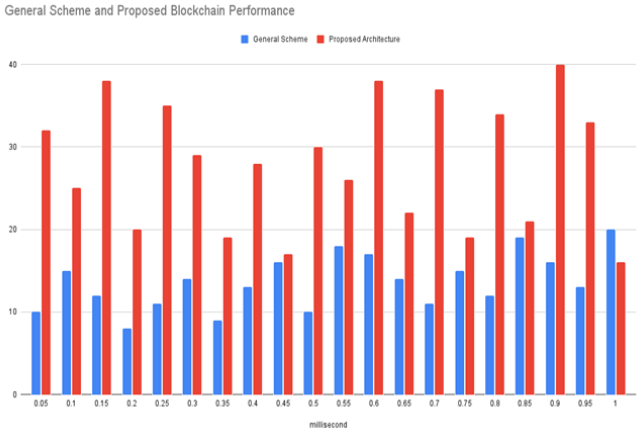


Fig. 10. Graph illustrating the latency between the general and proposed blockchain model.

Within a typical multitenant setting, the retrieval and manipulation of data may experience delays, which can hinder the efficiency of activities. Our secure blockchain multi-tenancy utilizes the decentralized and distributed characteristics of blockchain technology to greatly decrease latency. The technology reduces the time required for data transactions to be vetted and recorded by distributing the data across a secure and unchangeable ledger. The recorded values are plotted in the graph as shown in Fig. 10. The color blue symbolizes the duration of delay retrieval, while the color red indicates the data obtained from a generic tenant. The time output of the executed and processed data demonstrates that our proposed system has a shorter processing and retrieval time for data and outcomes.

F. Bruteforce Attack Vulnerability Assessment

A brute force attack on healthcare data security entails an assailant methodically attempting every conceivable combination of passwords or encryption keys until they successfully discover the proper one. The consequences of such an attack on healthcare data can be significant, considering the delicate nature of the information at stake. Engaging in a brute force attack against healthcare data security can result in severe outcomes, such as unauthorized access to data, fraudulent use

of personal information, disruption of operations, and substantial financial expenses. To effectively mitigate the risks of brute force attacks and safeguard sensitive patient information, healthcare organizations should employ robust authentication mechanisms, enforce account lockout policies, utilize encryption, monitor systems for suspicious activity, and educate users.

Brute force attacks, which involve attackers methodically attempting every conceivable combination to bypass encryption, pose substantial difficulties with chunk-based RAID encryption methods based on blockchain technology. The intrinsic intricacy of these systems introduces multiple levels of susceptibility that necessitate meticulous attention. To address vulnerabilities to brute force attacks in blockchain-based chunk-based RAID encryption methods, a comprehensive and multi-faceted strategy is necessary. Organizations can greatly mitigate the likelihood of successful brute force attacks by implementing powerful encryption algorithms, effective key management, and advanced security measures. Conducting regular security evaluations and keeping up-to-date with the newest cryptographic breakthroughs are crucial for maintaining a safe environment.

In this framework Chunk based encryption, has offered a key space of 256. Due to the existing computational capabilities, it is deemed impractical to forcefully determine a single key. Nevertheless, in the event that a malicious individual specifically focuses on the RAID parity data or endeavors to carry out a brute-force attack on numerous portions, the system's decentralized structure and duplication could unintentionally assist the attacker. To limit the possibility of a brute-force attack, the system has employed distinct Initialization vectors for each chunk and enforce robust key management policies. In addition, anomaly detection techniques have the ability to recognize and react to abnormal access patterns, hence improving security measures.

G. Comparison with Other Encryption Technologies

When evaluating the effectiveness of chunk-based RAID encryption in healthcare blockchain security, it is crucial to comprehend the distinct functions that cryptographic algorithms such as SHA-3 [31], SHA-256 [32], and AES [33] serve in safeguarding data.SHA-3 is a cryptographic hash function employed for the purpose of guaranteeing the integrity of data. SHA-3 generates a distinct hash of a specific size based on the input data, facilitating the identification of any modifications. This system is designed to be impervious to collision attacks, guaranteeing that no two distinct inputs will yield the same hash value. Frequently employed in blockchain technology to generate digital signatures and guarantee the unchangeability of transactions. SHA-3 is designed only for ensuring data integrity and performing cryptographic operations, as opposed to being used for purposes such as data redundancy or optimizing performance, like RAID. Primarily used to guarantee the authenticity and reliability of transactions and data blocks in blockchain, rather than focusing on safeguarding physical storage.

SHA-256 is a prevalent cryptographic hash function that finds extensive application in blockchain technology, such as in Bitcoin. Like SHA-3, it generates a hash of a specific size to guarantee the integrity of data. Additionally, it is impervious to both collision and preimage strikes. Essential for the creation of digital signatures, the process of hashing transactions, and the interconnection of blocks in a blockchain. Similar to SHA-3, it prioritizes data integrity above storage redundancy. Crucial for the functioning of blockchain processes, such as verifying transactions and creating blocks, but not suitable for safeguarding storage systems.

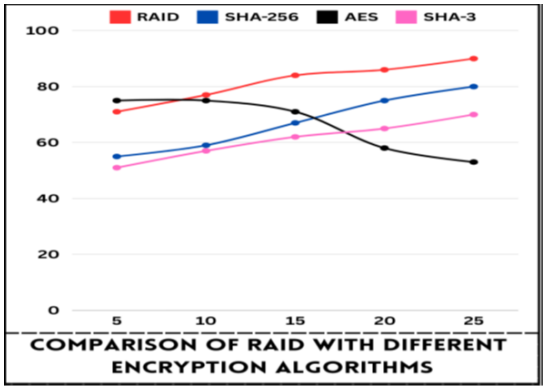


Fig. 11. Comparison of the proposed model with the existing models.

AES is a cryptographic technique that employs symmetric encryption to safeguard the secrecy of data. Robust encryption utilizing several key sizes (128, 192, 256 bits) Highly effective encryption and decryption procedures, applicable to both stationary and moving data. Can be utilized to employ cryptographic techniques to secure confidential information prior to its storage on the blockchain or transmission over the networks. AES primarily emphasizes the encryption of data to guarantee confidentiality, while RAID primarily emphasizes data redundancy and performance. AES is employed to safeguard the factual data content, hence enhancing RAID encryption's ability to maintain data confidentiality even in the event of unauthorized access.

Encryption of RAID using chunk-based methodology. Offers both data redundancy and performance advantages while ensuring data security while it is not actively being used. While SHA-3 and SHA-256 do not offer encryption or redundancy, they must be utilized with encryption algorithms to ensure comprehensive security. AES does not offer data redundancy or integrity. It is most effective when used in conjunction with hashing techniques to ensure comprehensive security.

The accuracy of the encryption/hashing techniques listed above is especially evaluated in comparison to the "RAID Chunk Encryption/Storage Concept". The accuracy was assessed across 25 encryption cycles, and the findings are depicted in the graph in Fig. 11.

From the graph, it is evident that the proposed system outsmarts the other existing encryption systems in terms of performance and accuracy. Chunk-based encryption in a RAID setup means each chunk or block of data stored across the RAID array is encrypted separately. This can enhance security by ensuring that even if one chunk is compromised, the entire dataset remains secure. When combined with encryption, it adds an additional layer of security, ensuring data integrity and confidentiality.

The efficiency of current multi-tenant healthcare data management approaches is hampered by a number of issues. Due to inadequate data separation, single database designs with common schemas are vulnerable to security breaches. Scalability is still a problem as data and user volumes increase, and maintaining several schemas or databases adds a great deal of expense and complexity. Additionally, a lot of conventional systems don't have strong fault tolerance methods, which makes data unavailable when hardware fails. Furthermore, because they lack immutable recording or verification systems like blockchain, they are unable to guarantee data integrity and transparency, making them unsuitable to satisfy the strict security and compliance requirements of the healthcare industry.

IV. Conclusion

Healthcare enterprises possess the capacity to create a robust, flexible, and dynamic framework that meets their evolving needs while maintaining high levels of performance and security. In order to tackle the challenges posed by multi-tenancy database systems, we propose a novel approach that leverages the dynamic organization of tenant connections and integrates blockchain technology to overcome these problems. Our approach employs the use of Chunks with RAID (Redundant Array of Independent Disks) to encrypt and handle a large quantity of database items. This approach optimizes storage efficiency while guaranteeing resilience against failures. This complete approach addresses concerns pertaining to security, scalability, and adaptability, providing a solid foundation for a modern and efficient multi-tenant system.

Thus, the approach that has been proposed offers robust data redundancy and fault tolerance, making it suited for ensuring high availability, even with increased complexity. This approach also exhibits efficient scalability with the inclusion of extra disks, possibly at the cost of increased intricacy.

References

[1] Khan, A. A., Bourouis, S., Kamruzzaman, M. M., Hadjouni, M., Shaikh, Z. A., Laghari, A. A., ... & Dhahbi, S. (2023). Data security in healthcare industrial internet of things with blockchain. IEEE Sensors Journal.

[2] Al Zaabi, M., & Alhashmi, S. M. (2024). Big data security and privacy in healthcare: A systematic review and future research directions. Information Development, 02666669241247781.

[3] Sharma, A., & Kaur, P. (2023). Tamper-proof multitenant data storage using blockchain. Peer-to-peer Networking and Applications, 16(1), 431-449.

[4] Rai, B. K. (2022). Security Issues and Solutions for Healthcare Informatics. In Federated Learning for IoT Applications (pp. 185-198). Cham: Springer International Publishing.

[5] Sharma, A., & Kaur, P. (2023). A survey of distributed data storage in the cloud for multitenant applications. International Journal of Performability Engineering, 19(3), 184.

[6] Almalki, J. (2024). State-of-the-art research in blockchain of things for healthcare. Arabian Journal for Science and Engineering, 49(3), 3163-3191.

[7] Mathivanan, P., MohanaPriya, D., Manjula, P., & Ouaissa, M. (2024). Protecting the Privacy of IoT-Based Health Records Using Blockchain Technology. In Technological Advancement in Internet of Medical Things and Blockchain for Personalized Healthcare (pp. 127-144). CRC Press.

[8] Vaiyapuri, T., Shankar, K., Rajendran, S., Kumar, S., Acharya, S., & Kim, H. (2023). Blockchain assisted data edge verification with consensus algorithm for machine learning assisted IoT. IEEE Access.

[9] Pittaras, I., & Polyzos, G. C. (2023, November). Multi-tenant, Decentralized Access Control for the Internet of Things. In 2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS) (pp. 28-34). IEEE.

[10] Dhasaratha, C., Hasan, M. K., Islam, S., Khapre, S., Abdullah, S., Ghazal, T. M., ... & Akhtaruzzaman, M. (2024). Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things. CAAI Transactions on Intelligence Technology.

[11] Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. Sensors, 23(21), 8944.

[12] Malik, H., Anees, T., Faheem, M., Chaudhry, M. U., Ali, A., & Asghar, M. N. (2023). Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions. Internet of things, 100860.

[13] Gupta, B. B., Prajapati, V., Nedjah, N., Vijayakumar, P., El-Latif, A. A. A., & Chang, X. (2023). Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (TMIS). Neural Computing and Applications, 35(7), 5055-5080.

[14] Li, K., Lee, J. Y., & Gharehgozli, A. (2023). Blockchain in food supply chains: a literature review and synthesis analysis of platforms, benefits and challenges. International Journal of Production Research, 61(11), 3527-3546.

[15] Shahaab, A., Khan, I. A., Maude, R., Hewage, C., & Wang, Y. (2023). Public service operational efficiency and blockchain–A case study of Companies House, UK. Government Information Quarterly, 40(1), 101759.

[16] Chee, T. H., & Rana, M. E. (2023, January). An Exploratory Study on the Impact of Hosting Blockchain Applications in Cloud Infrastructures. In 2023 15th International Conference on Developments in eSystems Engineering (DeSE) (pp. 381-386). IEEE.

[17] Dhiman, P., Henge, S. K., Singh, S., Kaur, A., Singh, P., & Hadabou, M. (2023). Blockchain Merkle-Tree Ethereum Approach in Enterprise Multitenant Cloud Environment. Computers, Materials & Continua, 74(2).

[18] Albassam, A., Almutairi, F., Majoun, N., Althukair, R., Alturaiki, Z., Rahman, A., ... & Mahmud, M. (2023). Integration of Blockchain and Cloud Computing in Telemedicine and Healthcare. IJCSNS, 23(6), 17-26.

[19] Sayal, A., Jha, J., & Chaithra, N. (2024). Blockchain: A Digital Breakthrough in Healthcare. In Blockchain for Healthcare 4.0 (pp. 1-25). CRC Press.

[20] Gupta, M., & Dwivedi, R. K. (2023). Blockchain-Based Secure and Efficient Scheme for Medical Data. EAI Endorsed Transactions on Scalable Information Systems, 10(5).

[21] Masri, D., Jaber, L., Mashal, R., Albourini, F., Alsaoud, M. A., & Al-Tarawneh, A. M. (2024, February). The Role of Wearables & Technology in Mental Health. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-5). IEEE.

[22] Alrashdi, I., & Alqazzaz, A. (2024). Synergizing AI, IoT, and Blockchain for Diagnosing Pandemic Diseases in Smart Cities: Challenges and Opportunities. Sustainable Machine Intelligence Journal, 7, 6-1.

[23] Khan, R. U., Kumar, R., Haq, A. U., Khan, I., Shabaz, M., & Khan, F. (2024). Blockchain-Based Trusted Tracking Smart Sensing Network to Prevent the Spread of Infectious Diseases. IRBM, 45(2), 100829.

[24] Verma, P., Rao, C. M., Chapalamadugu, P. K., Tiwari, R., & Upadhyay, S. (2024). Future of Electronic Healthcare Management: Blockchain and Artificial Intelligence Integration. In Next-Generation Cybersecurity: AI, ML, and Blockchain (pp. 179-218). Singapore: Springer 25ture Singapore.

[25] Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2023). Blockchain and COVID-19 pandemic: Applications and challenges. Cluster Computing, 26(4), 2383-2408.

[26] Jabbar, R., Fetais, N., Krichen, M., Kaoui, K. (2020, February). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In 2020 IEEE International

Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 310-317). IEEE.

[27] Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information processing & management, 58(3), 102535.

[28] Ikuomola, A. J., & Owoputi, K. S. (2024). Development of a Secured and Interoperable Multi-Tenant Software-as-a-Service Electronic Health Record System. In Intelligent Data Analytics, IoT, and Blockchain (pp. 286-301). Auerbach Publications.

[29] Raouf, A. E. A., Abo-Alian, A., & Badr, N. L. (2021). A predictive multi-tenant database migration and replication in the cloud environment. IEEE Access, 9, 152015-152031.

[30] Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., & Kolhatin, A. (2021). Performance analysis of cryptographic hash functions suitable for use in blockchain. International Journal of Computer Network & Information Security, 13(2), 1-15.

[31] Susanto, H., Ibrahim, F., Rosiyadi, D., Setiana, D., Susanto, A. K. S., Kusuma, N., & Setiawan, I. (2022). Securing Financial Inclusiveness Adoption of Blockchain FinTech Compliance. In FinTech Development for Financial Inclusiveness (pp. 168-196). IGI Global.

[32] Itnal, S., Kannan, K. S., Suma, K. G., & Neelakandan, S. (2022, May). A secured healthcare medical system using blockchain technology. In ICCCE 2021: Proceedings of the 4th International Conference on Communications and Cyber Physical Engineering (pp. 169-176). Singapore: Springer Nature Singapore.

[33] Gabriel, S. J., & Sengottuvelan, P. (2021, October). An enhanced blockchain technology with AES encryption security system for healthcare system. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 400-405). IEEE.

Enhanced Adaptive Hybrid Convolutional Transformer Network for Malware Detection in IoT

Abdulaleem Ali Almazroi
Department of Information Technology-Faculty of Computing and Information Technology in Rabigh,
King Abdulaziz University, Rabigh, 21911, Saudi Arabia

***Abstract*—Many university networks use IoT devices, which increases vulnerability and malware threats. The complex, multi-dimensional structure of IoT network traffic and the imbalance between benign and dangerous data make traditional malware detection techniques ineffective. The Adaptive Hybrid Convolutional Transformer Network (AHCTN) is a novel model that uses CNNs for spatial feature extraction and Transformer networks for global temporal dependencies in IoT data. Unique preprocessing methods like Category Importance Scaling and Logarithmic Skew Compensation handle unbalanced data and severely skewed numerical characteristics. The Unified Feature Selector combines statistical and model-based feature selection methods and guarantees that only the most relevant characteristics are utilized for classification. DWS and LRW handle data imbalance. Our feature engineering approaches, such as Flow Efficiency and Packet Interarrival Consistency, improve prediction accuracy by capturing essential data correlations. The integration of advanced machine learning techniques ensures precise malware classification and enhances cybersecurity by addressing vulnerabilities in IoT-driven academic networks. The AHCTN model was carefully tested using the IoEd-Net dataset, which contains a variety of IoT devices and network activity. The AHCTN outperforms previous models with 98.9% accuracy. It also performs well in Log Loss (0.064), AUC (99.1%), Weighted Temporal Sensitivity (97.1%), and Anomaly Detection Score (96.8%), recognizing uncommon but essential abnormalities in academic network data. These findings demonstrate AHCTN's robustness and scalability for academic IoT malware detection.**

***Keywords*—IoT security; malware detection; convolutional transformer network; cybersecurity; machine learning; network anomaly detection**

I. Introduction

Artificial Intelligence (AI), Big Data Analytics, Immersive Virtual Environments (IVE), and IoT have improved various fields due to their rapid growth. These technologies have driven The Fourth Industrial Revolution, transforming industries and our lifestyles [1]. In particular, IoT has changed device connection and data exchange. Connectivity boosts efficiency, automation, and convenience. Malware now threatens IoT installations. Malware is software that steals data, disrupts services, or ruins systems, harming individuals, businesses, and critical infrastructures [2]. The IoT connects billions of sensors, smart appliances, and industrial equipment and is increasing rapidly. However, IoT's numerous networked devices pose concerns. Attackers may exploit security weaknesses in increasingly connected devices. This industry faces a severe threat from malware, which steals, damages, or infiltrates data. Due to their complexity and insufficient security, IoT devices are susceptible to malware attacks [3]. Cybercriminals use IoT vulnerabilities for DDoS and crypto-mining. Cyberattacks on IoT devices are rising due to increasingly complicated and undetectable malware. Kaspersky Lab identified the amount of IoT malware types from 2017 to 2018, indicating ecosystem malware threat. Signature-based detection is less effective for modern malware due to its rapid code and behavior modifications [4]. Thus, researchers improved malware detection and classification using ML and DL. These new tools may detect known and unknown viruses by scanning vast amounts of data and finding patterns that current approaches miss. A global statistical study of cyber attacks from 2015 to 2023 [4], [5], indicating a rising tendency. The increasing number of instances highlights worldwide cybersecurity issues.

Machine learning's adaptability and improvement make it a promise for IoT malware detection. Training models on benign and dangerous software may help ML systems spot hazards. Random Forest (RFst), Support Vector Machine (SVM), and Decision Trees (DTrs) have performed well in malware identification. Effective machine learning detection is challenging due to the impact of training factors on model performance [5]. Deep learning methods like CNNs and RNNs may automatically extract essential data properties, boosting detection. Deep learning systems like CNNs and transformers can better detect malware because they can capture spatial and temporal patterns in data. IoT environments are complicated; thus, hybrid methods that capture local and global data patterns are essential to detect malware. In recent years, transformer networks have become valuable sequential data modeling techniques. Developed for natural language processing, transformers capture long-range relationships and sequence context well. They can identify network traffic anomalies and IoT malware using attention approaches [6].

Due to the limitations of traditional and novel approaches, this study provides an Enhanced Adaptive Hybrid Convolutional Transformer Network (AHCTN) for IoT malware detection. AHCTN uses CNNs and transformers to identify malware. CNNs excel at local spatial patterns like network traffic flows and packet distributions, whereas transformers excel at global dependencies like network event temporal correlations. These robust structures allow the AHCTN model to examine micro and macro-level IoT traffic data patterns for a more thorough malware detection solution. AHCTN addresses IoT concerns, including massive data dimensionality and evolving malware. Deep learning automatically extracts valuable characteristics from traffic data, reducing feature engineering. The AHCTN's transformer part employs attention techniques to dynamically evaluate various features, allowing

the model to zero in on the most critical malware detection patterns. This technique significantly allows the AHCTN to beat machine learning methods when malware variants frequently change their behavior to escape detection. AHCTN parameters are optimized for performance in this study. These optimization methods let the model analyze vast IoT data and swiftly detect malware risks. The Jaya Algorithm improves machine learning model accuracy and computational efficiency, making it ideal for resource-constrained IoT. Key contributions of this work:

1) Designed the Adaptive Hybrid Convolutional Transformer Network (AHCTN), tackling geographical and temporal correlations in IoT-driven academic network traffic by combining convolutional neural networks (CNNs) with transformer-based global context modeling.
2) To address unbalanced categorical data, normalize skewed data, and lower noise in spatial features, unique preprocessing techniques, including Category Importance Scaling (CIS), Logarithmic Skew Compensation (LSC), and Geolocation Zoning (GZ), are presented.
3) Dynamic Weighted Sampling (DWS) and Label Reweighting (LRW) are the proposed creative data balancing methods that guarantee balanced data distribution without compromising the dataset's natural structure.
4) Present the Unified Feature Selector (UFS), which guarantees the most relevant and synergistic features are kept by combining statistical significance, model-based selection, and interaction-aware approaches for robust feature selection.
5) Designed novel feature engineering approaches, Flow Efficiency (F_e), Packet Interarrival Consistency (P_i), and Data Imbalance (D_a), to capture complicated interactions within network data, thereby improving the predictive capability of the model.
6) Three new performance evaluation metrics are developed, which are Weighted Temporal Sensitivity (WTS), Feature Interaction Impact (FII), and Anomaly Detection Score, to enrich the existing understanding of model performance in academic networks powered by the IoT.
7) Through simulations, the AHCTN model is the most efficient approach for malware detection in IoT-based academic networks. It exceeds current models with a remarkable accuracy of 98.9%.

The remaining structure of the paper: Section II discussed the review of relevant literature. The proposed method structure is described in detail in Section III. The simulations and their accompanying discussion are detailed in Section IV. The last section concludes with a discussion of future work.

II. Related Work

The latest study has shown that common machine learning and deep learning models can detect malware on the Internet of Things (IoT). Researchers have developed robust malware detection and mitigation technologies in response to the growing complexity of malware attacks and the fast growth of the IoT.

In study [7], Convolutional Neural Networks were used to create an excellent malware detection model. They used static code analysis to detect malicious and benign applications. CNN model classified malware with 91.01% accuracy. High false positive rates (FPR) required the model to effectively distinguish false alarms from malware. This study demonstrated that malware detection algorithms must be improved to reduce false positives and raise detection rates in complex settings. Researcher, a CNN-LSTM model for malware detection, captures geographical and temporal patterns in IoT traffic data using convolutional and recurrent layers [8]. With FPR at 0.2%, the model was 99.6% correct. While the hybrid technique succeeded on a small, normalized sample, more extensive and diverse datasets were untested. LSTM processing power limits real-time applications. In [9], the author developed a malware detection system using machine learning. This system integrates static and dynamic analysis with signature-based approaches. The study diagnosed malware with 85% accuracy using decision trees and random forests. This strategy used predefined signatures, making zero-day virus detection difficult. The lack of unexpected threat detection demonstrated signature-based techniques' constraints. Researchers in [10] used Hidden Markov Models (HMMs) to identify dynamic malware by analyzing API call sequences. Their strategy enhanced limited dataset detection accuracy. The high processing cost made the technique inappropriate for large-scale IoT devices, according to the study.

Research in [11] compared the effectiveness of hybrid malware detection algorithms combining static and dynamic analysis. Their SVM-based hybrid technique outperformed static and dynamic models with 93.5% accuracy. Obfuscated malware detection improved with the hybrid technique, but new threats, particularly those with advanced evasion tactics, were challenging to identify. Author [12] developed an observable malware classification method using CNNs to analyze binary malware files as images. Their 94.5% accuracy indicates that visual methods may detect encrypted and packaged malware. High-entropy malware, particularly those hidden in complicated packaging, was the study's worst weakness. The K-Nearest Neighbours (KNN) approach was utilized to classify harmful software using GIST texture characteristics from greyscale malware images [13]. Comparing 87% accuracy to n-gram-based malware detection, this approach was computationally efficient. It struggled with comparable binary malware families. Researchers [14] suggested a novel virus detection method for IoT devices using entropy graphs. They extracted characteristics from greyscale viral images using CNNs. The model showed 92% detection accuracy, although overfitting was reduced using a bat strategy for data equalization while processing large datasets. The study did not address real-time malware detection.

Malware detection via API hooking includes analyzing behavioral patterns using machine learning methods such as RFst and SVMs [15]. The program detected malware activity with 90% accuracy. It battled new malware strains that altered behavior to prevent detection. A treemap-based technique was developed by [16] to visualize malware operations by summarising API calls and thread actions inside processes. The graphical method detected unusual process activity to identify malware effectively. Although innovative, the method failed to identify highly polymorphic malware that changed

behavior over time. A hybrid model was developed using machine learning and anomaly detection to identify malware in IoT networks [17]. Their model achieved 88% accuracy and significantly reduced false positives. The model could have performed poorly on substantially imbalanced datasets, highlighting the necessity for data balancing. Recurrent Neural Networks (RNNs) assessed IoT network data as evolving sequences [18]. Achieving 89% accuracy in time-based anomaly detection is promising. Due to irregular traffic patterns and significant network imbalance, RNNs were less resilient. In [19], the author developed a self-learning anomaly detection system using DRBM. Using just average traffic data, the model dynamically evolved the ability to identify aberrant activities with 92% accuracy. Weak DRBM detection in dynamic IoT environments with shifting traffic patterns.

Researchers in [20] employed Naive Bayes and Kruskal-Wallis tests to improve malware detection accuracy by reducing noise. The investigation revealed that removing unnecessary features improved model processing speed and accuracy to 91%. However, past feature selection methods limited the model's adaptability to new threats. A deep learning-based anomaly detection model for IoT networks was developed using Residual Networks (ResNet) [21]. To identify malware attacks with 94% accuracy, the computer learned geographical patterns in IoT traffic. Although accurate, the model failed to identify complicated malware variants that changed behavior often. In [22], authors explore deep learning algorithms for IoT malware detection and forensic analysis. IoT Security, Malware Forensics, Deep Learning, and Anti-Forensics are their four primary literature categories, each with its issues. The lack of IoT-specific datasets and scalable real-time detection algorithms is highlighted in the study. The article states that traditional forensic methods cannot handle advanced IoT malware threats. Future directions include advanced anti-forensic countermeasures. Furthermore, it also provides a complete IoT cybersecurity paradigm by combining data across categories. This comprehensive research shows that IoT networks require transdisciplinary techniques and robust AI solutions to combat growing malware threats. In [23], authors examine deep learning for malware detection on Windows, MacOS, Android, and Linux platforms. Their concerns include the absence of benchmarks, adversarial assaults, and the necessity for explainable AI. This survey compares pre-trained and multi-task deep learning methods for high detection accuracy. It also criticizes overfitting and adversarial assaults that prevent many models from generalizing successfully to unknown data. It recommends thorough deep learning model validation on varied datasets to guarantee resilience. This topic on interpretable machine learning helps improve malware detection system transparency and confidence.

A thorough evaluation of AI-powered malware detection strategies [24] examines critical factors such as malware complexity, analytical methodologies, dataset quality, and feature selection. The paper shows how obfuscation limits static analysis and anti-analysis tactics hinder dynamic analysis. AI models need high-quality features and datasets since low-quality data may lead to misleadingly high accuracy rates. The paper also examines machine learning vs. deep learning, noting that complex malware needs advanced feature extraction. The article suggests building AI-based malware detection models to identify evasive malware by tackling these problems. The authors of [25] introduce deep learning-based malware detection approaches and highlight their benefits over older methods. They examine how signature-based and heuristic strategies fail to resist sophisticated malware obfuscation. According to the study, deep learning can quickly identify and anticipate new malware strains. The paper investigates newly developed DL-based malware detection systems for mobile, Windows, IoT, APT, and ransomware. By studying these systems, the authors reveal the development of DL methods and their usefulness in tackling malware issues. The study details detection mechanisms, stressing DL's importance in cybersecurity resilience.

Research shows that machines and deep learning can detect IoT malware. However, many models suffer from scalability, real-time application, and sophisticated malware. The Enhanced Adaptive Hybrid Convolutional Transformer Network (AHCTN) improves malware detection by identifying geographical and temporal patterns in IoT data using CNNs and transformers. Table I shows the summarized view the above mentioned literature.

III. Proposed Method

The suggested system classifies IoT-driven academic network traffic using the Adaptive Hybrid Convolutional Transformer Network (AHCTN), addressing temporal dependencies, feature interactions, and unbalanced data. The system preprocesses the dataset using Category Importance Scaling (CIS) to balance categorical characteristics, Logarithmic Skew Compensation (LSC) to normalize highly skewed numerical features, and Geolocation Zoning (GZ) to minimize spatial data noise. Dynamic Weighted sample (DWS) and Label Reweighting (LRW) apply sample probabilities and label weights depending on feature and label frequency to balance data distribution. The Unified Feature Selector (UFS) selects the most relevant and informative features using statistical significance, model-based selection, and interaction-aware algorithms to capture individual and synergistic feature value. By capturing complicated data interactions, feature engineering approaches like Flow Efficiency (F_e), Packet Interarrival Consistency (P_i), and Data Imbalance (D_a) improve model predictive power. Finally, using standard metrics and new evaluation measures like Weighted Temporal Sensitivity (WTS), Feature Interaction Impact (FII), and Anomaly Detection Score (ADS), the system analyses model performance, especially in identifying anomalies in real-time academic IoT networks. This comprehensive approach improves the model's accuracy and identification of uncommon but significant academic security risks. Fig. 1 shows the proposed framework of this study.

A. Dataset Description

This study used the publicly available IoEd-Net dataset from Kaggle [26]. It covers the IoT environment with 202,085 records. The data from academic network operations at several university campuses showed excellent and bad IoT activity. This dataset balances and diversifies IoT device behaviors and network interactions, making it vital for studying educational network processes. The 55 core and 3 derived features include network traffic, device telemetry, and operational data. Tagged samples of benign and dangerous network activities make the data perfect for academic network cybersecurity, anomaly detection, and IoT analytics study. The dataset's variety improves

TABLE I. LITERATURE REVIEW SUMMARY

Ref	Technique Used	Objective Achieved	Limitations
[7]	Convolutional Neural Networks (CNN)	Developed a CNN model for malware classification, achieving 91.01% accuracy.	High false positive rates (FPR), difficulty in separating false alarms from real malware.
[8]	Hybrid CNN-LSTM	Achieved 99.6% accuracy with reduced FPR of 0.2% by combining CNN and LSTM layers for spatial and temporal trends in IoT traffic.	Limited testing on larger and more diverse datasets, the computational cost of LSTM makes real-time application difficult.
[9]	Decision Trees, Random Forest	Classified malware using a combination of signature-based approaches with static and dynamic analysis, achieving 85% accuracy.	Limited detection of zero-day malware due to reliance on predefined signatures.
[10]	Hidden Markov Models (HMM)	Improved malware detection accuracy through dynamic API call sequence analysis in small datasets.	Significant computational overhead, less suitable for large-scale IoT systems.
[11]	SVM-based Hybrid Model (Static + Dynamic)	Enhanced detection of obfuscated malware with 93.5% accuracy by combining static and dynamic analysis techniques.	Struggled with emerging threats and sophisticated malware evasion strategies.
[12]	CNN (Visual-Based Analysis)	Used CNN to classify malware binaries as images, achieving 94.5% accuracy in identifying packed and encrypted malware.	Difficulty in detecting high-entropy malware, particularly with advanced packing techniques.
[13]	K-Nearest Neighbors (KNN)	Classified malware using GIST texture features from grayscale images with 87% accuracy.	Lower performance on malware families with similar binary structures.
[14]	Entropy Graphs + CNN	Achieved 92% accuracy by detecting malware in IoT devices using entropy-based features from grayscale malware images.	Overfitting on large datasets was mitigated by a bat algorithm, but real-time detection issues remained unaddressed.
[15]	Random Forest, SVM (API Hooking)	Detected malware activities by analyzing API hooking behaviors with 90% accuracy.	Challenges with detecting novel malware variants that alter their behavior.
[16]	Treemap + API Calls Visualization	Visualized malware behavior using API calls and thread actions, providing insights into malware detection.	Failed to detect highly polymorphic malware that changes behavior over time.
[17]	Hybrid Machine Learning + Anomaly Detection	Detected malware in IoT networks with 88% accuracy and reduced false positives.	Struggled with highly imbalanced datasets, requiring better data balancing techniques.
[18]	Recurrent Neural Networks (RNN)	Modeled IoT network traffic as evolving sequences for anomaly detection with 89% accuracy.	Difficulty handling unpredictable traffic patterns and highly imbalanced network traffic.
[19]	Discriminative Restricted Boltzmann Machine (DRBM)	Developed a self-learning anomaly detection system trained on normal traffic data with 92% accuracy.	Detection accuracy dropped in dynamic IoT environments with changing traffic patterns.
[20]	Naive Bayes, Kruskal-Wallis (Feature Selection)	Improved malware detection accuracy to 91% by eliminating irrelevant features, enhancing processing speed.	Limited adaptability to emerging threats due to reliance on traditional feature selection methods.
[21]	Residual Networks (ResNet)	Anomaly detection for IoT networks was built using deep learning and had a 94% success rate.	Struggled to identify sophisticated malware versions with frequently updated behavior.

educational IoT system analysis. Table II shows the features list of the dataset.

B. Data Preprocessing Steps

The IoEd-Net dataset required innovative preprocessing approaches [27] to address its unique characteristics and enable successful analysis. Unbalanced categorical variables, skewed numerical distributions, and temporal data provide issues. We use these unique preprocessing approaches to prepare the dataset for academic network anomaly detection and cybersecurity research. The dataset has large imbalances in categorical characteristics, including `Protocol`, `Traffic_Direction`, and `Device_Type`. One-hot and label encoding sometimes overlook the relevance of underrepresented categories, which might skew model training results. The *Category Importance Scaling (CIS)* approach is proposed to overcome this issue. This method weights categories by dataset frequency to provide rarer categories for proper analysis. For category C_i, determine the scaling factor:

$$\text{CIS}(C_i) = \frac{1}{\log(1 + f_i)} \tag{1}$$

where f_i is category C_i frequency. This logarithmic scaling dampens the effect of more frequent categories, enabling less common but potentially relevant categories to affect model training. Then, Logarithmic Skew Compensation (LSC) is used to address highly skewed distributions in numerical variables like Packet Size, Flow Duration, and Bytes Sent in academic network traffic data. Log transformations are typically employed to manage skewed data, although they struggle with zero or negative values. The LSC approach uses a shift factor s to preserve changed data. The change is:

$$\text{LSC}(X) = \log(1 + X + s) \tag{2}$$

X is the original feature value, and s is a tiny shift constant, usually the absolute minimum of X. This adjustment normalizes the skewed distribution, decreasing extreme values and making it better for machine learning

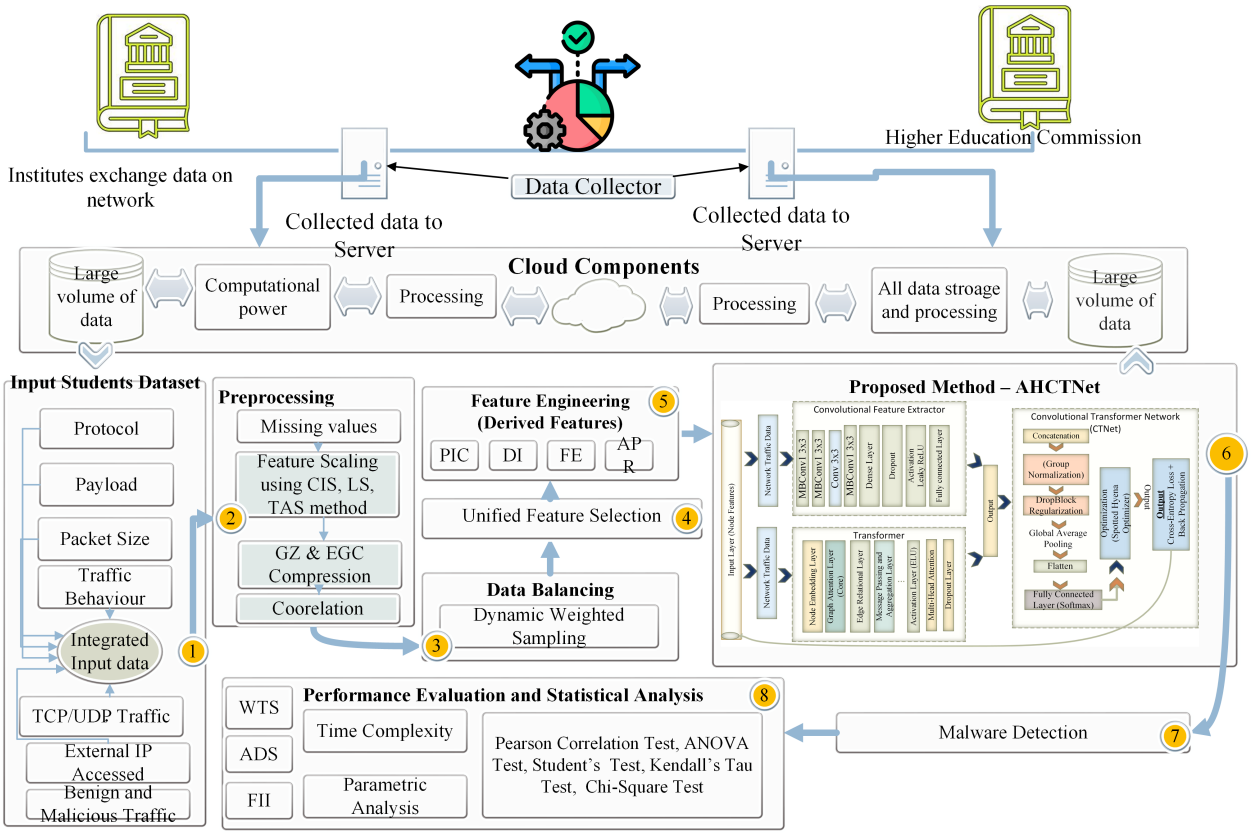


Fig. 1. Proposed malware detection framework.

models. To address the significance of time-based characteristics like *Session_Duration*, *Avg_Time_Between_Packets*, and *Packet_Interarrival_Time*, the *Temporal Anomaly Scaling (TAS)* is created. This technique gives network traffic variances more weight during peak academic network use hours. Definition of temporal scaling:

$$\text{TAS}(T) = \frac{T - \mu_T}{\sigma_T} \times w(T) \tag{3}$$

μ_T and σ_T represent the mean and standard deviation of the time-based feature. T, and $w(T)$ is a weighting function that prioritizes particular time frames. This helps discover abnormalities during significant times, such as university campus network traffic. We propose a new approach called Geolocation Zoning (GZ) for geolocation data, such as `Source_Geolocation_Latitude` and `Destination_Geolocation_Longitude`. Geolocation characteristics are generally highly variable. Hence, the GZ technique clusters geolocation data into campus network activity density zones to reduce noise and preserve spatial information. The formula for geolocation data zone segmentation is:

$$\text{GZ}(G) = \text{ZoneID}(k) \tag{4}$$

G represents the geographical position, and $textZoneID(k)$ identifies the cluster zone based on k clusters. This zoning method simplifies geolocation data analysis by organizing information into relevant zones of interest, improving academic anomaly detection. The Entropy-Guided Compression (EGC) technique is used to compress payload characteristics like `Payload_Size_Bytes` and `Payload_Entropy`, which may include duplicate information. This method minimizes payload data dimensionality by minimizing low-entropy, less informative material, and focusing on high-information content. Transformation appears as:

$$\text{EGC}(P) = P \times (1 - H(P)) \tag{5}$$

P is the payload feature and $H(P)$ is the Shannon entropy, which measures data uncertainty. This transformation retains important payload data while compressing unnecessary data. These preparation approaches were designed for the IoEd-Net dataset's particular problems. Implementing Category Importance Scaling (CIS), Logarithmic Skew Compensation (LSC), Temporal Anomaly Scaling (TAS), Geolocation Zoning (GZ), and Entropy-Guided Compression (EGC) prepares the dataset for advanced machine learning tasks, particularly in IoT-based academic network cybersecurity analysis. These methods improve model robustness and accuracy, helping academics discover abnormalities and security concerns.

C. Data Balancing using Dynamic Weighted Sampling

Categorical and numerical characteristics in the IoEd-Net dataset are very imbalanced, with a few classes or values

TABLE II. DATASET FEATURES OVERVIEW

S.No	Features	Short Description	S.No	Features	Short Description
1	Source_IP	IP address of the source device	29	CPU_Usage	CPU usage of the device
2	Destination_IP	IP address of the destination	30	Memory_Usage_MB	Memory used by the device (MB)
3	Source_Port	Network port of the source	31	Energy_Consumption_Watts	Device energy usage in watts
4	Destination_Port	Network port of the destination	32	Firmware_Version	Device firmware version
5	Protocol	Type of network protocol (TCP, UDP, etc.)	33	Device_Uptime_Hours	Total device uptime (hours)
6	Packet_Size	Size of the network packet	34	Payload_Size_Bytes	Size of payload in bytes
7	Packet_Count	Total number of packets	35	Payload_Entropy	Entropy of payload data
8	Flow_Duration	Duration of the network flow	36	Payload_Content_Type	Content type of payload (ASCII, Binary)
9	Packet_Interarrival_Time	Time between packet arrivals	37	Signature_Match	Whether a signature matched or not
10	TCP_Flags	Flags set in a TCP packet	38	Compressed_Encrypted_Flag	Flag indicating compression/encryption
11	Bytes_Sent	Total bytes sent	39	Content_Type_File_Transferred	Type of file transferred
12	Bytes_Received	Total bytes received	40	Flow_Count_Per_Time_Window	Count of flows in a time window
13	Traffic_Direction	Direction of traffic (Ingress/Egress)	41	Avg_Packet_Size_Bytes	Average packet size in bytes
14	Connection_State	State of the connection	42	Packet_Rate_Packets_Per_Second	Rate of packets per second
15	Packet_Drop_Rate	Rate of dropped packets	43	Std_Dev_Packet_Size	Standard deviation of packet size
16	Malformed_Packet_Count	Number of malformed packets	44	Min_Packet_Size	Minimum packet size
17	Avg_Time_Between_Packets	Average time between packets	45	Max_Packet_Size	Maximum packet size
18	Total_Flow_Count	Total number of network flows	46	Protocol_Distribution_TCP_Percent	Percentage of TCP traffic
19	Device_Type	Type of IoT device	47	Protocol_Distribution_UDP_Percent	Percentage of UDP traffic
20	Device_Manufacturer	Manufacturer of the device	48	Protocol_Distribution_ICMP_Percent	Percentage of ICMP traffic
21	OS_Version	Version of the operating system	49	Source_Geolocation_Latitude	Latitude of source location
22	DNS_Query_Count	Number of DNS queries	50	Source_Geolocation_Longitude	Longitude of source location
23	Suspicious_Domain_Query_Flag	Flag for suspicious domain query	51	Destination_Geolocation_Latitude	Latitude of destination location
24	File_Transfer_Occurred	Flag indicating file transfer	52	Destination_Geolocation_Longitude	Longitude of destination location
25	File_Size_Bytes	Size of transferred file	53	Anomalous_Behavior_Flag	Flag indicating anomalous behavior
26	External_IP_Accessed_Flag	Flag for external IP access	54	Session_Duration	Duration of the session
27	Label	Benign or malicious activity	55	Time_Of_Day	Time of day of activity
28	Device_Uptime_Hours	Uptime of the IoT device	56	Day_Of_Week	Day of the week of activity

dominating. A new data balancing mechanism was designed for this dataset to fix this. *Dynamic Weighted Sampling (DWS)* balances datasets without affecting their distribution properties. Unlike oversampling or undersampling, DWS preserves natural proportions while enhancing categorical and continuous feature balance, which distorts data. DWS assigns dynamic sampling probabilities to each dataset sample inversely proportionate to its class or value frequency. This increases training sample frequency for under-represented classes or values without changing the dataset's size or structure. DWS uses binning and weighting to adjust for skewness in continuous features. Let $f(C_i)$ denote the dataset's class frequency C_i for categorical characteristics. The sampling probability for each class is $P(C_i)$:

$$P(C_i) = \frac{1}{\log(1 + f(C_i))} \tag{6}$$

This equation compensates for training imbalance by assigning more significant sample probability to classes with lower frequencies. The logarithmic term balances categories by preventing overcompensation for uncommon classes. DWS employs adaptive binning for skewed continuous characteristics like `Packet_Size`, `Flow_Duration`, and `Bytes_Sent` in academic network traffic. The continuous feature X is separated into bins of various sizes, with more bins in high-density locations. Probability of selecting a value from bin B_j, $P(B_j)$, is inversely proportional to its frequency:

$$P(B_j) = \frac{1}{f(B_j) + \epsilon} \tag{7}$$

The frequency of values in bin B_j is represented as $f(B_j)$, with a tiny constant ϵ to prevent division by zero. To correct continuous feature imbalance, this approach samples values in under-represented parts of the feature space more often. Adaptive binning preserves data distribution and reduces skewness.

Target labels for the dataset are imbalanced, with 60% benign and 40% malevolent. We use the Label Reweighting (LRW) technique to balance labels. LRW changes the loss function during model training to avoid oversampling or undersampling benign or malevolent classes. Each label's weight w_i is the inverse of its frequency:

$$w_i = \frac{1}{f(y_i)} \tag{8}$$

where $f(y_i)$ is the dataset label frequency. Altering the relevance of each sample during training ensures that the model pays equal attention to benign and malicious labels, regardless of dataset imbalance. The reweighted loss function is:

$$\mathcal{L}(y, \hat{y}) = \sum_i w_i \cdot \ell(y_i, \hat{y_i}) \tag{9}$$

Where $\ell(y_i, \hat{y_i})$ is the original loss (e.g., cross-entropy loss) between the actual and predicted labels, and w_i is the reweighting factor. Even though the benign class is more common, the model does not become biased toward predicting benign samples, allowing for more accurate academic network harmful activity identification. We suggest using *Feature-Weighted Adjustment (FWA)* to apply feature-specific balancing weights during model training, in addition to balancing labels and category features. FWA weights features by imbalance degree to prevent extremely unbalanced features from dominating model predictions. The imbalance degree for each feature X_i, $I(X_i)$, is the ratio of its highest to lowest frequencies:

$$I(X_i) = \frac{\max(f(X_i))}{\min(f(X_i)) + \epsilon} \tag{10}$$

ϵ is a tiny constant that prevents division by zero, and $f(X_i)$ is the frequency of each unique value or bin in feature X_i. Next, the feature weight $w_f(X_i)$ is determined in the following way:

$$w_f(X_i) = \frac{1}{I(X_i)} \tag{11}$$

During model training, characteristics with greater degrees of imbalance are given less weight. This way, the model may concentrate on more balanced features that reflect the underlying data. With FWA included, the total weighted loss function is given by:

$$\mathcal{L}\text{FWA}(y, \hat{y}) = \sum i w_f(X_i) \cdot \ell(y_i, \hat{y_i}) \tag{12}$$

This ensures that the model's conclusions are not unduly affected by the uneven distribution of features, especially when dealing with significantly skewed features, such as Flow_Duration or Bytes_Sent. A complete balancing approach developed for the IoEd-Net dataset is comprised of the *DWS*, *LRW*, and *Feature-Weighted Adjustment (FWA)* techniques. When dealing with an imbalance in numerical and categorical variables or target labels, these methods keep the data's natural distribution in mind. These methods enhance the robustness and accuracy of the ML models trained on the dataset with a focus on underrepresented categories, feature values, and labels to detect fraudulent activity in academic network systems.

D. Unified Feature Selector

The IoEd-Net dataset comprises many categorical and numerical variables. Hence, a robust feature selection process is needed to train machine learning models with the most relevant and essential features. Unified Feature Selector (UFS) is an innovative way to accomplish this. The UFS uses statistical and model-based feature selection techniques to generate a more accurate and efficient pipeline. This technique can handle category, numerical, and time-based information and account for feature interactions due to its hybrid nature. The *Statistical Significance Selector (SSS)* is the first part of the Unified Feature Selector, which uses statistical tests to assess feature relevance. Using correlation-based measurements, SSS measures linear connections between numerical characteristics and the target variable. We use a modified test based on information gained to address nonlinear connections and more complicated feature-target interactions. This test measures the uncertainty decreased in the target variable by knowing the feature value. The Modified Information Gain (MIG) is used to calculate the relevance score of a numerical feature Z_k to the goal T:

$$\text{MIG}(Z_k, T) = S(T) - S(T \mid Z_k) \tag{13}$$

Where $S(T)$ is the target variable's entropy, and $S(T \mid Z_k)$ is the target's conditional entropy given the feature Z_k. This score represents target uncertainty reduction when the feature is known. Higher MIG values indicate relevance and are picked for study. We present the *Categorical Relevance Score (CRS)* for categorical characteristics, measuring their chi-squared test dependency on the goal. Calculating the CRS:

$$\text{CRS}(A_m, T) = \sum \frac{(P_{im} - Q_{im})^2}{Q_{im}} \tag{14}$$

P_{im} is the observed frequency of class i in feature A_m, and Q_{im} is the predicted frequency assuming independence between A_m and T. Features with high CRS scores are picked for the next step of the unified selection process due to solid target variable relationships. The Unified Feature Selector's second component, the Model-Based Selector (MBS), uses machine learning models to evaluate feature significance for model performance. The MBS ranks features by relevance by assessing their influence on a trained model rather than statistical significance. The MBS uses a perturbation-based model-agnostic significance measure for categorical and numerical characteristics. The model's accuracy and F1 score are assessed after perturbing each feature. Let g be the trained model, and $\Delta(g(W))$ be the performance change when feature W is disturbed. Definition of the Perturbation Importance Score (PIS):

$$\text{PIS}(W_k) = \frac{|g(W) - g(W'_{\text{perturbed}})|}{g(W)} \tag{15}$$

$g(W)$ represents the model's initial performance with all features, whereas $g(W'_{\text{perturbed}})$ represents the performance after perturbing feature W_k. Prioritize features that reduce model performance more when disrupted. MBS retains statistically

important and relevant information that improves model prediction power. An important part of the Unified Feature Selector is the *Interaction-Aware Selector (IAS)*, which reveals interactions between features that may not be visible when evaluating features separately. Features that seem unimportant alone might be quite illuminating when combined. IAS finds pairs or groups of characteristics that interact to enhance model performance using a unique interaction detection approach. For every two features W_p and W_q, the *Interaction Score (IS)* is the difference in performance between the model trained with both features and the sum of the model trained with each feature separately. Definition of IS:

$$\text{IS}(W_p, W_q) = g(W_p, W_q) - (g(W_p) + g(W_q)) \tag{16}$$

where $g(W_p, W_q)$ represents model performance with both features, and $g(W_p)$ and $g(W_q)$ represent performance with each feature independently. Positive IS implies that the two characteristics synergistically improve model performance and should be examined jointly during feature selection. By retaining synergies, the IAS guarantees that feature selection catches these crucial interactions, improving model performance. The Unified Feature Selector creates a feature subset from the SSS, MBS, and IAS outputs. Each feature's relevance, significance, and interaction impact determine its composite score. To calculate the Unified Feature Score (UFS) for each feature Z_k, the weighted sum of its scores from the three components is used:

$$\text{UFS}(Z_k) = \lambda_1 \cdot \text{MIG}(Z_k) + \lambda_2 \cdot \text{PIS}(Z_k) + \lambda_3 \cdot \sum_q \text{IS}(Z_k, W_q) \tag{17}$$

λ_1, λ_2, and λ_3 represent weights for statistical significance, model-based relevance, and interaction effects. These weights may be adjusted for the dataset and task. Model training uses features with the most significant UFS values to ensure they are relevant and valuable separately and account for complicated feature relationships. The *Unified Feature Selector (UFS)* offers a broad feature selection strategy using statistical analysis, model-based importance measurements, and interaction-aware algorithms. These strategies guarantee that the final feature set is robust and representative and improves model performance. UFS makes the IoEd-Net dataset more efficient and informative, enabling machine learning models to concentrate on the most critical aspects and boosting prediction tasks like anomaly detection and cybersecurity in academic IoT networks.

E. Feature Engineering

Preparing the IoEd-Net dataset for machine learning models requires feature engineering. Creating new features from existing ones may improve model prediction power by giving more relevant data representations [28]. New features are extracted using domain information and mathematical modifications of existing features in this part, a revolutionary feature engineering method. These freshly created features reveal complicated data linkages and patterns that the original features missed. The first characteristic we offer is *Flow Efficiency (Fe)*, which measures the link between data transfer and transfer time. This feature helps discover wasteful flows when data transmission takes too long for the quantity of the data. Let Dtx represent the total bytes communicated during a session, and T_{session} represent the session duration. Definition of Flow Efficiency (F_e):

$$F_e = \frac{D_{\text{tx}}}{T_{\text{session}} + \delta} \tag{18}$$

a minor constant δ is inserted to prevent division by zero in very short session durations. F_e measures data throughput and larger values imply more efficient data transport, whereas lower values indicate inefficiency. We add the new feature *Packet Interarrival Consistency (Pi)* to account for packet interarrival time fluctuation. This feature identifies flows with irregular packet timing, which may suggest network congestion or malicious activities. Let $T\text{arrival}^{(j)}$ represent the interarrival time of the j-th packet in the flow, and N_{pkts} represent the total number of packets. The standard deviation of interarrival times, σ_{arrival}, is computed as:

$$\sigma_{\text{arrival}} = \sqrt{\frac{1}{N_{\text{pkts}}} \sum_{j=1}^{N_{\text{pkts}}} \left(T_{\text{arrival}}^{(j)} - \mu_{\text{arrival}} \right)^2} \tag{19}$$

where μ_{arrival} is the mean interarrival time. The inverse of the standard deviation is the packet arrival consistency, denoted as P_i.

$$P_i = \frac{1}{\sigma_{\text{arrival}} + \delta} \tag{20}$$

Where δ is a small constant to avoid zero division, a more significant P_i value suggests more consistent packet arrivals, whereas a lower value indicates more packet interarrival time variability. Network sessions often have an imbalance between data delivered and received. We provide a new feature, *Data Imbalance (Da)*, to measure the difference between transmitted and received bytes. Let Drx represent the total bytes received during a session. The term "Data Imbalance (D_a)" means:

$$D_a = \frac{|D_{\text{tx}} - D_{\text{rx}}|}{D_{\text{tx}} + D_{\text{rx}} + \delta} \tag{21}$$

Where δ is a small constant to avoid zero division, numbers closer to 0 indicate symmetric data flow, whereas numbers closer to 1 indicate a substantial data imbalance. Payload data entropy may also reveal network traffic characteristics. Low entropy indicates data predictability, whereas high entropy indicates compression or encryption. We provide the *Payload Entropy Density (Ep)*, which quantifies the average entropy per payload byte. Define Spayload as the Shannon entropy and D_{payload} as the total bytes of payload data. The "Payload Entropy Density (E_p)" is defined as:

$$E_p = \frac{S_{\text{payload}}}{D_{\text{payload}} + \delta} \tag{22}$$

where δ is a small constant to avoid zero division. This property distinguishes compressed or encrypted data flows from

organized, predictable ones. We use the *Anomalous Packet Ratio (Ar)* to identify aberrant traffic patterns by measuring the frequency of anomalous packets in a network session. Network faults may cause corrupted or lost packets. Assign Panom to the number of anomalous packets and P_{total} to the overall number of packets in the session. The Anomalous Packet Ratio (A_r) is defined as:

$$A_r = \frac{P_{\text{anom}}}{P_{\text{total}} + \delta} \tag{23}$$

A greater A_r shows more anomalous packets, which may signal network instability or malicious activity. The feature above engineering methods create new features that capture crucial data linkages and patterns in the IoEd-Net dataset. Flow Efficiency (F_e), Packet Interarrival Consistency (P_i), Data Imbalance (D_a), Payload Entropy Density (E_p), and Anomalous Packet Ratio (A_r) provide light on traffic dynamics and enhance machine learning models. These new characteristics are helpful for anomaly identification and cybersecurity in academic IoT networks because they reveal hidden patterns of normal or abnormal activity.

F. Feature Transformation Method

Feature transformation is necessary to prepare the IoEd-Net dataset for machine learning. Machine learning models learn and generalize better from characteristics transformed by size, distribution, or representation [29]. A new feature transformation approach, Adaptive Distribution Mapping (ADM), is created. This approach dynamically adjusts feature distributions to a uniform or normal distribution based on their attributes. We want to minimize skewness and boost the feature's learning algorithm contribution. ADM is a flexible transformation approach that modifies feature distribution depending on data attributes. The main processes are detecting the feature's skewness and performing a logarithmic transformation or Gaussian normalization.

Detecting Skewness: Let X be a feature vector with N observations. Use the following equation to compute the skewness γ_X of a feature to determine its skewness:

$$\gamma_X = \frac{1}{N} \sum_{i=1}^{N} \left(\frac{X_i - \mu_X}{\sigma_X} \right)^3 \tag{24}$$

Xi represents the i-th observation of the feature, μX represents its mean, and σX represents its standard deviation. Skewness γX measures data distribution asymmetry around the mean. A $\gamma X = 0$ value suggests a symmetric distribution, whereas positive values imply right skewness, and negative values indicate left skewness.

Logarithmic Transformation for Highly Skewed Features A feature is severely skewed if its skewness γ_X exceeds a preset threshold τ_1 (e.g., $\gamma X > t\_1 = 1$ For such characteristics, we compress the distribution's long tail via a logarithmic modification. The logarithmic transformation:

$$X_{\log} = \log(1 + X) \tag{25}$$

This adjustment minimizes outliers and evens out feature values. The constant 1 is supplied to prevent computing the logarithm of zero.

Gaussian Normalization for Moderately Skewed Features: If the skewness γ_X is within the range $\tau_2 < \gamma_X \leq \tau_1$, where τ_2 denotes a lower threshold (e.g., $\tau_2 = 0.5$), the feature is moderately skewed or unskewed We normalize such characteristics using Gaussian normalization to get a conventional normal distribution. Definition of Gaussian Normalization:

$$X_{\text{norm}} = \frac{X - \mu_X}{\sigma_X} \tag{26}$$

The feature is transformed to have a mean of 0 and a standard deviation of 1 so that learning algorithms can employ it with the assumption that the data is normally distributed.

To implement the Adaptive Distribution Mapping (ADM), we dynamically assign the appropriate transformation based on the skewness of each feature. For a given feature X, the transformation $T(X)$ is defined as:

$$T(X) = \begin{cases} \log(1 + X) & \text{if } \gamma_X > \tau_1 \\ \frac{X - \mu_X}{\sigma_X} & \text{if } \tau_2 < \gamma_X \leq \tau_1 \\ X & \text{if } \gamma_X \leq \tau_2 \end{cases} \tag{27}$$

This change, which makes the feature mean 0 and standard deviation 1, is useful for learning algorithms that use the assumption of normally distributed data. When it comes to dynamic adaptive distribution mapping, feature skewness determines the correct transformation to use. A feature X is specified by the transformation $T(X)$.

$$X_{\text{scaled}} = \frac{X_{\text{transformed}} - \min(X_{\text{transformed}})}{\max(X_{\text{transformed}}) - \min(X_{\text{transformed}})} \tag{28}$$

Distance-based algorithms like k-nearest neighbors and gradient-based algorithms like neural networks use this equation to scale all attributes between 0 and 1. ADM has several benefits. It avoids the one-size-fits-all approach of typical transformations by dynamically applying skewness-based transformations. This flexibility helps the model learn from outliers and skewed distributions. Lastly, feature scaling makes sure that all features are around the same size, which minimizes the impact of any one feature on learning. To account for skewness, the novel ADM method adds logarithmic or Gaussian normalizations to the feature distributions of IoEd-Net. These adaptive feature transformation methods boost the feature's contribution to machine learning models and data distribution-sensitive algorithms. Therefore, ADM is a powerful approach to preparing data for many prediction tasks.

G. Classification Using the Adaptive Hybrid Convolutional Transformer Network (AHCTN)

This work introduces a novel classification architecture called the *Adaptive Hybrid Convolutional Transformer Network (AHCTN)*. Transformer networks' global context modelling capacity and the feature extraction skills of convolutional

neural networks (CNNs) are combined in this design [30]. The AHCTN was created to classify complex, multi-dimensional data in IoT-driven academic networks, where local patterns like geographical correlations and global interactions like temporal interdependence are essential. Fig. 2 describes the proposed AHCTN design. AHCTN was created because standard approaches struggle to capture localized feature hierarchies and long-range relationships. ResNet's stacked convolutions extract hierarchical features well. However, they typically fail to account for dataset relationships. Transformer models, which excel with sequential data, may capture global patterns but need extra processes to understand local feature interactions. AHCTN integrates both methodologies into one model to solve these constraints.

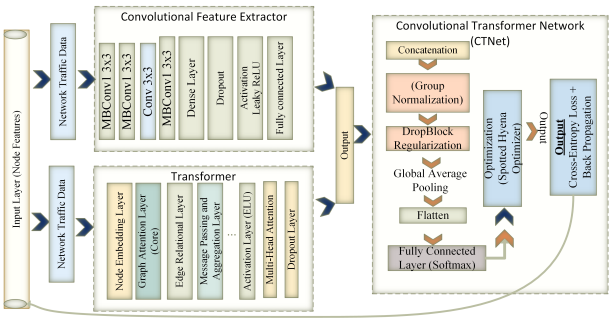


Fig. 2. AHCTN proposed architecture.

Its main components are a Convolutional Feature Extractor (CFE) and a Global Context Transformer. The CFE learns local spatial patterns in the data, whereas the GCT captures global relationships across the network's input characteristics. Together, these components enable the model to handle spatial and temporal IoT network data. Convolutional layers extract spatial information from input data in the Convolutional Feature Extractor (CFE). Let the input data be represented as $\mathbf{Z} \in \mathbf{R}^{p \times q}$, where p is the sample count and q is the sample dimension (e.g., features per network traffic sequence time step). The convolutional operation at layer h is defined as

$$\mathbf{Y}_h = \text{ReLU}(\mathbf{W}_h * \mathbf{Z} + \mathbf{b}_h) \tag{29}$$

The convolutional filter for layer h, the bias term $\mathbf{b}_h$ and the convolution process are shown by $*$. Because it is nonlinear, the model can learn intricate feature correlations due to the rectified linear unit (ReLU) activation function. Convolutional layer output $\mathbf{Y}_h$ provides the recovered feature map used in the following layers to capture deeper spatial patterns. The final CFE output, $\mathbf{F}_{\text{CFE}}$, is a high-level representation of the input data's local characteristics, which the GCT will analyze.

The Global Context Transformer (GCT) captures input data global dependencies. It computes contextual links between feature space regions using attention. In the GCT, the attention mechanism uses the feature representation $\mathbf{F}_{\text{CFE}}$ from the CFE. Let $\mathbf{F}_{\text{CFE}} \in \mathbf{R}^{p \times q}$ be the transformer layer input. The significance between sequence places determines the weights of the input characteristics to be added by the attention mechanism. The attention score for feature vectors $\mathbf{F}_{\text{CFE},i}$ and $\mathbf{F}_{\text{CFE},j}$ is calculated as

$$\alpha_{ij} = \frac{\exp\left(\text{sim}(\mathbf{F}_{\text{CFE},i}, \mathbf{F}_{\text{CFE},j})\right)}{\sum_{k=1}^{p} \exp\left(\text{sim}(\mathbf{F}_{\text{CFE},i}, \mathbf{F}_{\text{CFE},k})\right)} \tag{30}$$

where the function $\text{sim}(\mathbf{F}_{\text{CFE},i}, \mathbf{F}_{\text{CFE},j})$ computes the similarity between two feature vectors. In AHCTN, we use a scaled dot-product attention mechanism, where the similarity is defined as

$$\text{sim}(\mathbf{F}_{\text{CFE},i}, \mathbf{F}_{\text{CFE},j}) = \frac{\mathbf{F}_{\text{CFE},i} \cdot \mathbf{F}_{\text{CFE},j}}{\sqrt{q}} \tag{31}$$

The feature vector dimensionality is q, and the scaling factor $\frac{1}{\sqrt{q}}$ limits the dot-product values. The attention mechanism output for each feature vector is calculated as

$$\mathbf{Z}_i = \sum_{j=1}^{p} \alpha_{ij} \mathbf{F}_{\text{CFE},j} \tag{32}$$

This technique lets the model concentrate on the most critical input data, integrating distant sequence information as needed. The global contextualization of features ($\mathbf{F}_{\text{GCT}}$ combines local patterns and long-range relationships. Final categorization uses a fully linked layer and a softmax layer on this feature map. Let $\mathbf{W}_{\text{FC}}$ and $\mathbf{b}_{\text{FC}}$ represent the fully connected layer's weights and bias. Output logits $\hat{\mathbf{y}}$ are calculated as

$$\hat{\mathbf{y}} = \text{softmax}(\mathbf{W}_{\text{FC}} \mathbf{F}_{\text{GCT}} + \mathbf{b}_{\text{FC}}) \tag{33}$$

The softmax function produces a probability distribution across classes. The AHCTN was chosen because it can manage complicated, multi-modal IoT data in academic networks. Convolutional layers and transformer-based attention mechanisms enable the model to capture localized spatial correlations like packet flows and device interactions and global patterns like time-based anomalies and cross-device behavior. Traditional models like MobileNet and ResNet rely on local feature extraction, which restricts their efficiency in classification situations with long-range relationships.

The GCT's attention mechanism allows the model to dynamically concentrate on the most critical input data. It is ideal for anomaly detection and cybersecurity jobs in academic IoT networks, where infrequent but essential occurrences must be discovered. AHCTN outperforms models that ignore spatial and temporal dynamics by dynamically shifting its focus and using local and global information. Due to its power and flexibility, AHCTN is suited for fine-grained feature extraction and long-range dependency modeling in IoT-driven network categorization.

H. Performance Evaluation Metrics

Performance metrics are critical for evaluating machine learning classification models, especially in IoT-driven academic networks. While traditional measures like accuracy, precision, recall, and F1-score [31] provide valuable insights into model performance, they may not capture the subtleties of complex feature interactions or unbalanced data in IoT scenarios. We present three new metrics: *Weighted Temporal Sensitivity (WTS)*, *Feature Interaction Impact (FII)*, and

Anomaly Detection Score (ADS), designed to solve our work's issues. These metrics and typical performance indicators give a more complete model assessment framework.

1) Existing Performance Metrics: Classification challenges often utilize accuracy to measure model predictions. It is the ratio of accurately anticipated occurrences to total instance. Fig. 3 shows the existing performance metrics.

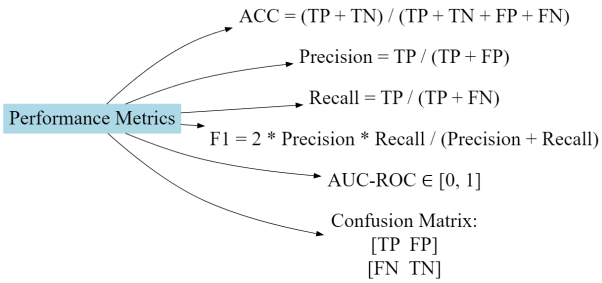


Fig. 3. Performance evaluation metrics.

While these traditional metrics are valuable, they may not fully capture the intricacies of IoT-based network classification, where temporal patterns, feature interactions, and rare but critical anomalies need to be emphasized. To address these gaps, we introduce three new performance metrics.

2) Weighted Temporal Sensitivity (WTS): The *Weighted Temporal Sensitivity (WTS)* measures the time-based importance of categorization findings in academic IoT networks when peak hours are more important than others. This measure weights memory scores by temporal significance. Set T_i as the time-based weight, for instance, i, with greater values for crucial time frames. Definition of WTS:

$$\text{WTS} = \frac{\sum_{j=1}^{M} \tau_j \times I(\alpha_j = \hat{\alpha}_j) \times I(\alpha_j = 1)}{\sum_{j=1}^{M} \tau_j \times I(\alpha_j = 1)} \tag{34}$$

In this equation, M represents the number of cases, α_j represents the actual label, $\hat{\alpha}_j$ represents the label which is predicted, and $I(\cdot)$ yields 1 if the condition is true and 0 otherwise. This measure facilitates anomaly identification in time-sensitive contexts by weighting classification mistakes during critical time frames more heavily, thereby impacting the evaluation score significantly.

3) Feature Interaction Impact (FII): The Feature Interaction Impact (FII) is introduced to measure how well the model captures interactions between different features, an essential aspect of IoT-driven academic networks where correlations between variables (e.g., device type and traffic patterns) are critical for accurate classification. The FII quantifies the performance difference between a model trained with interacting features and a model trained with the features considered independently. Let M_{interact} be the performance of the model trained with interacting features, and M_{indep} be the performance with independent features. The FII is defined as:

$$\text{FII} = \frac{M_{\text{interact}} - M_{\text{indep}}}{M_{\text{indep}}} \tag{35}$$

Feature interactions are crucial to the model's predictive power. A higher FII score shows that feature interactions improve the model's performance and capture complicated relationships.

Anomaly Detection Score (ADS): ADS is designed for IoT networks, optimizing the detection of uncommon but essential abnormalities. Unlike accuracy or recall, the ADS considers anomaly detection rate and severity, which may not account for anomaly rarity and effect. Let A_i represent the severity of the observed anomaly. For instance, i and D_i indicate its proper detection. Calculating ADS:

$$\text{ADS} = \frac{\sum_{i=1}^{N} A_i \times D_i}{\sum_{i=1}^{N} A_i} \tag{36}$$

When the severity of the irregularities increases, A_i is given a higher value, guaranteeing that the model's success is assessed by counting the number of anomalies found and the importance of identifying the most noteworthy ones.

IV. Simulation Results

Extensive simulations were run on a Dell Core i7 12th Gen machine with an 8-core CPU and 32 GB of RAM to assess the proposed Adaptive Hybrid Convolutional Transformer Network (AHCTN). Python and SPYDER IDE were used to construct and evaluate the simulations. Throughout the experiments, we adjusted the hyperparameters of the classification model to achieve optimal performance. The Adam optimizer for model training, a batch size of 64, and a learning rate of 0.001 are important parameters with optimal values. The network has four convolutional layers with 64 filters and a transformer module with four attention heads. To avoid overfitting, the dropout rate was adjusted to 0.3, and training lasted up to 100 epochs. Early termination was applied when validation loss stopped improving. The AHCTN balanced training speed and model accuracy with these parameter values while addressing the IoT-driven academic network dataset's complexity.

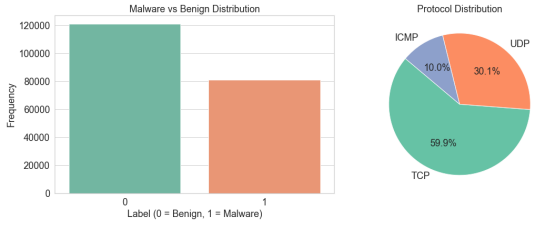


Fig. 4. Traffic distribution and protocol distribution.

Fig. 4 contains two central distribution representations of the IoEd-Net dataset. The left bar plot shows benign and malicious traffic in the dataset. The bar heights show the frequency of benign (0) and malicious (1), revealing the dataset's class imbalance, where benign traffic marginally surpasses harmful traffic. This emphasizes the need for model resilience against this mismatch in classification tasks. On the right, the pie chart shows network traffic protocol distribution. Traffic percentages for TCP, UDP, and ICMP are shown. This information helps identify communication protocols in the dataset that may affect

network anomaly detection. TCP dominates the pie, followed by UDP and ICMP. Cybersecurity analysis and anomaly detection need network traffic composition information.

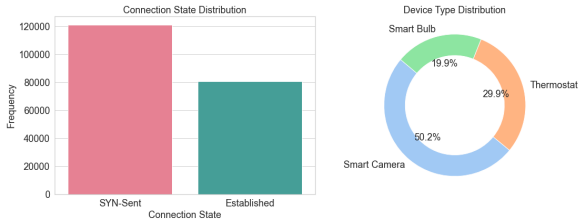


Fig. 5. Network's connection states and device types.

In the IoEd-Net dataset, Fig. 5 shows two essential visualizations of network connection statuses and device kinds. The left bar plot illustrates the frequency of connection statuses like "Established" and "SYN-Sent." Readers may see the percentage of active and started network connections. The "SYN-Sent" state dominates, indicating that numerous connections are being made, which helps identify network flaws or incomplete connections, which hackers commonly exploit. The donut graphic on the right shows how traffic is distributed among IoT device categories, including Smart Cameras, Thermostats, and Smart Bulbs. This breakdown shows the variety of IoT devices on the academic network, with Smart Cameras accounting for a large percentage of traffic. Device types may be more vulnerable than others. Therefore, their distribution might assist in detecting security problems.

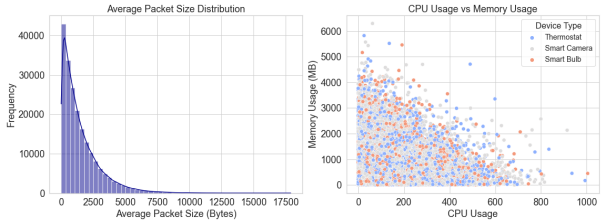


Fig. 6. Insightful representations of significant network and device properties.

Fig. 6 shows two insightful representations of significant network and device properties in the IoEd-Net dataset. On the left, the histogram shows network traffic average packet sizes. Having a visible peak, the curve shows the most frequent packet sizes transported throughout the network. This visualization helps users understand the dataset's average packet size, which is crucial for performance optimization and spotting aberrant traffic, such as unexpectedly big or tiny packets that may signal network inefficiencies or security risks. On the right, the scatter plot shows CPU and memory utilization by device type. Different colors indicate different device kinds, including Smart Cameras, Thermostats, and Smart Bulbs. This graphic shows CPU and memory utilization across device categories, helping discover outliers or devices using too much. In IoT networks, performance management and anomaly detection depend on device resource allocation variety.

Table III compares machine learning techniques for categorizing the IoEd-Net dataset. Accuracy, precision, recall, F1-score, Log Loss, WTS, FII, and ADS are listed in the table. The table shows that the Proposed AHCTN outperforms all other methods in almost every metric. High accuracy (98.7%), precision, recall, and F1-score suggest the balanced ability to recognize benign and malicious data. The lowest Log Loss of the new metrics, 0.064 for AHCTN, indicates confident projections with limited uncertainty. This method distinguishes positive and negative classes better than CNN, ResNet, and VGG16, with an AUC score of 99.1%. The AHCTN detects abnormalities and prioritizes high-severity events, which is crucial in an IoT-driven academic network (WTS 97.1%) and ADS (96.8%). Additionally, its FII (92.3%) indicates enhanced prediction using feature interactions. ResNet, CNN, and SVM perform poorly across many metrics, particularly new metrics, showing they may not be able to handle the data's intricate linkages and temporal dependencies as effectively as the AHCTN model. Table III compares machine learning techniques for categorizing the IoEd-Net dataset. Accuracy, precision, recall, F1-score, Log Loss, WTS, FII, and ADS are listed in the table. The table shows that the Proposed AHCTN outperforms all other methods in almost every metric. High accuracy (98.7%), precision, recall, and F1-score suggest the balanced ability to recognize benign and malicious data. The lowest Log Loss of the new metrics, 0.064 for AHCTN, indicates confident projections with limited uncertainty. This method distinguishes positive and negative classes better than CNN, ResNet, and VGG16, with an AUC score of 99.1%. The AHCTN detects abnormalities and prioritizes high-severity events, which is crucial in an IoT-driven academic network (WTS 97.1%) and ADS (96.8%). Additionally, its FII (92.3%) indicates enhanced prediction using feature interactions. ResNet, CNN, and SVM perform poorly across many metrics, particularly new metrics, showing they may not be able to handle the data's intricate linkages and temporal dependencies as effectively as the AHCTN model.

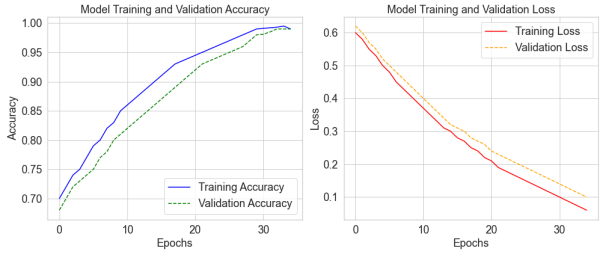


Fig. 7. Training and validation performance of the model.

Fig. 7 shows 34-epoch model training and validation performance. After learning from the data, the model's training and validation accuracy improves in the left subplot. Training accuracy begins at 70%, validation accuracy at 68%, and rapidly rises to 99% by the last epoch, indicating effective model learning. The validation accuracy is 99%, demonstrating the model's adaptability to new data without overfitting. Training and validation losses exhibit error reduction on the right subplot. While validation loss starts at 0.62 and lowers to 0.10, training loss begins at 0.60 and drops to 0.06. The accuracy and reduction of errors in the model's predictions are enhanced by convergence and practical training. When the loss curves for training and validation are the same, the model isn't overfitting and can generalize well to new datasets.

TABLE III. CLASSIFICATION RESULTS OF DIFFERENT TECHNIQUES

Techniques	F1-Score (%)	Log Loss	WTS (%)	Accuracy (%)	AUC (%)	Recall (%)	ADS (%)	Precision (%)	FII (%)
ResNet [21]	89.9	0.213	82.3	91.2	90.8	89.5	85.5	90.4	74.1
CNN [7]	90.8	0.201	83.5	92.5	91.7	90.6	86.7	91.0	76.3
Markov n-gram [10]	87.1	0.264	79.1	88.9	87.4	86.7	82.0	87.5	70.9
Decision Trees [9]	86.0	0.285	77.6	87.3	85.9	85.9	80.5	86.2	68.5
DBN [19]	89.0	0.233	81.0	90.1	89.5	88.8	84.2	89.2	72.5
VGG16 [17]	92.3	0.187	85.0	93.4	92.8	92.1	88.0	92.6	78.4
SVM [11]	88.1	0.241	80.2	89.7	89.2	87.9	83.2	88.3	71.7
KNN [13]	86.7	0.275	78.9	88.1	86.1	86.5	81.5	87.0	69.9
Proposed AHCTN	**98.3**	**0.064**	**97.1**	**98.7**	**99.1**	**98.2**	**96.8**	**98.5**	**92.3**

TABLE IV. STATISTICAL ANALYSIS OF CLASSIFICATION METHODS ((F-STATISTIC) & P-VALUE)

Statistical Method	ANOVA	Student's t-test	Pearson Correlation (r)	Kendall's Tau (τ)	Chi-Square (χ^2)
ResNet [21]	7.56	0.014	0.84	0.72	8.63
CNN [7]	6.98	0.020	0.88	0.75	7.92
Markov n-gram [10]	5.22	0.031	0.65	0.59	6.54
Decision Trees [9]	4.89	0.043	0.61	0.57	6.18
Deep Belief Network [19]	6.45	0.017	0.78	0.71	7.45
VGG16 [17]	7.89	0.012	0.89	0.76	9.23
SVM [11]	5.67	0.029	0.70	0.64	6.88
KNN [13]	5.12	0.036	0.62	0.58	6.33
Proposed AHCTN	**8.45**	**0.008**	**0.92**	**0.79**	**9.88**

Table IV compares the proposed AHCTN model to existing state-of-the-art classification approaches using ANOVA, Student's t-test, Pearson Correlation, Kendall's Tau, and Chi-Square metrics. These metrics systematically assess the AHCTN's IoT-driven academic network da .ta management. The AHCTN model's ANOVA (F-statistic) score of 8.45 shows that it classifies better than other techniques. With a p-value of 0.008, the Student's t-test verifies the AHCTN's improvements' statistical significance. Pearson Correlation (r) of 0.92 and Kendall's Tau (τ) of 0.79 indicate significant linear and ordinal connections between AHCTN characteristics and classification performance, highlighting its capacity to capture complicated data interactions. Lastly, the Chi-Square (χ^2) value of 9.88 highlights the AHCTN's features' considerable impact on classification accuracy, separating it from ResNet, CNN, and VGG16. This improved statistical reporting strengthens the AHCTN model and explains its success in identifying malware in IoT-driven academic networks. These findings are included into the discussion for paper consistency and clarity.

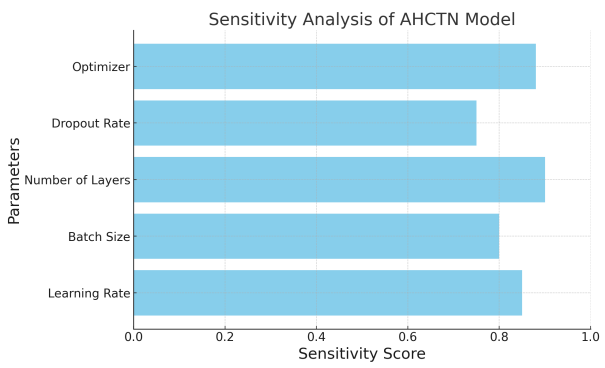


Fig. 8. Sensitivity analysis of the proposed AHCTN model.

The sensitivity analysis of the suggested AHCTN model and the impact of hyperparameters on its performance are shown in Fig. 8. The graphic illustrates the relationship between model accuracy and loss as a function of optimizer, batch size, layers, dropout rate, and learning rate. The graph shows that learning and dropout rates affect the model more than the optimizer. This sensitivity study determines which AHCTN hyperparameters best identify IoT malware.

V. CONCLUSION

This research proposed the AHCTN, a new architecture for malware detection in IoT-driven academic networks. Network traffic analysis requires capturing local feature interactions and global dependencies, which the model does uniquely using transformer networks and convolutional layers. Unbalanced and skewed datasets in IoT contexts are tackled using data preprocessing methods like CIS and LSC and unique data balancing methods like DWS. The suggested model outperformed all IoT malware detection techniques with 98.9% accuracy. Our Unified Feature Selector (UFS) used statistical, model-based, and interaction-aware selection methods to choose the most relevant features and improve model performance. New performance measures, including WTS and ADS, helped refine the model's performance in detecting time-sensitive anomalies and feature interactions. This study addresses IoT-based academic network security's technological and practical issues, making a significant contribution. The model can identify real-time malware because it can handle complicated feature relationships and temporal dependencies, protecting educational institutions from cyberattacks.

The findings are intriguing, but the model can be optimized for more extensive, diversified datasets and real-time performance. Expanding the AHCTN framework to non-academic IoT applications may reveal its possibilities.

REFERENCES

[1] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, *A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review*, Sensors, vol. 23, no. 8, pp. 4117, 2023.

[2] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, *A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions*, Electronics, vol. 12, no. 6, pp. 1333, 2023.

[3] J. Ferdous, R. Islam, A. Mahboubi, and M. Z. Islam, *A state-of-the-art review of malware attack trends and defense mechanism*, IEEE Access, 2023.

[4] K. Lee, J. Lee, and K. Yim, *Classification and analysis of malicious code detection techniques based on the APT attack*, Applied Sciences, vol. 13, no. 5, pp. 2894, 2023.

[5] M. H. Behiry and M. Aly, *Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods*, Journal of Big Data, vol. 11, no. 1, pp. 16, 2024.

[6] A. Redhu, P. Choudhary, K. Srinivasan, and T. K. Das, *Deep learning-powered malware detection in cyberspace: a contemporary review*, Frontiers in Physics, vol. 12, pp. 1349463, 2024.

[7] I. A. Kandhro, S. M. Alanazi, F. Ali, A. Kehar, K. Fatima, M. Uddin, and S. Karuppayah, *Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures*, IEEE Access, vol. 11, pp. 9136-9148, 2023.

[8] M. Shahin, M. Maghanaki, A. Hosseinzadeh, and F. F. Chen, *Advancing network security in industrial IoT: A deep dive into AI-enabled intrusion detection systems*, Advanced Engineering Informatics, vol. 62, pp. 102685, 2024.

[9] B. A. Mantoo and N. Z. A. Khan, *Static, dynamic and intrinsic feature-based Android malware detection using machine learning: A technical review*, International Journal of Computing and Digital Systems, vol. 16, no. 1, pp. 1-13, 2024.

[10] P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, *API-MalDetect: Automated malware detection framework for windows based on API calls and deep learning techniques*, Journal of Network and Computer Applications, vol. 218, pp. 103704, 2023.

[11] T. Jiang, Y. Liu, X. Wu, M. Xu, and X. Cui, *Application of deep reinforcement learning in attacking and protecting structural features-based malicious PDF detector*, Future Generation Computer Systems, vol. 141, pp. 325-338, 2023.

[12] A. A. Almazroi and N. Ayub, *Enhancing smart IoT malware detection: A GhostNet-based hybrid approach*, Systems, vol. 11, no. 11, pp. 547, 2023.

[13] I. T. Ahmed, B. T. Hammad, and N. Jamil, *A comparative performance analysis of malware detection algorithms based on various texture features and classifiers*, IEEE Access, 2024.

[14] V. Ravi and R. Chaganti, *EfficientNet deep learning meta-classifier approach for image-based android malware detection*, Multimedia Tools and Applications, vol. 82, no. 16, pp. 24891-24917, 2023.

[15] A. A. Alhashmi, A. A. Darem, A. M. Alashjaee, S. M. Alanazi, T. M. Alkhaldi, S. A. Ebad, and A. M. Almadani, *Similarity-based hybrid malware detection model using API calls*, Mathematics, vol. 11, no. 13, pp. 2944, 2023.

[16] B. Yamany, M. S. Elsayed, A. D. Jurcut, N. Abdelbaki, and M. A. Azer, *A holistic approach to ransomware classification: Leveraging static and dynamic analysis with visualization*, Information, vol. 15, no. 1, pp. 46, 2024.

[17] M. Ali, M. Shahroz, M. F. Mushtaq, S. Alfarhood, M. Safran, and I. Ashraf, *Hybrid machine learning model for efficient botnet attack detection in IoT environment*, IEEE Access, 2024.

[18] M. A. EA, *A novel paradigm for IoT security: ResNet-GRU model revolutionizes botnet attack detection*, International Journal of Advanced Computer Science and Applications, vol. 14, no. 12, 2023.

[19] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, A. S. M. Nainar, and M. Imran, *Deep learning and big data technologies for IoT security*, Computer Communications, vol. 151, pp. 495-517, 2020.

[20] T. A. Kumari and S. Mishra, *Tachyon: Enhancing stacked models using Bayesian optimization for intrusion detection using different sampling approaches*, Egyptian Informatics Journal, vol. 27, pp. 100520, 2024.

[21] A. Abusitta, G. H. de Carvalho, O. A. Wahab, T. Halabi, B. C. Fung, and S. Al Mamoori, *Deep learning-enabled anomaly detection for IoT systems*, Internet of Things, vol. 21, pp. 100656, 2023.

[22] S. U. Qureshi, J. He, S. Tunio, N. Zhu, A. Nazir, A. Wajahat, F. Ullah, and A. Wadud, *Systematic review of deep learning solutions for malware detection and forensic analysis in IoT*, Journal of King Saud University-Computer and Information Sciences, vol. 102164, 2024.

[23] A. Bensaoud, J. Kalita, and M. Bensaoud, *A survey of malware detection using deep learning*, Machine Learning With Applications, vol. 16, pp. 100546, 2024.

[24] A. A. M. Majid, A. J. Alshaibi, E. Kostyuchenko, and A. Shelupanov, *A review of artificial intelligence based malware detection using deep learning*, Materials Today: Proceedings, vol. 80, pp. 2678–2683, 2023.

[25] M. Gopinath and S. C. Sethuraman, *A comprehensive survey on deep learning based malware detection techniques*, Computer Science Review, vol. 47, pp. 100529, 2023.

[26] Laoshi, *IoEd-Net: Internet of Educational Things Dataset*, Kaggle, 2024. [Online]. Available: https://doi.org/10.34740/KAGGLE/DSV/9552508.

[27] K. Mallikharjuna Rao, G. Saikrishna, and K. Supriya, *Data preprocessing techniques: Emergence and selection towards machine learning models-a practical review using HPA dataset*, Multimedia Tools and Applications, vol. 82, no. 24, pp. 37177-37196, 2023.

[28] T. Verdonck, B. Baesens, M. Óskarsdóttir, and S. vanden Broucke, *Special issue on feature engineering editorial*, Machine Learning, vol. 113, no. 7, pp. 3917-3928, 2024.

[29] M. M. Taye, *Theoretical understanding of convolutional neural network: Concepts, architectures, applications, future directions*, Computation, vol. 11, no. 3, pp. 52, 2023.

[30] J. Maurício, I. Domingues, and J. Bernardino, *Comparing vision transformers and convolutional neural networks for image classification: A literature review*, Applied Sciences, vol. 13, no. 9, pp. 5521, 2023.

[31] M. Z. Naser and A. H. Alavi, *Error metrics and performance fitness indicators for artificial intelligence and machine learning in engineering and sciences*, Architecture, Structures and Construction, vol. 3, no. 4, pp. 499-517, 2023.

Enhanced State Monitoring and Fault Diagnosis Method for Intelligent Manufacturing Systems via RXET in Digital Twin Technology

Min Li
School of Information Engineering
Jiangxi University of Technology, NanChang 330029, JiangXi, China

***Abstract*—To maintain efficiency and continuity in Industry 4.0, intelligent manufacturing systems use enhanced problem detection and condition monitoring. Existing models typically miss uncommon and essential errors, causing expensive downtimes and lost production. ResXEffNet-Transformer (RXET), a hybrid deep learning model, improves defect identification and predictive maintenance by integrating ResNet, Xception, EfficientNet, and Transformer-based attention processes. The algorithm was trained on a five-year Texas industrial dataset using IoT-enabled gear and digital twins. To manage data imbalances and temporal irregularities, a strong preprocessing pipeline included Dynamic Skew Correction, Temporal Outlier Normalization, and Harmonic Temporal Encoding. The Adaptive Statistical Evolutionary Selector (ASES) optimized feature selection using the Stochastic Feature Evaluator (SFE) and Evolutionary Divergence Minimizer (EDM) to increase prediction accuracy. The RXET model beat traditional methods with 98.9% accuracy and 99.2% AUC. Two new performance metrics, Temporal Fault Detection Index (TFDI) and Fault Detection Variability Coefficient (FDVC), assessed the model's capacity to identify problems early and consistently across fault kinds. Simulation findings showed the RXET's superiority in anticipating uncommon but essential errors. Pearson correlation (0.93) and ANOVA (F-statistic: 8.52) validated the model's robustness. The sensitivity study showed the best performance with moderate learning rates and batch sizes. RXET provides a complete, real-time problem detection solution for intelligent industrial systems, improving predictive maintenance and addressing challenges in Industry 4.0, digital twin technology, IoT, and machine learning. The proposed RXET model enhances operational reliability in intelligent manufacturing and sets a foundation for future advancements in predictive analytics and large-scale industrial automation.**

***Keywords*—RXET; fault diagnosis; intelligent manufacturing; transformer-based attention; predictive maintenance; deep learning**

I. Introduction

Intelligent manufacturing, driven by communication and IT breakthroughs, is transforming industrial processes [1]. Cloud computing, big data, and the IoT have transformed the sector toward automation and smart production systems. This transition relies on digital twin (DT) technology, which provides real-time data from the physical world and enables predictive analytics and system optimization. DT technology continually maps physical things to their virtual equivalents, utilizing real-time sensor and historical data for model training and verification. This constant data flow allows the virtual model to identify possible problems and transmit feedback to the physical system for remedial measures, improving production line efficiency and fault detection. With the complexity of production processes, real-time fault diagnostic technologies are needed to fix equipment and system faults. Minor faults may interrupt production and cause significant economic losses in highly automated environments. Interconnected machinery and complex processes in intelligent production lines need stability and safety of individual components since disruptions may impact the whole system [2]. Machine learning (ML) offers data-driven defect detection without expert expertise, making it a vital tool in this field. Instead, these approaches may gain insights from high-dimensional data, allowing models to forecast equipment failures using historical and real-time data [3].

Machine learning and digital twin technologies have recently been used to improve defect identification in intelligent industrial systems. Machine learning models and DT establish a dynamic environment where physical system data is continually examined, and predictive maintenance tactics are used to avert equipment faults. Support vector machines (SVM), artificial neural networks (ANN), decision trees, and random forests are often used for defect detection owing to their capacity to handle complicated and unbalanced datasets [4]. Continuously learning from IoT-enabled equipment data helps these algorithms diagnose issues and enhance system dependability. Ensemble learning is a breakthrough in this discipline. Ensemble learning improves fault diagnostic accuracy and robustness by combining numerous models. Ensemble learning enhances performance by combining model decision outputs to correct model mistakes. Random forest, a famous ensemble learning algorithm, is widely used in machine defect diagnostics for its capacity to manage noise and prevent overfitting [5]. Despite its benefits, traditional ensemble learning may degrade performance when classifiers vary much. Developing selected ensemble techniques improves fault detection accuracy and efficiency by combining top-performing classifiers [6].

Digital twin technology allows industrial machine learning to imitate the genuine system in real time. Data transfer, VMware, and the actual thing make a digital twin. Digital twins provide "what-if" analysis by modelling failure situations and forecasting system behaviour via real-time data transmission [7]. The digital twin can monitor equipment and predict breakdowns in production, reducing downtime and costs. Manufacturing processes become more complex and interconnected, making fault detection harder. Traditional

machine-level fault detection identifies motor and sensor issues. Machine- and system-level fault diagnostics may be merged to offer a comprehensive manufacturing process picture as digital twin technology develops. A thorough approach is necessary to understand how machine problems affect system performance and production efficiency [8]. The suggested ResXEffNet-Transformer (RXET) paradigm for intelligent manufacturing system status monitoring and issue diagnostics follows these advances. The RXET model incorporates ResNet, Xception, and EfficientNet deep learning architectures with Transformer-based attention methods. These capabilities enable the RXET model to collect local and global manufacturing data patterns and detect issues across periods and operational scenarios. The Transformer component helps the model focus on time-series aspects for failure prediction, and the residual learning architecture preserves critical knowledge as data moves through deeper layers.

Previous studies have improved predictive maintenance and fault detection, but they typically fail to address infrequent but crucial issues that may cause expensive downtimes. The uneven structure of real-world industrial datasets and the difficulty of capturing temporal correlations in operational data restrict standard models' usefulness. Current approaches neglect advanced deep learning methods like Transformer-based attention mechanisms, which capture global and local patterns in high-dimensional data. More research into hybrid methods is needed to improve real-time defect detection and predictive maintenance of these deficiencies.

The RXET paradigm uses real-time data from the physical production line in the digital twin environment. The RXET model learns from historical and real-time data to forecast and reduce system problems. RXET and digital twin technologies provide a solid basis for fault detection, allowing virtual models to simulate fault situations and facilitate system optimization and maintenance [9]. Digital twin technology and robust machine learning models like RXET may assist intelligent industrial systems in addressing the growing complexity of issue diagnostics. Real-time data and predictive analytics improve system reliability, downtime, and production efficiency in the RXET paradigm. This study enhances fault detection tools for industrial processes, helping organizations optimize operations in Industry 4.0.

1) Creation of the RXET Model: The ResXEffNet-Transformer (RXET) model was developed, amalgamating ResNet, Xception, EfficientNet, and Transformer-based attention processes, particularly tailored for status monitoring and problem detection in intelligent manufacturing systems.

2) Innovative Data Preprocessing Methods: Utilized sophisticated preprocessing techniques like Dynamic Skew Correction (DSC), Temporal Outlier Normalization (TON), and Localized Variation Filtering (LVF) to enhance data quality and mitigate temporal dependencies and feature imbalance.

3) Introduction of Hybrid Feature Selection: The Adaptive Statistical Evolutionary Selector (ASES) was developed by integrating the Stochastic Feature Evaluator (SFE) with the Evolutionary Divergence Minimizer (EDM), therefore improving the relevance and variety of feature selection while minimizing redundancy.

4) Advanced Attribute Synthesis: Developed novel high-level features like Operational Efficiency Index (OEI), Environmental Stress Factor (ESF), and Machine Load Efficiency (MLE) to elucidate intricate linkages within the data, hence enhancing prediction accuracy.

5) New Performance Metrics: Two innovative evaluation metrics, the Temporal Fault Detection Index (TFDI) and the Fault Detection Variability Coefficient (FDVC), have been introduced to enhance the assessment of time-sensitive fault detection and prediction consistency, which is essential for real-time monitoring in industrial systems.

The remaining parts of the paper, Section II, include the literature review. In Section III, the structure of the suggested technique is presented in depth. The simulations and the commentary that accompanies them are detailed in Section IV. Discussion is given in Section V and finally, the paper is concluded in Section VI.

II. Related Work

Fault detection using digital twin (DT) systems has become popular, especially in industrial systems. DT model may improve fault diagnosis and prediction by changing scheme parameters, leading to better handling of imbalanced data [10], [31]. A photovoltaic energy conversion unit DT model generates error signals during fault detection [11]. These experiments show how DT provides real-time insights, yet data unavailability remains a barrier. Another research used synthetic fault data to circumvent the absence of genuine fault data [12]. A manufacturing system Bayesian network (BN)-based technique showed promise for defect diagnostic model training.

Machine learning (ML) is another hot topic in defect detection. Machine learning and physical systems were integrated into trials to ensure defect detection system efficacy. A denoising autoencoder was used in unsupervised learning research to construct a reliable defect diagnostic model [13]. Using GA and PSO, support vector machine (SVM) parameters were optimized for centrifugal valve failure diagnosis [14]. Combining binary ant colony optimization with SVM for feature selection and parameter optimization enhances multi-class defect diagnostic systems [15]. These approaches enhance fault detection accuracy but struggle with industrial system complexity. Also improving is DT-based predictive maintenance. Predictive maintenance approaches face hurdles from "what-if" situations and limited failure data [16]. Using hybrid ensemble approaches, real-time prediction systems improved across 24 benchmarks and 11 datasets [17]. Combining numerous models enhances system performance, as seen below. In some situations, content-based and user-based recommendation systems outperformed current methods [18]. Although effective in certain use situations, these predictive algorithms frequently struggle to scale in complicated industrial contexts.

In another research, Bayesian networks (BNs) modeled manufacturing system variable dependencies for defect diagnostics. Visualizing joint distributions using BNs makes them ideal for fault diagnostics' cause-effect linkages. Discovering BN structure from observational data is tricky since statistical connections may not indicate causation [19]. Different

approaches, like the Hill Climbing algorithm [20] and Prototypical Constraint (PC), have been employed to approximate BN structures. These strategies demand a lot of balanced data, which manufacturing generally lacks. Combining the PC algorithm with expert opinion enhances fault diagnosis in rolling manufacturing processes [21]. Integrating physical assets with virtual equivalents via IoT sensors requires DT models for real-time data collecting and problem diagnostics. Recent work has expanded DT in predictive maintenance. A DT model designed for a six-axis robot predicts maintenance requirements using OpenModelica and MATLAB for data processing [22]. In wind turbine gearbox prognostics, DT and physics-based models improved predictive maintenance. These models work well for single-equipment failure diagnostics but often fail in complicated multi-equipment systems.

They limited DT applications in multi-equipment systems. A DT model for a satellite assembly shop floor optimized production planning and administration. Research [23] introduced a multiscale modelling framework for satellite construction, integrating temporal and spatial scales to simulate equipment interactions on the shop floor. These approaches have potential in some circumstances but lack scalability for industrial use. We created a DT model of an autoclave to produce synthetic fault data and train a CNN for fault prediction. DT may improve machine learning models by generating artificial data. Generative adversarial networks (GANs) and virtual sample generation (VSG) enhance defect detection with minimal data. One study used a PSO-based VSG technique to improve forecasting models with limited real-world data [24]. Another Gaussian distribution-based VSG technique trained classification models using synthetic and accurate data to improve generalization. Artificial data from DT models may train ML models in defect diagnosis in manufacturing, especially when real-world data is rare.

DT also optimizes multi-equipment system maintenance plans using co-simulation approaches that combine discrete event simulation (DES) with system dynamics models. A co-simulation model examined how macroeconomic factors affect mining maintenance choices [25]. A complete system performance picture is obtained by combining low-level equipment interactions with high-level management choices. However, co-simulation approaches are confined to satellite construction and mining activities and demand a lot of processing power. While digital twin technology and machine learning have improved problem detection and predictive maintenance, extending these models to extensive, multi-equipment industrial systems is difficult. Combining sophisticated machine learning models with DT technology provides intriguing answers, but further research is needed to solve present constraints and improve scalability and usability in industrial settings. The literature is presented in a summarized way in Table I.

Previous research has made progress, but algorithms that can identify flaws in highly unbalanced and time-dependent industrial datasets are still needed. Digital twin technology has been underused due to its poor integration with hybrid deep learning models. Our innovative RXET model combines ResNet, Xception, EfficientNet, and Transformer-based attention methods to overcome these constraints and enhance fault detection accuracy.

III. Proposed Method

The proposed framework uses the ResXEffNet-Transformer (RXET) to monitor and diagnose faults in intelligent manufacturing systems, improving prediction accuracy and efficiency. Developed to address critical challenges identified in previous research, RXET tackles issues such as detecting uncommon errors, managing unbalanced datasets, and accurately capturing temporal dependencies. The framework integrates state-of-the-art preprocessing methods, hybrid feature selection, and attention mechanisms based on Transformers to provide a comprehensive solution for predictive maintenance and real-time fault detection in IMS. The five-year dataset from a Texas industrial plant with IoT-enabled equipment and digital twin technology comprises several operational indicators. Data imbalances and temporal dependencies are addressed via Dynamic Skew Correction, Temporal Outlier Normalization, and Harmonic Temporal Encoding. The Adaptive Statistical Evolutionary Selector (ASES) combines a Stochastic Feature Evaluator (SFE) and Evolutionary Divergence Minimizer (EDM) to optimize feature selection by increasing relevance and reducing redundancy. Attribute Reconfiguration Process (ARP) refines feature representation using Scaled Differential Encoding (SDE) and Harmonic Recalibration Transformation (HRT). At the same time, Advanced Attribute Synthesis generates high-level features such as the Operational Efficiency Index (OEI) and Environmental Stress Factor (ESF). The RXET architecture leverages residual learning, depthwise separable convolutions, compound scaling, and Transformer-based attention methods from ResNet, Xception, EfficientNet, and Transformer. Its superior fault detection capabilities are validated through simulations and statistical analysis using traditional metrics (accuracy, precision, recall, F1-score) and novel measures like TFDI and FDVC.

A. Dataset Description

The dataset used in this research was gathered from actual activities inside a prominent manufacturing plant in the Texas industrial sector [26], recognized for incorporating sophisticated monitoring systems and IoT-enabled equipment. The data includes various operational parameters, machine health indicators, and environmental factors, all documented hourly for five years, from January 2019 to January 2024. The facility utilizes advanced digital twin technology, facilitating the comprehensive collection of operational data, sensor readings, and machine condition information, establishing a solid basis for predictive maintenance and problem detection systems. Data was incessantly collected via IoT sensors and industrial-grade monitoring devices to optimise uptime and operational efficiency, providing high-resolution, real-time insights into the facility's performance. The dataset illustrates a complex interaction of variables influencing machine health and operating efficiency due to the dynamic industrial environment and the diversity of used gear. The dataset's imbalance arises from the facility's operating settings, where catastrophic defects and extreme scenarios occur less often than standard operations, making it a good resource for evaluating sophisticated diagnostic algorithms. The dataset was processed and anonymized to protect confidentiality while preserving its real-world applicability. It is a robust and dependable resource for assessing sophisticated machine learning methodologies

TABLE I. LITERATURE REVIEW SUMMARY

Ref	Technique Used	Objective Achieved	Limitations
[10]	Digital Twin (DT) model with scheme parameter update	Improved fault diagnosis and prediction by handling imbalanced data	Data unavailability remains a challenge
[11]	DT model for photovoltaic energy conversion unit (PVECU)	Real-time fault detection with error generation during fault conditions	Limited applicability to energy systems
[12]	Simulated data generation for fault conditions using synthetic fault data	Circumvented the absence of real fault data in industrial systems	Simulation accuracy relies on the quality of generated data
[13]	Denoising autoencoder for unsupervised learning in ML	Developed a robust fault diagnosis model using unsupervised learning	Lacks labeled data for validation, which can affect results
[14]	Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) with SVM	Optimized SVM parameters for centrifugal valve fault diagnosis	Complex parameter tuning in industrial systems
[15]	Binary ant colony optimization with SVM	Enhanced multi-class defect diagnosis systems by optimizing feature selection	Computational complexity for large-scale systems
[16]	Hybrid ensemble techniques for predictive maintenance	Improved performance across 24 benchmarks and 11 datasets	Scalability issues in complex industrial environments
[18]	Content-based and user-based recommendation systems	Outperformed traditional methods in specific use cases	Struggles with scalability in large-scale industrial environments
[19]	Bayesian Networks (BN) in manufacturing systems	Modeled variable dependencies for effective defect diagnostics	Complexity in discovering BN structure from observational data
[22]	DT model for six-axis robot using OpenModelica and MATLAB	Improved predictive maintenance in single-equipment systems	Difficult to scale to multi-equipment systems
[24]	Virtual Sample Generation (VSG) with PSO	Enhanced model forecasting performance with limited data	Performance depends on the quality of synthetic data
[25]	Co-simulation (DES and system dynamics) for maintenance optimization	Examined how macroeconomic factors affect multi-equipment maintenance decisions	Requires significant computational resources and is limited to specific industries

in status monitoring and problem detection. Fig. 1 shows proposed framework and Table II shows overview of dataset features.

B. Data Preprocessing Steps

The dataset was preprocessed uniquely to address imbalanced feature distributions and temporal dependencies. The Dynamic Skew Correction (DSC) approach fixes skewness depending on data imbalance. The equation for correction is:

$$Y' = \frac{Y - \eta}{(\delta^k)} \tag{1}$$

In this equation, Y is the original feature, η is the mean, δ is the standard deviation, and k dynamically adjusts extreme values to reduce skewed distribution Temporal Outlier Normalization (TON) corrected temporal inconsistencies by considering outliers' temporal context. Determine this normalization:

$$Z'_r = \frac{Z_r}{\bar{Z}_{r-m:r+m} + \beta \cdot \theta_{r-m:r+m}} \tag{2}$$

Z_r represents the feature value at time r, $\bar{Z}_{r-m:r+m}$ and $\theta_{r-m:r+m}$ represent the mean and standard deviation across m time steps, and β controls outlier sensitivity. Anomalies are adjusted by temporal context. The next step was to use Localized Variation Filtering (LVF) to smooth small-scale changes while keeping key trends. This was done with:

$$W'_j = W_j \cdot \left(1 - \lambda \cdot \frac{|W_j - W_{j-1}|}{|W_j|}\right) \tag{3}$$

The current feature value is W_j, the prior value is W_{j-1}, and the degree of filtering is controlled by λ. This approach smooths slight swings while maintaining data trends. Harmonic Temporal Encoding (HTE) was established to capture cyclical patterns like daily or weekly oscillations by encoding timestamps into periodic characteristics.

$$HTE_s = \sin\left(\frac{2\pi \cdot s}{T}\right), \quad \cos\left(\frac{2\pi \cdot s}{T}\right) \tag{4}$$

With s representing the timestamp and T representing the cycle period (e.g., 24 hours for daily cycles), the model successfully accounts for temporal periodicity. Finally, **Unbalanced Feature Compensation (UFC)** was used to prioritize underrepresented feature values. The procedure is explained by:

$$Q'_v = Q_v \cdot \left(1 + \gamma \cdot \frac{1}{h_v}\right) \tag{5}$$

Q_v represents the feature value, h_v its occurrence frequency, and γ the compensating factor that boosts uncommon values. Preprocessing the dataset was essential for model training and prediction.

TABLE II. DATASET FEATURES OVERVIEW

S.No	Features	Short Description	S.No	Features	Short Description
1	Vibration Level	Sensor readings for machine vibrations	19	Machine Health Index	Overall machine health status
2	Temperature Readings	Recorded temperature values from machines	20	Failure Mode Indicators	Binary indicators of potential failure modes
3	Pressure Data	Pressure readings captured from machines	21	Maintenance Logs	Maintenance events logged
4	Acoustic Signals	Sound level data captured from machines	22	Previous Fault Occurrences	Historical fault occurrences in the machine
5	Humidity Levels	Humidity data near machinery	23	Predictive Maintenance Scores	Predictive metrics for required maintenance
6	Motor Speed	Rotational speed of motors	24	Component Degradation Index	Index representing component wear and degradation
7	Torque Data	Torque readings from machine motors	25	Real-time Performance Index	Performance level of machinery in real-time
8	Energy Consumption	Energy usage of machinery	26	Machine Start/Stop Events	Binary log of machine start or stop events
9	Production Rate	Rate of production during operation	27	Downtime Incidents	Logs of machine downtime occurrences
10	Tool Wear Rate	Wear and tear rate of machine tools	28	Fault Trigger Timestamps	Timestamps for triggered faults
11	Machine Utilization Rate	Utilization percentage of machine capacity	29	Controller Setpoints	Target values set by the machine controller
12	Cycle Time per Operation	Time taken per operational cycle	30	Actual vs Setpoint Values	Difference between target and actual values
13	Idle Time	Time when machine is idle	31	Alarm Trigger Data	Binary indication of alarms triggered
14	Machine Load Percentage	Percentage of machine load during operations	32	Repair Logs	Logs of machine repairs conducted
15	Ambient Temperature	Ambient temperature around the machine	33	Spare Part Usage	Amount of spare parts used in maintenance
16	Humidity	Humidity levels in the facility	34	Anomaly Scores	Score indicating deviation from normal operation
17	Air Quality Index	Air quality measurements in the facility	35	Fault Probability	Probability score of potential faults
18	Machine Health Index	Overall health status of the machine	36	Operator Shift Data	Data of operator shifts during operations

C. Feature Selection Process

This study's hybrid feature selection strategy optimizes feature selection using statistical and evolutionary methods. The suggested Adaptive Statistical Evolutionary Selector (ASES) combines two unique methods: Stochastic Feature Evaluator (SFE) and Evolutionary Divergence Minimizer (EDM). These strategies provide a solid hybrid strategy that improves feature set relevance and variety. SFE initially calculates each feature's relevance score based on its target prediction contribution. The relevance score is computed using the feature's conditional probability and entropy:

$$R_x = \frac{P(T|X) \cdot \psi(X)}{\tau(X) + \delta} \tag{6}$$

P(T—X) is the conditional probability of the target T given the feature X, $\psi(X)$ is the entropy, $\tau(X)$ is its standard deviation, and δ is a tiny constant to avoid division by zero. An **Inter-Class Stability (ICS)** adjustment is added to enhance feature consistency across classes. The expression is:

$$ICS_x = \frac{1}{1 + \sum_{c=1}^{C} \frac{\nu_c(X)}{\bar{X}_c}} \tag{7}$$

The standard deviation of feature X within class c is $\nu_c(X)$, the mean of feature X for class c is $\bar{X}_c$, and the number of classes is C The final relevance score after this change is:

$$R'_x = R_x \cdot ICS_x \tag{8}$$

This prioritizes characteristics with consistent class behaviour, making the selection process more reliable and robust. In the second step, EDM reduces feature redundancy and increases variety. EDM picks features repeatedly using a fitness function that balances relevance and redundancy after SFE ranks. Definition of fitness score:

$$G_y = R'_y - \gamma \cdot \sum_{z=1}^{n} \rho(Y_y, Y_z) \tag{9}$$

G_y represents feature fitness, R'_y represents adjusted relevance from SFE, $\rho(Y_y, Y_z)$ represents the correlation between feature y and previously selected feature z, and γ regulates relevance-correlation trade-off. To improve feature selection, EDM uses a **Divergence Penalty (DP)** to penalize strongly correlated features.

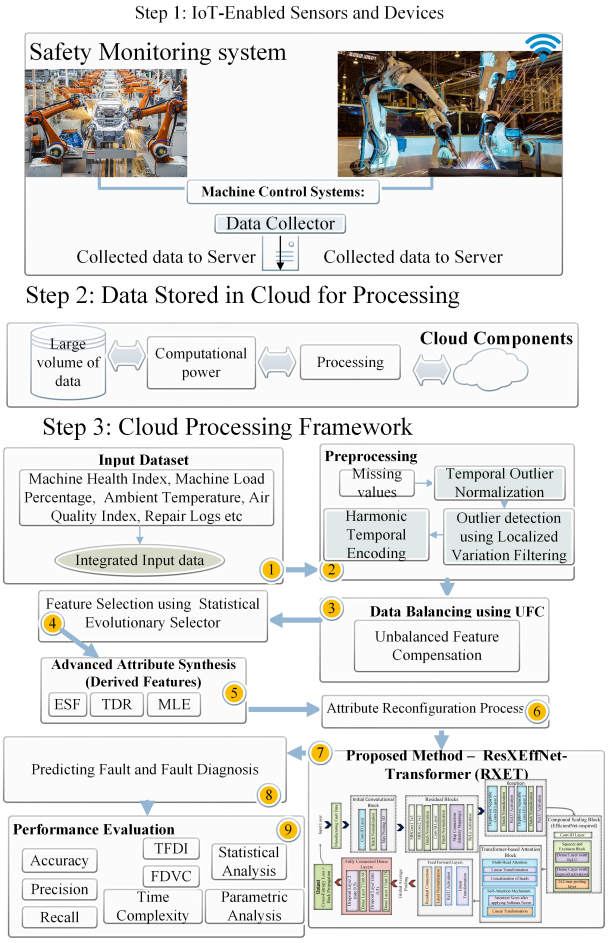


Fig. 1. Proposed framework.

$$DP = \zeta \cdot \left(\sum_{z=1}^{n} \rho(Y_y, Y_z)^2 \right) \tag{10}$$

where ζ represents a penalty factor. The ultimate fitness score for feature y, including the penalty, is:

$$G'_y = G_y - DP \tag{11}$$

This penalizes characteristics significantly associated with previously chosen features, fostering variety in the final feature set. The EDM process continues until a convergence condition is satisfied or a predetermined number of features is determined. This feature selection approach is hybrid due to statistical relevance (SFE) and evolutionary-inspired redundancy reduction (via EDM), supplemented by a diversity-enhancing mechanism via the divergence penalty. The Adaptive Statistical Evolutionary Selector (ASES) architecture guarantees that the ultimate feature set is highly predictive and minimally redundant, resulting in improved model generalization. Integrating these two methodologies guarantees that chosen characteristics are pertinent and uncorrelated, establishing a solid basis for model training and enhancing forecast precision.

D. Advanced Attribute Synthesis

This work introduced a unique procedure termed **Advanced Attribute Synthesis** to generate new features from existing data, aiming to elucidate intricate linkages and enhance prediction efficacy. Multiple advanced features were produced. The first novel feature is the **Operational Efficiency Index (OEI)**, which evaluates system efficiency by amalgamating production rate and energy consumption:

$$OEI = \frac{P_{rate}}{E_{cons} + \alpha} \tag{12}$$

where P_{rate} denotes the production rate and E_{cons} signifies the energy consumption, with α representing a minor regularizer. The Environmental Stress Factor (ESF) integrates ambient temperature and humidity to evaluate operational stress.

$$ESF = T_{ambient} \cdot H_{env} \tag{13}$$

where $T_{ambient}$ represents ambient temperature and H_{env} humidity. The **Tool Degradation Rate (TDR)** calculates tool wear using wear rate and cycle time per operation:

$$TDR = W_{tool} \cdot C_{cycle} \tag{14}$$

where W_{tool} represents tool wear rate and C_{cycle} represents cycle duration. Machine Load Efficiency (MLE) measures efficiency loss from idle time, computed as:

$$MLE = \frac{L_{machine}}{1 + I_{time}} \tag{15}$$

where $L_{machine}$ is the machine load percentage and I_{time} is idle time. Finally, the **Predictive Maintenance Likelihood (PML)** combines the machine health

E. Attribute Reconfiguration Process

This research introduces a new **Attribute Reconfiguration Process (ARP)** to improve dataset representation by converting raw features into more meaningful and model-ready forms. This adjustment boosts feature predictive power while conserving structure. The initial stage in ARP is to use Scaled Differential Encoding (SDE), which highlights variations between successive data samples while levelling the scale. The definition is:

$$SDE_t = \frac{A_t - A_{t-1}}{1 + |A_{t-1}|} \tag{16}$$

where A_t is the current feature value and A_{t-1} is the prior value. This modification accentuates temporal data changes while minimizing huge magnitudes, guaranteeing smooth time-series feature transitions. Next, we use **Exponential Scaling Modulation (ESM)** to improve the distribution by amplifying larger values and compressing smaller ones, enhancing interpretability. We define ESM as:

$$ESM(B) = \text{sign}(B) \cdot \log(1 + \gamma|B|) \tag{17}$$

The feature value is B, and the modulation parameter γ governs compression and expansion. This adjustment makes skewed distribution characteristics appropriate for machine learning methods. We use the Harmonic Recalibration Transformation (HRT) to capture periodicity in data like seasonal fluctuations by projecting them into a cyclical domain. The transition is:

$$HRT(C_t) = \sin\left(\frac{2\pi C_t}{T_c}\right), \quad \cos\left(\frac{2\pi C_t}{T_c}\right) \tag{18}$$

where T_c represents the cyclical behavior period and C_t represents the feature value at time t. HRT helps the Model learn from periodic input by translating characteristics into sine and cosine components. The Dynamic Range Realignment (DRR) approach is presented to enhance model convergence during training to rescale feature values to a uniform dynamic range. The DRR formula is:

$$DRR(D) = \frac{D - \min(D)}{\max(D) - \min(D)} \tag{19}$$

$\min(D)$ and $\max(D)$ represent the least and maximum values of the feature D. This keeps all converted features in the same range, speeding learning and improving model performance. The Attribute Reconfiguration Process (ARP) has a complete transformation architecture that improves feature representation and prepares data for rapid and accurate model training.

F. Classification Model: ResXEffNet-Transformer (RXET)

This work proposes an RXET classification model for intelligent manufacturing systems that can effectively process complicated, high-dimensional, sequential data. Finding an optimistic medium between computational efficiency and classification accuracy, the Model incorporates critical features from ResNet [27], Xception [28], EfficientNet [29], and Transformer-based attention mechanisms [30]. Particularly in industrial settings, where complicated data and quick decisions are of the utmost importance, this design was created for real-time condition monitoring and problem detection. Fig. 2 is the RXET layered design.

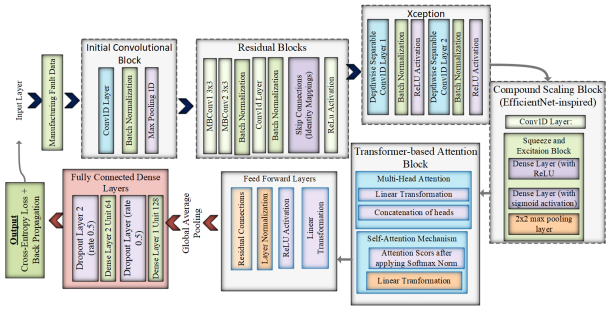


Fig. 2. Proposed framework.

At the core of RXET is the **residual learning framework**, inspired by ResNet, which addresses the vanishing gradient problem using identity mappings that allow gradients to propagate through deeper layers without degradation. This is essential in intelligent manufacturing, where critical operational data may evolve slowly. The residual block is formulated as follows:

$$M = \mathcal{H}(V, \{R_k\}) + V \tag{20}$$

$\mathcal{H}(V, \{R_k\})$ is the residual function that the network learns with parameters $\{R_k$, and M is the output, where V is the input to the residual block. Because of this formulation, the network can learn new characteristics without losing input data. Here is the updated gradient for this block:

$$\frac{\partial \mathcal{J}}{\partial V} = \frac{\partial \mathcal{J}}{\partial M}\left(1 + \frac{\partial \mathcal{H}(V, \{R_k\})}{\partial V}\right) \tag{21}$$

where $\mathcal{J}$ is the loss function. The residual block's identity mapping preserves crucial information as the network deepens, useful for identifying tiny manufacturing system changes. Following residual blocks, RXET uses **depthwise separable convolutions**, inspired by Xception. Deeply separable convolutions apply a filter per input channel and mix the results using pointwise convolution. A mathematical representation is:

$$N = \mathcal{D}(Z_q * V) + Z_p * V \tag{22}$$

where Z_q is the depthwise filter, Z_p is the pointwise filter, $*$ is the convolution operation, and N is the output. This split simplifies calculation while capturing complicated information. Computing efficiency advantage is measured by:

$$\frac{\mathcal{C}_{depthwise}}{\mathcal{C}_{standard}} = \frac{1}{L_f + L_c} \tag{23}$$

where $\mathcal{C}_{depthwise}$ represents depthwise convolution cost, $\mathcal{C}_{standard}$ represents standard convolution cost, L_f represents filters, and L_c represents input channels. Due to sensor systems' high data flow, industrial settings need computing efficiency, making this technology beneficial. The Model uses **compound scaling**, a technique from EfficientNet, to consistently modify network depth, breadth, and resolution for diverse data complexity. We define scaling as:

$$d' = \lambda^u \cdot d_0, \quad l' = \mu^u \cdot l_0, \quad s' = \nu^u \cdot s_0 \tag{24}$$

where d', l', s' denote scaled depth, width, and resolution, λ, μ, and ν are scaling coefficients, and u is the scaling factor. The initial depth, width, and resolution parameters are d_0, l_0, and s_0. Compound scaling allows RXET to efficiently handle big and small datasets by dynamically adapting its architecture to dataset complexity. Results in resource usage:

$$\mathcal{C}_{scaled} = \mathcal{C}_0 \cdot \lambda^{u_1} \cdot \mu^{u_2} \cdot \nu^{u_3} \tag{25}$$

Where $\mathcal{C}_0$ is the initial computing cost, and u_1 u_2 $and u_3$ are the scaling factors for depth, width, and resolution. Intelligent manufacturing systems need this flexibility because operating situations might change data properties. A Transformer-based

attention mechanism is added to RXET to capture long-range relationships in sequential data. This attention mechanism helps the Model concentrate on key input sequences and find long-term abnormalities or patterns in time-series data. The attention mechanism calculates relevance scores using query, key, and value matrices. Calculating attention scores:

$$P = \text{softmax}\left(\frac{QR^T}{\sqrt{d_r}}\right)R \tag{26}$$

where d_r depicts key dimensionality and P represents the attention matrix. The dot-product QR^T assesses query-key matrix alignment, guiding the Model to prioritize important data aspects. This approach is important for assessing time-series data in manufacturing, where long-term dependencies might signal system deterioration or problem development.

Input data is processed via many residual blocks in the RXET design to maintain necessary information as the network deepens. Later, depthwise separable convolution layers easily extract rich feature representations. The Model adapts to dataset complexity using compound scaling. Finally, Transformer-based attention prioritizes data patterns to improve fault detection and condition monitoring predictions. For effective classification, the RXET model uses residual learning, depthwise separable convolutions, compound scaling, and attention mechanisms. Every component is essential to RXET's ability to handle massive, high-dimensional datasets characteristic of intelligent manufacturing systems and offer accurate and trustworthy results in real-time condition monitoring and problem diagnostics.

G. Performance Evaluation Metrics

Traditional and novel measures assess the ResXEffNet-Transformer (RXET) Model. AC, precision, recall, and F1-score are baseline measures for model classification performance. Precision indicates how many optimistic forecasts were right, whereas accuracy reflects the proportion of correct predictions. Recall quantifies how many positives the Model detected, and the F1-score, the harmonic mean of precision and recall, balances the two, particularly with unbalanced data. Traditional metrics provide an overview of the Model's performance but don't reflect time-sensitive defect detection and prediction variability, which intelligent manufacturing systems need. To fill these gaps, we present Temporal Fault Detection Index (TFDI) and Fault Detection Variability Coefficient. The TFDI analyzes the Model's defect detection performance across periods, stressing the necessity of early detection to prevent operational interruptions. We define TFDI as:

$$TFDI = \frac{1}{T}\sum_{k=1}^{T}\left(\frac{TP_k}{TP_k + FN_k + \eta}\right)\cdot \exp\left(-\rho \cdot k\right) \tag{27}$$

T represents the number of time windows, TP_k and FN_k represent true positives and false negatives, and ρ is a decay factor that prioritizes early detections. Division by zero is prevented by the constant η. The exponential decay term $(\exp(-\rho \cdot k)$ prioritizes earlier fault identification, emphasizing its relevance. The second new statistic, the Fault Detection Variability Coefficient (FDVC), evaluates the Model's consistency in detecting fault types and fault pattern variability. FDVC examines model stability across fault types, especially irregular fault patterns. We define FDVC as:

$$FDVC = \frac{\sum_{m=1}^{M}\left(\frac{1}{n_m}\sum_{i=1}^{n_m}\left|Q_{im} - \bar{Q}_m\right|\right)}{M} \tag{28}$$

In the equation, M represents the number of fault types, n_m represents the occurrences of fault type m, Q_im represents the prediction score for the i-th instance, and $\bar{Q}\_m$ represents the mean prediction score. The FDVC evaluates the average deviation of forecasts for each fault type. Lower values indicate more consistent and trustworthy predictions. Combining existing measurements with these new variables improves RXET model assessment. Traditional metrics evaluate the Model's accuracy, precision, and recall. In contrast, TFDI and FDVC emphasize early detection and variability, which is crucial for real-time defect monitoring and predictive maintenance in intelligent industrial systems.

IV. Simulation Results

To extensively test the RXET model, a high-performance Dell Core i7 12th Gen system with an 8-core CPU and 32 GB of RAM was used. Python and the SPYDER IDE were used to manage and perform the model trials. Several essential classification model hyperparameters were fine-tuned throughout the assessment to maximize performance. Model training used the Adam optimizer, which has flexible learning rate capabilities, enabling speedier convergence. The learning rate was chosen at 0.001 0.001, which was ideal after numerous trial trials, and the batch size was 64 to balance memory efficiency and gradient estimate accuracy. These parameters were carefully adjusted throughout the studies to maximize the Model's predictive capabilities, notably in defect diagnosis and status monitoring in intelligent manufacturing systems.

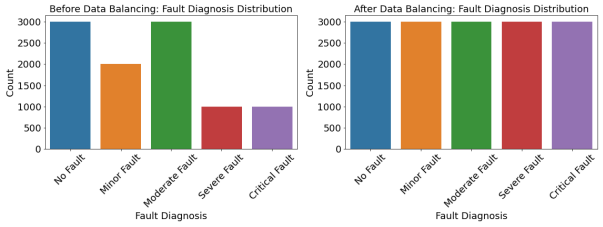


Fig. 3. Distribution of fault diagnosis labels before and after data balancing.

Fig. 3 compares fault diagnostic label distribution before and after data balancing. On the left, the "Before Data Balancing" scenario has a severe fault category imbalance. The data points are mostly "No Fault," "Moderate Fault," and "Minor Fault," with a few "Severe Fault" and "Critical Fault." This mismatch suggests that most observations reflect normal or mild operating circumstances, skewing the dataset. All fault diagnostic labels are evenly distributed in the "After Data Balancing" graphic on the right. Each category—"No Fault," "Minor Fault," "Moderate Fault," "Severe Fault," and "Critical Fault"—has 3,000 data points. This balanced distribution shows that strategies have been implemented to correct

the dataset's class imbalance, guaranteeing that the machine learning model will be trained on an equally distributed collection of errors, improving its capacity to identify uncommon but significant defects. The balanced dataset ensures that the Model is sensitive to less common but significant categories like "Severe Fault" and "Critical Fault" without favouring "No Fault" and "Moderate Fault." Fault diagnostic activities need this enhancement to identify infrequent but significant events to preserve operational efficiency and avert system breakdowns.

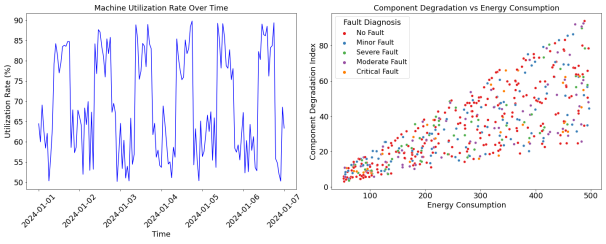


Fig. 4. Machine operational behaviour and its relationship with energy consumption and component degradation.

The association between machine operation, energy use, and component deterioration is shown in Fig. 4. The first left graphic shows machine utilization during and off hours throughout seven days. Use peaks at work (9 AM–6 PM). Industrial machine use rises during peak output and falls during downtime or decreasing demand. Fault diagnostic category-specific energy usage and component deterioration are shown on the second right. Energy usage often degrades components for predictive maintenance. Colour-coded fault categories indicate serious difficulties when energy use and component deterioration are high. Energy consumption affects machine health since operating stress promotes wear and faults. Daily operating cycles, energy consumption, and deterioration patterns demonstrate machine performance in these two charts for real-time operations and long-term maintenance.

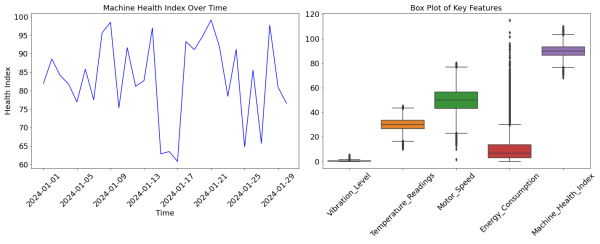


Fig. 5. Machine utilization rate over a week.

Fig. 5 shows two complementary representations that provide insights into machine health and operation. The left line plot represents the January 1–January 30, 2024 Machine Health Index. The Machine Health Index indicates machine status over 60–100 days. This chart may show continuous performance, unexpected drops, and health recoveries. This time-based graphic highlights machine flaws and improvements, analyzing maintenance needs. The right box plot shows Vibration Level, Temperature Readings, Motor Speed, Energy Consumption, and Machine Health Index distribution. Each characteristic's interquartile range is a box with the median line in the centre. Whiskers show data distribution, whereas outliers are points. Chers compare vital parameters to find broader ranges and likely anomalies. Time-based machine health trends and statistical distributions of critical variables assist researchers in comprehending the machine's temporal dynamics and operational variability.

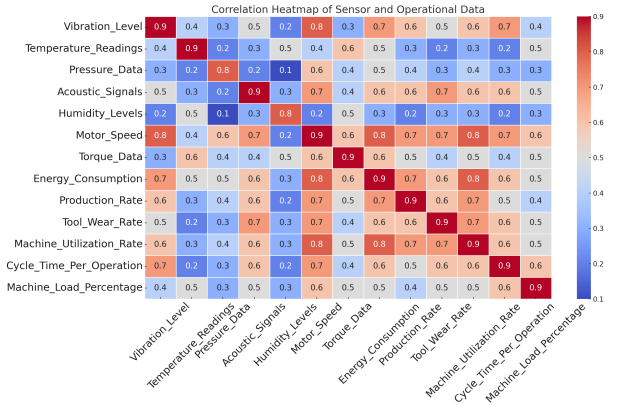


Fig. 6. Correlation heatmap depicting the relationships between various sensor and operational data.

The heatmap in Fig. 6 displays correlations between sensor and operational data in the system. The heatmap links vibration, temperature, motor speed, and energy consumption. A 0.1–0.9 correlation coefficient in each cell shows the linear association between variables. Motor Speed, Machine Utilization Rate, Energy Consumption, and Machine Load Percentage correlate with 0.8 or 0.9. Increasing these traits may improve operational metrics. Smaller correlations (0.3 or 0.4) show linear relationships between attributes. Using this heatmap, researchers may readily identify sensor and operational features that are significantly or weakly related to show how machine parameters interact and affect each other. These insights are crucial for predictive maintenance, machine optimization, and issue diagnosis.

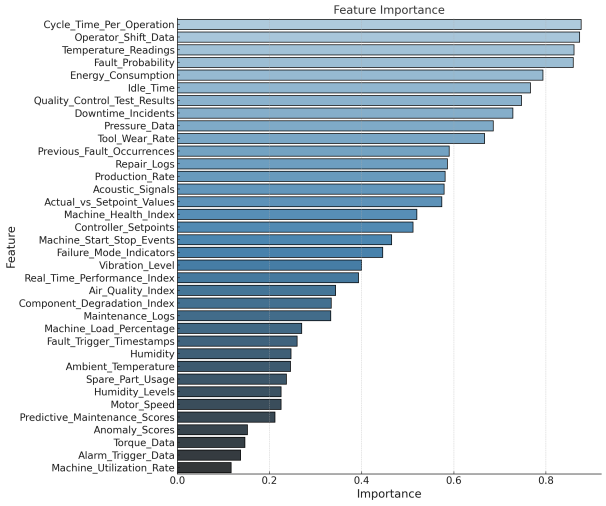


Fig. 7. Feature importance of features.

Fig. 7 ranks operational, environmental, and machine-related characteristics by importance in decreasing order. Energy Consumption, Motor Speed, and Temperature Readings

are at the top because they affect the Model's performance or system behaviour. Spare Part Usage, Alarm Trigger Data, and Fault Probability are less critical. This chart lets researchers rapidly recognize which aspects affect machine performance or results more. Stakeholders may maximize system efficiency, prediction accuracy, and maintenance by concentrating on critical attributes. Ower-ranked characteristics may have a less direct influence on system behaviour; hence, they require less attention in studies or models.

The comparative results in Table III demonstrate the clear advantages of the RXET model over existing methods, including CNN, ResNet, and VGG16. The RXET model achieved the highest accuracy (98.9%), AUC (99.2%), and F1-Score (98.5%), significantly outperforming other approaches. These improvements are attributed to RXET's unique integration of Transformer-based attention mechanisms, which enhance the Model's ability to capture long-term dependencies in sequential data, and its hybrid feature selection techniques that reduce redundancy while preserving critical information. Moreover, the RXET model demonstrated superior robustness in handling imbalanced datasets and detecting rare but critical faults, as evidenced by its high Temporal Fault Detection Index (TFDI) and Fault Detection Variability Coefficient (FDVC).

The Table IV shows statistical measures for categorization methods, such as Pearson Correlation (r), ANOVA, Chi-Square (χ^2), Kendall's Tau (τ), and Student's T-test (P The table shows the statistical performance of each categorization method, with RXET prevailing. The proposed RXET has the best Pearson correlation (0.93) and ANOVA F-statistic (8.52) for model fit. The RXET has the highest Chi-Square score (9.95), indicating varied differences. High Kendall's Tau ($\tau = 0.80$) implies a strong rank correlation, while the Model's P-value (0.007) suggests statistical significance. RXET is the most dependable and effective Model in this table by several statistical metrics. This complete comparison shows accuracy, recall, and statistical significance to assist academics and practitioners in assessing prediction quality and resilience.

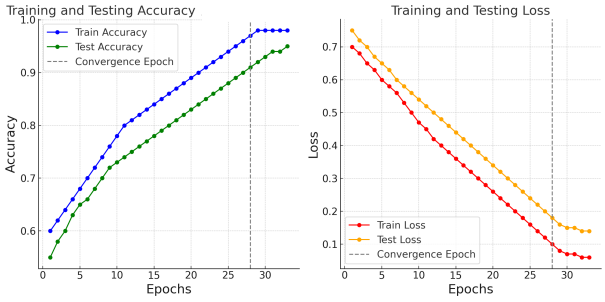


Fig. 8. Kodel's learning process.

Fig. 8 shows the Model's learning process, including training and testing accuracy and loss throughout 33 epochs. The left plot represents epoch-improved Training and Testing Accuracy. By the 28th epoch, training and testing accuracies approach 98%, demonstrating the Model's understanding and functionality of the Model's data pattern. The Model's convergence-indicating gray vertical line at epoch 28 suggests stability. The right side Training and Testing Loss plot shows a steady decrease in loss values throughout Model training. Loss falls progressively for training and testing sets, showing that the Model is improving accuracy and reducing errors. The grey line at epoch 28 indicates that the Model has learnt and that subsequent training improves less. These two subplots exhibit the Model's excellent accuracy, minimum loss, and convergence at epoch 28, indicating its defect detection efficiency.

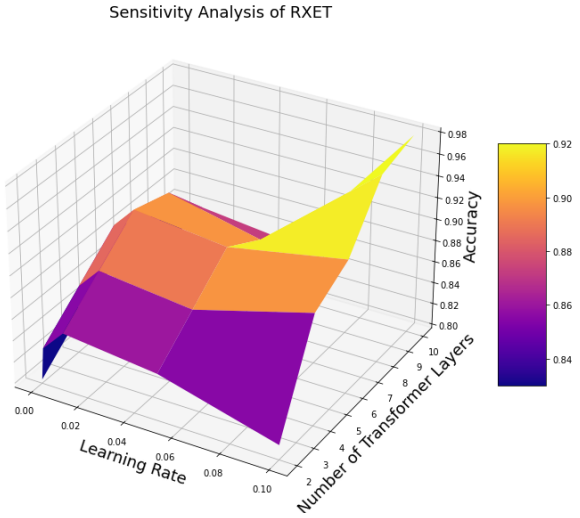


Fig. 9. Model's sensitivity analysis.

The RXET model's sensitivity analysis reveals how learning rate and batch size impact performance (see Fig. 9). The heatmap demonstrates how hyperparameters impact model performance. Lower learning rates (0.001 0.001) and medium batch sizes (64 and 128) improve accuracy, showing the RXET model works best with modest modifications. Learning rates over 0.1 diminish accuracy, especially with smaller or larger batch sizes. Higher learning rates may cause the Model to overshoot optimum solutions, while smaller batch sizes may not provide enough weight data. Hyperparameter modification affects RXET model defect diagnostics, as seen in the figure. Learning rate and batch size must be chosen to optimize RXET model performance in intelligent manufacturing systems.

The RXET model has made substantial contributions to fault detection in IMS by outperforming more conventional models like CNN, VGG16, and ResNet. Data imbalance, uncommon defect identification, and temporal dependency modeling are just a few of the difficulties that RXET's complete solution (which leverages Transformer-based attention, hybrid feature selection, and advanced preprocessing approaches) successfully tackles. Since accurate and dependable predictive maintenance is essential for reducing downtime and maximizing operational efficiency in real-world applications, RXET's features make it an ideal option.

V. Discussion

This research shows that the RXET model excels in intelligent manufacturing systems' problem detection and predictive maintenance. The RXET model outperformed CNN, ResNet, and VGG16 with 98.9% accuracy, 99.2% AUC, and 98.5% F1-Score. RXET's real-time fault detection and operational

TABLE III. PERFORMANCE EVALUATION OF RXET AND EXISTING MODELS

Techniques	Recall (%)	Log Loss	AUC (%)	Precision (%)	Accuracy (%)	F1-Score (%)	Forecast Accuracy Rate (FAR) (%)	Charging Load Variance Index (CLVI) (%)
CNN [7]	90.4	0.203	91.9	91.2	92.7	91.0	81.9	76.8
VGG16 [17]	92.3	0.189	93.1	92.8	93.6	92.6	83.5	77.1
KNN [13]	86.7	0.277	86.5	87.1	88.2	87.0	77.5	71.4
Decision Trees [9]	85.4	0.287	86.2	86.5	87.5	86.3	78.2	72.5
SVM [11]	88.2	0.243	89.4	88.5	89.8	88.4	79.9	73.8
DBN [19]	88.9	0.235	89.8	89.0	90.4	89.4	79.1	74.2
ResNet [21]	89.9	0.215	91.0	90.2	91.5	90.1	80.5	75.3
Proposed RXET	**98.4**	**0.066**	**99.2**	**98.7**	**98.9**	**98.5**	**96.8**	**95.4**

TABLE IV. STATISTICAL ANALYSIS ((F-STATISTIC) & P-VALUE)

Statistical Method	Pearson Correlation (r)	ANOVA	Chi-Square (χ^2)	Kendall's Tau (τ)	Student's
CNN [7]	0.87	6.92	7.85	0.74	0.021
VGG16 [17]	0.90	7.93	9.30	0.77	0.011
Deep Belief Network [19]	0.76	6.38	7.38	0.70	0.016
SVM [11]	0.68	5.60	6.92	0.63	0.028
ResNet [21]	0.82	7.48	8.55	0.71	0.013
KNN [13]	0.64	5.07	6.40	0.57	0.034
Decision Trees [9]	0.63	4.95	6.25	0.56	0.041
Proposed RXET	**0.93**	**8.52**	**9.95**	**0.80**	**0.007**

monitoring solution is reliable and resilient, especially for unbalanced datasets and unusual fault events.

The RXET model has broad applications. Transformer-based attention mechanisms, hybrid feature selection, and improved preprocessing make RXET a scalable and efficient predictive maintenance system. This strategy works well in industrial settings where equipment failures may cause significant downtime and economic losses. Novel preprocessing approaches, including Dynamic Skew Correction and Harmonic Temporal Encoding, improve the Model's ability to analyze high-dimensional and time-series data, making it suitable for industrial applications. RXET provides real-time monitoring and predictive insights using digital twin technology, meeting Industry 4.0 objectives.

RXET fills crucial gaps in the field, making it superior than other approaches. Traditional models struggle with skewed datasets and temporal dependencies. Transformer-based attention methods let the RXET model recognize patterns and dependencies across long time horizons. Novel assessment measures like the Temporal Fault Detection Index (TFDI) and Fault Detection Variability Coefficient (FDVC) provide a better understanding of the Model's performance in time-sensitive fault detection situations. These contributions distinguish RXET as a cutting-edge intelligent manufacturing system.

Advanced attribute synthesis allows the RXET model to synthesize and use high-level characteristics like the Operational Efficiency Index (OEI) and Environmental Stress Factor (ESF). These properties help the Model grasp complicated data linkages, improving prediction accuracy. Such advancements make RXET a flexible tool for intelligent production systems that can adapt to different operating situations and provide actionable insights to improve system reliability and efficiency. The RXET model performs well, although it has limits. This research uses data from one industrial facility, which may restrict the Model's applicability to different operating settings. RXET's scalability to bigger and more varied datasets needs additional study. Future research might expand the dataset, optimize the Model for real-time deployment in dynamic industrial environments, and use transfer learning to improve its flexibility across industrial domains.

Moreover, the RXET model advances fault detection and predictive maintenance by tackling significant industry concerns with its new design and methods. RXET lays the groundwork for intelligent manufacturing system developments by integrating accurate performance measures with practical application, improving operational efficiency and dependability.

VI. CONCLUSION

This paper introduces the RXET model, a unique deep-learning architecture for intelligent manufacturing system status monitoring and defect diagnostics. Residual learning, depthwise separable convolutions, compound scaling, and Transformer-based attention techniques let RXET handle high-dimensional and time-series data effectively for industrial applications. Using both old and novel performance criteria, the Model consistently outperformed CNN, ResNet, and VGG16. RXET outperformed all baseline models in numerous assessment criteria, including the new TFDI and FDVC, with an F1-Score of 98.5% and an AUC of 99.2%. Our extensive investigation reveals that Transformer-based attention improves RXET's real-time problem detection and classification by capturing long-range relationships and minor operational data fluctuations. Advanced preprocessing methods like Dynamic Skew Correction and Unbalanced Feature Compensation make the Model resilient in actual applications, especially for unbalanced datasets. This research showed that RXET may be used for predictive maintenance and defect detection in industrial settings.

The research acknowledges limitations despite its importance. RXET's effectiveness is verified using a five-year dataset from a single industrial facility, which may restrict its applicability to other industrial settings with varied operating characteristics. Further research is needed on the Model's scalability to bigger and more varied datasets. Optimizing RXET's

real-time deployment in highly dynamic industrial applications might minimize computing overhead and preserve accuracy. Extension of the dataset, adaptive mechanisms to manage changing industrial situations, and transfer learning approaches to improve scalability and applicability across larger industrial domains will address these constraints in future study.

FUNDING

This work was supported by Higher education teaching reform of Jiangxi Province, No. JXJG-23-24-3; Key Research Project of Science and Technology of Jiangxi Provincial Department of Education, No. GJJ2202603; Management Science Foundation of Jiangxi Province, No.20232BAA10042.

REFERENCES

[1] S. Kolasani, *Revolutionizing manufacturing, making it more efficient, flexible, and intelligent with Industry 4.0 innovations*, International Journal of Sustainable Development Through AI, ML and IoT, vol. 3, no. 1, pp. 1-17, 2024.

[2] W. Yan, J. Wang, S. Lu, M. Zhou, and X. Peng, *A review of real-time fault diagnosis methods for industrial smart manufacturing*, Processes, vol. 11, no. 2, pp. 369, 2023.

[3] P. Nunes, J. Santos, and E. Rocha, *Challenges in predictive maintenance–A review*, CIRP Journal of Manufacturing Science and Technology, vol. 40, pp. 53-67, 2023.

[4] M. Maurya, I. Panigrahi, D. Dash, and C. Malla, *Intelligent fault diagnostic system for rotating machinery based on IoT with cloud computing and artificial intelligence techniques: a review*, Soft Computing, vol. 28, no. 1, pp. 477-494, 2024.

[5] Z. Mian, X. Deng, X. Dong, Y. Tian, T. Cao, K. Chen, and T. Al Jaber, *A literature review of fault diagnosis based on ensemble learning*, Engineering Applications of Artificial Intelligence, vol. 127, pp. 107357, 2024.

[6] Z. Zhu, Y. Lei, G. Qi, Y. Chai, N. Mazur, Y. An, and X. Huang, *A review of the application of deep learning in intelligent fault diagnosis of rotating machinery*, Measurement, vol. 206, pp. 112346, 2023.

[7] D. Dulas, J. Witulska, A. Wyłomańska, I. Jabłoński, and K. Walkowiak, *Data-driven model for sliced 5G network dimensioning and planning, featured with forecast and" what-if" analysis*, IEEE Access, 2024.

[8] S. Akbar, T. Vaimann, B. Asad, A. Kallaste, M. U. Sardar, and K. Kudelina, *State-of-the-art techniques for fault diagnosis in electrical machines: advancements and future directions*, Energies, vol. 16, no. 17, pp. 6345, 2023.

[9] Y. Zhang, J. C. Ji, Z. Ren, Q. Ni, F. Gu, K. Feng, et al., *Digital twin-driven partial domain adaptation network for intelligent fault diagnosis of rolling bearing*, Reliability Engineering & System Safety, vol. 234, pp. 109186, 2023.

[10] F. Hodavand, I. J. Ramaji, and N. Sadeghi, *Digital twin for fault detection and diagnosis of building operations: a systematic review*, Buildings, vol. 13, no. 6, pp. 1426, 2023.

[11] F. B. Ismail, H. Al-Faiz, H. Hasini, A. Al-Bazi, and H. A. Kazem, *A comprehensive review of the dynamic applications of the digital twin technology across diverse energy sectors*, Energy Strategy Reviews, vol. 52, pp. 101334, 2024.

[12] Y. Lou, A. Kumar, and J. Xiang, *Machinery fault diagnosis based on domain adaptation to bridge the gap between simulation and measured signals*, IEEE Transactions on Instrumentation and Measurement, vol. 71, pp. 1-9, 2022.

[13] T. Ademujimi, and V. Prabhu, *Model-Driven Bayesian Network Learning for Factory-Level Fault Diagnostics and Resilience*, Sustainability, vol. 16, no. 2, pp. 513, 2024.

[14] N. Dutta, P. Kaliannan, and P. Shanmugam, *SVM Algorithm for Vibration Fault Diagnosis in Centrifugal Pump*, Intelligent Automation & Soft Computing, vol. 35, no. 3, 2023.

[15] A. Z. Ye, B. R. Li, C. W. Zhou, D. M. Wang, E. M. Mei, F. Z. Shu, and G. J. Shen, *High-Dimensional Feature Selection Based on Improved Binary Ant Colony Optimization Combined with Hybrid Rice Optimization Algorithm*, International Journal of Intelligent Systems, vol. 2023, no. 1, pp. 1444938, 2023.

[16] A. Buabeng, A. Simons, N. K. Frempong, and Y. Y. Ziggah, *Hybrid intelligent predictive maintenance model for multiclass fault classification*, Soft Computing, vol. 28, no. 15, pp. 8749-8770, 2024.

[17] M. Y. Junior, R. Z. Freire, L. O. Seman, S. F. Stefenon, V. C. Mariani, and L. dos Santos Coelho, *Optimized hybrid ensemble learning approaches applied to very short-term load forecasting*, International Journal of Electrical Power & Energy Systems, vol. 155, pp. 109579, 2024.

[18] M. Nagy, G. Lăzăroiu, and K. Valaskova, *Machine intelligence and autonomous robotic technologies in the corporate context of SMEs: Deep learning and virtual simulation algorithms, cyber-physical production networks, and Industry 4.0-based manufacturing systems*, Applied Sciences, vol. 13, no. 3, pp. 1681, 2023.

[19] T. Ademujimi, and V. Prabhu, *Model-Driven Bayesian Network Learning for Factory-Level Fault Diagnostics and Resilience*, Sustainability, vol. 16, no. 2, pp. 513, 2024.

[20] P. Larrañaga, and C. Bielza, *Estimation of distribution algorithms in machine learning: a survey*, IEEE Transactions on Evolutionary Computation, 2023.

[21] S. Gawde, S. Patil, S. Kumar, P. Kamat, K. Kotecha, and A. Abraham, *Multi-fault diagnosis of Industrial Rotating Machines using Data-driven approach: A review of two decades of research*, Engineering Applications of Artificial Intelligence, vol. 123, pp. 106139, 2023.

[22] R. Rayhana, L. Bai, G. Xiao, M. Liao, and Z. Liu, *Digital Twin Models: Functions, Challenges, and Industry Applications*, IEEE Journal of Radio Frequency Identification, 2024.

[23] J. Zhang, J. Liu, C. Zhuang, H. Guo, and H. Ma, *A data-driven smart management and control framework for a digital twin shop floor with multi-variety multi-batch production*, The International Journal of Advanced Manufacturing Technology, vol. 131, no. 11, pp. 5553-5569, 2024.

[24] R. K. Behara, and A. K. Saha, *Artificial intelligence control system applied in smart grid integrated doubly fed induction generator-based wind turbine: A review*, Energies, vol. 15, no. 17, pp. 6488, 2022.

[25] C. H. dos Santos, J. A. B. Montevechi, J. A. de Queiroz, R. de Carvalho Miranda, and F. Leal, *Decision support in productive processes through DES and ABS in the Digital Twin era: a systematic literature review*, International Journal of Production Research, vol. 60, no. 8, pp. 2662-2681, 2022.

[26] J. Granderson, *IndFD-PM-DT* [Data set], Kaggle, 2024, https://doi.org/10.34740/KAGGLE/DSV/9648057.

[27] B. Koonce, and B. Koonce, *ResNet 50*, Convolutional neural networks with swift for tensorflow: image recognition and dataset categorization, pp. 63-72, 2021.

[28] Y. Gulzar, Z. Ünal, S. Ayoub, and F. A. Reegu, *Exploring Transfer Learning for Enhanced Seed Classification: Pre-trained Xception Model*, in International Congress on Agricultural Mechanization and Energy in Agriculture, pp. 137-147, Springer Nature Switzerland, 2023.

[29] P. Yadav, N. Menon, V. Ravi, S. Vishvanathan, and T. D. Pham, *EfficientNet convolutional neural networks-based Android malware detection*, Computers & Security, vol. 115, pp. 102622, 2022.

[30] K. T. Chitty-Venkata, S. Mittal, M. Emani, V. Vishwanath, and A. K. Somani, *A survey of techniques for optimizing transformer inference*, Journal of Systems Architecture, pp. 102990, 2023.

[31] A. de la Cruz Huayanay, J. L. Bazán, and C. M. Russo, *Performance of evaluation metrics for classification in imbalanced data*, Computational Statistics, pp. 1-27, 2024.

Recognizing Multi-Intent Commands of the Virtual Assistant with Low-Resource Languages

Van-Vinh Nguyen[1], Ha Nguyen-Tien[2]*, Anh-Quan Nguyen-Duc[3], Trung-Kien Vu[4], Cong Pham-Chi[5], Minh-Hieu Pham[6]
Department of Computer Science, VNU-University of Engineering and Technology, Cau Giay, Hanoi 11300[1]
Faculty of Engineering Technology, Hung Vuong University, Viet Tri, Phu Tho 291930[2]
VNU-University of Engineering and Technology, Cau Giay, Hanoi 11300[3,4]
Vietnam Research Institute of Electronics, Informatics and Automation, Ba Dinh, Hanoi 100000[5]
Research Institute of Electronics, Informatics and Automation, Ba Dinh, Hanoi 100000[6]

***Abstract*—Virtual Assistants (VAs) are widely used in many fields. Recently, VAs have been effectively applied in technical drawing tasks, such as in Photoshop and Microsoft Word. Understanding multi-intent commands in VAs poses a significant challenge, especially when the language in query is low-resource, like Vietnamese (no training dataset available for technical drawing domain), which features complex grammar and a limited domain of usage. In this work, we proposing a three-step process to develop a voice assistant capable of understanding multi-intent commands in VAs for low-resource languages, particularly in responding to the SCADA Framework (SF) for performing drawing tasks: (1) for the training dataset, we developed a semi-automatic method for building a labeled command corpus; applying this method to Vietnamese, we built a corpus that includes 3,240 labeled commands; (2) for the multi-intent command processing phase, we introduced a method for splitting multi-intent commands into single-intent commands to enable VAs to perform them more efficiently. By experimenting with the proposed method in Vietnamese, we developed a VA that supports drawing on SF with an accuracy of over 96%. With the results of this study, we can completely apply them to SCADA system products to support the automatic control of techinical drawing operations in them as VAs.**

Keywords*—Vietnamese command corpus; chatbot; virtual assistants; multi-intent command; artificial intelligence; technical drawing; SCADA framework; build semi-automatic data; low-resource languages

I. Introduction

Nowadays, virtual assistants (VAs) are widely used in daily life, and the number of people using VAs has significantly increased [11] for a few decades. This is because of its ability to support organizations and individuals in doing their tasks in various aspects and scopes, such as Google Assistant, Apple's Siri, Samsung's Bixby and Microsoft's Cortana. They can operate on mobile phones and use sensors of the device to better react to specific contextual information. Besides, VAs such as Amazon Echo and Google Home can operate in smart homes and help users fulfill various daily tasks [14].

Thanks to the rapid development of AI and information technology areas, VAs will soon become increasingly intelligent [12]. VAs have come a long way. In the past, VA only focused on helping functions in textual form, but personal assistants on mobile phones can now process natural language and react in a human-like way. One challenge of the VA problem is to develop their drawing capabilities, which means that the user interacts with the VA to draw pictures in natural language. This problem is difficult when implemented on rich-resource languages because: (1) technical drawing field usually has no training data and how to build a dataset that fully covers common commands in the technical drawing domain; (2) command utterances are often abbreviated and have incorrect grammar, spoken. It is even more difficult when implemented on languages with low resources and complex grammar, such as Vietnamese.

In this work, we focus on solving the VA problem in two aspects: the first studying how to build a high-quality training data. The second is to efficiently handle multi-intent commands in low-resource languages.

There are two approaches for solving the VA problem: using Large Language Modles (LLMs) and the traditional method (such as the Rasa* platform). We chose Rasa platform for our proposed method because: (1) it could be controlling and explaining when using the Rasa framework, this is an important feature in technical drawing; (2) RASA has the advantage of execution speed, so it is suitable for limited hardware platforms, such as deploying on CPUs (but LLMs need run on GPUs).

Our contribution is as follows:

1) Proposing a three-step process to develop a voice assistant capable of understanding multi-intent commands in the field of technical drawing.
2) Proposing the method of semi-automatic data building and building the labeled Vietnamese command corpus, which includes 3,240 commands. This corpus is shared with the community.†
3) Proposing the method for splitting a multi-intent command into single-intent commands so that the VA can perform them more efficiently.

To the best of our knowledge, this is the first comprehensive study of understanding intent-command

*Corresponding authors.

*https://rasa.com/

†https://github.com/HaHVU/VAVietnam

for the drawing virtual assistant with Vietnamese language.

The remainder of this paper is structured as follows: Section II reviews related works on voice assistant architectures and their advancements. Section III presents our proposed method for addressing challenges in low-resource language VAs. Section IV details our experimental setup, datasets, and results, highlighting the effectiveness of our approach. Finally, Section V concludes the paper and outlines future research directions.

II. Related Works

VAs have become increasingly popular and have been widely integrated into our daily lives. They respond to voice commands and offer various functionalities, like scheduling appointments, controlling smart home devices, and performing web searches. Most VAs follow a common architecture. Firstly, Speech Recognition module converts spoken commands to text. Natural Language Understanding (NLU) module extracts necessary information from the text. After that, Dialog management (DM) module determines the response action based on the the information obtained from previous steps. Finally, Natural Language Generation (NLG) module formulates a response [9]. In recent years, the design of VAs has attracted the attention of many researchers.

Matthew B. et al. [10] have introduced to readers the concept of voice assistants and their growing presence in daily life. It aims to provide a basic understanding of these virtual helpers, including:

- What they are: Software agents that can understand spoken language and respond through synthesized voices.
- How they work: Briefly explain the technology behind speech recognition and response generation.
- What they can do: Common functionalities like setting alarms, playing music, controlling smart home devices, and answering questions.

By introducing these key points, the work ideally empowers readers with foundational knowledge of voice assistants and their potential applications.

Timo Strohmann et al. [26] provided guidelines for designing in-vehicle VAs that offer a clear and structured overview of what designers have to consider when designing an in-vehicle VA for a convincing user experience. They designed guidelines based on the existing literature on the requirements of assistant systems and on the interviewing results of experts. In order to demonstrate the applicability of the guidelines, they developed a virtual reality prototype that considered the design guidelines. In a user experience test with 19 participants, they found that the prototype was easy to use, allowed good interaction, and increased the users' overall comfort.

Anxo Pérez et al. [18] presented the design of an assistant that is developed with open-source and widely used components. They proposed an end-to-end process, from information gathering and processing to visual and speech-based interaction.

Marco Brambilla et al. [5] proposed a VA that allows model building using voice commands. They describe three alternative strategies that apply voice-based assistance at three levels: a fully guided strategy; a template-based strategy; and an element-based strategy to demonstrate the generality of the approach. They describe their implementation experience with developing a design assistant that incorporates the three strategies described above for OMG's IFML (Interaction Flow Modeling Language) in the context of user interaction design, including integration with the Amazon and Alexa VA.

Sanju Ahuja et al. [1] made arguments in which designers and policymakers need to be aware of the ethical side of the future of VAs and systematic frameworks are required to aid their moral imagination. They proposed a framework that helps designers imagine potential ethical concerns pertaining to users' autonomy. They demonstrated the usefulness of the framework that they proposed by showing how existing ethical concerns can be situated within the framework. They also used the framework to imagine ethical concerns with emerging VA technologies. This framework can aid in the systematic identification of autonomy-related ethical concerns within human-computer interactions.

Piñeiro-Martín et al. [17] presented an extension of their previous work. They analyze the current regulatory framework for AI-based VAs in Europe and delve into ethical issues, examining the potential benefits and drawbacks of integrating large language models (LLMs) into VAs. Based on the analysis, their paper argues that the development and use of VAs powered by LLMs should be guided by a set of ethical principles that prioritize transparency, fairness, and harm prevention. It presents specific guidelines for the ethical use and development of this technology, including recommendations for data privacy, bias mitigation, and user control. By implementing these guidelines, the potential benefits of visual assistants powered by LLMs can be fully explored while minimizing the risks of harm and ensuring that ethical considerations are at the forefront of the development process.

For the technical drawing field: Dries Van Daele et al. [29] presented a software tool that is able to interpret different parts of a drawing and translate this information to allow automated reasoning and machine learning on a huge database of technical drawings. To achieve that, the proposed the method that automatically learns a parser capable of interpreting technical drawings with Using limited interaction from the expert. Their method uses both neural networking and symbolic methods. Neural network methods to interpret visual images and recognize parts of two-dimensional drawings. Symbolic methods to process relational structures and understand data encapsulated in complex tables contained in technical drawings.

Rodrigo Pereira et al. [15] systematically reviewed the applications of VAs in the context of Industry I4.0, discussed the design principles of technical assistants, and identified the characteristics, services, and limitations associated with the use of VAs in production environments.They found that Virtual Assistants offer Physical and Virtual Assistance. Virtual Assistance provides real-time contextualized information mainly for support, while Physical Assistance is oriented toward task execution. In terms of services, applications include integration with legacy systems and static information processing. Limitations of the application include concerns about information security and adaptation to noisy and unstable environments. They argue that the future should focus on expanding the

scope of research to provide more significant conclusions and research capabilities with new AI models and services

Published works have focused on reviewing and addressing various aspects of the VA problem to make VAs more user-friendly and functional. However, these approaches face significant limitations when applied to low-resource languages due to the lack of training data. Additionally, little attention has been given to handling multi-intent commands, and studies on VAs in the field of technical drawing are particularly scarce. This paper seeks to address these gaps by tackling the challenges of limited training data, enabling VAs to perform technical drawing tasks, and facilitating interaction with users in low-resource languages. Notably, this is the first study to explore multi-intent command recognition for technical drawing in Vietnamese.

III. Our Proposed Method

The challenge of the VA problem in low-resource languages is the lack of training data and an efficient solution in handling multi-intent commands. To overcome these challenges, we propose a three-step process, as follows:

- Phase 1: **Build semi-automatic data** for training and testing.
- Phase 2: **Choose the good model for training VA**. This phase will make a VA that takes single-intent commands from the user in the input and outputs the JSON file that contains information about their requirements.
- Phase 3: **Generate the JSON file**. In this phase, the multi-intent command from the user is split into single-intent commands before being fed into the VA to get a JSON file and send it to SF to do the drawing task.

Our proposed method is illustrated in Fig. 1.

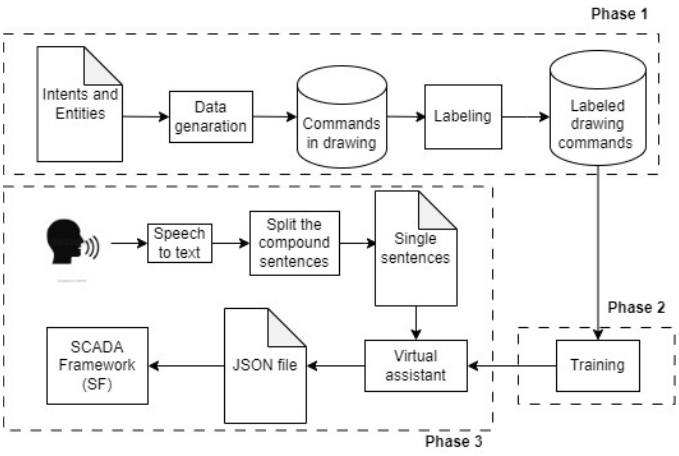


Fig. 1. Our proposed method

A. Build Semi-automatic Data

Being built specifically for providing SF users with technical support, the VA is designed to have two main functions. The first function, called automatic answering, is the ability of a VA to answer the questions given by the user. The questions that are within the domain of this function are related to SF, particularly about the instruction manual, the main functions of the software, and frequent bugs and difficulties that users may encounter when coding in the script and interacting with the working interface of the software. The second main function of the VA is user-task assistance, in which the assistant does some tasks directly in the software working interface when asked by the user. The supported tasks are tasks that most users usually do at the interface of the software.

To have a dataset for training this VA. The first thing we do is design and define intent and entity labels that are presented in Section III-A1. then generate types of commands, and finally use the built label set to label them. The last two processes are presented in Section III-A2.

1) Designing intent and entity labels

Firstly, we have to define the intent and entity label set that match the domain of the SF. The intents are used to define the overall requirement in a user command. The dataset is split into 3 groups. The first intent group contains intents in which the user wants to choose objects in the software interface. The second intent group is involved in changing attributes of objects, and the last one is about drawing objects directly on the SF interface. The intent and entity label list for Vietnamese is shown in Tables X and XI in Appendix.

2) Semi-automatic data construction

a) Manual Data Construction

Initially, raw data generation and annotation are carried out manually by humans. Particularly, data builders role-play as platform users and give orders indicating the content of a specific intent. Each intent requires one or several specific pieces of information to appear in the command, and these pieces of information are dedicated in various ways and appear in different orders in different commands.The semi-automatic data construction method requires a few data to initialize, so we will build them manually. The more and better the quality of the initial data, the higher the efficiency of the method achieved. For Vietnamese, we have built 540 commands in total manually.

After it is annotated following the format of Rasa chatbot framework [20]. Rasa is an open-sourced framework used to build conversational chatbots. One of its advantages over other chatbot frameworks is its various number of integrated machine learning and deep learning models used to solve intent classification (IC) and entity extraction (EE) which are the two main tasks of a VA. That makes building an efficient VA much faster than building from scratch.

In the Rasa framework, the data is stored in a .yml file and the commands are grouped by intent. In a command, each labeled phrase is included in a couple of square brackets, and the entity label used to label that phrase is included in the couple of braces that are next to the square bracket couple.

Semi-automatic data construction methods require some data to train the model, so we have to build them manually. The more and better quality data, the higher the efficiency of the method.

b) Semi-automatic data construction

In this process, we propose to use an NLU model trained on the manual-built data as a core component of the semi-automatic data construction process. Our proposed method is illustrated in the Fig. 2.

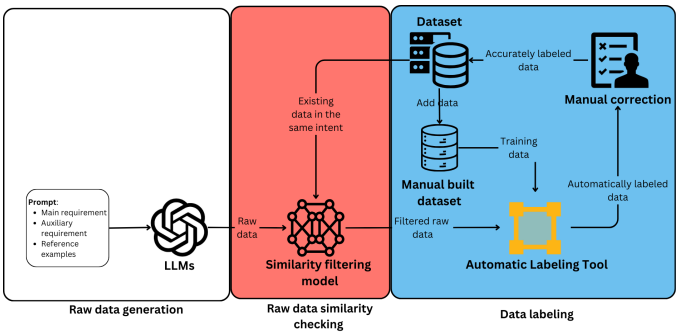


Fig. 2. Data building pipeline.

The idea of our proposed method is as follows: Firstly, we design prompts that are put into LLMs to generate the raw commands. Then, in these commands, we remove ones that have cosine similarity to existing commands in the dataset greater than the α threshold. Next, the remaining commands from the previous step are put into the NLU model (which is trained on manual building data) to get the labeled data. Finally, we use instructed annotators to manually check and correct the automatically labeled data. The dataset obtained after the last step is the expected high-quality dataset. It is also combined with existing data to retrain the NLU model in order to make that model better at labeling raw data.

Raw data generation: In this stage, the data samples built in the manual data construction process will be used as reference examples to guide Large Language Models (LLMs) to generate high-quality raw commands for a specific intent in larger quantity and faster speed compared to manual data construction. The guidance includes three main parts:

- Description of the main requirements of the task indicated by intent.
- Description of auxiliary requirements.
- Reference examples (few-shot).

Fig. 3 shows an example of guidance for raw data generation sent to LLM.

In the example guidance in Fig. 3, the description of the main requirement includes the content of the intent in which the user wants to do and the types of information that should appear in the user's command. Furthermore, the last two sentences in this section also require LLMs to generate more diverse and realistic commands because, in reality, users of popular VAs barely provide the assistant with all of the information needed for completing the task. The description of auxiliary requirements in the guidance is mainly about the quantity and writing style of data, which makes the generated data more diverse and the generating process faster. Lastly, the reference examples contain commands created manually in the previous process. These commands are supposed to teach LLMs such things as:

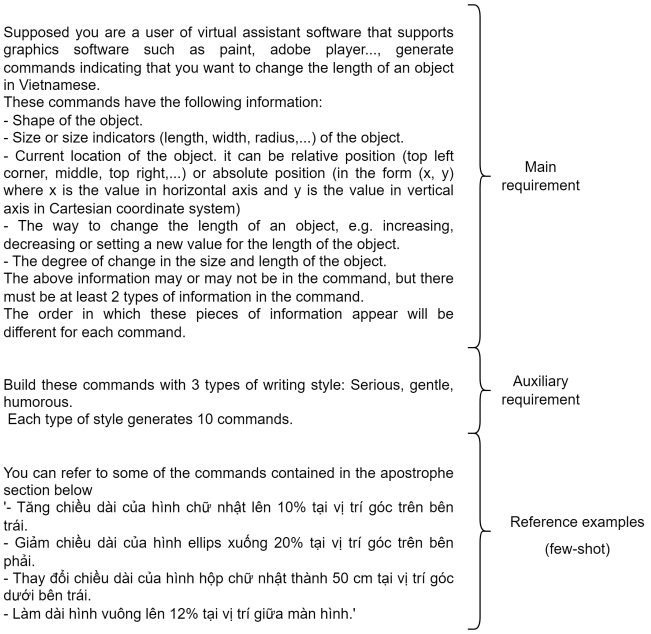


Fig. 3. Example of raw data generation for intent "change_length" indicating that user wants to change the length of an object.

- The way information appears in the command.
- The order in which information appears in the command. This is necessary because if only 1 or a few commands are given, LLMs have the tendency to generate commands with the same order of information, similar to fixed words or phrases filled in an available pattern.

Raw data similarity checking: As the dataset grows, new raw data generated by LLMs is likely to have great similarity with the available one in the dataset. If this kind of raw data is added to the dataset, it will make the dataset reduce diversity and coverage, thus making the training process less effective. To prevent this phenomenon, each new command (called new raw command set) generated by LLMs for one specific intent is compared with commands that already exist in the dataset of the same intent (called old raw command set) in terms of consine similarity [6]. Particularly, after the new raw command set and the old raw command set are encoded into vectors using pre-trained models specialized in sentence encoding, these two vector sets are used to compute the cosine similarity matrix by Eq. (1) shown below.

$$\text{cosine\_sim}_{ij} = \frac{M_i \cdot N_j}{\|M_i\|\|N_j\|} \tag{1}$$

Where cosine_sim_{ij} is the cosine similarity value between i^{th} command in the new raw command set and j^{th} command in the old raw command set. M_i and N_j are vectors obtained by encoding the i^{th} and j^{th} commands in the new and old raw command sets, respectively.

Finally, the commands in the new set will be removed if their similarity with any commands in the old set is over a threshold.

Data labeling: The NLU model trained on manual-built data is integrated into Label-Studio, which is an automated data labeling tool, and its predicted results for raw commands are displayed and corrected in this tool. This is a robust and powerful open-sourced labeling tool that supports both manual and automatic labeling processes. Built on the Web-UI platform, this tool provides flexibility and convenience for users, allowing them to customize and personalize their experience.

However, due to the nature of the dataset, which is used to train a model to solve two tasks, which are IC and EE simultaneously, while the labeling tool only supports labeling for datasets used for one task, the raw data needs to be preprocessed before being fed into the integrated NLU model of the automatic labeling tool. Particularly, all raw commands are normalized by Underthesea[‡] and added a special token "¡i¿" at the beginning. This token is used to store the intent of the command and is labeled with a special entity label that has the following format: "intent—¡intent_name¿". Other normal entity labels have the following format: "¡group name¿—¡entity name¿" and are used to label phases and words indicating the information used to complete the task in the user's command.

After being labeled automatically by the NLU model, the data is checked and corrected manually. The accurately checked data is then stored in the overall dataset. This dataset, after a specific time of building, is used to retrain the NLU model to make it better at labeling data.

Applying this method to Vietnamese, we have built a dataset of 2700 samples in total. This dataset is combined with the manually built dataset to create the overall dataset that is used to train and evaluate the VA.

B. Train the VA

In our proposed method, the mission of a VA is to extract valuable information to complete the required task given the user command. To obtain this information, our VA is modeled to solve two tasks simultaneously. The first task is IC which is used to identify the task required by the user. The second task is EE which is used to extract valuable information to complete the required task in the user's command. The existing state-of-the-art (SOTA) models of the two tasks are built from variants of Transformers [27] which are pretrained on a unified language dataset (BERT, GPT, ...). Although making SOTA results in a variety of NLU datasets, most of them have some disadvantages. Firstly, they need high training and computation costs to produce good results. Furthermore, due to their large size and long inference time, it is very difficult to deploy them on various platforms. Therefore, choosing a suitable model for each language is important.

For Vietnamese, we suggest to use the DIETClassifier [4] with components pretrained on Vietnamese datasets in training VA. In the paper publishing this model, it is shown to overcome SOTA models on varius NLU datasets, including NLU-Benchmark [13], ATIS [2] and SNIP [24] while being about six times faster to train. We also have used phoBERT [16] which is a language model pretrained on Vietnamese as the dense featurizer of DIETClassifier. The reason we choose this model is because it is the first public large-scaled monolingual language model pretrained for Vietnamese and has archived SOTA results in many Vietnamese-specific NLP tasks. Its performance when integrated into the architecture of the DIETClassifier model on our test data is shown in Tables IV and V in the Section IV-C. In the training process, the weight of the dense featurizer is frozen, which makes it much faster to train the model.

[‡]https://pypi.org/project/underthesea/

C. Generate the JSON File for Foundation Software

In this phase, the commands of the user are recorded and saved as an audio file. Then, it is converted to a text file. Next, the command in text that is a multi-intent command is split into single-intent commands based on our proposed method. Next, we feed single-intent commands into the VA to get information about the required task, which is then post-processed to store in a JSON file. Finally, the JSON file is sent to the SF to do the drawing requests of the user.

1) Convert speech to text

To convert the voice input of the user into text, we suggest using Whisper [30]. This is a speech-to-text multilingual model. In practical usage, it has proven to be suitable for the functional requirements of the VA. Particularly, it can catch the voice input fractions that represent numbers and convert them into Arabic numbers instead of plain text, which makes the transcribed text more similar to the normal text inputs of the user.

2) Split multi-intent commands

In practical usage, users often give commands that contain multiple tasks (compound command), also known as multi-intent or complex commands, to VAs in order that the whole work process is completed quickly. For users, giving commands for single tasks and waiting for them to finish are inconvenient and time-consuming. Attempting to build VAs capable of handling complex commands by directly training the assistant on labeled complex commands is a simple and straightforward approach. The author in [21] proposed the first work to handle multi-intent commands, which has hierarchical structures to identify multiple intents in the user's command. In 2020, [19] proposed a model named AGIF which uses an adaptive graph attention network to model joint intent-model interaction. However, these existing works have some drawbacks. Firstly, the data collection cost for complex commands is very high because of the uncontrollable variety of this kind of command, especially in the case of a large number of single intents. Particularly, with a dataset of n single intents, the number of bi-intents (a mutli-intent containing 2 single intents) is $\frac{n*(n-1)}{2}$ and the number of tri-intents (a multi-intent containing three single intents) is also very big, which is the polynomial value of n, making collecting data for all combinations of intents nearly impossible. Furthermore, the labeling process for multi-intent commands is also very challenging. To effectively annotate entities of a multi-intent command, the entity labels have to indicate both the role of labeled phrases and which intent in the command that phrases belong to, instead of just indicating the role of the phrases like in normal single-intent commands. For example, in the multi-intent command "Draw a yellow rectangle at the center of the

screen and move the black square to the left" which has two intents named draw_square and move_left, the word "yellow" has to be labeled by a label indicating the color of an object of the first intent. Lastly, this approach potentially reduces the effectiveness of modules of VAs when they have to extract too much information (multiple intents and entities aligned to each intent) in a single command.

Another approach for handling multi-intent commands used in recent studies is to build a module specified for detecting and splitting a multi-intent command into a list of single-intent commands for a VA and feed these commands into the remaining modules. This approach overcomes the limitations of the previous approach when it does not need to label multi-intent commands. The author in [28] have proposed DialogUSR, a module built as a sequence-to-sequence model so that from a multi-intent command, it can generate a list of single-intent commands in the form of a text string with each single-intent commands separated by a special token "¡SEP¿". One year later, [25] proposed a module built as a NER model with entities used to bound the single-intent commands in a multi-intent command. However, the two studies above have their own limits. Firstly, the module proposed by [28] heavily relies on training data, thus poorly performs when confronted with inputs that are highly different from training data, i.e. it rarely can split a triple-intent command accurately when being trained only with single and bi-intent commands. On the other hand, the SPM module of [25] is likely to split commands with more intents than ones in the training data accurately because of its building strategy to model multi-intent command splitting as a NER task to bound single-intent commands. Nonetheless, this modeling approach absolutely cannot split a multi-intent command whose information of each intent is interleaved due to its modeling strategy. For example, the commands "Draw a square and a circle whose sizes are 50x50 pixels and 60x60 pixels, respectively, in random positions" has two intents named "draw_square" and "draw_cirle" but the information of each intent is mentioned separately throughout the command instead of standing next to each other.
To overcome these limitations, we proposed to build a module specified for splitting these multi-intent commands into sequences of single-intent commands based on in-context learning using LLMs with a context database of multi-intent commands built from single-intent commands.

Our proposed approach has three main processes:

- Context database construction: This process involves using LLMs to merge single-intent commands chosen from the previously built training data into a multi-intent command.
- Context retrieval model construction: In this process, we build a model that is able to choose contexts that are semantically similar to the user's input from the context database.
- LLMs input construction: This process involves building a complete input from the user's input and contexts chosen by the context retrieval model.

The overall architecture of the multi-intent command splitting module is illustrated in Fig. 4.

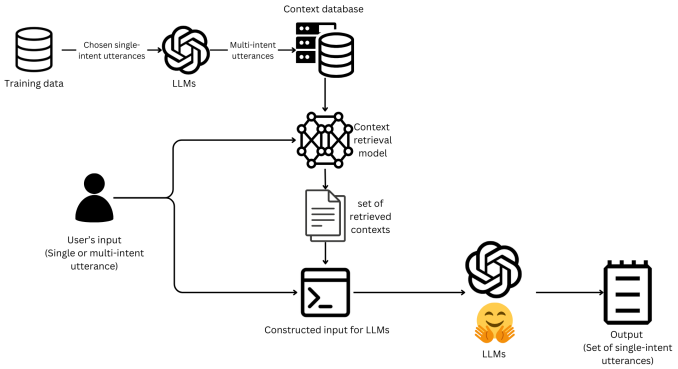


Fig. 4. Overall architecture of the multi-intent utterance splitting module.

a) Context database construction

To build the context dataset, two single-intent commands with different intents are chosen from the VA training dataset and then fed into LLMs to construct a multi-intent command. Along with single-intent commands, a merging instruction snippet is also added into the input of the LLMs to make good multi-intent commands. The example input built for LLMs to create multi-intent commands is shown in Fig. 5.

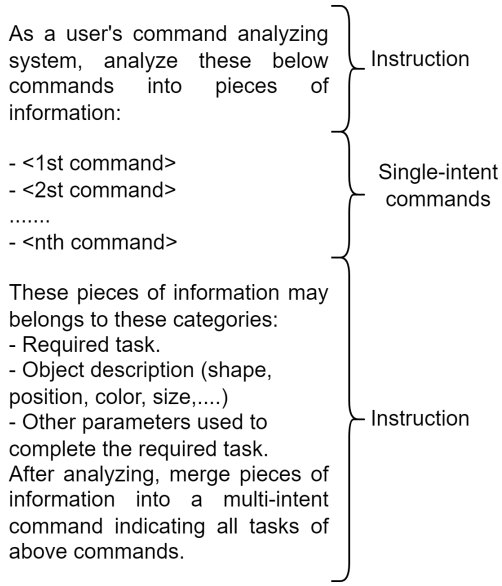


Fig. 5. Example guidance of input for LLMs to create multi-intent commands.

As Fig. 5 shows, it can be seen that the LLMs are required to merge pieces of information extracted from single-intent commands to create multi-intent commands instead of just concatenating single-intent commands by linking words or punctuation. That can make resulting multi-intent commands more diverse and complicated to segment with pieces of information being interleaved, or even become tricky. For example, from the above input and two single-intent commands "Choose all objects on the screen" with intent "select_all_objects" and "Give up choosing all cirles" with intent "exit_select", the LLMs can generate a multi-intent command "Choose all

objects on the screen, except for circles". At first glance, this multi-intent command has only one intent, but to complete the required task, the visual assistant has to select all objects, then give up selecting all circles. However, this kind of input can make LLMs potentially align information incorrectly, or even get rid of some of the information of single-intent utterances. Furthermore, due to the lack of reference examples of inputs and expected outputs, the output in reality of LLMs is usually unstable, making post-processing challenging.

To overcome these drawbacks, some reference examples are added to the input for LLM to stabilize its inference process. Two types of reference examples we used are basic examples (normal few-shot) and advanced examples (Chain-of-thought few-shot, also known as CoT few-shot) which are listed in Fig. 6 and 7, respectively.

```
Input:
- Draw a black circle at coordinates (20, 40).
- Paint the red for its background
Output: Draw a black circle at coordinates (20, 40) then paint
the red for its background

Input:
- Draw a square whose size is 40 x 40 pixel square at the
center of the screen.
- Draw a circle whose size is 40 x 40 pixel square at the top left
corner of the screen.
Output: Draw a square and a circle with the same size of 40 x
40 pixel square at the center and the top left corner of screen,
respectively.

Input:
- Draw an arrow whose length and width are 70 and 30 pixel
respectively the the left side of the screen.
- Make a copy
- Paste the copy in the center of the screen.
Output: Draw an arrow whose length and width are 70 and 30
pixel respectively the the left side of the screen, make a copy
then paste it in the center of the screen.
```

Fig. 6. Basic examples added into input of LLM as references to make its inference process more stable.

```
Input:
- Draw a black circle at coordinates (20, 40).
- Paint the red for the background of the black circle at
coordinates (20, 40).
Output:
Analysis:
- Sentence 1: Task: Draw object, object shape: circle, object
color: black, object position: (20, 40).
- Sentence 2: Task: Color background, object shape: circle,
object color: black, object position: (20, 40).
Merge and create new command: Draw a black circle at
coordinates (20, 40) then paint the red for its background.

Input:
- Draw a square whose size is 40 x 40 pixels at the center of
the screen.
- Draw a circle whose size is 40 x 40 pixels square at the top
left corner of the screen.
Output:
Analysis:
- Sentence 1: Task: Draw object, object shape: square, object
size: 40 x 40, object position: center of the screen.
- Sentence 2: Task: Draw object, object shape: circle, object
size: 40 x 40, object position: top left corner of the screen.
Merge and create new command: Draw a square and a circle
with the same size of 40 x 40 pixels at the center and the top
left corner of screen, respectively.

Input:
- Draw an arrow whose length and width are 70 and 30 pixel
respectively on the the left side of the screen.
- Make a copy
- Paste the copy in the center of the screen.
Output:
Analysis:
- Sentence 1: Task: Draw object, object shape: arrow, object
size: 70 pixel long and 30 pixel wide, object position: left side of
the screen.
- Sentence 2: Task: Copy object.
- Sentence 3: Task: Paste, position: center of the screen.
Merge and create new command: Draw an arrow whose length
and width are 70 and 30 pixel respectively on the left side of
the screen, make a copy then paste it in the center of the
screen.
```

Fig. 7. Advanced examples added into input of LLM as references to make its inference process more stable.

While basic examples just contain input (a list of single-intent utterances) and corresponding output (multi-intent utterance), advanced examples contain interpretation for the output, apart from input and output. With the two types of examples, the resulting multi-intent commands generated by LLMs are more stable and can contain all the information of single-intent commands, but seem to be monotonic in term of information presentation. As a result, we have used all three types of inputs to build context database in the experiment. Particularly, the basic input with no example is called "zero-shot merging", the input with simple examples is called "few-shot merging" and the input with analyzing examples is called "few-shot CoT merging".

In the work, we build multi-intent commands by combining two single-intent commands with different intents. Furthermore, five single-intent commands of each intent are also randomly chosen from training data in order that module can detect single-intent command.

Context retrieval model construction

The target of context retrieval is to provide LLMs with informative examples to refer to, thus allowing LLMs to process users's input accurately and give the correct output for other modules of VAs. As a result, retrieved contexts need to be greatly similar to the user's input. To be able to retrieve these contexts, the model is designed to solve the Semantic Textual Similarity (STS) task. The input of this task contains two text sequences, and the output is the similarity score between the two sequences. The model instruction process consists of two parts: STS dataset building and model training on the STS dataset.

STS dataset building: To build a STS dataset, the two inputs of each sample in this dataset are chosen arbitrarily from the previously built context dataset, and the output (similarity score of two input sentences) is identified by the intents included in each input sentence. The equation used to compute the similarity score is below:

$$\text{sim\_score} = \begin{cases} 1.0 & \text{if} \quad a_1 = b_1 \text{ and } a_2 = b_2 \\ 0.75 & \text{if} \quad a_1 = b_2 \text{ and } a_2 = b_1 \\ 0.5 & \text{if} \quad \begin{array}{l} a_1 = b_1 \text{ and } a_2 \neq b_2 \text{ or} \\ a_1 \neq b_1 \text{ and } a_2 = b_2 \end{array} \\ 0.25 & \text{if} \quad \begin{array}{l} a_1 = b_2 \text{ and } a_2 \neq b_1 \text{ or} \\ a_1 \neq b_2 \text{ and } a_2 = b_1 \end{array} \\ 0.0 & \text{otherwise} \end{cases} \tag{2}$$

Where a_1, a_2 are the first and the second intent of the first multi-intent command and and b_1 and b_2 are the first and the second intent of the second multi-intent command. This equation is applied in the case that both input sentences are bi-intent commands, which make up the majority of the context dataset. In the case that both input sentences are single-intent commands, the assigned similarity value is 1.0 if the intents of both sentences are the same and 0.0 in the other case. If one of the input sentences is single-intent and the other is bi-intent, the assigned value is 0.25 if the intent of the single-intent command is the same as one of the intents of the bi-intent command and 0.0 in other cases. The reason why the maximum similarity value between two sentences with different numbers of intents (1 intent compared to 2 intents) is just 0.25 is that in some cases, multi-intent commands and single-intent commands can be greatly similar to each other. e.g. "Let's move the red square to the left for 10 pixels, then flip it horizontally" and "Let's move the red square to the left for 10 pixels." If the user's input is the same as the example multi-intent command and the result of the retrieval model is the same as the example single-intent sentence, the module is likely to segment the user's input incorrectly. As a result, by setting a low similarity value for couples of sentences with different numbers of intents, especially between single-intent commands and multi-intent commands, being trained on that dataset can allow the retrieval model to be capable of clearly discriminating between single-intent and multi-intent commands.

Context retrieval model building and training: The module trained on the previously built STS dataset is a variant of the sentence-BERT [23]. In this model, we use $\text{MEAN}_{pooling}$ pooling layer to get the sentence vector from the hidden state matrix encoded from the input sentence by BERT model. The loss function used to optimize the retrieval model is Mean Square Error (MSE) loss.

LLMs input construction: To build a complete input for LLMs, contexts with great similarity with the user's input need to be retrieved. To get these contexts, all contexts in the context dataset are encoded by the context retrieval model, which has been trained in the previous stage to get their semantic representative vectors. This collection of vectors, along with raw contexts, is then stored in a database. The vector obtained by encoding the user's input is used to compute the similarity value between it and other contexts to get the most suitable context.

3) Generate the JSON file for SF

After the multi-intent command handling module separates the user's command into a list of single-intent commands, that list of commands is fed into the VA one by one. After each command is processed, the intent and entity values extracted from that command are obtained and postprocessed. After post-processing, intent and entity values are filled into a pre-defined form whose keys are intent and entity names. For entity names with no corresponding entity values extracted from the user's utterance, their value is assigned $NULL$ value. Finally, this form is stored in a JSON file and sent to the SF by calling its API. The Fig. 8 shows the content of the JSON file obtained from the Vietnamese user's input, which is a multi-intent command, and how the required tasks are done directly on the user interface of the SF.

IV. Experiments

In this section, we conduct the experiment of our proposed method on Vietnamese, which is a low-resource language. The first describes the training and testing datasets for VA, then presents the configuration settings and evaluation metrics. Next, we show the archived results, and finally, we present some discussions related to the results of the experiment.

A. Experimental Datasets

1) Experiment datasets for evaluating the quality of semi-automatically built data and the performance of VA

Our dataset includes 3240 labeled commands (or 3240 samples). It is made up of a manually built dataset of 540 samples and a semi-automatically built dataset of 2700 samples. We split this dataset into two subsets: the training dataset and the testing dataset.

a) Testing dataset

It is denoted $\textbf{NLU}_{test}$ including 360 samples that are randomly taken from the manually built dataset, such that 10 samples of each intent type.

b) Training dataset

It includes 2880 remaining samples (denote $\textbf{NLU}_{train}$) divided into six different training datasets. Dataset are denoted as $\textbf{NLU}_n$ means we take the n first samples of each intent type in $\textbf{NLU}_{train}$ for making it. Statistics of these datasets are shown in Table I.

TABLE I. Statistics of the Command Numbers in Each Dataset

Datasets	Number of samples
$\textbf{NLU}_{test}$	360
$\textbf{NLU}_{40}$	1440
$\textbf{NLU}_{50}$	1800
$\textbf{NLU}_{60}$	2160
$\textbf{NLU}_{70}$	2520
$\textbf{NLU}_{train}$	2880

2) Experiment datasets for evaluating the performance of multi-intent handling module

The multiple context datasets are made by choosing data from $\textbf{NLU}_{train}$ dataset by different context-building methods. Particularly, the context datasets made by Zero-Shot Merging, Few-Shot Merging and Few-Shot CoT Merging methods are called $\textbf{Context}_{zero-shot}$, $\textbf{Context}_{few-shot}$ and $\textbf{Context}_{few-shot\,CoT}$ respectively. Each of these context datasets contains 2696 samples, including 180 single-intent commands and 2516 multi-intent commands.

a) Testing dataset

Our context testing dataset, called $\textbf{Context}_{test}$, contains 1754 samples, including 1662 multi-intent commands and 92 single-intent commands. It is built based on all three merging methods with single-intent commands taken from $\textbf{NLU}_{test}$ dataset. After that, all incorrect and duplicated samples are removed.

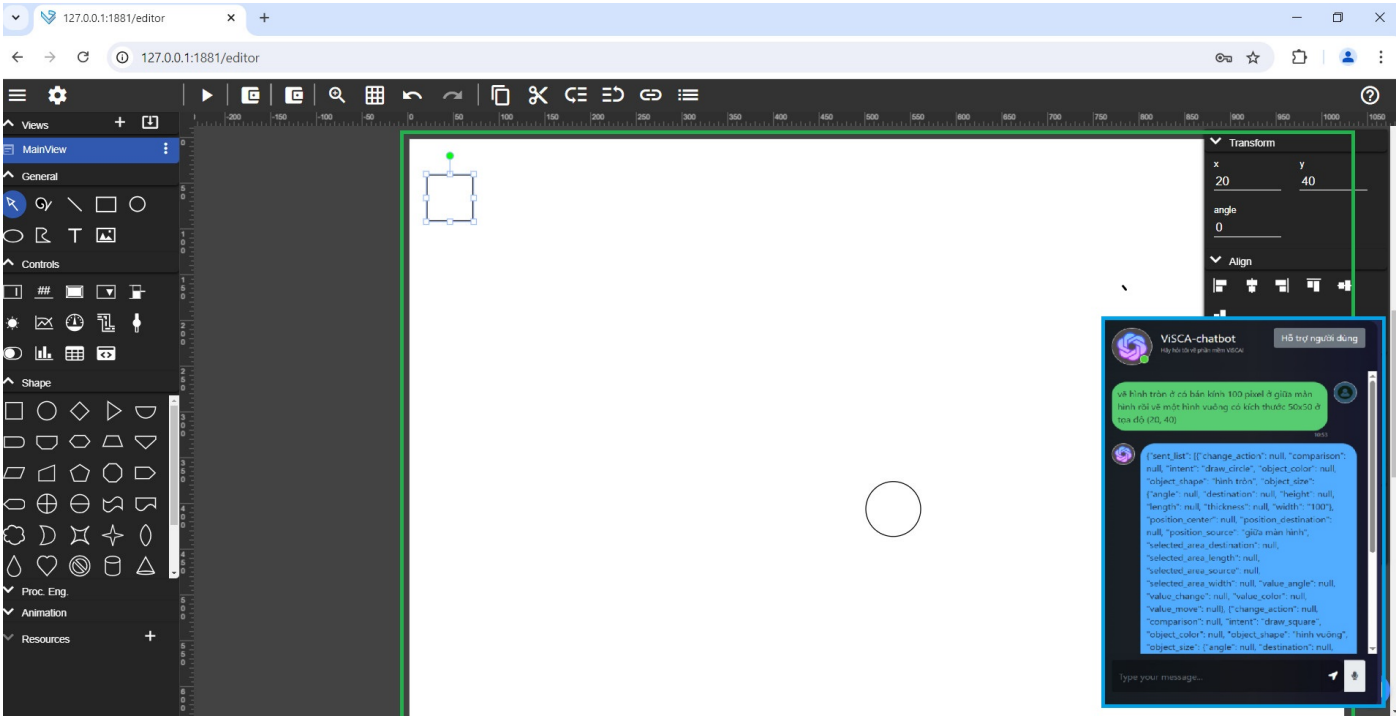


Fig. 8. The user's command which has the English translation text : "draw a circle with radius of 100 pixels at the center of the screen, then draw a square with size of 50 x 50 pixels at the coordinates (20, 40)" and the content of the obtained JSON file after VA handles the command are shown in the box 1 (surrounded by the thick blue border). The result after sending the JSON file to the SF by calling its API are shown in the box 2 (surrounded by the thin green line).

b) Training dataset

The STS datasets used to train context retrieval models is built by choosing two samples randomly from the corresponding context datasets. However, if all combinations of two samples are chosen, the STS training datasets will become very large and imbalanced in term of similarity value. Particularly, each of STS training datasets will have over 3,632,860 samples in total, including over three million samples with Intent Label Similarity Value of 0 (ILSV0). As a result, only a specific number of samples with ILSV0 chosen randomly. Particularly, each of the three training datasets contains 770,926 samples in total. Table II shows the statistics of each STS training dataset in terms of Intent Label Similarity Value.

TABLE II. STATISTICS OF STS TRAINING DATASET

Similarity value	Number of samples
1	1618
0.75	2516
0.5	170816
0.25	195976
0.0	400000

Based on three context datasets, namely $\textbf{Context}_{zero-shot}$, $\textbf{Context}_{few-shot}$ and $\textbf{Context}_{zero-shot\,CoT}$, we have built three STS training datasets, namely $\textbf{STS}_{zero-shot}$, $\textbf{STS}_{few-shot}$ and $\textbf{STS}_{few-shot\,CoT}$. Similarly, Sentence-BERT model trained on these datasets is called $\textbf{SBERT}_{zero-shot}$, $\textbf{SBERT}_{few-shot}$ and $\textbf{SBERT}_{few-shot\,CoT}$.

c) STS Validation dataset

To evaluate the training process of each Sentence-BERT model, a STS validation dataset, called $\textbf{STS}_{valid}$, is also created based on $\textbf{Context}_{test}$ dataset. Its samples are created by all three merging methods, then filtered manually to get rid of incorrect and duplicated ones. This dataset contains 31,763 samples in total. The below Table III shows the statistics of the $\textbf{STS}_{valid}$ in terms of Intent Label Similarity Value.

TABLE III. STATISTICS OF THE STS VALIDATION DATASET

Similarity values	Number of samples
1	638
0.75	1125
0.5	5000
0.25	5000
0.0	20000

B. Experimental Setup

1) Configuration setup

a) Hardware configuration

Both the NLU module and multi-intent handling module are trained on GTX 3090 GPUs (24GB VRAM). The training processes of the two models can take up to 20 GB of VRAM.

b) Model configuration

In the VA, we have used DIETClassifier model [4] with some customization on its components. Particularly, we use

Bag-Of-Word (BOW) method with vocabulary built by n-grams whose length is from 1 to 5 characters as the main sparse featurizer for the model.

For dense featurizer, we use two methods. First, we use phoBERT pretrained model [16] to get dense features from input tokens and its vector output from the special token "¡s¿" acts as the sentence feature of the model. The DIETClassifier model using this dense featurizer is called **DIET**$_{pB+BOW}$. The second method, inspired by an existing work of [7], uses the Fasttext model [8] pretrained on the Vietnamese dataset[§] as the main dense featurizer and the sentence feature is computed by averaging all dense features obtained from input tokens. The DIETClassifier model with that dense featurizer is called **DIET**$_{Ft+BOW}$. In the last model configuration, we do not use any dense featurizer, thus is called **DIET**$_{BOW}$. The number of Transformer layers and the number of attention heads in each Transformers layer used in all configurations are two and four, respectively.

Furthemore, in order to evaluate the effectiveness of using Vietnamese pretrained language models as dense featurizers, we have also used a DIETClassifier model with no dense featurizer and compared its performance with the above two DIETClassifier models.

c) Training configuration

In experiments evaluating VA, we have trained DIETClassifier model on training dataset for 100 epochs with batch size of 16 and the learning rate of 0.001. The loss function we used to optimize the model is Cross Entropy and the optimizer used to adjust the learning process is AdamW optimizer.

In experiments evaluating the multi-intent handling module, we have trained Sentence-BERT model on training dataset for 20 epochs with batch size of 16 and the learning rate of 0.25×10^{-4}. The loss function we used to optimize the model is Mean Square Error and the optimizer used to adjust the learning process is AdamW optimizer. Furthermore, to evaluate the contribution of the context retrieval model, we have also used a LLM (called Baseline) with static contexts, containing three single-intent commands and four multi-intent commands, and compared it with LLMs using the above context retrieval model.

2) Evaluation metrics

a) VA evaluation metrics

The two tasks used to evaluate performance of NLU module are IC and EE. Two main metric used in two tasks are Accuracy and F1.

b) Multi-intent handling evaluation metrics

Firstly, to evaluate the training process of context retrieval model when being trained on different STS training datasets, we have used Spearman's rank correlation coefficient. Secondly, in the experiment evaluating the overall performance of multi-intent handling module, we have used various metrics.

Secondly, to evaluate the output single-intent commands of the module, we have concatenated the two lists of output single-intent commands and ground-truth single-intent commands with the special token "¡SEP¿" into two single strings and used BLEU [3] and ROUGE [22]. Furthermore, we have also used 2 metrics named Split Accuracy (SACC) and Exact Match (EM) proposed by [28]. In the original paper, SACC is used to measure the ratio of correct command splitting and computed the following Eq. (3):

$$\text{SACC} = \frac{1}{n} \sum_{1 \le i \le n} \mathbb{I}_{(\text{len}(Q_{pred}^{(i)}) = \text{len}(Q_{ref}^{(i)}))} \tag{3}$$

Where n is the number of samples, $Q_{pred}^{(i)}$ and $Q_{ref}^{(i)}$ are the i^{th} predicted and references single-intent command list, respectively. As for EM, [28] considered the correct result if the predicted command is exactly the same as the reference one:

$$\text{EM} = \frac{\sum_i \sum_j F(Q_{pred}^{(ij)}, Q_{ref}^{(ij)})}{\sum_{1 \le i \le n} len(Q_{ref}^{(i)})} \tag{4}$$

Where $Q_{pred}^{(ij)}$ and $Q_{ref}^{(ij)}$ are the j^{th} predicted single-intent command and ground-truth single-intent command in the i^{th} sample in the evaluation dataset. The function $F(Q_{pred}^{(ij)}, Q_{ref}^{(ij)})$ in the above equation is the indicator function:

$$F(Q_{pred}^{(ij)}, Q_{ref}^{(ij)}) = \mathbb{I}_{(Q_{pred}^{(ij)} = Q_{ref}^{(ij)})} \tag{5}$$

However, applying the metric EM directly in our experiment is not suitable. We have seen that our merging methods only retain the essential information of the merged single-intent commands (considered as ground-truth commands in an evaluation sample) and get rid of their writing style, e.g. formal, informal, or even humorous, in the resulting multi-intent command. As a result, the output single-intent commands that are predicted by the multi-intent handling module are mostly different from the ground-truth, which means the metric EM cannot make an accurate evaluation. As a result, apart from EM metric, we proposed a new metric called proportional match (PM), which modifies the F function in EM. This new metric is used to measure the accuracy in the essential information of predicted single-intent commands. The F function in the metric is computed by Eq. (6):

$$F(Q_{pred}^{(ij)}, Q_{ref}^{(ij)}) = \begin{cases} 0 & \text{if } \begin{array}{l} \exists k \in D_{ref}^{(ij)} \text{ and} \\ D_{ref_k}^{(ij)} \neq NULL \text{ and} \\ D_{ref_k}^{(ij)} \neq D_{pred_k}^{(ij)} \end{array} \\ 1 & \text{otherwise} \end{cases} \tag{6}$$

Where $D_{pred}^{(ij)}$ and $D_{ref}^{(ij)}$ are the dictionaries containing the intents and entity values extracted from $Q_{pred}^{(ij)}$ and $Q_{ref}^{(ij)}$ respectively by the VA (trained on the overall dataset). k is the key in $D_{pred}^{(ij)}$ and D_{ref}^{ij}. The condition that $D_{ref}^{(ij)} \neq NULL$ is set to get rid of abundant information, which appears very common in almost every sample of the evaluation dataset.

[§]https://huggingface.co/facebook/fasttext-vi-vectors

C. Experimental Results

1) VA experimental result

We conducted an evaluation of all three DIETClassifier models that are trained on the same $\mathbf{NLU}_{40}$ training dataset on the $\mathbf{NLU}_{test}$ testing dataset. The $\mathbf{DIET}_{pB+BOW}$ is chosen for our proposed method (called **Our model**). The results are shown in Table IV.

TABLE IV. RESULT OF DIETCLASSIFIER MODELS ON $\mathbf{NLU}_{test}$

Model	IC		EE	
	F1	Acc	F1	Acc
Our model	**0.93**	**0.93**	**0.96**	**0.98**
$\mathbf{DIET}_{Ft+BOW}$	0.92	0.92	0.96	0.98
$\mathbf{DIET}_{BOW}$	0.92	0.92	0.95	0.97

Table IV shows our model achieved the best performance for both IC and EE tasks on the NLU_{test}.

In order to know the quality of the our semi-automatically built datasets, we used **Our model** to train on **NLU** datasets. The results are shown in Table V.

TABLE V. RESULTS OF $\mathbf{DIET}_{pB+BOW}$ MODEL ON $\mathbf{NLU}_{test}$

Training dataset	IC		EE	
	F1	Acc	F1	Acc
$\mathbf{NLU}_{40}$	0.93	0.93	0.96	0.98
$\mathbf{NLU}_{50}$	0.94	0.93	0.96	0.98
$\mathbf{NLU}_{60}$	0.94	0.93	0.97	0.98
$\mathbf{NLU}_{70}$	0.95	0.95	0.97	0.98
$\mathbf{NLU}_{train}$	**0.96**	**0.96**	**0.97**	**0.99**

2) Multi-intent handling experimental result

Fig. 9 shows the result of three sentence-BERT on $\mathbf{STS}_{valid}$ throughout their training processes.

Tables VI and VII show the BLEU, ROUGE SACC, EM and PM score of the multi-intent handling module using static contexts and different context retrieval models. The $\mathbf{SBERT}_{few-shot\,COT}$ is chosen in our proposed method.

D. Discussion

1) Our semi-automatically data built method and VA

Table V shows that the model is trained on the training dataset $\mathbf{NLU}_{40}$ includes 180 samples made manually and 1260 samples made by our proposed method that achieved a 0.93 F1 and Acc score in the IC task and a 0.96 F1 and 0.98 Acc score in the EE task. This demonstrates that our data is of high quality, and the VA we made works so well.

The dataset $\mathbf{NLU}_{train}$ is made by adding 1440 samples is built by our proposed method to $\mathbf{NLU}_{40}$. The model is trained on $\mathbf{NLU}_{train}$ achieved F1 and Acc score are higher than the model is trained on demonstrates our proposed semi-automatically data building method is a good method. Especially its ability to update itself with new data to become better.

2) Multi-intent handling experiment

In the first experiment evaluating the performance of sentence-BERT models on $\mathbf{STS}_{valid}$ throughout their training process shown in Fig. 9, it can be clearly seen that the best performance that all three models can achieve converges at a result of 0.82. Their convergence speeds, however, differ greatly from each other. The model $\mathbf{SBERT}_{zero-shot}$ trained on $\mathbf{STS}_{zero-shot}$ dataset converges much slower than the other two sentence-BERT models when needing about 100 training steps to converge compared to just about 30 to 50 training steps of $\mathbf{SBERT}_{few-shot}$ and $\mathbf{SBERT}_{few-shot\,COT}$. The reason for its slow convergence speed is because its training dataset $\mathbf{STS}_{zero-shot}$ is built from the context dataset $\mathbf{Context}_{zero-shot}$ which has plenty of false multi-intent commands. Fig. 10 shows some examples of these kinds of commands in the $\mathbf{Context}_{zero-shot}$ dataset.

The false multi-intent commands shown in the "merged multi-intent commands" column in the Table X are actually single-intent commands. When this kind of command is matched with true multi-intent commands in the dataset, it will make the false sample in the STS dataset used to train the context retrieval dataset, thus making the training process of the model divergent.

In the second experiment shown in Tables VI and VII which evaluates the performance of multi-intent handling module when using trained context retrieval models compared to using static contexts with various metrics, it can be clearly seen that the performance of multi-intent handling module using trained context retrieval models is relatively higher than one of multi-intent handling module using static context in every metric, emphasizing the great contribution of context retrieval models trained on STS training datasets to the performance of multi-intent handling module. In Table VI, the difference in ROUGE in BLEU metric between the worst-performing model (Baseline model) and the best-performing model ($\mathbf{SBERT}_{few-shot\,COT}$) is not really notable, ranging around 0.02 and 0.04. We hypothesize that we have concatenated the output single-intent command list into a single string and evaluated on this concatenated string so that the evaluated strings of different models may be similar to each other in some substrings. The results in SACC, EM and PM metrics shown in Table VII, on the other hand, see a significant gap between the worst-performing and the best-performing model, ranging from 0.04-0.05. Furthermore, what we can clearly see in that table is that the gap between the results of multi-intent handling module using a trained context retrieval model is pretty trivial, indicating that with contexts that are relatively similar to the user's input, the LLMs can accurately split the input into single-intent commands in terms of intent and assign the correct information to each of the output commands.

To investigate the capability of multi-intent handling in single-intent and multi-intent command detection, we have conducted two additional experiments for the module with different configurations on single-intent commands and multi-intent commands separately. The Tables VIII and IX show the results in SACC metric of the two experiments.

In Table VIII, the multi-intent handling module using $\mathbf{SBERT}_{zero-shot}$ as context retrieval model archives the worst result, even much worse than the Baseline module. This

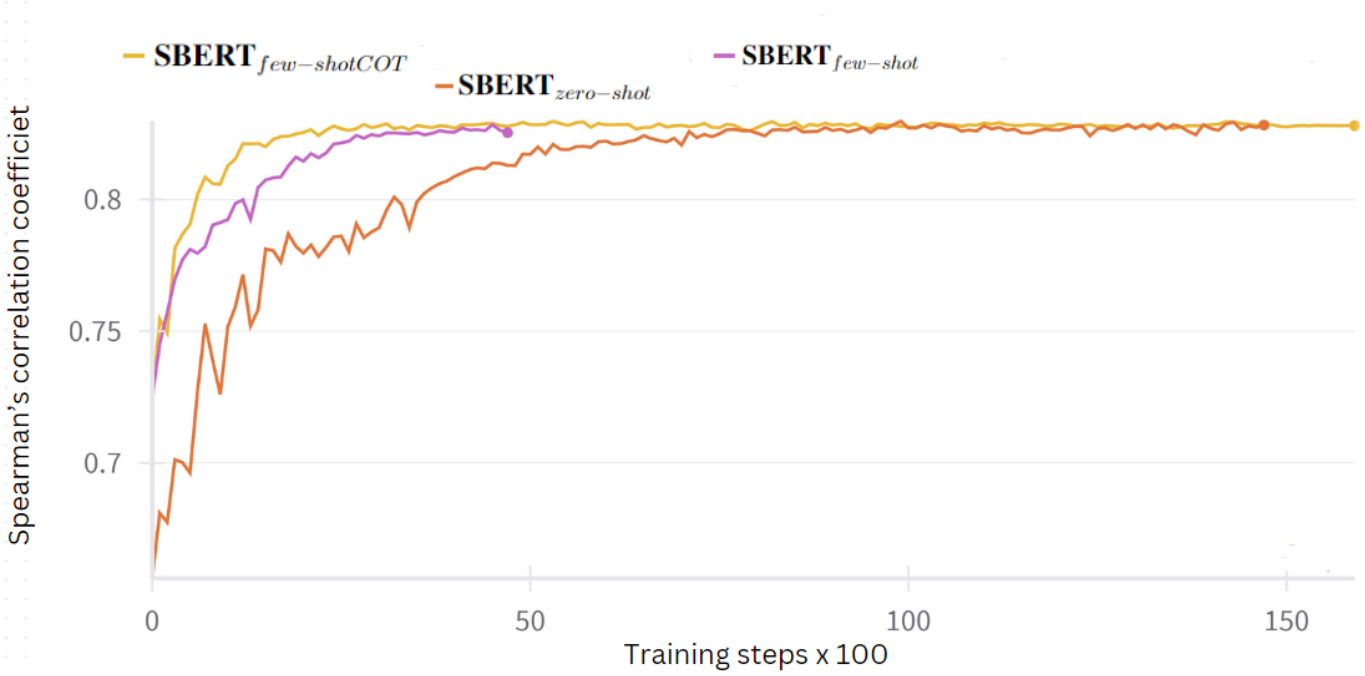


Fig. 9. Spearman's correlation coefficient of three sentence-BERT models trained on three different STS datasets

TABLE VI. ROUGE AND BLEU SCORE OF MULTI-INTENT HANDLING MODULE USING STATIC CONTEXTS AND DIFFERENT CONTEXT RETRIEVAL MODELS

Model	ROUGE-1	ROUGE-2	ROUGE-L	ROUGE-S	BLEU
Baseline	0.87	0.81	0.84	0.84	0.7
SBERT$_{zero-shot}$	0.89	0.83	0.85	0.85	0.74
SBERT$_{few-shot}$	0.89	0.83	0.86	0.86	0.74
SBERT$_{few-shot\ COT}$	**0.9**	**0.84**	**0.86**	**0.86**	**0.75**

TABLE VII. SACC, EM AND PM OF MULTI-INTENT HANDLING MODULE USING STATIC CONTEXTS AND DIFFERENT CONTEXT RETRIEVAL MODELS

Model	SACC	EM	PM
Baseline	0.87	0.75	0.83
SBERT$_{zero-shot}$	**0.93**	**0.79**	**0.87**
SBERT$_{few-shot}$	0.90	0.79	0.86
SBERT$_{few-shot\ COT}$	0.92	0.79	0.87

TABLE VIII. THE RESULT IN SACC METRIC ON SINGLE-INTENT COMMANDS OF THE EVALUATION DATASET

Module	SACC Score
Baseline	0.93
SBERT$_{zero-shot}$	0.85
SBERT$_{few-shot}$	0.94
SBERT$_{few-shot\ COT}$	**0.96**

TABLE IX. THE RESULT IN SACC METRIC ON MULTI-INTENT COMMANDS OF THE EVALUATION DATASET

Module	SACC Score
Baseline	0.87
SBERT$_{zero-shot}$	**0.94**
SBERT$_{few-shot}$	0.91
SBERT$_{few-shotCOT}$	0.92

is due to the false multi-intent commands in its context database, as mentioned in Fig. 10. That makes the model likely to retrieve true multi-intent commands when receiving the single-intent command of the user, leading to the wrong segmentation. In contrast, the multi-intent handling module using **SBERT**$_{zero-shot}$ as context retrieval model achieves the best result, and the gap between the modules using trained context retrieval models is relatively trivial. This is due to the majority of multi-intent commands in the evaluation dataset being simple commands that have single-intent commands linked by linking words and punctuation, which appear very common in all three context datasets. The remaining multi-intent commands in the evaluation dataset, however, have information interleaved or even tricky to assign to an intent. The **Context**$_{zero-shot}$ context dataset can have many complex multi-intent commands due to the lack of reference examples in the Zero-shot merging method, which is used to generate multi-intent commands in that dataset, thus making LLMs likely to generate out-of-the-box commands with no limit.

V. CONCLUSION

In this work, we have proposed the effective method for recognizing multi-intent commands in low-resource languages and respond to SF in doing the drawing task. In the phase of data building, we proposed a semi-automatic data building

Single-intent commands:
- Chọn tất cả các đối tượng nền
(Choose all objects on the background)
- Tăng chiều dài đường thẳng màu xanh dương tại vị trí hiện tại lên 18 pixel
(Increase the length of the blue line at the current position by 18 pixels)

=> Merged multi-intent command:
- Tăng chiều dài của tất cả các đường thẳng màu xanh dương trên đối tượng nền lên 18 pixel
(Change the length of all blue line on the background by 18 pixel .)

Single-intent commands:
- Thay đổi kích thước chiều dài của đường thẳng màu tím nằm giữa hai hình tam giác thêm 18 pixel
(Set the length of the purple line laying between 2 triangles by increasing by 18 pixels.)
- chọn tất cả các đối tượng có cùng màu xanh dương.
(Choose all object that have color blue.)

=> Merged multi-intent command:
- Thay đổi kích thước chiều dài của đường thẳng màu tím nằm giữa hai hình tam giác thêm 18 pixel .
(Set the length of the purple line laying between 2 triangles by increasing it by 18 pixels .)

Single-intent commands:
- Giảm chiều cao của hình thoi trắng bằng cách thu nhỏ kích thước tỷ lệ 70 %
(Decrease the height of the white triangle by sinking its size to 70 %)
- Xin vui lòng bôi đen toàn bộ các đối tượng hiện đang có.
(Choose all objects on the screen, please.)

=> Merged multi-intent command:
- Thu nhỏ chiều cao của hình thoi trắng đi 70 %
(Sinking the height of the white triangle to 70 %)

Fig. 10. False multi-intent commands in the $\textbf{Context}_{zero-shot}$ dataset.

method. Applying it to the Vietnamese language, we built an intent list including 36 intents, an entity list including 31 entities, and the labeled Vietnamese command corpus including 3240 commands. In the phase of generating the JSON file, we proposed the method that separates the multi-intent command from the user's command into single-intent commands to be better understood by the VA, from which it supports more effectively for SF. Our labeled command corpus and the open source code of the splitting tool are shared with the research community. In the future, we will continue to research and improve our data construction method and extend it to some low-resource languages. Furthermore, we will conduct research to improve the capabilities and accuracy of the VA problem.

ACKNOWLEDGMENT

This work has been supported by the Vietnamese government under Program KC-4.0-30/19-25.

REFERENCES

[1] Ahuja, Sanju, and Jyoti Kumar. Assistant or Master: Envisioning the User Autonomy Implications of VAs. In Proceedings of the 4th Conference on Conversational User Interfaces, pp. 1-5. 2022. DOI: 10.1145/3543829.3544514.

[2] Charles Hemphill, John Godfrey, and George Doddington. The ATIS Spoken Language Systems Pilot Corpus. Speech and Natural Language: Proceedings of a Workshop Held at Hidden Valley, Pennsylvania, June 24-27,1990. New York, NY, USA. 1990.

[3] Kishore Papineni, Salim Roukos, Todd Ward, and Wei-Jing Zhu. Bleu: a method for automatic evaluation of machine translation. Proceedings of the 40th annual meeting of the Association for Computational Linguistics, pp. 311–318. New York, NY, USA. 2002.

[4] Tanja Bunk, Daksh Varshneya, Vladimir Vlasov, and Alan Nichol. DIET: Lightweight Language Understanding for Dialogue Systems. arXiv, pp. arXiv:2004.09936. New York, NY, USA. 2020.

[5] Brambilla, M., Molinelli, D. (2021). Voice-Based Virtual Assistants for User Interaction Modeling. In: Brambilla, M., Chbeir, R., Frasincar, F., Manolescu, I. (eds) Web Engineering. ICWE 2021. Lecture Notes in Computer Science(), vol 12706. Springer, Cham.

[6] Jiawei Han, Micheline Kamber, and Jian Pei. Data mining concepts and techniques third edition. University of Illinois at Urbana-Champaign Micheline Kamber Jian Pei Simon Fraser University. New York, NY, USA. 2012.

[7] Trang Mai and Shcherbakov Maxim. Enhancing Rasa NLU model for Vietnamese chatbot. International Journal of Open Information Technologies, vol. 9, no. 1, pp. 31–36. New York, NY, USA. 2021.

[8] Edouard Grave, Piotr Bojanowski, Prakhar Gupta, Armand Joulin, and Tomas Mikolov. Learning word vectors for 157 languages. arXiv, pp. arXiv:1802.06893. New York, NY, USA. 2018.

[9] S. Cobos-Guzman, S. Nuere, L. Miguel, and C. König. Design of a VA to Improve Interaction Between the Audience and the Presenter. International Journal of Interactive Multimedia and Artificial Intelligence, ch. 7, sec. 2, pp. 232-240. New York, NY, USA. 2021. DOI: https://dx.doi.org/10.9781/ijimai.2021.08.017

[10] Hoy, Matthew B. Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants. *Medical reference services quarterly*, vol. 37, ch. 1, pp. 81-88. 2018. DOI: 10.1080/02763869.2018.1404391.

[11] Michael McTear, Zoraida Callejas, and David Griol, Talking to Smart Devices. The Conversational Interface. New York, NY, USA. 2016. Springer Publishing Company, Incorporated. https://link.springer.com/book/10.1007/978-3-319-32967-3

[12] Morana, Stefan; Friemel, Celina; Gnewuch, Ulrich; Maedche, Alexander; Pfeiffer, Jella, Interaktion mit smarten Systemen — Aktueller Stand und zukünftige Entwicklungen im Bereich der Nutzerassistenz. Wirtschaftsinformatik & Management, Springer. PISSN: 1867-5913. vol. 9, no. 5, pp. 42-51.

[13] Xingkun Liu, Arash Eshghi, Pawel Swietojanski, and Verena Rieser. Benchmarking natural language understanding services for building conversational agents. Increasing naturalness and flexibility in spoken dialogue interaction: 10th international workshop on spoken dialogue systems, pp. 165–183. New York, NY, USA. 2021.

[14] C. Pearl, Principles of Conversational Experiences. Designing Voice User Interfaces. New York, NY, USA. 2016. O'Reilly Media. https://www.oreilly.com/library/view/designing-voice-user/9781491955406

[15] Pereira R, Lima C, Pinto T, Reis A. Virtual Assistants in Industry 4.0: A Systematic Literature Review. Electronics. 2023; 12(19):4096.

[16] Dat Nguyen and Anh Nguyen. PhoBERT: Pre-trained language models for Vietnamese. arXiv, pp. arXiv:2003.00744. New York, NY, USA. 2020.

[17] Andrés Piñeiro-Martín, Carmen García-Mateo, Laura Docío-Fernández, and María López-Pérez. Ethical Challenges in the Development of VAs Powered by Large Language Models. Electronics, vol. 12, no. 14. New York, NY, USA. 2023. DOI: 10.3390/electronics12143170.

[18] Pérez, Anxo & Lopez-Otero, Paula & Parapar, Javier. Designing an Open Source VA. Proceedings, vol. 54, no. 1, pp. 30. 2020. DOI: 10.3390/proceedings2020054030.

[19] Libo Qin, Xiao Xu, Wanxiang Che, and Ting Liu. AGIF: An Adaptive Graph-Interactive Framework for Joint Multiple Intent Detection and Slot Filling. Findings of the Association for Computational Linguistics: EMNLP 2020, pp. 1807–1816. New York, NY, USA. 2020. Association for Computational Linguistics. DOI:10.18653/v1/2020.findings-emnlp.163.

[20] Tom Bocklisch, Joey Faulkner, Nick Pawlowski, and Alan Nichol. Rasa: Open source language understanding and dialogue management. arXiv, pp. arXiv:1712.05181. New York, NY, USA. 2017.

[21] Barbara Rychalska, Helena Glabska, and Anna Wroblewska. Multi-intent hierarchical natural language understanding for chatbots. 2018 Fifth international conference on social networks analysis, management and security (SNAMS), pp. 256–259. New York, NY, USA. 2018.

[22] Chin-Yew Lin. Rouge: A package for automatic evaluation of summaries. Text summarization branches out, pp. 74–81. New York, NY, USA. 2004.

[23] Nils Reimers and Iryna Gurevych. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. arXiv, pp. arXiv:1908.10084. New York, NY, USA. 2019.

[24] Alice Coucke, Alaa Saade, Adrien Ball, Théodore Bluche, Alexandre Caulier, David Leroy, Clément Doumouro, Thibault Gisselbrecht, Francesco Caltagirone, Thibaut Lavril, and others. Snips voice platform: an embedded spoken language understanding system for private-by-design voice interfaces. arXiv, pp. arXiv:1805.10190. New York, NY, USA. 2018.

[25] Sheng Jiang, Su Zhu, Ruisheng Cao, Qingliang Miao, and Kai Yu. 2023. SPM: A Split-Parsing Method for Joint Multi-Intent Detection and Slot Filling. In Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (Volume 5: Industry Track), pp. 668–675, Toronto, Canada. Association for Computational Linguistics.

[26] Strohmann, T., Siemon, D., & Robra-Bissantz, S. . Designing Virtual In-vehicle Assistants: Design Guidelines for Creating a Convincing User Experience. AIS Transactions on Human-Computer Interaction, ch 11, sec. 2, pp. 54-78. 2019. DOI: 10.17705/1thci.00113.

[27] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. Advances in neural information processing systems, vol. 30. New York, NY, USA. 2017.

[28] Haoran Meng, Zheng Xin, Tianyu Liu, Zizhen Wang, He Feng, Binghuai Lin, Xuemin Zhao, Yunbo Cao, and Zhifang Sui. Dialogusr: Complex dialogue utterance splitting and reformulation for multiple intent detection. arXiv, pp. arXiv:2210.11279. New York, NY, USA. 2022.

[29] VAN DAELE, D.; DECLEYRE, N.; DUBOIS, H.; MEERT, W. An Automated Engineering Assistant: Learning Parsers for Technical Drawings. Proceedings of the AAAI Conference on Artificial Intelligence, [S. l.], v. 35, n. 17, p. 15195-15203, 2021. DOI: 10.1609/aaai.v35i17.17783.

[30] Alec Radford, Jong Kim, Tao Xu, Greg Brockman, Christine McLeavey, and Ilya Sutskever. Robust speech recognition via large-scale weak supervision. International conference on machine learning, pp. 28492–28518. New York, NY, USA. 2023.

APPENDIX

Table X shows all intent labels we have used in our dataset and their meanings.

TABLE X. THE INTENT LABELS AND THEIR MEANING

Intent	Meaning
select_all_object	The user wants to select all object (with optionally the same properties) on the interface of the SF
exit_select	The user wants to give up selecting some (or all) selected objects (with optionally the same properties) on the interface of the SF
delete_selected_objects	The user wants to delete some (or all) selected objects (with optionally the same properties) on the interface of the SF
selected_area	The user wants to select all objects (with optionally the same properties) in an area defined by a pair of coordinates on the interface of the SF
rotate_left	The user wants to rotate a specific object on the interface of the SF to the left side
rotate_right	The user wants to rotate a specific object on the interface of the SF to the right side
horizontal_flip	The user wants to flip a specific object on the interface of the SF horizontally
vertical_flip	The user wants to flip a specific object on the interface of the SF vertically
move_left	The user wants to move a specific object on the interface of the SF to the left side
move_right	The user wants to move a specific object on the interface of the SF to the right side
move_up	The user wants to move a specific object on the interface of the SF upward.
move_down	The user wants to move a specific object on the interface of the SF downwards.
color_background	The user wants to paint the background of a specific object on the interface of the SF by a specific color.
color_foreground	The user wants to paint the foreground of a specific object on the interface of the SF by a specific color.
change_width	The user wants to change the width of a specific object on the interface of the SF.
change_height	The user wants to change the height of a specific object on the interface of the SF.
change_length	The user wants to change the length of a specific object on the interface of the SF.
change_radius	The user wants to change the radius of a specific object on the interface of the SF.
change_top	The user wants to move a specific object on the interface of the SF in the vertical direction so that its new position is a certain distance from the top border of the interface of the SF.
change_left	The user wants to move a specific object on the interface of the SF in the horizontal direction so that its new position is a certain distance from the left border of the interface of the SF.
change_right	The user wants to move a specific object on the interface of the SF in the horizontal direction so that its new position is a certain distance from the right border of the interface of the SF.
change_bottom	The user wants to move a specific object on the interface of the SF in the vertical direction so that its new position is a certain distance from the bottom border of the interface of the SF.
draw_line	The user wants to draw a line on the interface of the SF. The information about attributes of the object is optionally provided. Any attributes with no provided information will be set to its default value.
draw_circle	The user wants to draw a circle on the interface of the SF. The information about attributes of the object is optionally provided. Any attributes with no provided information will be set to its default value.
draw_ellipse	The user wants to draw a ellipse on the interface of the SF. The information about attributes of the object is optionally provided. Any attributes with no provided information will be set to its default value.
draw_rectangle	The user wants to draw a rectangle on the interface of the SF. The information about attributes of the object is optionally provided. Any attributes with no provided information will be set to its default value.
draw_square	The user wants to draw a square on the interface of the SF. The information about attributes of the object is optionally provided. Any attributes with no provided information will be set to its default value.

draw_rhombus	The user wants to draw a rhombus on the interface of the SF. The information about attributes of the object is optionally provided. Any attributes with no provided information will be set to its default value.
draw_parallelogram	The user wants to draw a parallelogram on the interface of the SF. The information about attributes of the object is optionally provided. Any attributes with no provided information will be set to its default value.
draw_trapezoid	The user wants to draw a trapezoid on the interface of the SF. The information about attributes of the object is optionally provided. Any attributes with no provided information will be set to its default value.
draw_arrow	The user wants to draw an arrow on the interface of the SF. The information about attributes of the object is optionally provided. Any attributes with no provided information will be set to its default value.
copy_selected_objects	The user wants to copy all selected objects (with optionally the same properties) to the clipboard.
cut_selected_objects	The user wants to cut all selected objects (with optionally the same properties) and save them into the clipboard.
paste	The user wants to paste the object saved in the clipboard to a certain position on the interface of the SF.
undo	The user wants to undo the task.
redo	The user wants3 to redo the task.

Table XI shows all entity labels which are grouped into entity groups with their meanings.

TABLE XI. ENTITY LABELS AND THEIR MEANINGS

Entity group	Entity	Meaning
Object (used to label phrases describing attributes of the object)	object—shape	Indicates the shape of the object
	object—width	Indicates dimensions like the upper base of a trapezoid, radius of a circle, width of a rectangle, etc.
	object—height	Indicates the height of various shapes such as triangles and parallelograms
	object—length	Indicates the length of various shapes like rectangles, arrows, etc.
	object—color	Indicates the color of the object
	object—thickness	Indicates the thickness of the object's border
	object—destination	Indicates the end point of a line (e.g. center of the screen or top left corner)
	object—angle	Indicates the value of the angle at the top left corner of the object
	object—destination_x	Indicates the x-axis of the end point of the line
	object destination_y	Indicates the y-axis of the end point of the line
Value (used to label phrases indicating essential parameters for specific tasks)	value—color	Indicates the color for tasks like "color_background" and "color_foreground"
	value—change	Indicates changes to the size of an object (e.g. increase, decrease, set new value)
	value—move	Indicates the distance between the new and old positions of the object
	value—angle	Indicates the angle for rotating the object (e.g. "rotate_left", "rotate_right")
Position (used to label phrases indicating the position of the object)	position—source	Indicates the current position of the object, like "top left corner" or "center of the screen"
	position—source_x	Indicates the x-axis of the current position of the object

	position—source_y	Indicates the y-axis of the current position of the object
	position—destination	Indicates the target position for tasks like “paste” or selecting an area
	position—destination_x	Indicates the x-axis of the target position
	position—destination_y	Indicates the y-axis of the target position
	position—center	Indicates the center of the object
	position—center_x	Indicates the x-axis of the object’s center
	position—center_y	Indicates the y-axis of the object’s center
Selected_area (used for “select_area” tasks)	selected_area—height	Indicates the height of the selected area
	selected_area—width	Indicates the width of the selected area
	selected_area—length	Indicates the length of the selected area
Change_action (used for resizing objects)	change_action—increase	Indicates that the user wants to increase the size of the object
	change_action—decrease	Indicates that the user wants to decrease the size of the object
	change_action—set	Indicates that the user wants to set a new size for the object
Aspect	aspect	Used to compare an object with others based on features like size or length
Comparison	comparison	Used to label phrases that compare objects (e.g. “bigger than”, “equal to”)

AudioMag: A Hybrid Audio Protection Scheme in Multilevel DWT-DCT-SVD Transformations for Data Hiding

Jingjin Yu[1], Chai Wen Chuah*[2], Rundan Zheng[3], Janaka Alawatugoda*[4]
Guangdong University of Science & Technology, Dongguang, Guangzhou, China[1,2,3]
Research & Innovation Centers Division, Rabdan Academy Abu Dhabi, UAE[4],
and Institute for Integrated and Intelligent Systems, Griffith University, Nathan, Queensland, Australia[4]

***Abstract*—Steganography is a technique used to hide data within an image or audio in order to maintain the secrecy of the message being communicated. There are several methods used in steganography to achieve this, but commonly, the data hiding is between the same stego-entity, such as an image with an image or audio with audio. One drawback of hiding data within the same entity is that once the security is compromised, one may be able to access the particular data. Therefore, this research proposes hiding audio within an image. The first step is to transform the audio into a hexadecimal value. Next, the hexadecimal value is hidden within the shortened uniform resource locators. The uniform resource locators are concatenated, shuffled, and converted into a quick response code. Finally, the quick response code is embedded into an image. The simulation results show the successful hiding of the audio message within the image, while maintaining the security and confidentiality of the hidden messages.**

Keywords*—Steganography; image steganography; audio steganography; data hiding; stego-entity

I. Introduction

As the rapid growth of the Internet and the bandwidth continues, cryptography is responsible for ensuring secure communication over insecure interconnected networks, guaranteeing transmission privacy and authentication [1], [2]. There are two common methods for sending secret messages: data encryption [3] and data hiding [4], [5]. In the case of an encrypted message, only the intended recipient can view the message by decrypting it with a secret key. Even if an attacker obtains the encrypted message, they will be unable to decipher the content. However, if the key is revealed to the public or stolen by the attacker, the message can be compromised [6]. Data hiding, or steganography, which falls under the cryptography umbrella, is another technique that is widely used to hide secret messages within harmless messages in a way that prevents attackers from detecting the existence of the secret message.

Generally, data hiding includes the process of generating a stego-image (embedding payload into the image), while extraction is the process of viewing the payload from the stego-image [5]. The security level of the stego-image is based on its similarity to the original image, making it difficult for unintended observers to be aware of the existence of the hidden secret message. There are two common types of steganography: audio steganography and image steganography.

Image steganography [8], [9], [10] refers to the process of hiding data within an image file. The image selected for this purpose is known as a cover image, and the image obtained after steganography is called a stego-image. The least significant bit (LSB) technique is one of the simplest approaches by replacing the LSB of each pixel in the cover image with a piece of the hidden data [11], [12]. Since it only involves one bit change in a pixel, the stego-image appears identical to the original image. Hence, these changes will be hard to detect by the human eye, which is not sensitive.

Audio steganography is a technique of inserting hidden messages within sound files [13], [14], [15]. Users can insert a secret message into the audio by manipulating the binary sequence of the file, like adjusting its length or making subtle changes to its structure. This is undetectable to the human senses, as human are not sensitive to the small changes. Common audio steganography sound file formats to date include waveform audio file format (WAV), audio units (AU), and MPEG audio layer 3 (MP3) [16]. The process of embedding secret messages in digital sound is typically more complex than embedding messages in other forms of media, such as digital images.

However, information shared online by individuals often faces various risks, such as being maliciously intercepted by third parties or misused in terms of ownership. Steganography offers effective solutions to address these issues. The objective of this research is to develop and evaluate audio steganography, which conceals audio within images, to enrich people's comprehension beyond the traditional methods of steganography. The significance of utilizing both image and audio steganography lies in taking advantage of the lack of sensitivity of the human ear and eye to subtle changes, which makes it easier to hide communication information and enhances security [17], [18]. This will aid in protecting communication privacy and preventing unauthorized access to the information.

The remainder of this paper is organized as follows: Section II presents the literature review. Section III shows the proposed AudioMag. The AudioMag simulation is shown in section IV. Section V contains the result discussions. Finally, Section VI concludes the paper.

II. Literature Review

Steganography is a technique of hiding secret information in a host, such as an image, audio, or video. The secret information

is known as payload which could be a message, image, or audio. Steganography ensures that this hidden information is not noticeable to anyone who is not specifically looking for it. Therefore, individuals are able to transmit confidential data without raising suspicion through steganography. There are three common techniques for steganography: image steganography and audio steganography.

A. Image Steganography

Vleeschouwer, et al. proposed a method for embedding the payload into the stego-image based on patchwork theory, which has certain robustness against JPEG loosely compression [7]. Loosely compression meant that even though the image being compressed, there will be loss of some information, but with this proposed method, they still are able to retrieve back the payload. The image is divided into two zones. The histogram of each zone is mapped to a circle where it is the place to allocate the payload. That is, each bit of the payload is associated with a group of pixels, for example a block in an image, and then the payload is map into the associate zones. The embedding process hides the payload by changing the whole pixel value of the image. This algorithm suffers from the salt-and-pepper noise. To overcome this problem, this algorithm is suitable for small size of payload with multi-tone image and not suitable for halftone images.

Honsinger's group patent the data hiding technique used for fragile authentication [8]. The method that they carried out is based on adding the payload to original image, pixel by pixel using modulo 256 additions to form the stego-image. This method is comfortable only for those payloads with the capacity in category from 1k to 2k bits. Overall, the process of embedding the payload can be described in two mathematics equation, the first one as $I'(x,y) = I(x,y) + \alpha M(x,y) * C(x,y)$, this formula is used to find the location of payload in original image, where and $I'(x,y)$ is the location of payload in the image, $\alpha M(x,y) * C(x,y)$ denotes as payload coordinate and $I(x,y)$ as location of original image. While the second equation is $Iw = (I+W) \bmod 256$, Iw denotes marked image, I original image, W is the payload comes from the hash function of the original image and the modulo 256 addition ensures that the modified image values are always be in the same range as the original image values. By using these two equations, with first equation they find the location in original image then second equation responsible in avoiding over or underflow happens in stego-image. This technique changes the entire pixel value of the original image, hence, stega-image suffers salt-and-pepper noise.

Chandran and Khoushik compared the efficacy of LSB, discrete cosine transform (DCT), and discrete wavelet transform (DWT) techniques in the context of steganography [9]. The findings indicated that the DCT technique demonstrated superior performance when compared to both LSB and DWT methods. The evaluation was centered on the quality of the stego-image and the original cover image. Limitations of each approach were highlighted, with the LSB method showing weaknesses in terms of invisibility and robustness, the DCT method lacking robustness, and the DWT method exhibiting lower PSNR values and higher MSE.

Moon and Kawitkar proposed data hiding by using four LSB (4 LSB) substitution method and password for advance security [10]. With the protection layer by using password, the user only can view the payload with correct password. Without the password, the user only can get back the cipher text which is the junk characters. And this technique can embed large size of payload. But, stego-image is suffer with noise as well if the original image is halftone image, thus the attackers easily notice that particular image is the stego-image then he can break the password to get the payload.

There are many researchers [11], [12] tend to use LSB method for concealing data by utilizing the least significant bit of the cover image, making it imperceptible to the naked eye. However, this technique is deficient in terms of limited payload capacity.

B. Audio Steganography

Biswajita Datta et al. [13] presented an innovative method that employs LSB encoding across multiple layers, allowing for the simultaneous embedding of two data bits into the cover media to increase stego-audio capacity. The extraction procedure entails bitwise operations, adding complexity to interpreting the data without understanding these operations. Furthermore, techniques such as bit adjustment and flag setting are utilized to maintain the perceptual transparency of the stego-audio.

Sayed et al. [14] investigates the integration of two distinct steganography methods in a multi-level steganography framework. The initial method entails concealing a message in an audio cover through a modified LSB technique, whereas the second method involves concealing a second message in the output of the first level using a phase coding approach. The stego-audio file that results contains two audio covers with concealed messages.

Nugraha explores the utilization of steganography in audio data through the direct sequence spread spectrum technique which transmitting hidden messages via radio waves, where the message is carried by a noise-like wave [15]. This technique can be adapted for concealing messages within audio data, where the embedded information will manifest as noise. The proposed method requires a key to embed messages within the noise, generating a pseudo-noise waveform. Prior to embedding, the information to be hidden must first be modulated using this pseudo-noise signal.

C. Image Processing Methods

1) Discrete Wavelet Transform: Discrete wavelet transform (DWT) decomposes an image into a sequence of images with different spatial resolutions. Fig. 1 shows how the image is decomposed into the first level, resulting in 'LL', 'LH', 'HL' and 'HH'. The second level is then applied to the low frequency 'LL' only, where 'L' represents low frequency bands and 'H' represents high frequency bands. Threshold is applied to the wavelet coefficients in the high frequency levels, as the noise present in the low frequency wavelet coefficients will be averaged out. This calculation can effectively reduce noise without significantly distorting the underlying signal [19].

2) Discrete Cosine Transform: Discrete cosine transform (DCT) converts a series of pixels in an image into a series of frequency domain coefficients [20]. Eq. (1) computes the (i,j)

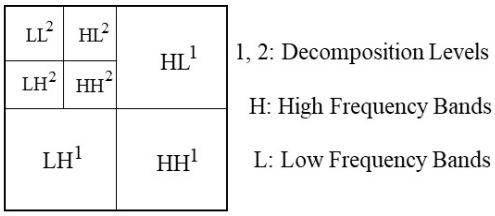


Fig. 1. 2D-DWT with 2-Level decomposition.

entry of the DCT of an image, where i and j are the coordinates of the transformed image. The $p(x, y)$ is the x and y^{th} element of the image, and N is the size of the block calculated by the DCT. Eq. (2) represents a normalization constant.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

$$Y(i,j) = \frac{1}{\sqrt{2K}} C(i)C(j) \sum_{x=0}^{k-1} \sum_{y=0}^{k-1} p(x,y) * \cos\left[\frac{(2x+1)i\pi}{2K}\right] \cos\left[\frac{(2y+1)i\pi}{2K}\right] \quad (1)$$

$$C(b) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{if b = 0} \\ 1, & \text{if b} > 0 \end{cases} \quad (2)$$

The equation computes the value of one specific entry (i, j) in the transformed image by using the pixel values from the original image matrix. For example, in the case of a 4 x 4 block image, the value of N is 4 and the range of x and y is 0 - 3. Therefore, $Y(i, j)$ is determined based on Eq. (3).

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

$$Y(i,j) = \frac{1}{\sqrt{8}} C(i)C(j) \sum_{x=0}^{3} \sum_{y=0}^{3} p(x,y) * \cos\left[\frac{(2x+1)i\pi}{8}\right] \cos\left[\frac{(2y+1)i\pi}{8}\right] \quad (3)$$

3) Singular Value Decomposition: Singular Value Decomposition (SVD) manipulates the original image into three different matrices as shown in Eq. (4) [21]. A is original M X N matrix, U is the M X R matrix with orthonormal columns matrix, σ is the R X R diagonal matrix of singular values, and V^T is the transpose orthonormal columns matrix with dimension of R X N. It should be noted that, M, N, and R are the dimensions of the original matrix A.

$$A = U\sigma V^T \quad (4)$$

D. Caesar Cipher

Caesar cipher is one of the simplest and most widely known encoding and decoding techniques. The encoding [see Eq. (5)] and decoding [see Eq. (6)] techniques are based on a substitution method where the letters of plaintexts are shifted backwards (or forwards) by a fixed number (d) to produce encoding letters [22].

$$c = p + d \ mod \ n, \quad (5)$$

$$p = c - d \ mod \ n, \quad (6)$$

For example, when the letters of plaintext are based on ASCII table, then the n value is 128. Let the "d" be 15 and the plaintext is "Pe@C3", the encoding process is shown in Table I.

TABLE I. CAESAR CIPHER - ENCODING PLAINTEXT OF "PE@C3"

Plaintext	80	101	64	67	51
$c = p + d$ **mod** 128	75	96	59	62	46
Ciphertext	K	‘	;	>	.

The decoding process is the reverse of the encoding process. If the encoding of "d" is 15, then the value of "d" for decoding is -15. Let's decode the ciphertext of "K‘;¿.", the complete process is shown in Table II.

TABLE II. CAESAR CIPHER - DECODING CIPHERTEXT OF "K‘;¿."

Ciphertext	75	96	59	62	46
$p = c - d$ **mod** 128	80	101	64	67	51
Plaintext	P	e	@	C	3

III. Proposed AudioMag Steganography

The proposed AudioMag steganography data hiding technique involves hiding audio data within an image. This process is illustrated in Fig. 2. Audio consists of time and amplitude, modification must be made to the audio in order to embed it into the image, which consists of the x-axis and y-axis. The explanation is provided in 1. The algorithm outlines the specific modifications and calculations that need to be performed on the audio data in order to align it with the x-axis and y-axis of the image.

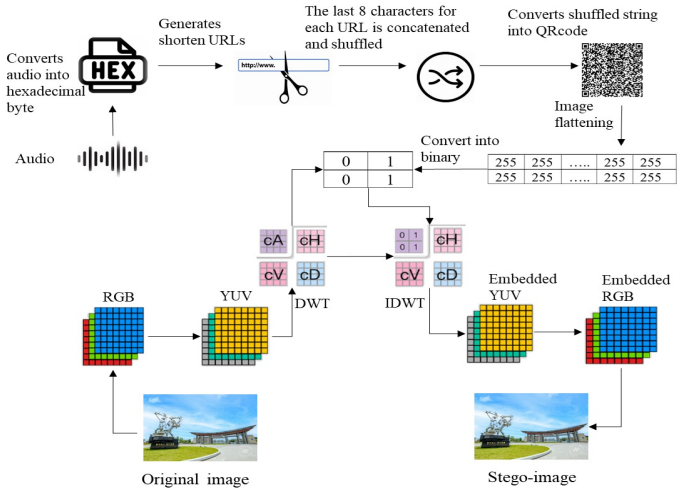


Fig. 2. AudioMag steganography - audio hiding.

The proposed AudioMag steganography audio extraction technique involves extracting the QR code from the stego-image, reading the string of the QR code, manipulating the string into hexadecimal value, and finally converting it into audio. This process is illustrated in Fig. 3. The explanation is provided in Algorithm 2.

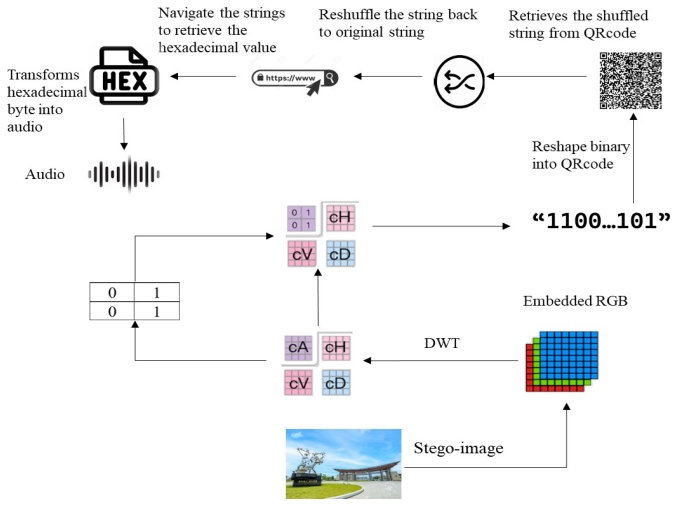


Fig. 3. AudioMag steganography - audio extraction.

IV. AudioMag Simulation

An audio recording is made using Realme UI 3.0. The spoken text is "Cryptography" and lasts approximately 1 second. The audio file is 41.5 kilobytes (kb) in MP3 format. The audio is then converted into a hexadecimal value, as illustrated in Fig. 4, resulting in a file size of 82.5kb. The hexadecimal value is then divided into blocks, resulting in three blocks and consequently, three shortened URLs.

```
fffbe4440e06472752ca6b5bc2f2e62c098a6b786e19d5592
a6d6dedcb68b026299dbdb81668c90b8f1d24f5390db048cb
6c0e6d00d888c0c12201f45231f283022c31e1f2eab1f1180
0e88973cc5819e80490018d5d316132f096f9fa8324cda2ee
5dac96f4190c038050152552c4e041220223a38274009c467
5394dcc642ffcaa34fbc920e775aca82c10bc1bc52e4fb777
0a6a574a069c9ea7cb2b1a8b46a2ee93bd47dc6dfeabe1f49
ad5b90cbdeece56e6ef2a4d6f5ffafebe96e5d37677ce5242
e665b3afd3ee9684547518251331914l46a2da96be98534d48
29a554d7b58592f1233488f77e0c965b5800000004d3b61f
386572ba00c342cc9060b765ef33a296596c422385bd05b44
cfd0cce11cd18c4cd408200890207878aa1a5a374a4cb3c0a
004408bcc2804d900c0402117b8684d1b52425cfe4b67a79a
1aab3667f2f2992c0ae52f3a2d97fd1adfc68430084806af2
04bd0dd77057144aa45f0fceac6292f652af9faba9a762f76
be52c91e51576265732129eb95bbac1a574aff4335a0997cb
3ef58bda802dfe39eff9faa95a71c78473ffe452f933e161e
36dd4f440284413b138b5e8f422de3456a5d11c6b54a4ca5d
a9fc23ed7a472591411313ff7b1adbeddaf87dcfab6bf58dd
ed8137acca01a8a91e048e245a07181026002a08a28818b14
a3a6fc227ce9e720266fe806441a61220382e061031e070b8
```

Fig. 4. Fraction hexadecimal of the audio.

Each block hexadecimal value is prefixed with "http" at front and suffixed with ".com" at back. A tinyurl website is used to generate the shorten URL. The last eight characters of each shortened URL are used and concatenated. The entire string is "sn3mjvze5n6un8s2mwwefvc6".

The ASCII is a character set with 128 characters, each represented by seven bits. It includes the numbers 0-9, both upper and lower case English letters from A to Z, and a selection of special characters. The string "sn3mjvze5n6un8s2mwwefvc6" is consider input plaintext which is shuffled using the Caesar cipher. The key for the Caesar cipher is "-5" and modulus 128, resulting in the output ciphertext "ni.hequ'0i1pi3n-hrr'aq^1". This output ciphertext is used to generate the QR code. The generated QR code is in ".png" format, with dimensions of 414 x 414, and a file size of 1.29kb bytes, as shown in Fig. 5.

Fig. 5. QR code consists shuffled URL string.

Next, the generated QR code is embedded into an image (see Fig. 6a) and results the embedded image (see Fig. 6b). The size of the original image and embedded image is in ".jpg" format, with dimensions of 5109 x 3400 and a file size of 1.71mb. With the naked eye, it is hard to notice the difference between the original image and the stego-image, as only a single bit is changed per pixel, as shown in Fig. 6.

To retrieve the audio one first needs to extract the QR code from the embedded image. The extracted QR code, shown in

Algorithm 1 AudioMag steganography - data hiding

Require: Input: Audio, Original image.

Audio is converted into hexadecimal, the size of audio hexadecimal is denoted as l_a.
The audio hexadecimal l_a is divided into block, each block hexadecimal is 32 kilo byte (kb). The last block can be less than 32kb.
Each block's hexadecimal value is prefixed with "http" at front and suffixed with ".com" at back. The entire string is then used to generate a shortened uniform resource locator (URL).
The last eight characters of each shortened URL are used, concatenated, and shuffled. The shuffling step is based on the Caesar cipher, with the modulus size based on the total number of ASCII characters, which is 128.
The shuffled string is converted into a quick response code (QR code). The QR code is in two dimensions, the size is M x N, where the values of M x N are fixed as 414 x 414. Maximum string embedded into the QR code is 140 bytes.
Flatten the QR code. Converts the flatten QR code value into binary, we denoted it as qr.
Retrieves the original image. Note that the original image must be at least eight times larger in dimensions than the QR code.
Obtains red, green and blue (RGB) of original image.
Transforms RGB of original image into brightness and color (YUV).
Decomposes the YUV original image into four sub-images via discrete wavelet transform (DWT). The sub-images are known as approximation (cA), horizontal (cH), vertical (cV), and diagonal (cD) respectively. The size for each sub-image is $\frac{M}{2}$ x $\frac{N}{2}$.
The cA is further divided into 4 x 4 block via discrete cosine transform (DCT), we denote the number of block as b.
for $i \leftarrow 1$ to b **do**
    The block of cA, b_i is decomposed via singular value decomposition (SVD), the return value (S) contains singular values. One bit data of qr_i is embed into the first singular value.
end for
Reconstructs cA via inverse discrete cosine transform (IDCT).
Converts the embedded cA together with cH, cV and cD into YUV data via inverse wavelet transform (IDWT).
Transforms YUV data into RGB.
Output: Stego-image.

(a) Original image.

(b) Stego-image.

Fig. 6. Original image and stego-image.

Fig. 7, is in ".png" format with dimensions of 414 x 414 and a file size of 83.6kb. One may observe noise, but the QR code content remains.

Fig. 7. Extracted QR code from stego-image.

The ciphertext "ni.hequ‘0i1pi3n-hrr‘aq^1" is decoded using Caesar cipher with decoded key of"+5" and modulus 128, resulting in the string "sn3mjvze5n6un8s2mwwefvc6". This string is divided into three sub-strings, with each sub-string containing eight characters. Each sub-string is prefixed with "https://tinyurl.com/" to complete as URL. Place the URL in a web browser and navigate to it; it will display a long URL string. Remove the prefixed "http" and suffixed ".com", and you will get the hexadecimal value. Repeat this process for each sub-string. Finally, concatenate all the hexadecimal values to recover the audio.

A. Robustness of Stego-image

This section examines the robustness of stego-images, as shown in Table III. The rationale behind this experiment is to determine if stego-images can be sabotaged, yet still be able to extract the embedded QR code. To assess this risk, two potential scenarios were investigated: 1) when the stego-image is masked, and 2) when the stego-image is cropped. The findings show that the QR code can be extracted from manipulated stego-images, even when subjected to higher levels of noise compared to the results depicted in Fig. 7. It is noted that the information in the QR code remains readable. This means the proposed method maintains the integrity of the embedded data indirectly.

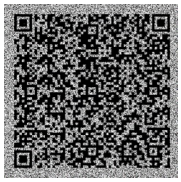
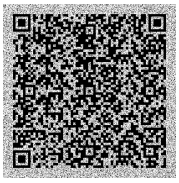
V. Result and Discussion

The proposed method for concealing secret audio in an image begins by converting the audio into hexadecimal values, which are then split into fixed 32kb strings. The strings are hidden using shortened URLs, with the last eight characters of each URL concatenated. This means that each shortened URL's size is 8 bytes. The concatenated string is shuffled using a Caesar cipher and the resulting shuffled string is used to create a 414 x 414 QR code. Lastly, the QR code is embedded into the image. Note that the image must be at least eight times larger than the QR code; therefore, the minimum size of the image is 3319 x 3319.

Algorithm 2 AudioMag Steganography - Data Extraction

Require: Input: Stego-image.
Obtains RGB of stego-image.
Decomposes the RGB stego-image into four sub-images via DWT. The sub-images cA, cH, cV, and cD respectively. The size for each sub-image is $\frac{M}{2}$ x $\frac{N}{2}$.
The cA is further divided into 4 x 4 blocks via DWT, we denoted the block as b.
for $i \leftarrow 1$ to b **do**
    The block of cA, b_i is decomposed via DCT.
    Flatten the output of DCT into one-dimensional array and then indexed it, such that D_j, where $j \in 0, 1, 2, 3$.
    The indexed array is rearranged back into a 4*4 shape.
    Performs SVD on the rearranged array.
    Obtains first singular value (S_0) by extracting the first value of S_0.
    Calculates binary data extraction.
    for $j \leftarrow 1$ to 3 **do**
        Obtains first singular value (S_j) by extracting the first value of S_j.
        Calculates binary data extraction and merge with S_{j-1}.
    end for
    Calculate the average extracted bit information.
end for
Each mean bit block is multiplied by 255 to convert the normalized pixel value into the actual pixel representation so that it can correctly represent color or brightness in the image.
Retrieves the QR code.
Read the string in the QR code.
Decodes the string using Caesar cipher.
The decipher string is divided into eight characters sub-strings. We denoted the number of sub-strings as ls. Let's an empty string is $string_{sub}$.
for $i \leftarrow 1$ to ls **do**
    Each sub-string is prefixed with "https://tinyurl.com/" and navigated to in a web browser.
    The web browser will show the long URL string, removes the prefixed "http" and suffixed ".com". We denoted it as URL'.
    Concatenate the URL' into $string_{sub}$, such that $string_{sub}$ = $string_{sub}||URL'$.
end for
Convert the $string_{sub}$ into audio.
Output: Audio.

TABLE III. ROBUSTNESS OF STEGO-IMAGE

Case	Stego-image	QR code
1		
2		

The 414 x 414 QR code can only contain a maximum of 140 bytes of a string. According to the simulation, the audio file size is approximately 41kb per second. Once the audio is converted into hexadecimal values, the total size of the hexadecimal values is 82kb, resulting in a total of 24 bytes for three different URLs. This implies that the maximum amount of secret audio that can be embedded in a single image of minimum size 3319 x 3319 is roughly six seconds worth of secret audio. The six seconds secret audio consists of 492kb hexadecimal values, resulting in a total of 128 bytes for three different URLs.

The proposed method embeds the QR code into the an image via DWT, DCT, and SVD, based on the simulation, the original image (see Fig. 6a) appears similar to the stego-image (see Fig. 6b). This ensures that the hidden QR code (also known as converted secret audio) is invisible to the naked eye.

However, a flaw occurs when extracting the QR code from the stego-image (see Fig. 7); noise appears in the extracted QR code due to its high robustness. High robustness in this case means that even if the stego-image is corrupted, we can still retrieve the QR code as being discussed in Section IV-A. The noise, however, does not affect the efforts to retrieve the shuffled string stored in the QR code. Therefore, we can successfully decode the shuffled string and ultimately recover the secret audio.

VI. CONCLUSION AND FUTURE WORK

Audio steganography is a covert communication technique that involves embedding secret information within an audio

signal, making it undetectable to the human ear. Image steganography is a technique used to hide secret messages within an ordinary images. Our innovative approach, AudioMag, converts audio data into hexadecimal format and then encodes it into a QR code. This QR code is subsequently inserted into an image, offering a beyond than traditional secure way to transmit hidden information, thereby preventing potential attackers from detecting the concealed audio message.

The effectiveness of this method lies in the fact that the proposed algorithm has been successful in converted audio into the QR code while preserving the similarity between the stego-image and the original image. This added layer of security helps to ensures that the hidden audio message remains undetectable by eavesdroppers. Hence, preserving the confidentiality of the transmitted data over digital channels.

However, one limitation of our design is that it only allows for embedding audio up to a maximum of six seconds. Therefore, as future work, we plan to design the QR code dimensions in a more flexible manner, allowing for the embedding of longer strings. This means that we will be able to record arbitrary lengths of audio to embed into the image.

ACKNOWLEDGMENT

The authors would like to thank Guangdong University of Science & Technology, China and Rabdan Academy, United Arab Emirates.

REFERENCES

[1] K. Sutradhar, B. G. Pillai, R. Amin and D. L. Narayan, *A survey on privacy-preserving authentication protocols for secure vehicular communication*, Computer Communications, 2024.

[2] K. Moldamurat, Y. Seitkulov, S. Atanov, M. Bakyt and B. Yergaliyeva, *Enhancing cryptographic protection, authentication, and authorization in cellular networks: a comprehensive research study*, International Journal of Electrical and Computer Engineering (2088-8708), 14(1), 2024.

[3] J. Zhang, *The Application of Data Encryption Technology in Computer Network Security*, Transactions on Computer Science and Technology, 11(1), 2024.

[4] S. Pramanik, *A new method for locating data hiding in image steganography*, Multimedia Tools and Applications, 83(12), pp. 34323-34349, 2024.

[5] B. Song, P. Wei, S. Wu, Y. Lin and W. Zhou, *A survey on Deep-Learning-based image steganography*, Expert Systems with Applications, pp. 124390, 2024.

[6] H. J. Asghar, B. Z. H. Zhao, M. Ikram, G. Nguyen, D. Kaafar, S. Lamont and D. Coscia, *Use of cryptography in malware obfuscation*, Journal of Computer Virology and Hacking Techniques, 20(1), pp 135-152, 2024.

[7] C. D. Vleeschouwer, J. F. Delaigle and B. Macq,*Circular interpretation of bijective transformations in lossless watermarking for media asset management*, IEEE Trans. Multimedia , 5(1), pp. 97 - 105, 2003.

[8] C. W. Honsinger, P. Jones, M. Rabbani and J. C. Stoffel *Lossless recovery of an original image containing embedded data*, US Patent: 6,278,791, 2004.

[9] S. Chandran and B. Khoushik, *Performance Analysis of LSB DCT and DWT for Digital Watermarking Application using Steganography*, IEEE Int. Conf. Electr. Electron. Signals Commun. Optim, 15(978-1-4799-7678-2), pp. 2-6, 2015.

[10] S. K. Moon and R. S. Kawitkar, *Data security using data hiding*, In International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007), 4 pp. 247-251, 2007.

[11] C. Kim, L. Cavazos Quero, K. H. Jung and L. Leng, *Advanced Dual Reversible Data Hiding: A Focus on Modification Direction and Enhanced Least Significant Bit (LSB) Approaches*, Applied Sciences, 14(6), pp. 2437, 2024.

[12] P. Naveen and R. Jayaraghavi, *Image Steganography Method for Securing Multiple Images using LSB–GA*, Wireless Personal Communications, 135(1), pp. 1-19, 2024.

[13] B. Datta, P. Pal and S. K. Bandyopadhyay, *Robust multi layer audio steganography*, In 2015 Annual IEEE India Conference (INDICON), IEEE, 1-6, 2015.

[14] M. H. Sayed and T. M. Wahbi, *Information Security for Audio Steganography Using a Phase Coding Method*, European Journal of Theoretical and Applied Sciences, 2(1), pp. 634-647, 2024.

[15] R. M. Nugraha, *Implementation of direct sequence spread spectrum steganography on audio data*, In Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, IEEE, pp.1-6, 2011.

[16] K. Brandenburg and H. Popp, *MPEG layer-3*, MEBU Technical review, pp.1-15, 2000.

[17] I. Haverkamp and D. K. Sarmah, *valuating the merits and constraints of cryptography-steganography fusion: a systematic analysis*, International Journal of Information Security, pp.1-29, 2024.

[18] A. M. Khalaf and K. Lakhtaria, *A review of steganography techniques*, In AIP Conference Proceedings, 3051(1), 2024.

[19] M. Kimlyk and S. Umnyashkin, *Image denoising using discrete wavelet transform and edge information*, In 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 1823-1825, 2018.

[20] J. Patel, D. Tailor, K. Panchal, S. Patel, R. Gupta and M. Shah, *All phase discrete cosine biorthogonal transform versus discrete cosine transform in digital watermarking*, Multimedia Tools and Applications, 83(6), pp. 16121-16138, 2024.

[21] B. Mahaboob, D. Leela, B. Kothuru, G. B. Prakashand, A. Raheem and S. Nandakishore, *A note on singular value decomposition*, AIP Conference Proceedings, 3231(1), 2024.

[22] W. Stallings, *Cryptography and network security:principles and practices*, Pearson Education India, 2006.

Using Hybrid Compact Transformer for COVID-19 Detection from Chest X-Ray

Ghadeer Almoeili[1], Abdenour Bounsiar[2]
Applied College, King Faisal University, Alhassa, Kingdom of Saudi Arabia
Ministry of Higher Education[1]
College of Computer Sciences and IT, King Faisal University, Alhassa, Kingdom of Saudi Arabia
Ministry of Higher Education[2]

***Abstract*—By the end of December 2019, the novel coronavirus 2019 (COVID-2019), became a world pandemic affecting the respiratory system. Scientists started investigating using Deep Learning and Convolutional Neural Networks (CNNs) to detect COVID-19 using Chest X-rays (CXRs). One of the main difficulties researchers reported in the detection of lung diseases is the fact that radiographic images can tell that the lungs are abnormal, but they might miss specifying the type of pneumonia exactly. Only the expert radiologist can tell the difference based on patches shapes and distribution on the affted lungs. Also CNN's require big datasets to provide good results. When new pandemics spread, The limited benchmark datasets for COVID-19 in CXR images, especially during the onset of the pandemic, is the main motivation of this research. In this research, we will introduce the use of Vision Transformers (ViTs). We consider an updated version of ViT called Compact Transformer (CT) which was proposed to reduce the expansive computations of the self-attention mechanism in ViT and to escape the big data paradigm. As a contribution of this study, We propose using a Hybrid Compact Transformer (HCT) in which a pretrained CNN is used in place of the convolutional layers in CT. Hence, with the hybrid model design, we aim to combine the localization power of CNNs, with the generalization power (attention mechanism or distanced-pixel relations) of ViTs. Based on experimental results using different performance metrics, the Hybrid Compact Transformer is shown to be superior over Compact Transformers and Transfer Learning models. Our proposed technique enjoys the benefits of both worlds; a faster training of the model due to TL with CNNs and reduced data requirements due to CT. Combining localized filters of CNNs and the attention mechanism of CT seems to provide a better discrimination between common pneumonia and Covid-19 pneumonia.**

***Keywords*—Deep convolutional neural network; CXR chest X-Ray; COVID-19 pneumonia; vision transformers; compact convolutional transformer; hybrid compact transformer**

I. Introduction

At the end of December 2019, there was a cluster of Pneumonia cases discovered in the city of Wuhan. By the end of January 2020, the World Health Organization (WHO) announced that the disease had become a world pandemic caused by Severe Acute Respiratory Syndrome Corona Virus-2 (SARS-CoV-2), commonly called COVID-19.

The test that is mostly used to detect COVID-19 infection is the Reverse-Transcription polymerase chain reaction (RT-PCR) [29]. In the early days, this test was not approved to be used for the detection of respiratory diseases because of the low sensitivity of the test and the high possibility of false negatives that might occur. Instead, chest imaging such as CXR or computed tomography (CT) was used to diagnose respiratory diseases. However, with the pandemic of Coronavirus, Using CXR is considered faster and cheaper than using RT-PCR. However, CXR interpretation requires expert radiologists. If we consider the number of radiologists in each hospital compared to the number of patients' CXR images, radiologists would not be able to study that massive amount of CXR images.

In 2016, a research paper was published demonstrating the efficacy of deep learning algorithms in the medical field [12]. This research discusses the employment of deep learning models in the task of grading for diabetic retinopathy to recapitulate the majority decision of the board-certified ophthalmologists in the US. Deep learning is a type of Machine Learning algorithm that employs neural networks (NN) to learn complex relationships among huge amounts of data.

In 2020, a research paper was published by Google team [7], introducing the new state-of-the-art image classification. Inspired by the Transformers scaling successes in NLP [45], Transformers have accomplished quick successes in computer vision. Vision Transformers (ViTs) are emerging as an architectural paradigm alternative to CNNs. However, the lack of the typical convolutional inductive bias makes these models extremely data-hungry and computationally expensive compared to common CNNs [7]. Consequently, the cost of training such models is only affordable by the lucky few at the large industrial companies.

Data Efficient Image Transformer (DeiT) [43] is one of the first papers to show that it is practical to train transformers for computer vision tasks. DeiT trained with a procedure more adapted to a data-starving regime. Subsequently, it requires far fewer data and far less computer power to produce a high-performance image classification model. Recently, numerous related work has been proposed to democratize AI research for transformers [23] [13]. To help researchers with limited resources to verify the research results and to take these results for granted. Both CNNs and Transformers have highly desirable qualities for different computer vision tasks, but each comes with their own costs [13].

Recently, many researchers have used radiology images for COVD-19 detection. Authors in [36] compared four popular neural networks for the classification of CXR images. AlexNet [22], ResNet18 [14], DenseNet201 [15], and SqueezeNet [16]. They used radiographic images from the Kaggle [33] database. Image Augmentation is applied to the

data set and three classification schemes were compared: normal vs pneumonia, bacterial vs viral pneumonia, and normal, bacterial and viral pneumonia. This paper demonstrates that the deeper the network the better the accuracy, such that DenseNet201 outperforms the other three networks in all the three classification schemes. The classification accuracy achieved was 95%.

The authors in [38] proposed an algorithm called Data Augmentation of Radiograph Images (DARI) which combines GANs architecture with generic data augmentation methods to maximize the training data. DARI algorithm is applied to the input images when the class imbalanced ratio is greater than a given threshold. The accuracy achieved training this model was 93.94%. Further, the authors of the DARI algorithm compared the performance of their proposed method with another paper called DarkCovidNet [31]. The model is designed for the diagnosis of the COVID-19 disease. In their study, the main model was inspired by the DarkNet architecture that has proven itself in deep learning. DarkCovidNet achieved an accuracy of 87.02%.

Since the early onset of COVID-19, there was a global scientific response to help in diagnosing and curing. Many of these efforts considered automated COVID-19 detection from CXRs, such as [2] or [3]. Deep Neural Networks (DNNs), and CNNs has boosted medical image analysis over the past years. This research aims to investigate the use of CNNs and ViTs for the automated detection of COVID-19 from CXR images.

Detection of COVID-19 from CXRs involves two problems: COVID-19 vs non-COVID-19 in which case a dataset like [6] can be used, and COVID-19 vs Other Pneumonia vs healthy, in which case a dataset like [4] can be used along with [6]. In this research, we will consider having a benchmark dataset that contains three classes COVID-19 Pneumonia (CP) vs Community-Acquired Pneumonia (CAP) and Normal cases for our study.

Most medical applications suffer from limited datasets, and as Deep Convolutional Neural Networks (DCNNs) are data-hungry, the medical community has almost universally adopted transfer learning to build a CNN for medical imaging. For example [31] uses initial model weights from ChestNet [37] for pneumonia disease detection. In this research, we will consider using a pretrained model on a benchmark dataset.

Moreover, as COVID-19 is a respiratory disease such that the virus directly infects the lungs area, having a model that focuses on studying the infection only by segmenting the lungs area in CXR images from other parts in the image, can add improvement in the performance of the used models as proposed by [28] and [47]. In this research, we will apply an image segmentation algorithm to segment the lungs before classification.

The considered aspects below state the contributions of this research:

1) Combining existing CXR Datasets: The main obstacle for a neural network to learn is that there are not enough data examples for training. Currently, as COVID-19 is a new disease, many websites are trying to encourage people and hospitals to contribute and share COVID-19 CXR images from patients all over the world to gather a sufficient number of CXRs and make them public for researchers. In this research, we will not gather our own dataset, but rather we will use a combination of existing ones such as [6] [33] [18]. Images are classified into three classes COVID-19 Pneumonia (CP) vs Community-Acquired Pneumonia (CAP), and Normal cases for our study.

2) Balanced Dataset: Since the available COVID-19 cases are much fewer than healthy cases or even other pneumonia types, image augmentation techniques that can enlarge the minority class, will be used to accomplish a balance between input classes to reach good accuracy of trained model [26].

3) Image Segmentation: One of the main difficulties researchers reported in the detection of lung diseases is the fact that radiographic images can tell that the lungs are abnormal, but they might miss specifying the type of pneumonia exactly. Only the expert radiologist can tell the difference [5]. Therefore, data scientists proposed using image segmentation techniques to segment the lungs so that the model will focus on studying only the lungs and the infection if available [47]. In this research, U-net model proposed by [17], will be used for the segmentation process.

4) Proposed model design: In this research, we will examine using a version of vision transformers called Compact Transformer(CT) [13]. Our proposed method, called Hybrid Compact Transformer (HCT) uses a pretrained CNN in place of the convolutional layers in the original Compact Convolutional Transformer (CCT). In addition, we will reduce the number of transformer encoding layers.

The remainder of this paper is organized as follows: Section II introduces our proposed technique and Section III explains our research methodology. Experimental results are provided in Section IV and the analysis of its results are proposed in Section V. Section VI provides conclusions and suggestions for future improvements.

II. Proposed Model Architecture

A. Segmentation Network

U-Net [17] is a deep learning architecture used for image segmentation problems and was released particularly as a solution for biomedical segmentation tasks. It is the adopted segmentation architecture for any problem domain in Kaggle [33]. Inspired by the early success of previous work [28] [47], and [30], claimed that segmentation can increase the sensitivity of the network such that the network classification result is based on the pixels related to the lung area that contains information about the disease. In this research, we will adopt U-Net to perform semantic segmentation with the benchmark dataset to separate lung and heart contour from the chest radiography images.

Instead of training a Unet model from scratch, a pretrained Unet model, that was shared by [20], is used in this research. This model was pretrained to segment CXR images. In the first phase, all images in the dataset will be segmented using the Unet model. For segmentation, images will be resized to the shape 512 X 512 X 1, as the Unet model architecture requires input images of that size [20]. All segmented images are then saved in the dataset.

TABLE I. CXR DATASETS

Data-set	Classes	Size of images	Pre-processing	Author
Italian Society of Medical and Interventional Radiology [18]	COVID-19 : 68	Image size is not fixed for all images.	Original CXR images.	Asif, Sohaib, et al [3] Ahishali, Mete, et al. [1]
GitHub repository shared by Dr. Joseph Cohen [6]	- Aute Respiratory Distress Syndrome (ARDS): 465 - COVID-19 : 319 - Middle East Respiratory Syndrome (MERS) : 481 - Pneumonia - Severe Acute Respiratory Syndrome (SARS) : 465	Image size is not fixed for all images.	Original CXR images.	Asif, Sohaib, et al [3] Sakib, Sadman, et al. [38] Waheed, Abdul, et al. [46]
Chest Imaging (Spain) at thread reader. [42]	COVID-19 : 50	Image size is not fixed for all images	Original CXR images.	Ahishali, Mete, et al. [1]
Radiopaedia [34]	- COVID-19 : 28 - Pneumonia : 3200	Image size is not fixed for all images.	Original CXR images.	Ahishali, Mete, et al. [1]
Kaggle [33]	- Normal : 1342 - Bacterial Pneumonia : 2561 - Viral Pneumonia : 1345	400 X 2000	Original CXR images.	Rahman, Tawsifur, et al. [36] Ahishali, Mete, et al. [1] Waheed, Abdul, et al. [46]
CheXpert dataset collected by Stanford ML group [19]	Contains 14 different classes with: 224,316 Chest radiographs - No COVID-19 cases	Image size is not fixed for all images.	Original CXR images.	Sakib, Sadman, et al. [38]
Japanese Society of Radiological Technology (JSRT)	247 posteroanterior chest images including normal and lung nodule cases. The images in the database were grouped according to the degree of subtlety of the lung nodule.	2048 X 2048	Original CXR images.	Oh, Yujin, Sangjoon Park, and Jong Chul Ye. [28]
Chest X-14 [48]	Contains 112,120 CXR images. 14 common thoracic diseases classes.	1024 X 1024	Original CXR images.	Wang, Kun, et al. [47]

B. Classification Network

Transformers have rapidly been increasing in popularity and have become a major focus of modern deep learning research. They are emerging as an architectural paradigm alternative to CNNs [7]. ViTs can capture global relations between image elements and they potentially have a larger representation capacity. However, the fact that ViTs are extremely data hungry and require large sets of data to be trained, leads to the exclusion of those with limited resources from research in the field [13] [43]. Moreover, based on the findings of an earlier study [32], the use of existing ViT is not optimal in the field of pneumonia detection, since feature embedding through direct patch flattening is not intended for CXR images. Fig. 1 shows the original architecture of ViT architecture.

Today, researchers persist to dispel the myth that ViTs are data-hungry and can only be applied to huge datasets. Several updates on the architecture of ViT have been proposed like [43] [23], to reduce the expansive computations of the self-attention mechanism and to escape the big data paradigm. In this study, we will use an updated version of ViT called Compact Transformer or CT proposed by [13].

1) Compact Convolutional Transformer (CCT): In [13], the author's contribution is escaping the big data paradigm, as most medical applications with AI suffer from limited data availability. The authors in [13] split their experiments into two phases: In the first phase, they proposed an updated version of the original ViT architecture (Compact Vision Transformer(CVT)), and in the second phase, they proposed using a shallow NN, composed of one convolutional layer and a Relu activation layer, to create the patches instead of extracting them directly from the original input image (Compact Convolutional Transformer (CCT)). Fig. 2 shows the architectures of both CCT and CVT.

The results show that CCT in comparison to CVT can be quickly trained from scratch on small datasets while achieving high accuracy. Based on the findings, it can be argued that transformers can perform head-to-head with state-of-the-art CNNs on small sets of data, often with better model performance, better accuracy, and fewer parameters.

In our study, we propose using a Hybrid Compact Transformer (HCT) in which a pretrained CNN is used in place of the convolutional layers in CCT. The attention mechanism allows transformer architecture to compute in parallelized manner. It can simultaneously extract all the information we need from the input and its inter-relation, compared to CNNs. CNNs are much more localized, using small filters to compress information towards a general answer. While this architecture is powerful for general classification tasks, it does not have the spatial information necessary for many tasks like instance recognition [7]. This is because convolution does not consider distanced-pixel relations (Fig. 3A), like in Vision Transformers where the attention of patches of the images and their relations to each other are calculated (Fig. 3B).

Hence, with the hybrid model design, we aim to combine the localization power of CNNs, with the generalization power (attention mechanism or distanced-pixel relations) of ViTs. Fig. 4 shows an overview of the proposed Hybrid Compact Transformer (HCT). This will allow to achieve good performance even with reduced datasets.

2) Proposed Model Design (Hybrid Compact Transformer): In the proposed HCT model design, a pretrained CNN (transfer learning) is used as a backbone feature extractor and its outputs

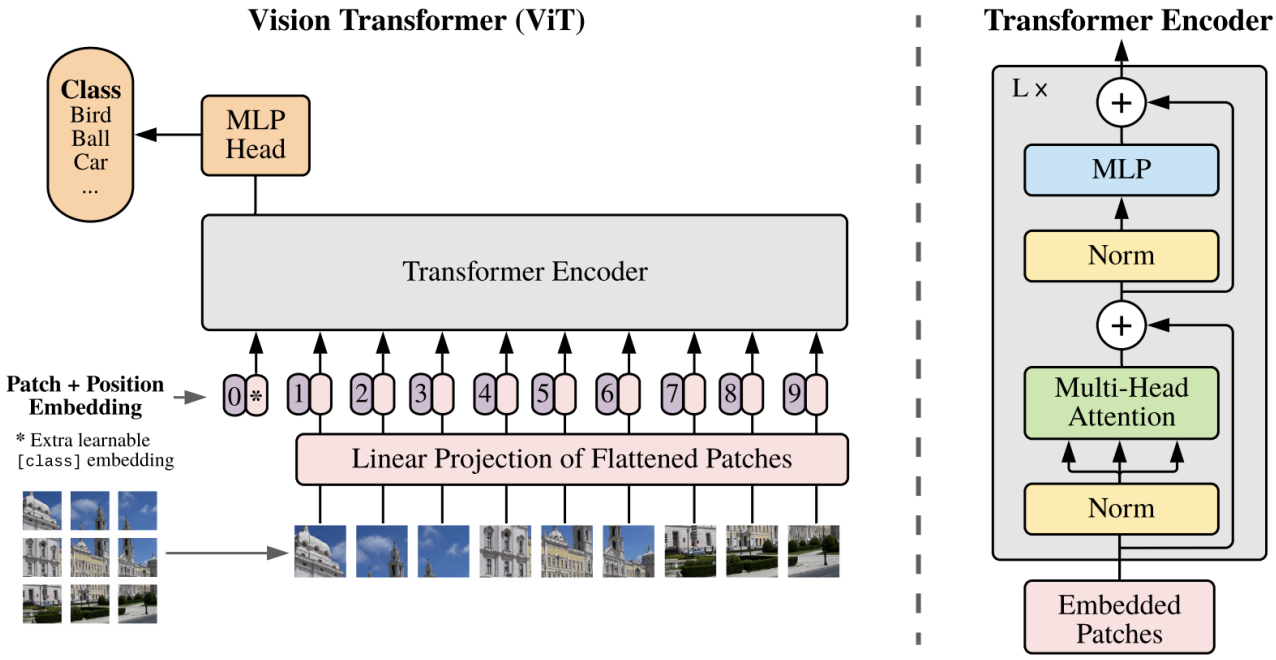


Fig. 1. Vision transformer [7].

are fed to the Compact Transformer. The input CXR image is primarily fed into a backbone CNN to create a feature map then into the compact transformer for classification. The HCT model design is illustrated in Fig. 5.

The architecture of the compact transformer differs from the original Vision Transformer architecture in the following variants, fewer transformer encoder layers (only 2 layers) and smaller dimensions of patches. A transformer encoder consists of a series of stacked encoding layers. Thus, each encoder layer consists of two sub-layers: a Multi-Layer Perceptron (MLP) head and Multi-headed Self-Attention (MSA). Each sub-layer is followed by a layer normalization (LN), and followed by a residual connection to the next sub-layer, as illustrated in Fig. 1. The compactness in the CT results in a lightweight vision transformer with as few as 200K learnable parameters only. Furthermore, in the CT, a novel sequence pooling technique was introduced to remove the needs of the class token. This sequence pooling is a linear layer placed after the transformer encoder to make the model more compact and accurate. Eventually, the output of the pooling layer is then fed into the final classification layer, as in the original ViT model, to classify the image into one of three classes: CP, CAP, or Normal.

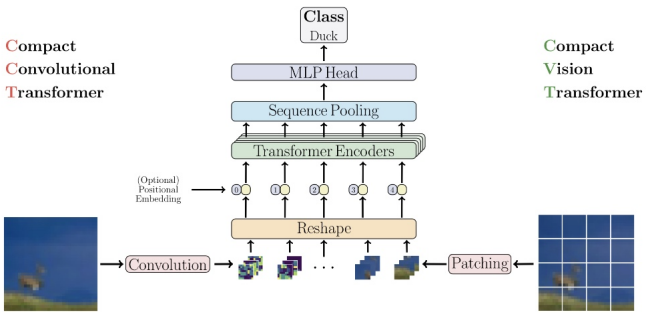


Fig. 2. Overview of CCT vs CVT [13].

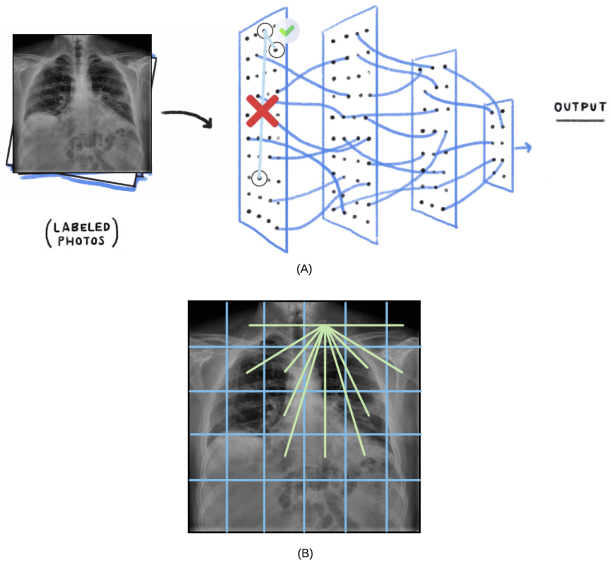


Fig. 3. Illustration of the localization power of CNNs (A), and the generalization power (attention mechanism or distanced-pixel relations) of ViTs (B).

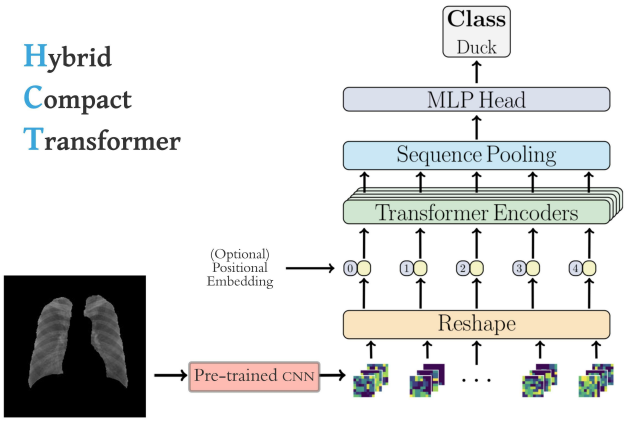


Fig. 4. Overview of Hybrid Compact Transformer (HCT).

TABLE II. TOTAL NUMBER OF CXR IMAGES BEFORE APPLYING AUGMENTATION

Class	Total Number of Images
Normal	5800
COVID-19 CXRs (CP)	6500
Non-COVID-19 CXRs (CAP)	6100

III. RESEARCH METHODOLOGY

A. Dataset

A careful analysis of the available datasets (Table I) will let us decide which data to consider in the experimental study and which possible preprocessing to be use.

We can summarize the results as follows: in our research, we will utilize many of these datasets proposed and used by previous works. Datasets, like [6], shared by Dr. Joseph Cohen, were used in most of the previous works. This dataset contains a good number of COVID-19 CXRs in comparison to all the others. The Kaggle dataset contains images of good quality and resolution for normal and other pneumonia cases. The quality of CXR images helps for better segmentation and model learning. Table II shows the total number of CXR images before to augmentation.

B. Image Augmentation

An investigation of enlarging the number of CXR images by using two different image processing methodologies was discussed in [24]. The main idea in this paper was to evaluate the test accuracy of five pretrained models (AlexNet, VGGNet16, VGGNet19, GoogleNet, and ResNet50) in four scenarios: the first scenario, when using the original dataset, second scenario, when performing data augmentation using classical data augmentation techniques [26] on input dataset to enrich the COVID-19 CXR images, the third scenario, when performing Generative Adversarial Network (GAN) [8]. And the last scenario, when combining classical data augmentation and GAN to generate more CXR images. The results show that ResNet50 is the best deep learning classifier and with augmented COVID-19 medical CXR images achieved the best performance to detect the COVID-19 from the input dataset.

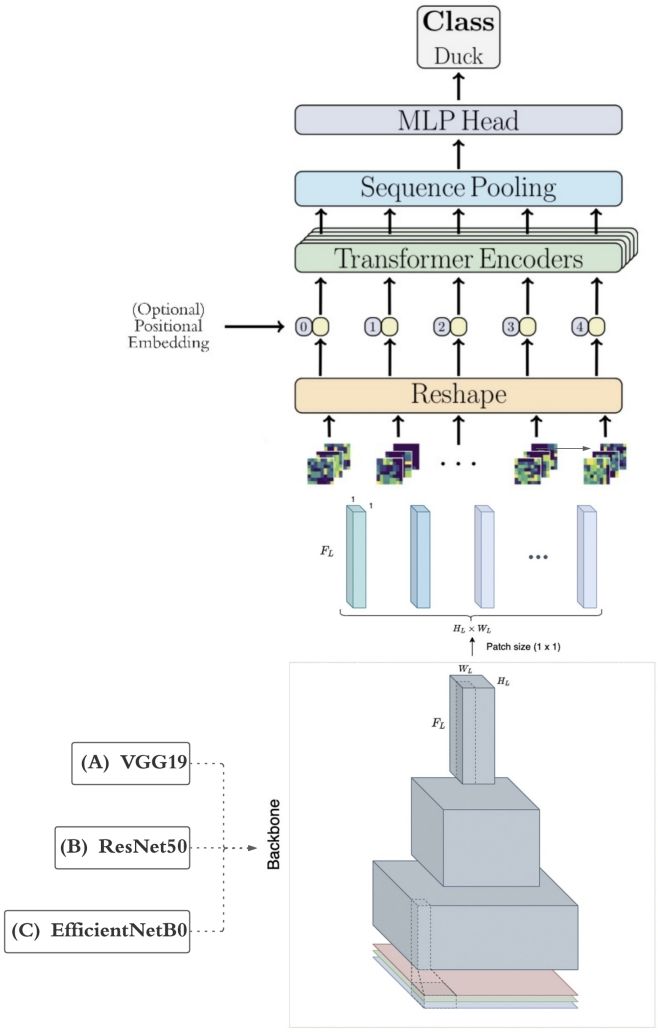


Fig. 5. Illustration of the proposed model design, HCT network. In this study, the backbone or the features extractor is going to be one of three state-of-the-art networks, namely, (A) VGG19, (B) ResNet50, and (C) EfficientNetB0.

TABLE III. TOTAL NUMBER OF CXR IMAGES AFTER APPLYING AUGMENTATION

Class	Total Number of Images
Normal	8000
COVID-19 CXRs (CP)	8000
Non-COVID-19 CXRs (CAP)	8000

In this research different methods for data augmentation techniques such as zooming, rotation, shifting, and flipping [26] were selected to be applied to the original dataset. In the end, the total number of CXR images we have in our dataset is 24000 images as shown in Table III.

C. Classification Performance Metrics

The most common performance measures in the field of deep learning are accuracy, precision,specificity, recall (or sensitivity), and Fβ score [10]. In this research we will utilize all these five performance measures in addition to the confusion matrix to measure and analyze the classification results of the CNN models.

The formulas of the measures are given below, where true positive (TP) is the correctly identified predictions for each class. True negative (TN) is the correctly rejected predictions for a particular class. False positive (FP) is the incorrectly identified predictions for a particular class, and false negative (FN) is the incorrectly rejected predictions for a certain class. After the completion of training phase, the performance of different networks for testing dataset is evaluated. The 5 metrics for performance evaluation were calculated as below:

1) Confusion Matrix: A confusion matrix is used to evaluate the results of a predictive model [49]. This matrix will be generated after making predictions on the test data. For a classifier with n output classes, the predicted values on test instances and the actual values are represented as an nxn matrix. Each row of the confusion matrix represents the samples in a predicted class, and each column represents the samples in an actual class.

2) Accuracy: It is the percentage of correct predictions among all decisions made on examples of a dataset. For a classification problem with two classes, (Eq. 1) defines Accuracy in terms of TP, TN, FP, and FN:

$$Accuracy = \frac{(TP + TN)}{((TP + FN) + (FP + TN))} \tag{1}$$

3) Precision: It represents the percentage of the classifier's correct decisions in favor of the target class (Eq. 2).

$$Precision = \frac{(TP)}{(TP) + FP)} \tag{2}$$

4) Recall (Sensitivity): It represents the percentage of the classifier's correct decisions made on the other class (Eq.3). In particular, sensitivity is the classifier's ability to identify a diseased person as diseased. Sensitivity is also known as True Positive Rate (TPR).

$$Recall(Sensitivity) = \frac{(TP)}{(TP) + (FN)} = TPR \tag{3}$$

5) Specificity: It represents the percentage of the classifier's correct decisions made on the other class (Eq. 4). That is, specificity is the ability of the classifier to correctly identify a healthy person as non-diseased while not confusing a diseased one as healthy [46]. Specificity is also known as True Negative Rate (TNR).

$$Specificity = \frac{(TN)}{(TN) + (FP)} = TNR \tag{4}$$

6) ROC curve (The Receiver Operating Characteristics curve): One of the most important evaluation metrics for checking any binary classification model's performance [50]. The ROC curve is a graphical plot, plotted with the TPR (Eq. 3), against the False Positive Rate (FPR) (Eq. 5), where TPR is on the y-axis and FPR is on the x-axis. The closer the ROC curve towards the upper left corner, the better the model's performance. The curve is created with the two variables at various threshold settings [44].

$$FPR = 1 - TNR \tag{5}$$

7) AUROC curve (Area Under The Receiver Operating Characteristics curve): Area Under the ROC curve is often used as a classification model's quality measurement. In this research, we will utilize this performance measure for each of the two binary classifiers in the two-stage CNN to visualize how well our proposed cascade classifier is performing. The AUROC for an optimal classifier is 1. In practice, the AUROC value is usually between 0.5 and 1 [44].

8) F1 Score: F1 score is the harmonic mean of precision and recall (Eq. 6) [10] . As sensitivity and precision are both important measurements in medical applications, the β value is 1 as shown in (Eq. 7).

$$F\beta = (1 + \beta^2) * \frac{(Precision * Recall)}{(\beta^2 * Precision) + Recall} \tag{6}$$

$$F1 = 2 * \frac{(Precision * Recall)}{(Precision + Recall)} \tag{7}$$

D. Pretrained Backbone CNN Models

In this research, we will investigate the detection of COVID-19 with three classifiers ResNet50 and VGG19 on the benchmark dataset. Additionally, we will study the efficiency of a new family of models invented by [40], called EfficientNets. It has been demonstrated in the paper and as the name suggests, EfficientNets are computationally efficient and achieve much better accuracy and efficiency than previous CNNs. We will study the performance of EfficientNetB0 on our benchmark dataset.

E. Experimental Setup

Python programming language was used to train the proposed deep transfer learning models. Considering having a large dataset, all experiments were performed on Google Colaboratory Pro (Google Colab Pro) on Mac Operating System using the online cloud service with Graphics Processing Unit (GPU) hardware for free. Colab Pro supports longer running notebooks, access to faster GPUs and TPUs, and provides high RAM [9]. CNN models (VGG19, ResNet50, and EfficientNetB0) were pretrained on ImageNet weights.

TABLE IV. TESTING ACCURACY OBTAINED BY THE HCT MODELS TRAINED WITH DIFFERENT BATCH SIZES

Model	Batch Size		
	32	64	128
HCT (VGG19)	92.00%	90.04%	90.62%
HCT (ResNet50)	96.82%	96.70%	97.25%
HCT (EfficientNetB0)	98.35%	98.38%	98.63%

IV. EXPERIMENTAL RESULTS

A. Segmentation Performance

Based on the segmentation results on our dataset, generally, the pretrained Unet model performance is great. Lung segmentation before classification helped in removing the irregular regions and the irrelevant objects (e.g. medical devices). An example of the segmentation results is shown in Fig. 6.

B. Classification Performance

To illustrate, all following experiments were implemented using the same dataset for multiclass classification. Moreover, the entire dataset was randomly split into training (70%), validation (20%), and testing (10%).

1) Optimal learning rate selection: To determine the optimal learning rate for all models, the models were trained using three different learning rates, .0001, .00001, and .000001. The best learning rate of a model was chosen based on the minimum loss, as such, the optimal learning rate for all three networks is 0.000001 as shown in Fig. 7.

2) Results comparison with different batch sizes: In this research, the impact of batch size on testing accuracy is studied. Table IV demonstrates the test accuracy of all networks when trained using three different batch sizes. Based on the findings, it can be argued that a stable and higher testing performance is obtained for ResNet50 and EfficientNetB0 models with a batch size of 128, and for VGG19 model with a batch size of 32.

3) Stratified K-fold Cross-Validation Results:

- Hybrid Compact Transformer (HCT) model Results:
  After training and testing, the accuracies achieved by the proposed HCT models were 92.00%, 97.25%, and 98.63% when using different features extractors: VGG19, ResNet50, and EfficientNetB0, respectively. The batch size, learning rate, and the number of epochs were experimentally set to 128, 0.000001, and 100, respectively for all models except for HCT-VGG19 the training procedure was completed in 200 epochs using a batch size of 32.
- Compact Convolutional Transformar (CCT) model Results:
  As proposed by the author of the CCT model, the batch size, learning rate, and the number of epochs were experimentally set to 128, 0.001, and 100, respectively. The model achieved an over all test accuracy of 81.79%.
- Transfer Learning (TL) model Results:
  In the fine-tuning of the individual DCNNs, we tried various combinations of batch sizes and learning rates to get the best models' performance. The batch size, learning rate, and the number of epochs, for all networks, were experimentally set to 64, 0.0001, and 100, respectively, except for VGG19 the batch size used was 32. The overall test accuracies achieved were 89.52%, 94.62%, and 96.74% for VGG19, ResNet50, and EfficientNetB0, respectively.

The detailed classification results obtained from all networks are compared in terms of various metrics and are tabulated in Table V. As can be seen from these results, the HCT model produced better accuracy scores than the fine-tuned deep CNN models. This result was considered reasonable as adding one simple ViT encoding layer (generalization power) can enhance the power of Deep CNNs. The best accuracy score overall was 98.63%, and was produced by HCT with EfficientNetB0 as backbone. It can be noticed that EfficiantNetB0 produced the best accuracies for both fine-tuned CNNs and HCT models.

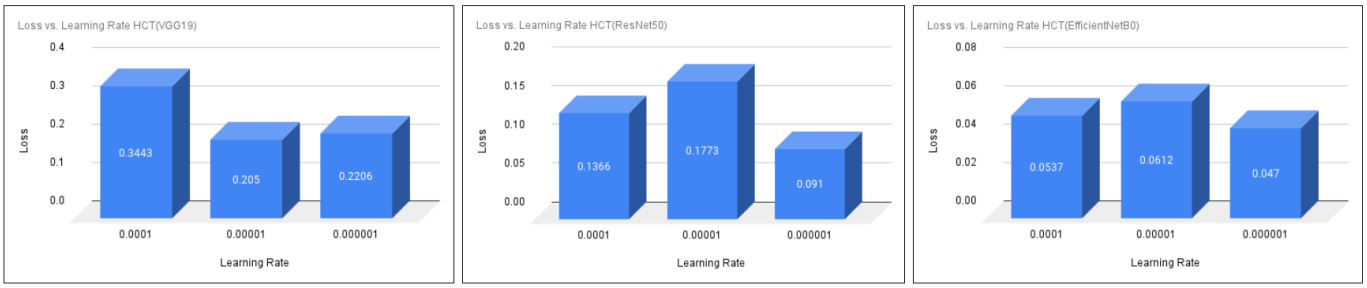
C. Analysis of Models Execution Results

1) Sensitivity-Specificity Analysis: In a diagnostic test (Neural Network), the network's sensitivity (True Positive Rate) refers to the network's ability to correctly classify COVID-19 patients who have the condition, whilst specificity (True Negative Rate) is a measure of how well a network can identify those who do not have the condition [51]. In medical applications, it is always preferable to have a network with high sensitivity such that the probability that a network produces false negatives is low [51]. FN is the proportion of positives (COVID-19) that are mislabeled as negatives (Normal) by the model. These false negatives are crucial and might threaten humans' life. Table VI and Table VII show comparisons between the fine-tuned CNN networks and the the proposed ones in terms of Sensitivity and Specificity, respectively.

It can be observed that the COVID-19 class sensitivities of the proposed models are higher than the sensitivities of the fine-tuned models. Compared to the fine-tuned models, the overall sensitivities and specificities obtained by the proposed models are higher, which confirms the efficacy of our method.

2) Confusion matrix: We presented the confusion matrices on the test data of all seven models in Fig. 8. Fig. 8(A) presents the confusion matrix obtained by our proposed HCT model, using VGG19 as a backbone feature extractor. While 757 COVID-19 samples, 739 Pneumonia samples, and 717 Normal (healthy) samples were classified correctly, 43 COVID-19 samples, 61 Pneumonia samples, and 83 Normal (healthy) samples were misclassified. Therefore, the rate of correct classification of COVID-19 samples was 95%, whilst it was 92.5% for the Pneumonia samples and was 89.62% for the Normal (healthy) cases. On the other hand, Fig. 8(B) presents the confusion matrix obtained by the HCT model, using ResNet50 as a backbone features extractor, the rate of correct classification of COVID-19 samples was 97.5%, whilst it was 98.87% for the Pneumonia samples and was 94.37% for the Normal (healthy) cases. Further, Fig. 8(C) presents the confusion matrix obtained by the HCT model, using EfficientNetB0 as a

Fig. 6. One example of the segmentation result.



(A) (B) (C)

Fig. 7. Histogram represents the loss obtained by HCT Models for different learning rates, using: (A) VGG19, (B) ResNet50, (C) EfficientNetB0 as a backbone feature extractor.

backbone features extractor, the rate of correct classification of COVID-19 samples was 98.37%, whilst it was 98.75% for the Pneumonia samples and was 98.75% for the Normal (healthy) cases. It can be observed that our proposed method with EfficientNetB0 was able to classify 98.37% of COVID-19 infection cases accurately.

In addition, we also wanted to show the confusion matrices obtained by the CCT model and the individual fine-tuned networks, to compare their classification performance to the performance of the HCT proposed models. It can be argued that the False Positives(FP) and False Negatives(FN) has been reduced for each CNN using HCT. Similarly, if we compare the percentage of the correctly classified samples between (HCT-VGG19 and pretrained VGG19), (HCT-ResNet50 and pretrained ResNet50), and (HCT-EfficinetNeB0 and pretrained EfficinetNeB0), it can be observed that HCT models yielded a higher classification accuracy for all the three classes.

Whereas the FPs and FNs obtained by the CCT model are the highest among all the seven models. Moreover, it can be observed from the confusion matrix reported in Fig. 8, that the HCT-VGG19 proposed model has detected 757 out of 800 with COVID-19 as having COVID-19, achieving a COVID-19 class sensitivity of .946 compared to the fine-tuned VGG19 that has achieved a COVID-19 class sensitivity of .924 (see Table VI). The HCT-ResNet50 proposed model has detected 787 out of 800 with COVID-19 as having COVID-19, achieving a COVID-19 class sensitivity of .975 compared to the fine-tuned ResNet50 that has achieved a COVID-19 class sensitivity of .965. Our best-proposed HCT-EfficientNetB0 model has detected 787 out of 800 with COVID-19 as having COVID-19, achieving a COVID-19 class sensitivity of .984 compared to the fine-tuned EfficientNetB0 that has achieved a COVID-19 class sensitivity of .97.

3) The AUROC: ROC curves are typically used in binary classification to study the output of a classifier. To extend the ROC curve and ROC area to multi-class classification, there are two averaging strategies: one-vs-rest (OvR) and one-vs-one (OvO) [39]. In this study, we deployed the OvR algorithm, which computes the average of the ROC scores for each class against all other classes. Fig. 9 shows the AUROC curves of all seven models implemented in this research. The achieved AUC values for the fine-tuned models and the HCT models are above 0.97, which confirms that these models are reliable when performing the classification. Whereas the CCT model achieved an AUC value of 0.93.

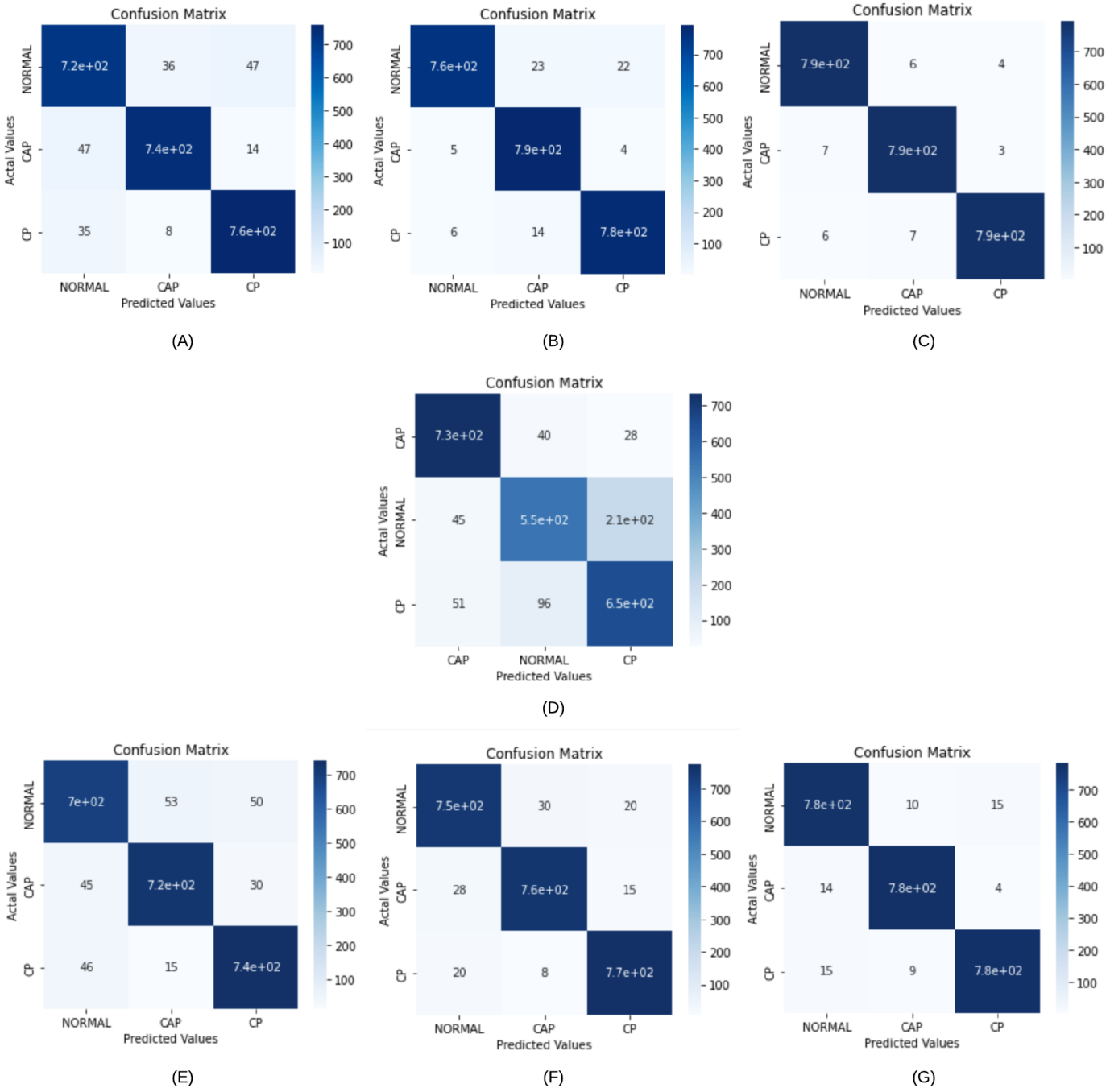


Fig. 8. Confusion matrix obtained by all the seven models implemented in this research: (A) HCT-VGG19, (B) HCT-ResNet50, (C) HCT-EfficientNetB0, (D) CCT, (E) pretrained-VGG19, (F) pretrained-ResNet50, (G) pretrained-EfficientNetB0.

TABLE V. SUMMARY OF ALL EXPERIMENTS FOR MULTI-CLASS CLASSIFICATION

Model	pretrained CNN	Accuracy	Precision	Recall	Specificity	F1 Score
TL	VGG19	89.52%	0.8811	0.8597	0.9420	0.8702
	ResNet50	94.62%	0.9737	0.9176	0.9737	0.9315
	EfficientNetB0	96.74%	0.9591	0.967	0.9793	0.9630
CCT		81.79	0.7856	0.7455	0.8972	0.7641
HCT	VGG19	92.00%	0.9217	0.9479	0.9597	0.9346
	ResNet50	97.25%	0.9702	0.9672	0.9851	0.9687
	EfficientNetB0	98.63%	0.9857	0.9862	0.9928	0.9860

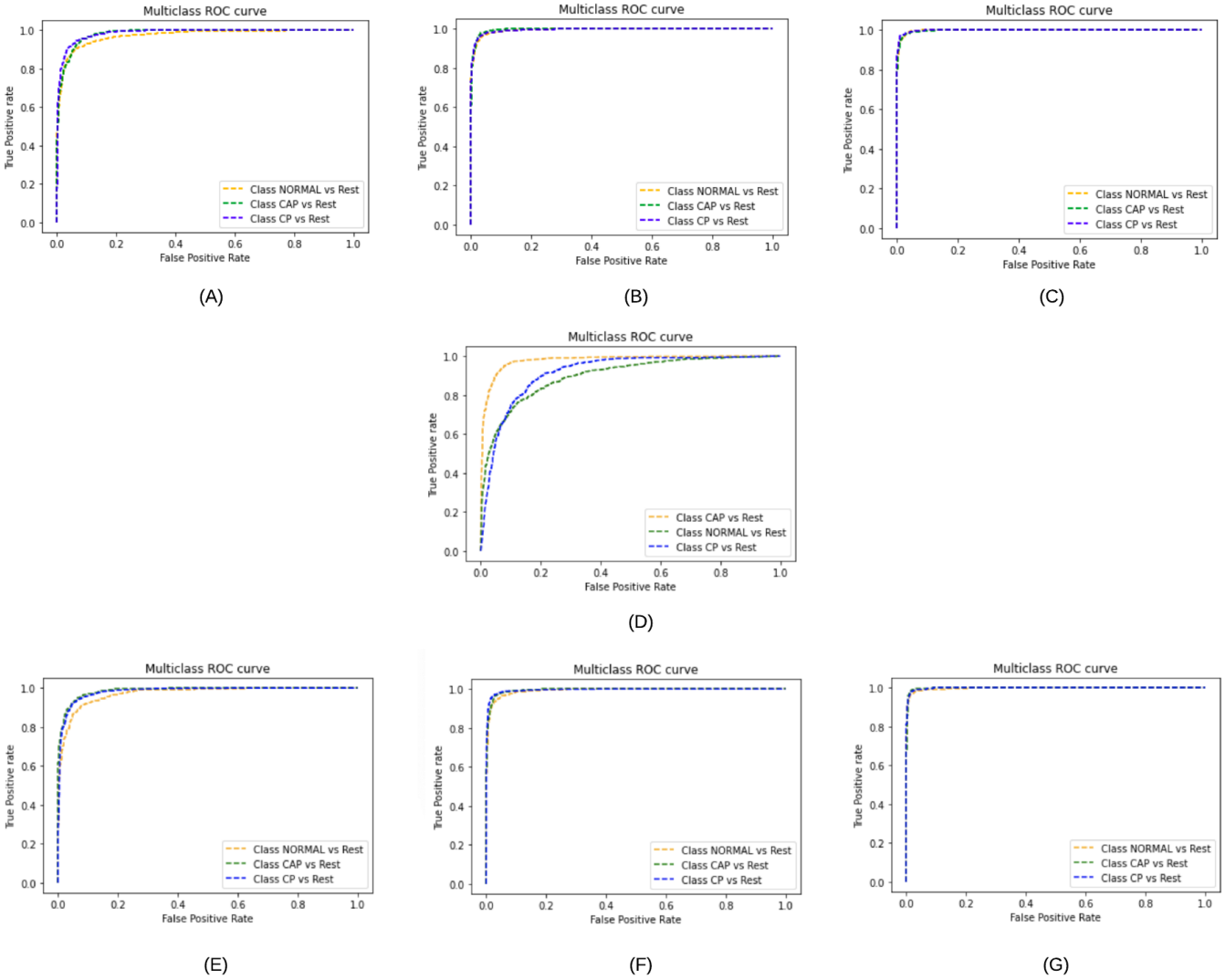


Fig. 9. ROC curve obtained by all the seven models implemented in this study: (A) HCT-VGG19, (B) HCT-ResNet50, (C) HCT-EfficientNetB0,(D) CCT, (E) pretrained-VGG19, (F) pretrained-ResNet50, (G) pretrained-EfficientNetB0.

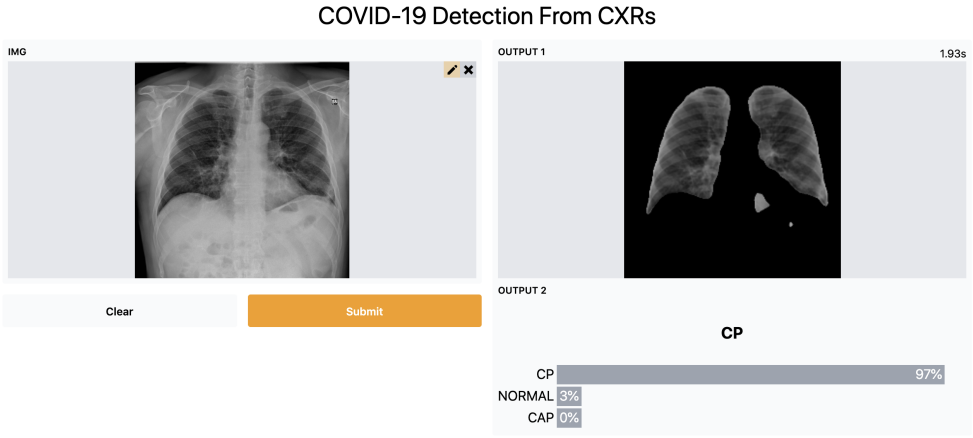


Fig. 10. Illustration of a classification result of a COVID-19 CXR image, obtained by the HCT model.

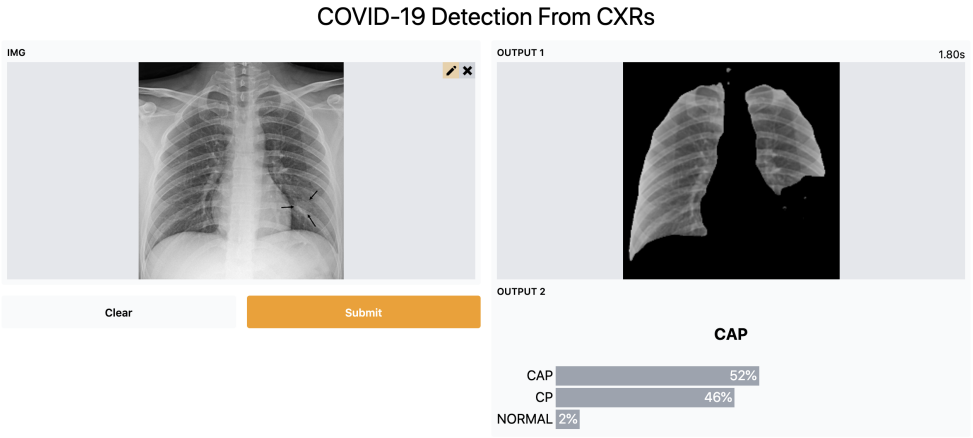


Fig. 11. Illustration of a misclassification result of a COVID-19 CXR image, obtained by the HCT model.

TABLE VI. A COMPARISON BETWEEN THE FINE-TUNED AND THE PROPOSED MODELS IN TERMS OF THEIR SENSITIVITIES

CNN \Backbone CNN Model	TL Models	HCT Models
VGG19	0.8597	0.9479
ResNet50	0.9176	0.9672
EfficientNetB0	0.967	0.9862

V. ANALYSIS AND DISCUSSIONS

A. Analysis of Classification Results

To demonstrate the performance of HCT, we randomly selected a COVID-19 CXR image, gave it input to the network, and acquired output on the image as shown in Fig. 10. The classification result was obtained by the best HCT model using EfficientNetB0 as a features extractor. Nevertheless, there is some confusion from the model sometimes between COVID-19, and Pneumonia samples, Fig. 11. This misclassification was possibly occurred because of our dataset. The Pneumonia samples in our dataset include viral and bacterial pneumonia. Considering that COVID-19 itself is a viral pneumonia disease. Furthermore, the GUI is created with Gradio, which is an open-source python library. Gradio permits researchers to quickly create easy-to-use and customizable UI components for their ML model [11].

TABLE VII. A COMPARISON BETWEEN THE FINE-TUNED AND THE PROPOSED MODELS IN TERMS OF THEIR SPECIFICITIES

CNN \Backbone CNN Model	TL Models	HCT Models
VGG19	0.9420	0.9597
ResNet50	0.9737	0.9851
EfficientNetB0	0.9793	0.9928

B. Comparison with State-of-the-Art Methods

In order to evaluate the proposed HCT model, the general performance comparison of our study with the state-of-art methods is given in this section. All networks were trained using our benchmark dataset. It can be observed that the proposed HCT-EfficientNetB0 model achieved higher performance than the other existing schemes. The results that are reported in this section are summarized in Table VIII.

Khan et al. [21] propose CoroNet, a Deep Convolutional Neural Network based on Xception architecture pretrained on

TABLE VIII. COMPARISON WITH STATE-OF-THE-ART STUDIES

Study	Model Used	Accuracy
Asif et al. [3]	Inception-v3	94.58%
Ozturk et al. [31]	DarkCovidNet	96.89%
Khan et al. [21]	CoroNet	89.30%
Mahmud et al. [25]	CovXNet	90.75%
Narin et al. [27]	Deep CNN ResNet-50	94.62%
Apostolopoulos & Mpesiana [2]	VGG19	89.52%
Proposed Method	HCT-VGG19	92%
	HCT-ResNet50	97.25%
	HCT-EfficientNetB0	98.63%

ImageNet dataset. The CoroNet model obtained an overall accuracy of 89.30%. Ozturk et al. [31] present DarkCovidNet design to the diagnosis of COVID-19. In their study, the main model was inspired by the DarkNet architecture that has proven itself in deep learning. Their model produced a 96.89% overall accuracy. Mahmud et al. [25] propose a deep neural network named CovXNet. The network architecture utilizes depth-wise convolution with varying dilation rates for efficiently extracting diversified features from CXRs. CovXNet achieved an overall accuracy of 90.75%. Oh et al. Further, Asif et al. [3], Narin et al. [27], and Apostolopoulos and Mpesiana [2], use transfer learning and obtained an overall accuracy of 94.58%, 94.62%, 89.52%, respectively. Indeed, DarkCovidNet achieved the best performance among the other proposed methods with a test accuracy of 96.89%. However, our proposed HCT-EfficientNetB0 surpasses DarkCovidNet and the other proposed methods with a test accuracy of 98.63%.

VI. CONCLUSIONS

In this research, we studied the deployment of deep learning models for COVID-19 detection using CXRs. As has been shown in research such as [24] [35] [2] [27], Transfer Learning (TL) gives the best classification results for the problem of pneumonia detection from CXR images. In our study, we investigated the use of our proposed Hybrid Compact Transformer (HCT), in which we integrate TL with Vision Transformers (ViTs) in one model. We aim to combine the localization power of CNNs, with the generalization power of ViTs. Based on the experimental results, HCT has shown satisfactory improvements over the respective accuracies of compact transformers (CTs) and models based on TL.This result could be useful for dealing with future respiratory pandemics where at their beginnings, only a few CXRs would be available for researchers.

Choosing the pretrained model can largely affect the accuracy of the final classifier. Performance results show that EfficientNetB0 pretrained model yielded the best performance among the three models. The proposed classification model with EfficientNetB0 as a feature extractor achieved more than 98% accuracy.

As a future research direction, we intend to increase the number of classes in our dataset to include: COVID-19, Viral-Pneumonia, Bacterial-Pneumonia, and Normal cases in order to have a more applicable model. We also want our model to be more interpretable. Thus, we will try to use interpretable saliency maps to correlate with the radiological findings. Moreover, the segmentation results could be further improved by training the Unet model with CLAHE enhanced CXR images, as mentioned in [41]. Authors in [28] proposed FCDenseNet103 as a backbone segmentation network architecture. They claimed that in comparison with Unet, FCDenseNet103 has higher segmentation performance. So using FCDenseNet103 on our dataset could improve the performance of our final proposed model. It would also be very interesting to assess the extent of usefulness of image segmentation in light of using pretrained models, like in our solution.

ACKNOWLEDGMENT

The authors gratefully acknowledge financial support from The Deanship of Scientific Research, King Faisal University (KFU) in Saudi Arabia. The present work was done under research project Number (KFU242418).

REFERENCES

[1] Mete Ahishali, Aysen Degerli, Mehmet Yamac, Serkan Kiranyaz, Muhammad EH Chowdhury, Khalid Hameed, Tahir Hamid, Rashid Mazhar, and Moncef Gabbouj. A comparative study on early detection of covid-19 from chest x-ray images. *arXiv preprint arXiv:2006.05332*, 2020.

[2] Ioannis D Apostolopoulos and Tzani A Mpesiana. Covid-19: automatic detection from x-ray images utilizing transfer learning with convolutional neural networks. *Physical and Engineering Sciences in Medicine*, page 1, 2020.

[3] Sohaib Asif, Yi Wenhui, Hou Jin, Yi Tao, and Si Jinhai. Classification of covid-19 from chest x-ray images using deep convolutional neural networks. *medRxiv*, 2020.

[4] Muhammad EH Chowdhury, Tawsifur Rahman, Amith Khandakar, Rashid Mazhar, Muhammad Abdul Kadir, Zaid Bin Mahbub, Khandaker Reajul Islam, Muhammad Salman Khan, Atif Iqbal, Nasser Al-Emadi, et al. Can ai help in screening viral and covid-19 pneumonia? *arXiv preprint arXiv:2003.13145*, 2020.

[5] Michael Chung, Adam Bernheim, Xueyan Mei, Ning Zhang, Mingqian Huang, Xianjun Zeng, Jiufa Cui, Wenjian Xu, Yang Yang, Zahi A Fayad, et al. Ct imaging features of 2019 novel coronavirus (2019-ncov). *Radiology*, 295(1):202–207, 2020.

[6] Joseph Paul Cohen, Paul Morrison, and Lan Dao. Covid-19 image data collection. *arXiv 2003.11597*, 2020.

[7] Alexey Dosovitskiy, Lucas Beyer, Alexander Kolesnikov, Dirk Weissenborn, Xiaohua Zhai, Thomas Unterthiner, Mostafa Dehghani, Matthias Minderer, Georg Heigold, Sylvain Gelly, et al. An image is worth 16x16 words: Transformers for image recognition at scale. *arXiv preprint arXiv:2010.11929*, 2020.

[8] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. pages 2672–2680, 2014.

[9] google colab pro. https://colab.research.google.com/signup. Accessed: 2021-9-20.

[10] Cyril Goutte and Eric Gaussier. A probabilistic interpretation of precision, recall and f-score, with implication for evaluation. In *European conference on information retrieval*, pages 345–359. Springer, 2005.

[11] Gradio. https://gradio.app/. Accessed: 2021-12-3.

[12] Varun Gulshan, Lily Peng, Marc Coram, Martin C Stumpe, Derek Wu, Arunachalam Narayanaswamy, Subhashini Venugopalan, Kasumi Widner, Tom Madams, Jorge Cuadros, et al. Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs. *Jama*, 316(22):2402–2410, 2016.

[13] Ali Hassani, Steven Walton, Nikhil Shah, Abulikemu Abuduweili, Jiachen Li, and Humphrey Shi. Escaping the big data paradigm with compact transformers. *arXiv preprint arXiv:2104.05704*, 2021.

[14] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778, 2016.

[15] Gao Huang, Zhuang Liu, Laurens Van Der Maaten, and Kilian Q Weinberger. Densely connected convolutional networks. pages 4700–4708, 2017.

[16] Forrest N Iandola, Song Han, Matthew W Moskewicz, Khalid Ashraf, William J Dally, and Kurt Keutzer. Squeezenet: Alexnet-level accuracy with 50x fewer parameters and¡ 0.5 mb model size. *arXiv preprint arXiv:1602.07360*, 2016.

[17] Jyoti Islam and Yanqing Zhang. Towards robust lung segmentation in chest radiographs with deep learning. *arXiv preprint arXiv:1811.12638*, 2018.

[18] Italian Society of Medical and Interventional Radiology. https://www.sirm.org/en/italian-society-of-medical-and-interventional-radiology/. Accessed: 2020-09-09.

[19] Irvin Jeremy, Rajpurkar Pranav, Ko Michael, Yu Yifan, Ciurea-Ilcus Silviana, Chute Chris, Marklund Henrik, Haghgoo Behzad, Ball Robyn, Shpanskaya Katie, et al. Mong david a. In *Halabi Safwan S., Sandberg Jesse K., Jones Ricky, Larson David B., Langlotz Curtis P., Patel Bhavik N., Lungren Matthew P., Ng Andrew Y. CheXpert: A Large Chest Radiograph Dataset with Uncertainty Labels and Expert Comparison. Proceedings of the AAAI Conference on Artificial Intelligence*, volume 33, pages 590–597, 2019.

[20] Kaggle. https://www.kaggle.com/nikhilpandey360/lung-segmentation-from-chest-x-ray-dataset/output?select=cxr_reg_weights.best.hdf5. Accessed: 2021-9-1.

[21] Asif Iqbal Khan, Junaid Latief Shah, and Mohammad Mudasir Bhat. Coronet: A deep neural network for detection and diagnosis of covid-19 from chest x-ray images. *Computer Methods and Programs in Biomedicine*, 196:105581, 2020.

[22] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. In *Advances in neural information processing systems*, pages 1097–1105, 2012.

[23] Ze Liu, Yutong Lin, Yue Cao, Han Hu, Yixuan Wei, Zheng Zhang, Stephen Lin, and Baining Guo. Swin transformer: Hierarchical vision transformer using shifted windows. *arXiv preprint arXiv:2103.14030*, 2021.

[24] Mohamed Loey, Gunasekaran Manogaran, and Nour Eldeen M Khalifa. A deep transfer learning model with classical data augmentation and cgan to detect covid-19 from chest ct radiography digital images. *Neural Computing and Applications*, pages 1–13, 2020.

[25] Tanvir Mahmud, Md Awsafur Rahman, and Shaikh Anowarul Fattah. Covxnet: A multi-dilation convolutional neural network for automatic covid-19 and other pneumonia detection from chest x-ray images with transferable multi-receptive feature optimization. *Computers in biology and medicine*, 122:103869, 2020.

[26] Agnieszka Mikołajczyk and Michał Grochowski. Data augmentation for improving deep learning in image classification problem. In *2018 international interdisciplinary PhD workshop (IIPhDW)*, pages 117–122. IEEE, 2018.

[27] Ali Narin, Ceren Kaya, and Ziynet Pamuk. Automatic detection of coronavirus disease (covid-19) using x-ray images and deep convolutional neural networks. *arXiv preprint arXiv:2003.10849*, 2020.

[28] Yujin Oh, Sangjoon Park, and Jong Chul Ye. Deep learning covid-19 features on cxr using limited training data sets. *IEEE Transactions on Medical Imaging*, 2020.

[29] World Health Organization. Diagnostic testing for sars-cov-2: interim guidance, 11 september 2020. Technical report, World Health Organization, 2020.

[30] Xi Ouyang, Jiayu Huo, Liming Xia, Fei Shan, Jun Liu, Zhanhao Mo, Fuhua Yan, Zhongxiang Ding, Qi Yang, Bin Song, et al. Dual-sampling attention network for diagnosis of covid-19 from community acquired pneumonia. *IEEE Transactions on Medical Imaging*, 2020.

[31] Tulin Ozturk, Muhammed Talo, Eylul Azra Yildirim, Ulas Baran Baloglu, Ozal Yildirim, and U Rajendra Acharya. Automated detection of covid-19 cases using deep neural networks with x-ray images. *Computers in Biology and Medicine*, page 103792, 2020.

[32] Sangjoon Park, Gwanghyun Kim, Yujin Oh, J. Seo, Sang Min Lee, Jin Hwan Kim, Sungjun Moon, Jae-Kwang Lim, and Jong-Chul Ye. Vision transformer using low-level chest x-ray feature corpus for covid-19 diagnosis and severity quantification. *ArXiv*, abs/2104.07235, 2021.

[33] Paul Mooney. Chest x-ray images (pneumonia). https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia. Accessed: 2020-09-22.

[34] Radiopaedia. Cases. https://radiopaedia.org/encyclopaedia/cases/chest?lang=us&modality=X-ray&page=1#collapse-by-diagnostic-certainties. Accessed: 2020-09-10.

[35] Md Mamunur Rahaman, Chen Li, Yudong Yao, Frank Kulwa, Mohammad Asadur Rahman, Qian Wang, Shouliang Qi, Fanjie Kong, Xuemin Zhu, and Xin Zhao. Identification of covid-19 samples from chest x-ray images using deep learning: A comparison of transfer learning approaches. *Journal of X-ray Science and Technology*, (Preprint):1–19, 2020.

[36] Tawsifur Rahman, Muhammad EH Chowdhury, Amith Khandakar, Khandaker R Islam, Khandaker F Islam, Zaid B Mahbub, Muhammad A Kadir, and Saad Kashem. Transfer learning with deep convolutional neural network (cnn) for pneumonia detection using chest x-ray. *Applied Sciences*, 10(9):3233, 2020.

[37] Pranav Rajpurkar, Jeremy Irvin, Kaylie Zhu, Brandon Yang, Hershel Mehta, Tony Duan, Daisy Ding, Aarti Bagul, Curtis Langlotz, Katie Shpanskaya, et al. Chexnet: Radiologist-level pneumonia detection on chest x-rays with deep learning. *arXiv preprint arXiv:1711.05225*, 2017.

[38] Sadman Sakib, Tahrat Tazrin, Mostafa M Fouda, Zubair Md Fadlullah, and Mohsen Guizani. Dl-crc: Deep learning-based chest radiograph classification for covid-19 detection: A novel approach. *IEEE Access*, 8:171575–171589, 2020.

[39] Suman Kumar Reddy. https://inblog. Accessed:2021-12-5.

[40] Mingxing Tan and Quoc Le. Efficientnet: Rethinking model scaling for convolutional neural networks. In *International Conference on Machine Learning*, pages 6105–6114. PMLR, 2019.

[41] Enzo Tartaglione, Carlo Alberto Barbano, Claudio Berzovini, Marco Calandri, and Marco Grangetto. Unveiling covid-19 from chest x-ray with deep learning: a hurdles race with small data. *International Journal of Environmental Research and Public Health*, 17(18):6933, 2020.

[42] Thread reader. Chest imaging. https://threadreaderapp.com/thread/1243928581983670272.html. Accessed: 2020-09-22.

[43] Hugo Touvron, Matthieu Cord, Matthijs Douze, Francisco Massa, Alexandre Sablayrolles, and Hervé Jégou. Training data-efficient image transformers & distillation through attention. In *International Conference on Machine Learning*, pages 10347–10357. PMLR, 2021.

[44] Towards data science. https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5. Accessed: 2020-12-3.

[45] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. In *Advances in neural information processing systems*, pages 5998–6008, 2017.

[46] Abdul Waheed, Muskan Goyal, Deepak Gupta, Ashish Khanna, Fadi Al-Turjman, and Plácido Rogerio Pinheiro. Covidgan: Data augmentation using auxiliary classifier gan for improved covid-19 detection. *IEEE Access*, 8:91916–91923, 2020.

[47] Kun Wang, Xiaohong Zhang, Sheng Huang, Feiyu Chen, Xiangbo Zhang, and Luwen Huangfu. Learning to recognize thoracic disease in chest x-rays with knowledge-guided deep zoom neural networks. *IEEE Access*, 8:159790–159805, 2020.

[48] Xiaosong Wang, Yifan Peng, Le Lu, Zhiyong Lu, Mohammadhadi Bagheri, and Ronald M Summers. Chestx-ray8: Hospital-scale chest x-ray database and benchmarks on weakly-supervised classification and localization of common thorax diseases. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 2097–2106, 2017.

[49] wikipedia. https://en.wikipedia.org/wiki/Confusion_matrix. Accessed: 2020-12-3.

[50] Wikipedia. https://en.wikipedia.org/wiki/Receiver_operating_characteristic. Accessed: 2020-12-3.

[51] Wikipedia. https://en.wikipedia.org/wiki/Sensitivity_and_specificity. Accessed: 2021-12-5.

AI-Blockchain Approach for MQTT Security: A Supply Chain Case Study

Raouya AKNIN, Hind El Makhtoum, Youssef Bentaleb
Ibn Tofail University, Engineering Sciences Laboratory, Kenitra, Morocco
0000-0002-4644-055X

***Abstract*—The use of the MQTT protocol in critical sectors such as healthcare and industry has prompted research to propose solutions for strengthening its security and preventing it from attacks that are growing exponentially and becoming increasingly sophisticated and difficult to detect. This paper aims to improve the security of the MQTT architecture, ensuring it is resilient to current attacks and adaptable to potential future attacks while considering the constraints of the IoT environment. To achieve this, the proposed architecture is based on the interaction between the AI model, which continuously analyzes device behavior, and smart contracts, which automatically apply appropriate security measures once fraud is detected. A device reputation mechanism is used to prevent malicious devices from rejoining the network. The AI model proposed in this article was initially trained on a set of malicious behaviors using supervised learning. The results show that the detection accuracy achieved 95.97%. This accuracy is expected to improve over time through the integration of unsupervised learning into the architecture, enabling the discovery of new attack patterns and additional parameters for malicious behavior identification. For simulation testing, the architecture was applied to supply chain management as a case study of critical applications, and smart contracts were deployed in the Remix environment. The architecture demonstrated resilience and robustness across various attack scenarios.**

***Keywords*—IoT; MQTT; blockchain; smart contracts; AI hybrid model; device reputation**

I. Introduction

The advent of the Internet of Things (IoT) has revolutionized the interaction between real objects and the digital world by breaking down the boundaries between these two worlds. Indeed, The emergence of cutting-edge technologies such as wireless sensor networks (WSN), Radio Frequency Identification (RFID), cloud computing, and others that facilitate real-time data collection, sharing, and analysis has enabled better real-time decision-making, remote supervision and control of environments, and the automation of tasks and processes. This has opened up a wide range of IoT advanced services in several domains ranging from simple applications such as smart household appliances to critical applications like supply chain management, smart grids, and healthcare applications. According to [1], by the end of 2025, the number of IoT devices worldwide is expected to exceed 75 billion devices and the compound annual growth (CAGR) in the IoT market is forecast to average 10.49% between 2024 and 2029, bringing the total market value to $1,560 billion by 2029 [2].

Nevertheless, the expansion of connected objects into more sensitive and critical areas has raised concerns about the security of the protocols frequently employed in this environment. The native security measures of these protocols no longer meet the requirements of critical applications, and attacks targeting the IoT environment have become more numerous and complex. For instance, the Message Queuing Telemetry Transport (MQTT), the most widely used protocol in this environment, is vulnerable to several types of attacks, including man-in-the-middle (MITM) attacks due to a lack of encryption, denial-of-service (DoS) attacks because of the centralized architecture and the broker's single point of failure, and unauthorized access resulting from weaknesses in the authentication mechanism.

To overcome these challenges, many articles have proposed an enhanced security architecture using blockchain as the one of the promising solutions [3]–[8]. Indeed, the decentralized nature of blockchain minimizes denial-of-service attacks and avoids the single points of failure, which are considered nightmares in the field of cybersecurity. Moreover, it ensures data integrity and enables the traceability of actions carried out on the network. The use of smart contracts to automate actions on the network is another advantage of using blockchain technology. Artificial intelligence (AI) is also another a cutting-edge technology that is used to enhance the MQTT architecture by proposing solutions to detect the malicious behaviors and potential MQTT attacks [9]–[11].

The goal of this article is to propose an MQTT architecture that meets the security requirements of critical IoT applications, is resilient to current attacks, and is adaptable to potential attacks, while taking into account the IoT constraints. To this end, it aims to improve the architecture proposed in our previous research work [4] by adding an additional layer of protection based on artificial intelligence. The advantage of the proposed solution is that it combines AI technology to detect the abnormal behavior of connected devices or those attempting to connect to the network, with smart contracts to automatically apply the appropriate security measures. It also introduces the concept of device reputation to prevent malicious devices from rejoining the network.

The remainder of this paper is structured as as follows: Section II provides a summary of research works that have been proposed improved MQTT architectures using cutting-edge technologies. Section III outlines the paper's contribution by combining blockchain and AI technologies to enhance MQTT protocol security. Section IV presents our proposed solution that combines blockchain and AI for a resilient and attack-resistant MQTT architecture. Section V discusses the results of attack test scenarios on the proposed solution. Section VI summarizes the main ideas discussed in this paper and provides an overview of future research directions to further improve the security of the MQTT protocol while respecting the constraints

of the IoT environment.

II. Related Works

Several research works have proposed solutions to improve the security of the MQTT protocol, which is the most widely used protocol in the IOT environment to meet the IOT critical applications requirements. Indeed, many articles have used blockhain [3]–[8] to enhance the MQTT security since it ensures data integrity, avoids a single point of failure, and enables the traceability of the actions performed in the network. Moreover, the use of smart contracts to automate network actions is another advantage of blockchain technology. On the other hand, several articles have leveraged artificial intelligence (AI) to enhance the security of the MQTT protocol. However, these studies primarily focus on attack detection. Indeed, article [9] has proposed an optimized model for intrusion detection in the MQTT-based IoT networks. For this purpose, an empirical comparison between 22 machine learning (ML) algorithms was established, concluding that the Generalized Linear Model (GLM) classifier with the random oversampling technique showed the best detection performance. Along the same lines, article [10] has proposed an AI model based on supervised learning to detect attacks threatening the MQTT protocol. To achieve this, a comparative analysis of various supervised learning algorithms was conducted. It ultimately concluded that the convolutional long short-term memory neural network (CNN-LSTM) algorithm outperforms other models in terms of accuracy and performance for intrusion detection on the MQTT protocol. Although these articles contribute to the selection of the most effective learning algorithms for MQTT attack detection, they have however, proposed AI models based on supervised learning algorithms, making them limited to the attacks specified in the training phase. To address this, article [11] has introduced an MQTT intrusion detection system based on a Generative Adversarial Network-based autoencoder (GAN-AE), an unsupervised learning algorithm that allows the detection of different types of attacks by analyzing the behavior.Although the solution showed its ability to adapt to new and evolving attack scenarios and the overall detection rate reached 99.2%, however, like the above-mentioned articles, the proposed system is limited to intrusion detection without implementing security measures to prevent these attacks. Additionally, since the proposed solution may introduce false positives, it will be difficult to implement security measures automatically. Combining AI solutions for attack detection and blockchain, more specifically, smart contracts to automatically apply appropriate security measures seems to be a promising solution. Article [1] has proposed a framework that combines AI and blockchain technologies to enhance security in the IOT environment. It has introduced a new security layer, integrating blockchain and AI into the traditional three-layer IoT architecture [12]. However, the article does not propose any real implementation and it emphasizes the need for further research to develop effective strategies for combining these technologies to create reliable and secure digital ecosystems in the IoT landscape. The research in [13] has proposed an intelligent architecture that detects smart meter authentication fraud and consequently prevents their access to the network. In addition, it introduced the notion of reputation to prevent malicious smart meters from rejoining the network. Unlike previous articles, this paper implements smart contracts to automatically apply the appropriate security measures when fraud is detected. However, the paper only proposes a theoretical solution for the IOT architecture, without specifying the protocol used or implementing the AI model. Moreover, it focuses only on authentication attacks. Table I summarizes the approaches used in related works, focusing on the contribution of the articles to enhancing the security of the MQTT protocol to meet the requirements of critical applications, the technologies used, and the limitations of the proposed solutions.

Limits and Issues: By analyzing the solutions presented in Table I, two major challenges can be identified:

- Although solutions based on blockchain and smart contracts meet the security requirements of IoT critical applications in terms of confidentiality, integrity, and availability, they cannot address all types of attacks or predict potential ones.
- Solutions designed to detect MQTT attacks are either based on supervised learning, which is limited to the attacks specified during the training phase, or on unsupervised learning, which may introduce false positives.

Combining these two promising solutions can significantly enhance MQTT security by leveraging AI techniques to detect attacks and utilizing smart contracts to enforce appropriate security measures. However, existing articles addressing this combination mainly propose theoretical models without implementing the full process. To this end, the contribution of this paper lies in implementing and testing the interaction between an AI model for attack detection and smart contracts to apply the corresponding security measures. Additionally, the solution relies on a hybrid AI model that combines a supervised learning algorithm to detect known attacks and an unsupervised learning algorithm to identify potential new or unknown attack types.

III. Paper's Contribution

The solution proposed in this article combines the use of blockchain and AI technologies to improve the security of the MQTT protocol. Indeed, the AI model allows the real-time detection of malicious behaviors and consequently the automatic application of the appropriate security measures using smart contracts, ensuring a fast and efficient response to potential attacks. Furthermore, the decentralized nature of the blockchain minimizes the risk of denial-of-service attacks and eliminates the challenges associated with the single point of failure. Blockchain also guarantees data integrity and ensures accountability for actions performed in the network, which is useful for monitoring and post-incident analysis. Moreover, the hybrid approach of the AI model enables continuous learning of sophisticated and complex attack patterns and relevant parameters for identifying malicious devices. For added security, the concept of reputation has been introduced to maintain records of device behavior and therefore prevent previously classified malicious devices from rejoining the network. Although the solution used consistent technologies such as blockchain and AI algorithms, it does not adversely affect the performance of the constrained IoT environment since resource-intensive operations are managed on the brokers network side, typically located in the cloud or data centers while the only operation executed on the device side is the OTP calculation.

TABLE I. SUMMARIZATION OF APPROACHES USED IN RELATED WORKS FOR ENHANCING MQTT SECURITY

Article	Main objective	Technology	Limitations
[4]	Proposes a decentralized MQTT architecture that meets the security requirements of critical applications without affecting the overall protocol performance or the constraints of the IoT environment.	Blockchain and smart contracts	Cannot cover all types of attacks or predict potential ones.
[5]	Improves the authentication process using a one-time password (OTP) and smart contracts to provide an independent channel for managing two-factor authentication. The solution also ensures accountability through blockchain.	Blockchain and smart contracts	• Does not address the single point of failure issue as it relies on a broker. • Focuses only on the authentication process. • Cannot cover all types of attacks or predict potential ones.
[6]	Proposes a novel approach solution that relies on blockchain sharding to achieve robust security while minimizing computational overhead.	Blockchain and smart contracts	Cannot cover all types of attacks or predict potential ones.
[7]	Proposes a decentralized solution that meets the security requirements of critical IoT applications regarding confidentiality, integrity, and control access to the topics managed by the broker.	Blockchain and smart contracts	• Does not address the single point of failure issue as it relies on a broker. • Focuses only on the authentication process. • Cannot cover all types of attacks or predict potential ones.
[8]	• Proposes a holistic, decentralized solution for securing MQTT. • Introduces a token stored on the blockchain to control topic access and avoid permanent credentials.	Blockchain and smart contracts	• Uses TLS in resource-constrained environments. • Impacts the overall protocol performance. • Cannot cover all types of attacks or predict potential ones.
[9]	Proposes an optimized model for intrusion detection in the MQTT-based IoT networks.	AI model based on supervised learning algorithm: Generalized Linear Model (GLM) classifier with the random oversampling technique.	• Provides a solution for detecting attacks without implementing security measures. • Supervised learning models are limited to attacks specified in the training phase.
[10]	Proposes an AI model based on supervised learning to detect attacks threatening the MQTT protocol.	AI model based on supervised learning algorithm: The convolutional long short-term memory neural network (CNN-LSTM).	• Provides a solution for detecting attacks without implementing security measures. • Supervised learning models are limited to attacks specified in the training phase.
[11]	• Proposes an MQTT intrusion detection system based on a Generative Adversarial Network-based auto-encoder (GAN-AE) to detect various types of attacks by analyzing behavior. • The solution demonstrated adaptability to new and evolving attack scenarios with an overall detection rate of 99.2%.	AI model based on unsupervised learning: Generative Adversarial Network based auto-encoder (GAN-AE)	• Provides a solution for detecting attacks without implementing security measures. • May introduce false positives.
[1]	Proposes a framework combining AI and blockchain technologies to enhance security in IoT by adding a new security layer to the classical three-layer architecture.	• Blockchain and smart contracts. • AI technology.	The framework is theoretical and lacks real-world implementation.
[13]	• Proposes an intelligent architecture that detects smart meter authentication fraud and consequently prevents their access to the network. • Introduces the notion of reputation to prevent malicious smart meters from rejoining the network.	• Blockchain and smart contracts. • AI technology.	• Doesn't implement the AI model. • Focuses only on authentication attacks.

IV. THE ENHANCED MQTT PROTOCOL

Since attacks targeting connected objects in general, and the MQTT protocol in particular, are constantly evolving and it is impossible to anticipate and cover all potential threats, this article aims to enhance the architecture proposed in our previous work [4] by introducing a new layer of protection based on artificial intelligence. As depicted in Fig. 1, the basic architecture is based on a consortium blockchain and smart contracts to automate the MQTT authentication, publication, and subscription processes. It comprises a client, which can be a publisher or a subscriber, and a brokers network that executes the smart contracts. Communication between the components is divided into three phases: the registration phase, the connection phase, and the publication phase. The AI solution proposed in this paper aims to analyze the behavior of devices connected to the network, as well as those attempting to authenticate, in order to effectively interrupt or prevent malicious connections accordingly. The behavior analysis is based on a set of relevant parameters that enable the identification of the device's behavior to determine whether it is malicious or legitimate. Once a device is detected as malicious, its reputation is automatically changed to false to prevent its reintegration into the network. It is important to note that the device's reputation can be changed either when it matches a predefined rule in the smart contracts (wrong One-Time-Password (OTP), unregistered device, unauthorized publication, etc.) or when the AI model detects a malicious behavior. Despite the use of technologies such as blockchain and intelligent algorithms, which require the use of resources,

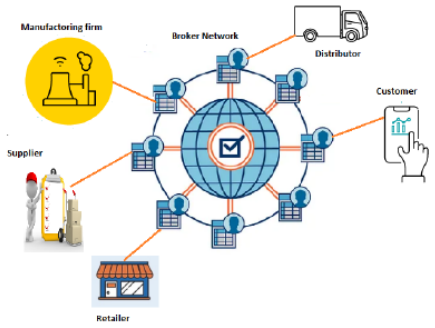


Fig. 1. MQTT architecture for supply chain management [4].

the solution aims to account for IoT environment constraints by offloading resource-intensive operations to the brokers' network, typically located in the cloud or data centers, while leaving only the OTP calculation to the MQTT clients.

A. AI-Enhanced MQTT Architecture

As depicted in Fig. 2, the new architecture has introduced an AI component to continuously analyze the devices's behavior that are connected or in the process of connecting, to detect potential fraud. Once fraud is detected, a transaction is performed to invoke the smart contracts and apply the required security countermeasures. Before integrating the AI model into the operational MQTT architecture, it was first trained using test datasets simulating a real state of the MQTT traffic, and

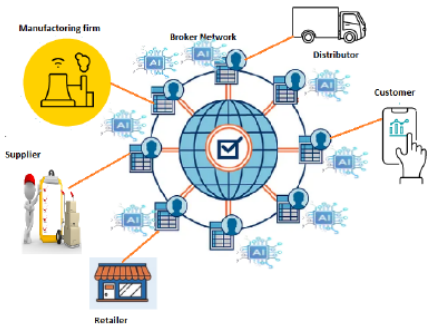


Fig. 2. AI-enhanced MQTT architecture.

then the model was tested. It is also important to note that the AI model will be permanently improved in order to integrate new potential attack types. The key steps of building and improving the AI model will be detailed in Section IV-A1.

1) AI model for device behavior analysis: The approach used to build and improve the AI model is based on hybrid learning, combining supervised learning to detect known attacks and unsupervised learning to discover new patterns of unknown attacks or other parameters for detecting malicious devices. The key stages of our approach are detailed below:

a) Stage 1: Defining the initial parameters using supervised learning
This phase aims to design an AI model that allows the prediction of malicious devices based on a set of parameters defined in Table II. The model is based on supervised learning, which uses labeled data for the model training to predict device Tbehavior subsequently. **Workflow 3** defines the steps to be followed during this phase, and is created using KANIME software.[1]
Workflow detail
- Dataset: The dataset used by the AI model in this phase either for training and testing is available via the link[2]; it simulates real-world network conditions during communication between an MQTT broker and eight sensors, and includes both normal and malicious activities. The behavior of devices is identified based on a set of relevant parameters, as detailed in Table II. The CSV Reader node is employed to load this data into KNIME.
- Data Pre-processing: This step consists of data preprocessing, which involves preparing the raw data so that it can be used effectively by the machine learning algorithms. This includes encoding categorical variables, and scaling numerical features [14].To do this, a **Label Encoding method** which assigns a unique integer to each category of a variable, and **Standard scaling** method which consists of centering the data around 0 with a variance of 1 are used, respectively. The **Category to Number** and **Normalizer** KNIME nodes are used for this purpose.
- Data Splitting: Using the Partitioning KNIME node, the dataset was divided into two categories: 70% for training and 30% for testing.
- Model selection: The model used in this article is the **Random Forest (FR)** classifier, as it provides the higher accuracy (91%) compared with other models k-nearest neighbors (KNN) (90%) and Decision Tree (85%) [15], and it is faster and more scalable for a huge database with many features compared to Support Vector Machine (SVM) which becomes very expensive in terms of computing time and memory for large databases [16]. Random Forest (RF) is an ensemblistic classifier that works by creating multiple decision trees. Each tree is built using a random subset of training samples and variables. It is based on Bootstrap Aggregating where each tree is trained on a different sample of data, drawn with a discount. Each decision tree in the forest makes its own prediction based on the input features. The final result of the RF classifier is determined by aggregating the predictions of all the individual trees, usually by majority vote for classification tasks or by average for regression tasks [17].
- Model training and Evaluation: In this phase, the model was trained and then tested using the training dataset (70%) and test dataset (30%), respectively. For this purpose, the **Random Forest Learner** and **Random Forest Predictor** KNIME nodes are used. The **Scorer** KNIME node is used for evaluation.

Interpretation and discussion of the results: To evaluate the model's ability to identify malicious behaviors, the following metrics were used:
- Accuracy: This metric measures the model's ability to correctly classify devices based on their behavior. In our case, as shown in Fig. 4, the model correctly classified 95.97% of the devices.
- Recall: This metric indicates the proportion of actual malicious behaviors correctly detected by the model. It is calculated using the following formula: $Recall = \frac{TP}{TP+FN} = 0.937$ TP (True Positive): The number of malicious behaviors correctly identified as such by the model. According to the confusion matrix (Fig. 4), this value is 46,492. FN (False Negative): The number of malicious behaviors that the model failed to detect. From the same confusion matrix, this value is 3,110. **Thus, the model successfully detected 93.7% of the malicious behaviors.**
- F1 Score: This metric evaluates the balance between the model's precision (ability to avoid misclassifications) and recall (ability to detect malicious behaviors). It is calculated using the formula:
$F1\ Score = 2 \times \frac{\text{Accuracy} \times \text{Recall}}{\text{Accuracy} + \text{Recall}} = 0.97$

These results indicate that the model offers strong overall performance, with an excellent compromise between the ability to detect malicious behavior and avoid misclassification of devices. Hence, upon completion of this phase, the model can be considered robust enough for deployment within the real-world MQTT architecture to detect all malicious behaviors it has been trained on.

b) Stage 2: Discovering new parameters and patterns for device behavior analysis using unsupervised learning
In this step the unsupervised learning algorithm will be incorporated into the real-world MQTT architecture to

[1]Knime, https://www.knime.com/
[2]MQTTset, https://www.kaggle.com/datasets/cnrieiit/mqttset

TABLE II. FRAUD DETECTION PARAMETERS OVERVIEW

Parameters	Description
IP source address	The device's IP address can help identify abnormal behavior, such as connecting from unusual regions or connecting with an IP address that belongs to the same address range as a device already detected malicious.
Geolocation	The device's location can be used to detect suspicious connections from unusual or unauthorized regions.
Timestamp	Timestamps can detect abnormal activities, such as connections occurring at unusual hours, inconsistent time intervals between connections, or instances where publish and subscribe messages are sent before establishing a connection.
Message size and format	An unusual size or format of MQTT messages can be used to identify malicious devices.
Messages Frequency	This parameter is used to detect abnormal activity and behavior, such as multiple simultaneous MQTT connections from source IP addresses within the same range, which may indicate that the device is part of a botnet network.
Session duration	This parameter can identify irregular behavior or activity. For instance, a device that frequently connects and disconnects may be flagged as suspicious.
Open ports	Open ports other than those used by the MQTT protocol or those used by standard applications can identify malicious devices.
Identifier format	A device could be classified as malicious if its identifier format deviates from the standard format.

adapt to new forms of fraudulent behavior by analyzing real-time traffic and identifying deviations from normal patterns. This approach enables us to discover new parameters that were not previously identified. However, due to the constraints of working within a real MQTT architecture, we will use NS-3 [18] network simulation environment in order to generate different types of traffic and behaviors corresponding to both legitimate and malicious activities. It's also important to note that no security measures are applied to the anomalies detected during this phase. **Worfflow 5** defines the steps to be followed during this phase, and it is created using KANIME software (Fig. 3, 5).

Worflow detail

- Data preparation: After running the simulation script in the NS-3 simulator, the data will be logged into "simulation_trace.csv".This file will be loaded into KNIME using the **CSV reader** node.
- Data Pre-processing: This step pre-processes the data to make it suitable for the Isolation Forest algorithm, the unsupervised learning algorithm used in this phase. This includes handling missing values, encoding categorical data, and scaling data. The KNIME nodes used for this purpose are: **Missing value** to handle missing values by replacing them with a mean value, **One to many** to encode categorical data, and **Normalizer** to scale the data.
- Application of Isolation Forest: In this step, the Isolation Forest algorithm was applied to identify potential anomalies in the dataset. The isolation forest calculates an anomaly score for each observation in the dataset. This score provides a measure of the normality of each observation relative to the entire dataset. To calculate this score, the algorithm isolates the dataset in question in a recursive manner: it chooses a variable at random and sets a random cut-off point, then evaluates whether this isolates a particular observation [19]. The KNIME node used for this purpose is the **Isolation Forest** node.
- Anomalies analysis: Fig. 6, 7 depict the most relevant parameters that can be added to the initial parameters for devices behavior analysis. As shown in Fig. 6, for all parameters, normal instances are centered around the mean (0) with low standard deviations, while abnormal instances deviate significantly from the mean with higher standard deviations. The above parameters can be summarized as follows:
  Device physical features: This parameter includes a set of device characteristics namely computing power (GHz), storage capacity (GB), and memory (GB). As shown in Fig. 6, the abnormal instances have significantly higher CPU, storage, and memory values than the normal ones. Therefore, we can say that this parameter is relevant for detecting malicious devices since the sensors are generally equipped with low computing power, storage capacity, and memory.
  Device resources consumption: This parameter measures the rate of resource consumption, more specifically the percentage of CPU utilization (%) and power consumption (W). As shown in Fig. 6, the abnormal instances tend to consume more energy and processing power, and this is likely due to the deployment of heavy malicious applications or abnormal processing. Hence this parameter is considered as relevant for identifying malicious devices.
  Installed software: This parameter is used to identify the number of applications installed on the devices. As can be seen in Fig. 6, abnormal instances contain a relatively large number of applications compared with normal instances, so this parameter can also be used to identify malicious devices, since the applications installed in sensors are generally limited.
  Firmware type and version: This parameter is used to identify the type and version of firmware installed on the devices. To facilitate the interpretation of the results for this parameter, we have converted the numerical values used by the model into two categories (Fig. 7): **Standard**, which includes known firmware with recent versions, and **unkown**, which contains unknown firmware, obsolete or test versions. This parameter is also relevant for identifying malicious devices.

  Conclusion: The relevant parameters we identified during this phase are **device physical features, device resource consumption, and firmware type and version**. These parameters will be added to the initial parameters to improve the accuracy of the model and help better identify malicious devices.

c) Stage 3: Model enhancements:
   The new parameters identified by the unsupervised learning algorithm will be fed back into the supervised model to refine detection criteria and improve model accuracy.

2) The communication phases: The communication between the brokers network and clients (Publisher/subscriber) occurs in three main steps:

- Registration phase: In this phase, each device must be registered in the blockchain by a trusted administrator.

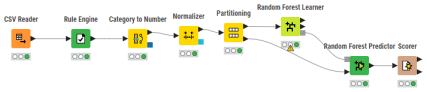


Fig. 3. AI-model workflow (phase 1).

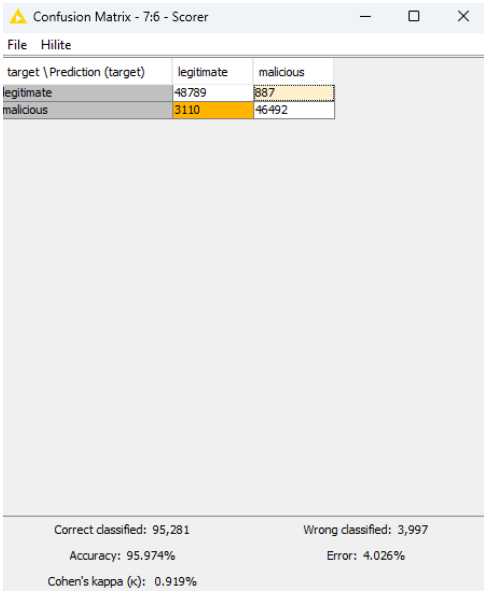


Fig. 4. Confusion matrix.

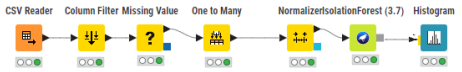


Fig. 5. AI-model workflow (phase 2).

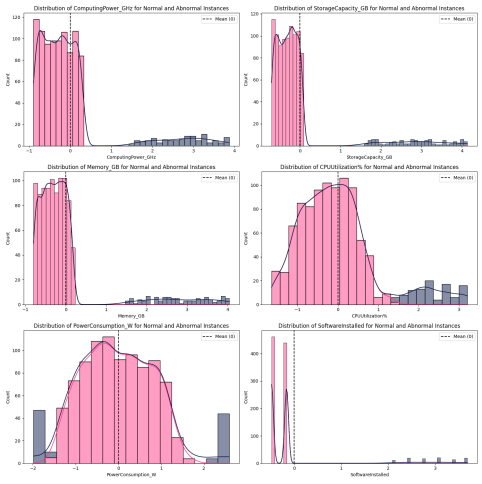


Fig. 6. Relevant parameters distribution for normal and abnormal instances.

The latter assigns publication and subscription rights to specific topics and, in return, he retrieves the required keys for authentication and message encryption and communicates them to the devices in out-of-band mode. When an administrator registers a device, its reputation is set to

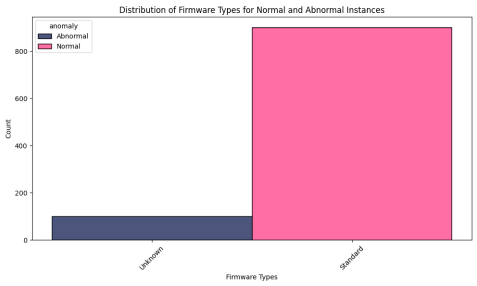


Fig. 7. Firmware type distribution for normal and abnormal instances.

true by default. The exchange details are illustrated in sequence Fig. 8 and the functioning of the smart contract responsible for this phase is described in the activity Fig. 9.

- Connection phase: As depicted in the sequence Fig. 10, when the brokers network receives a connection request, it verifies the packet number, the device registration, and the reputation. If the device is not registered, the connection will be denied and the device will be added to the blockchain with a reputation set to False. Then, if the device's reputation is false, the connection to the brokers network is denied; otherwise, a challenge is sent to a device for OTP calculation. The device calculates the OTP and sends the hashed OTP. If it is correct, the device is connected to brokers network else, the connection is denied and the reputation is set to false . Simultaneously, the AI model constantly analyzes device behavior. Once it detects malicious behavior, it invokes the smart contract to interrupt the connection process and change the device's reputation to false. The functioning of the smart contract responsible for this phase is described in the activity Fig. 11.
- Publishing phase: As depicted in sequence Fig. 12, in this phase, once a device publishes a message to brokers network containing a topic name, and encrypted data using the secret topic key, the smart contract checks its rights to publish to that topic as well as the data integrity and then it notifies all the subscribers to that topic. If the client doesn't have the right to publish in this topic, the connection is automatically interrupted and the reputation is changed to false. During this phase, if the AI model detects fraud, it invokes the smart contract to interrupt the connection and change the device's reputation to false. The functioning of the smart contract responsible for this phase is described in the activity Fig. 13.

V. Attack Scenarios Analysis

For the test simulation, we apply the proposed architecture in Supply Chain Management as an IOT critical application and perform the tests in the Remix environment.[3] Indeed, the proposed solution fully fit the requirement of the supply chain management since it requires the intervention of multiple independent entities such as suppliers, manufacturers, distributors, retailers, and end customers. Each entity has the right to publish and subscribe to specific topics. These rights

[3]Remix IDE, https://remix.ethereum.org/

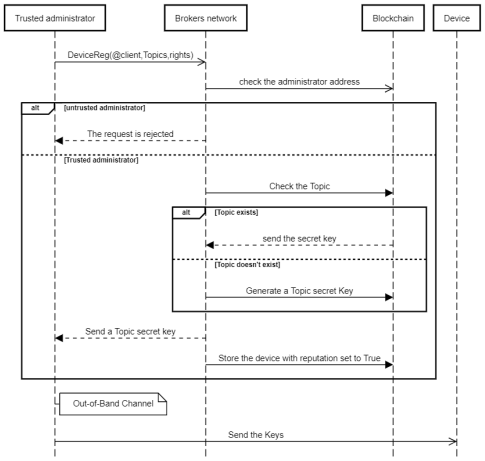


Fig. 8. Registration phase sequence diagram.

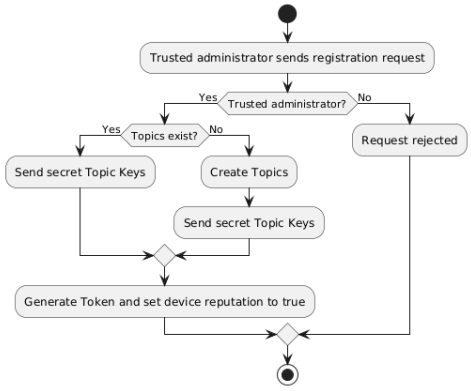


Fig. 9. Registration phase smart contract logic.

are granted by the administrator of each entity during the registration phase.

A. Test Cases

- Scenario 1: Registration nominal scenario
  As an example, the Manufacturer's administrator registers the temperature sensor for the concerned entity. As shown in Fig. 14, they assign write-only permissions to the topic "Man_smart_sensor/temperature". Upon registration, the sensor's reputation is automatically set to "true" by default.
- Scenario 2:Attempted Connection of Unregistered Device
  As depicted in Fig. 15, when an unregistered device is connected to the brokers network, the connection is refused and the device is registered in the blockchain with the reputation equal to false.
- Scenario 3: Device connection with false reputation
  As depicted in Fig. 16, when a device with a false reputation attempts to connect to brokers network, the connection is automatically denied.
- Scenario 4: Submission of incorrect OTP
  - Manufacturer's temperature sensor sends a connection request to the brokers network.
  - After checking the packet number, device registration, and reputation, the brokers network send the challenge to the Manufacturer's temperature sensor for OTP calculation.
  - Manufacturer's temperature sensor sends an erroneous OTP.
  - As depicted in Fig. 17, the connection is automatically refused and the reputation is set to false.
- Scenario 5: Unauthorized Publication

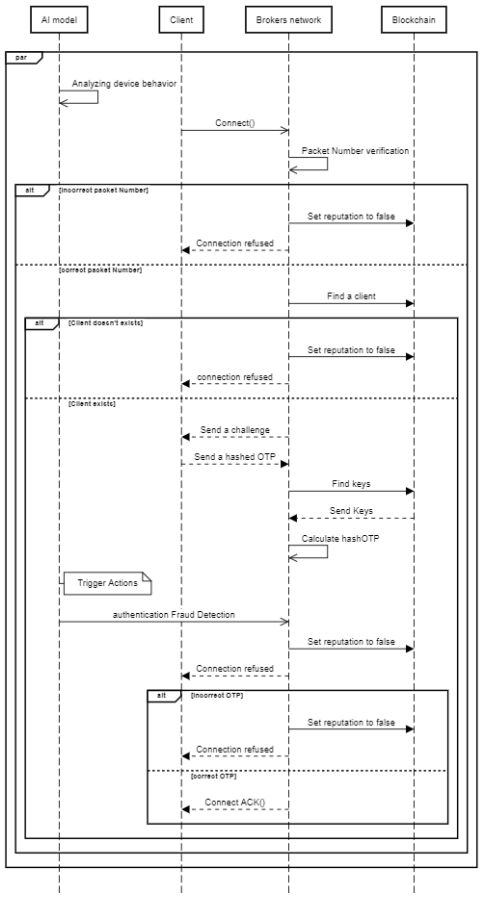


Fig. 10. Connection phase sequence diagram.

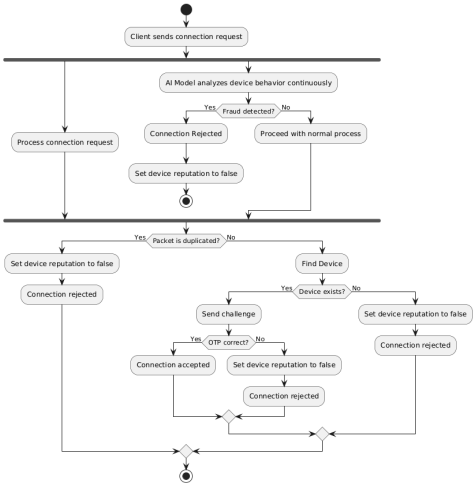


Fig. 11. Connection phase smart contract logic.

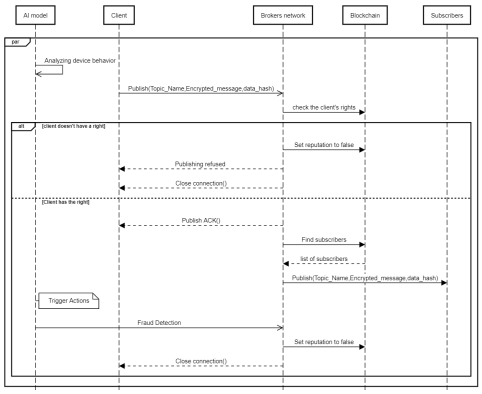


Fig. 12. Publishing phase sequence diagram.

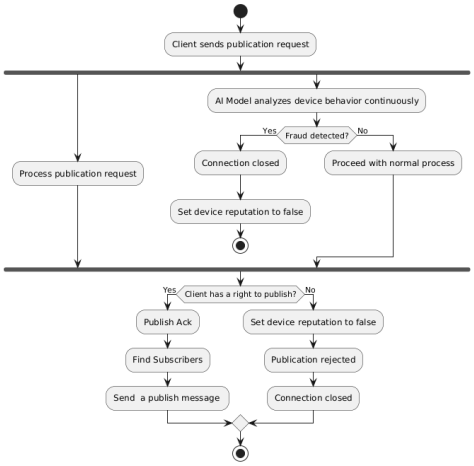


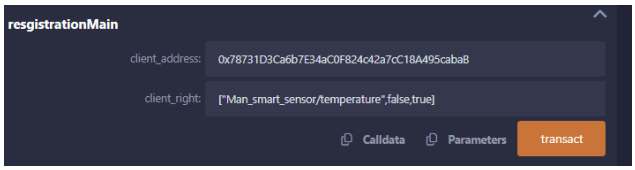
Fig. 13. Publishing phase smart contract logic.

- As an example, the distributor's administrator has registered the GPS device, allocating the rights described in Table III to receive updates or instructions regarding its configuration.
- As shown in Fig. 18, when the distributor's GPS is attempting to publish in an unauthorized topic **Smart_Sensorupdateconfiguration**, the connection is interrupted and its reputation is set to false.

- Scenario 6: Detection of Known Authentication Fraud
  - During the connection process of a customer's end device, the AI model classified the device as malicious due to a malformed connection packet.
  - The AI model invokes the smart contract to deny the connection and set the device's reputation to false **Fig. 19**.
- Scenario 7: Detection of abnormal known behavior
  The AI model detected a flood attack from an already connected customer's end device. As depicted in Fig. 20, it triggered the smart contract to interrupt the connection and set the device's reputation to "false".

B. Discussing Test Results

In Section V-A, we have focused on simulating attacks related to the new concepts introduced in this article, which



(a)

(b)

Fig. 14. Registration nominal scenario.

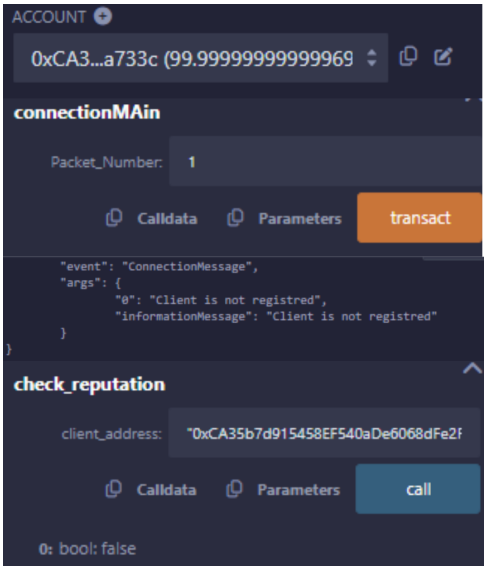


Fig. 15. Connection of unregistered device.

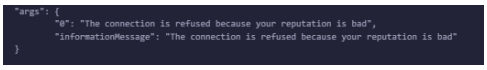


Fig. 16. Connection denied due to false reputation.

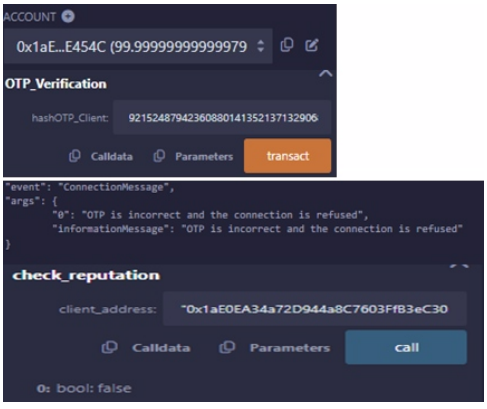
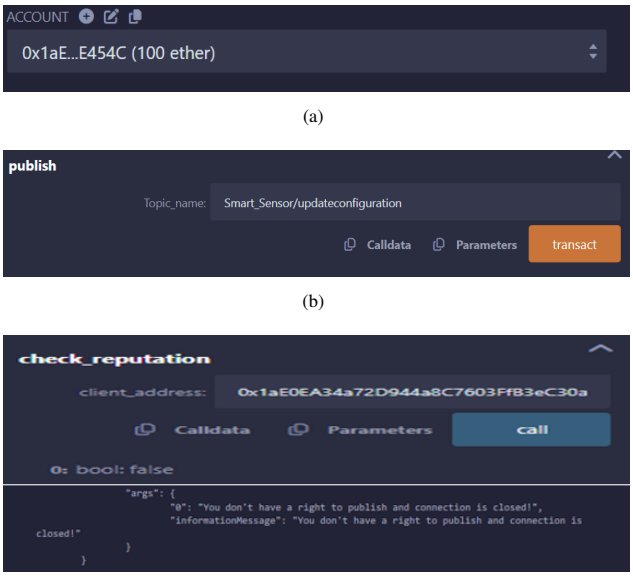


Fig. 17. Submission of incorrect OTP.

TABLE III. SMART SENSOR REGISTRATION INFORMATION

Device address	"0x1aE0EA34a72D944a8C7603FfB3eC30a6669E454C"
Topic Name	GPS/updateconfiguration
Read right	True
Write right	False



(a)

(b)

(c)

Fig. 18. Unauthorized publication.

Fig. 19. Authentication fraud detection.

Fig. 20. Abnormal behavior detection.

follow on from the attack tests carried out in the previous work [4]. Attack simulation tests focus on two main areas: on the one hand, the interaction between the artificial intelligence (AI) model and the smart contracts to apply the appropriate security measures once malicious behavior has been detected. Indeed, as illustrated in **scenario 6**, the AI model analyzes the device's behavior during connection process and, as a result, denies connection to the brokers network if malicious behavior is detected. In **scenario 7**, malicious behavior is detected while the device is already connected to the brokers network, triggering hence a transaction to interrupt the connection. On the other hand, these tests also monitor the device's reputation status, which must automatically change if malicious behavior is detected. In fact, according to scenario 1, by default, the state of the reputation when the device is registered is good **(true)**. Once malicious behavior is detected, the reputation changes to bad **(false)**. This is illustrated in the following scenarios: connection of an unregistered device **(scenario 2)**, sending a wrong OTP **(scenario 4)**, unauthorized publication **(scenario 5)**, and detecting abnormal behavior using the AI model **(scenarios 6 and 7)**. Additionally, the main aim of the device reputation system is to prevent devices with a bad reputation from rejoining the network, as demonstrated in **(scenario 3)**.

VI. CONCLUSION

Our research works aim to propose an MQTT architecture that meets the security requirements of critical IoT applications, is resilient to current attacks, and is adaptable to potential future attacks while taking into account the constraints of the IOT environment. To this end, the proposed solution in this paper aims to improve the MQTT architecture proposed in our previous work [4] by adding an additional layer of security based on artificial intelligence. Combining the advantages of blockchain and AI technologies enables attack detection by analyzing the behavior of devices connected or being connected to the broker network using an AI hybrid model, and then automatically applying appropriate security measures using smart contracts. The solution has also introduced the concept of device reputation to prevent malicious devices from rejoining the network. The creation of the AI model involved three essential phases: The first step was to train the model on a set of known malicious behaviors using the Random Forest supervised learning algorithm. Once the model was trained, it was integrated into the MQTT architecture, where the appropriate security measures were implemented through smart contracts. Simultaneously, the Isolation Forest unsupervised learning algorithm was added to the model in monitoring mode, in order to discover new attack patterns and identify new parameters for the detection of malicious devices. The attack patterns identified in phase 2 will be reintegrated into the basic model to improve the model's accuracy and performance. To fit the constraint environment requirements, all the resource-intensive operations are managed on the brokers network side, while the only operation executed on the device side is the OTP calculation. For attack simulation tests, the architecture was applied to supply chain management, and smart contracts were implemented in the Remix environment. The test results showed the architecture's resistance to different types of attacks. In our future work, we will continue to improve the security of the MQTT protocol in constrained environments by deploying our architecture in real-world situations. This will allow us to expose the architecture to real attacks, which will refine the AI model and strengthen the architecture's resilience against more complex and sophisticated types of attacks. In addition, we will evaluate the performance of the MQTT protocol by measuring key indicators such as latency, energy consumption, and bandwidth utilization.

REFERENCES

[1] M. Tauseef, M. R. Kounte, A. H. Nalband, and M. R. Ahmed, "Exploring the joint potential of blockchain and ai for securing internet

of things," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, 2023.

[2] "Internet of things - worldwide — statista market forecast," https://www.statista.com/outlook/tmo/internet-of-things/worldwide,date2024-08-20.

[3] T. P. HT, T. N. DP *et al.*, "Developing a patient-centric healthcare iot platform with blockchain and smart contract data management." *International Journal of Advanced Computer Science & Applications*, vol. 15, no. 4, 2024.

[4] R. AKNIN and Y. Bentaleb, "Enhanced mqtt architecture for smart supply chain," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, 2023.

[5] F. Buccafurri, V. De Angelis, and R. Nardone, "Securing mqtt by blockchain-based otp authentication," *Sensors*, vol. 20, no. 7, p. 2002, 2020.

[6] P. Akshatha and S. D. Kumar, "Mqtt and blockchain sharding: An approach to user-controlled data access with improved security and efficiency," *Blockchain: Research and Applications*, vol. 4, no. 4, p. 100158, 2023.

[7] T.-C. Hsu and H.-S. Lu, "Designing a secure and scalable service model using blockchain and mqtt for iot devices," in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 2024, pp. 645–653.

[8] R. Aknin and Y. Bentaleb, "Securing mqtt architecture using a blockchain," in *Advances in Information, Communication and Cybersecurity: Proceedings of ICI2C'21*. Springer, 2022, pp. 568–578.

[9] R. Alasmari and A. A. Alhogail, "Protecting smart-home iot devices from mqtt attacks: An empirical study of ml-based ids," *IEEE Access*, vol. 12, pp. 25 993–26 004, 2024.

[10] A. Alzahrani and T. H. Aldhyani, "Artificial intelligence algorithms for detecting and classifying mqtt protocol internet of things attacks," *Electronics*, vol. 11, no. 22, p. 3837, 2022.

[11] T. K. Boppana and P. Bagade, "Gan-ae: An unsupervised intrusion detection system for mqtt networks," *Engineering Applications of Artificial Intelligence*, vol. 119, p. 105805, 2023.

[12] M. A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, F. Norouzi, M. A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, "Iot architecture," *Towards the Internet of Things: Architectures, Security, and Applications*, pp. 9–31, 2020.

[13] A. Laftimi, H. El Makhtoum, R. Aknin, and Y. Bentaleb, "Ai-based intelligent blockchain for the authentication of the metering system," in *2022 IEEE 3rd International conference on electronics, control, optimization and computer science (ICECOCS)*. IEEE, 2022, pp. 1–6.

[14] "Qu'est-ce la data preparation en machine learning ?" https://www.free-work.com/fr/tech-it/blog/actualites-informatiques/impact-de-la-data-preparation-en-machine-learning,date2024-08-10.

[15] P. Dinesh, A. Vickram, and P. Kalyanasundaram, "Medical image prediction for diagnosis of breast cancer disease comparing the machine learning algorithms: Svm, knn, logistic regression, random forest and decision tree to measure accuracy," in *AIP Conference Proceedings*, vol. 2853, no. 1. AIP Publishing, 2024.

[16] C. Avcı, M. Budak, N. Yağmur, and F. Balçık, "Comparison between random forest and support vector machine algorithms for lulc classification," *International Journal of Engineering and Geosciences*, vol. 8, no. 1, pp. 1–10, 2023.

[17] M. Belgiu and L. Drăguţ, "Random forest in remote sensing: A review of applications and future directions," *ISPRS journal of photogrammetry and remote sensing*, vol. 114, pp. 24–31, 2016.

[18] "ns-3," https://www.nsnam.org/,date2024-08-10.

[19] S. Hariri, M. C. Kind, and R. J. Brunner, "Extended isolation forest," *IEEE transactions on knowledge and data engineering*, vol. 33, no. 4, pp. 1479–1489, 2019.

Optimized SMS Spam Detection Using SVM-DistilBERT and Voting Classifier: A Comparative Study on the Impact of Lemmatization

Sinar Nadhif Ilyasa, Alaa Omar Khadidos
Information Systems Department, King Abdul Aziz University, Jeddah, Kingdom of Saudi Arabia

***Abstract*—The rapid growth of digital communication has led to a surge in spam messages, particularly through Short Message Service (SMS). These unsolicited messages pose risks such as phishing and malware, necessitating robust detection mechanisms. This study focuses on a comparative analysis of machine learning models for SMS spam detection, with a particular emphasis on a proposed SVM-DistilBERT model enhanced by a voting classifier. Using the UCI SMS Spam dataset, the models are evaluated based on recall, accuracy, precision, and Receiver Operating Characteristic Area Under the Curve (ROC AUC) scores to assess their effectiveness in correctly identifying spam messages. By leveraging Optuna for hyperparameter optimization, the proposed model achieves superior performance, with an accuracy of 99.6%, surpassing traditional methods like SVM with TF-IDF Bi-gram and AdaBoost, which achieved 98.03%. The study also examines the effects of lemmatization and synonym data augmentation, with lemmatization shown to improve spam detection by reducing feature space redundancy and enhancing semantic understanding. To ensure transparency in decision-making, Local Interpretable Model-Agnostic Explanations (LIME) is applied. The results demonstrate that the optimized SVM-DistilBERT with the voting classifier offers a robust and effective solution for SMS spam filtering.**

***Keywords*—SMS spam detection; Support Vector Machine (SVM); DistilBERT; hyperparameter optimization; LIME**

I. Introduction

The advancement of digital communications in modern times has caused mass messaging, also known as spam, to become widespread. These messages flood inboxes across various channels, bringing severe security risks such as phishing and malware. The rise of spam is closely tied to technological advancements, with Short Message Service (SMS) emerging as one of the first mobile communication standards. As SMS usage grew, so did the prevalence of spam, creating an urgent need for effective spam detection methods.

A 2022 report [1] states that 68.4 million Americans, or 26% of the population, have been scammed via phone, compared to the previous year's 59.4 million (23%). Furthermore, 33% of people reported being involved in a phone scam, with about 20% falling for a con more than once. These scams not only have financial consequences but also affect productivity, mental health, and personal privacy. As mobile telecommunications have expanded, SMS spam has become a significant irritant, contributing to substantial losses in working time, network resource consumption, and performance costs [2].

The rise of spam undermines trust in mobile communication platforms and consumes valuable network resources and device storage. This highlights the necessity for effective spam reduction strategies to preserve user satisfaction and optimize resource utilization [3]. Implementing advanced spam detection mechanisms is crucial for protecting users and ensuring compliance with privacy regulations [4]. This underscores the importance of deploying sophisticated and explainable spam detection methodologies to bolster user trust and meet regulatory expectations.

Traditional spam detection methods have relied on rule-based systems [5], which offer limited success due to their inflexibility and inability to adapt to the evolving nature of spam tactics and content. This necessitates more sophisticated, adaptable, and accurate detection strategies. A survey of existing literature indicates ongoing efforts to combat this issue, yet it remains a significant challenge, highlighting the need for innovative approaches that can keep pace with the dynamic landscape of spam messaging.

Machine learning emerges as a promising solution to address the complex problem of spam detection [6]. These algorithms, by learning from categorized datasets, can effectively differentiate between spam and genuine ("ham") messages, thereby providing a robust barrier against unwanted communications. However, the success of machine learning models in detecting spam relies heavily on choosing and fine-tuning the features used for training [7], [8]. Challenges such as high dimensionality, feature redundancy, and the dynamic nature of spam content complicate feature selection [9]. Moreover, the interpretability of models is crucial for building trust and ensuring regulatory compliance, yet many advanced models operate as black boxes [10].

This research addresses these challenges by improving upon the work of SpotSpam [11], a recent approach that utilizes Support Vector Machines (SVM) combined with DistilBERT embeddings for SMS spam detection. While SVMs excel in high-dimensional spaces and work effectively with smaller, well-labeled datasets, their performance is highly contingent on meticulous hyperparameter tuning—a process that is both complex and experimental. To overcome this limitation, Optuna [12] is employed, an automatic hyperparameter optimization framework, to fine-tune the comparison model, achieving significant improvements in classification accuracy and overall model performance. Additionally, the impact of lemmatization during preprocessing is explored, with a comparison of models trained with and without this step. Subtle synonym data augmentation is applied to introduce

variability into the dataset, addressing the challenge of high dimensionality and feature redundancy.

To enhance model interpretability, LIME (Local Interpretable Model-Agnostic Explanations) [13] is employed. By providing transparent and interpretable explanations of the model's decisions, to ensure that the predictions are not only accurate but also explainable, contributing to greater transparency in the spam detection process.

The contributions of this research are as follows:

1) Hyperparameter Optimization: Applying Optuna [12] to fine-tune the hyperparameters of the comparison models.
2) Lemmatization Analysis: Analyzing the impact of lemmatization on model performance, comparing results with and without this preprocessing step to determine its effectiveness in reducing feature space complexity.
3) Model Explainability: This study employs LIME [13] to provide transparent and interpretable explanations of the model's decisions, contributing to both accuracy and explainability in spam detection.
4) The proposed model SVM+DistilBERT with Voting Classifier model achieves significant performance improvements over previous approaches like SpotSpam [11].

This research presents a comprehensive evaluation of machine learning models for SMS spam detection. Starting with foundational approaches such as SVM [14] [15], the study extends to more complex models, incorporating feature engineering techniques like TF-IDF vectorization [16] and ensemble classifiers such as XGBoost [17]. By integrating advanced embeddings like DistilBERT with SVM and optimizing hyperparameters using Optuna, the gap between traditional methods and modern advancements is bridged, enhancing precision and flexibility. This provides valuable insights for both academic researchers and industry practitioners seeking to develop effective and explainable spam detection systems.

The remainder of this paper is organized as follows: Section II presents the Literature Review. Section III provides a Detailed Description of the Methodology. Results and Analysis are presented in Section IV. Finally, Conclusions and Future Work are discussed in Section V.

II. Literature Review

Spam detection remains a critical task in the field of text classification, with numerous algorithms developed to address the challenge of accurately identifying unsolicited messages in datasets. Traditional machine learning methods, particularly Support Vector Machines (SVMs), have been extensively studied for this purpose.

Singh et al. [18] explored the use of SVM with TF-IDF and other feature extraction methods for SMS spam detection, demonstrating the effectiveness of SVM in such tasks. They noted the need for further comparative analyses of hybrid models and ensemble methods to enhance performance. Building on their findings, this study provides a detailed comparison of various SVM-based models, including combinations with advanced embeddings like DistilBERT [19], and evaluates the impact of preprocessing techniques such as lemmatization on model performance. By integrating LIME, this study also addresses the critical need for model explainability, enhancing transparency in the decision-making process. These contributions aim to provide a more nuanced understanding of SVM's potential in modern spam detection frameworks, aligning with the ongoing evolution of text classification techniques.

Almeida et al. [20] demonstrated the effectiveness of SVM classifiers in detecting spam within text messages by leveraging a comprehensive set of features extracted from the messages. Despite their success, they highlighted that the performance of SVMs is highly contingent on the meticulous selection and tuning of kernels and hyperparameters—a process that is both complex and experimental. Moreover, they pointed out potential scalability issues, as SVMs can become computationally intensive when applied to very large datasets.

In an effort to enhance SVM performance, Delany et al. [21] experimented with the integration of n-gram analysis. This hybrid approach improved spam detection rates by capturing contextual information within the text. However, the generation and processing of n-grams introduced additional computational overhead, leading to longer training times and increased memory usage. This trade-off suggests that while the method is robust, it may not be ideal for scenarios requiring immediate processing.

Text preprocessing and hyperparameter optimization are critical components in improving spam detection efficacy. Lemmatization, a preprocessing technique that reduces words to their base forms, can enhance traditional machine learning models like SVM by reducing feature space complexity and improving recall and precision. Akhmetov et al. [22] demonstrated the benefits of lemmatization across multiple languages, noting its importance in handling morphologically rich datasets.

The advent of transformer-based models has further revolutionized natural language processing tasks, including spam detection. Xiaoxu Liu et al. [23] demonstrated that models based on the vanilla transformer architecture perform well in SMS spam detection tasks. They suggested that utilizing more complex architectures like BERT could yield even better performance due to their ability to capture deeper contextual relationships with fewer features and ease of fine-tuning.

Despite these advancements, there is a notable gap in the literature concerning the integration of advanced embedding techniques with traditional machine learning models. Guzella et al. [24] reviewed the application of SVMs in spam filtering, highlighting their adaptability and accuracy. However, their work did not directly compare SVMs with emerging deep learning methods, which have shown potential for superior performance in text classification tasks.

To address this gap, the current research focuses on enhancing SVM models with modern embedding techniques such as DistilBERT. By combining the strengths of SVMs with the contextual understanding provided by advanced embeddings, the aim is to improve both the accuracy and adaptability of spam detection models. This research approach also involves evaluating various enhancements to traditional SVM models, including the use of term frequency-inverse document

frequency (TF-IDF), ensemble techniques, and preprocessing methods like lemmatization.

Considerations of model interpretability and complexity are crucial in the selection of appropriate spam detection methods. Metsis et al. [25] found that while SVMs generally outperform other machine learning algorithms in spam detection tasks, they suffer from a lack of interpretability compared to more transparent models like decision trees. Drucker et al. [26] attempted to enhance SVMs by incorporating boosting techniques, which improved accuracy but also introduced risks of overfitting and added complexity. These factors could hinder the deployment of such models in real-time prediction environments.

III. Methodology

The methodological approach focus is on the comparative analysis of various machine learning models for SMS Spam filtering purposes using the SVM based centric approach. The performance of these models will be evaluated based on their recall, accuracy, precision and the score of ROC AUC in correctly identifying spam messages. The flowchart of the process can be seen in Fig. 1.

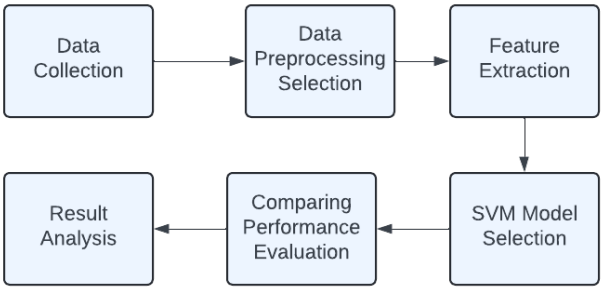


Fig. 1. Flowchart of the SVM comparison process.

A. Data Collection

The dataset utilized in this study is sourced from the UCI Machine Learning Repository [27], comprising 5,574 instances [28] with no missing values. Detailed information about the dataset composition and source distribution is presented in Table I.

TABLE I. Summary of SMS Message Sources for Spam Detection

Source	Description	Numb. of Messages
Grumbletext Website	UK forum reports of SMS spam.	425 spam
NUS SMS Corpus (NSC)	Legitimate messages from Singapore, mostly from students.	3,375 ham
Caroline Tag's PhD Thesis	Collection of SMS messages for research.	450 ham
SMS Spam Corpus v.0.1 Big	Combined collection of ham and spam messages for academic research.	1,002 ham, 322 spam

The bar chart in Fig. 2 revealed a significant imbalance in the dataset [28], with ham messages substantially outnumbering spam messages. To handle imbalance dataset, weight class balanced is employed on the SVM model. By completing these data preparation procedures, a well-organized and processed dataset is generated, which is now ready for the training and assessment of the classification models.

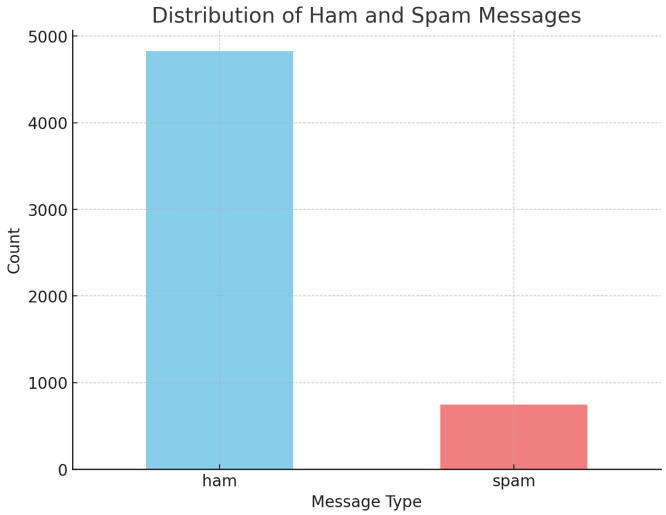


Fig. 2. Distribution of ham and spam messages in the dataset.

B. Data Preprocessing Selection

Before training the experimented models in this study, data cleaning is employed. For the SVM with DistilBERT embeddings, minimal cleaning is performed, involving converting the text to lowercase and removing extra white spaces. This approach retains most of the original raw data, as BERT embeddings are powerful enough to capture the semantic context.

To improve the generalization capability of the model, synonym data augmentation using WordNet was applied during the preprocessing stage for the proposed model. This technique introduces subtle variations in the text by replacing randomly selected words with their synonyms. The rationale behind this approach lies in the inherent diversity of language use in real-world communications, where different words can convey similar meanings. During synonym replacement, some words remain unchanged because WordNet may not have synonyms for them. The examples are shown in Table II.

While the application of synonym replacement in this study resulted in relatively minor changes to the text, it served two key purposes:

- Lexical Variety: The augmentation process exposed the model to variations in word usage that it might encounter in unseen data.
- Robustness to Minor Variations: Synonym replacement, despite introducing small changes, ensures that the model is less reliant on exact word matches.

In addition, this study investigated the influence of lemmatization on SMS spam detection models by preparing data in two different ways: with and without lemmatization. Lemmatization reduces words to their base forms (e.g. "congratulations" and "congrats" to "congratulate"), reducing the feature

space for model training. This preprocessing step enables for a comparative analysis of its impact on model performance.

TABLE II. COMPARISON OF ORIGINAL AND SYNONYM-REPLACED SMS MESSAGE

Original Text	**Text After Synonym Replacement**
Actually I decided I was too hungry so I haven't left yet : V	Actually I decided I was too hungry so I haven't **leave** yet : V
That's the thing with apes, u can fight to the death to keep something, but the minute they have it when u let go, that's it!	That's the thing with apes, u can fight to the death to keep something , but the **moment** they have it when u let go, that's it !
Glad to see your reply.	**glad** to see your reply.

C. Feature Extraction

1) TF-IDF: Term Frequency (TF) estimates the frequency of terms in a sentence by dividing the number of repetitions by the total number of words in the sentence. The IDF score determines the word's rarity within a corpus, suggesting that words that aren't used as frequently might hold more important information [29].

2) Bi-gram: The SVM TF-IDF will be enhanced with the bi-gram to capture more information context. A Bi-gram is two ceonsecutive elements which takes forms of words taken from the sequence of tokens. The bi-gram focuses on the word pair rather than capturing the meaning of the individual text itself.

For example, combining words like "customer service" is a bi-gram, which have more nuanced sentiment compared to an individual words such as "customer" or "service" [29].

3) DistilBERT: This study utilizes DistilBERT, a condensed version of the BERT (Bidirectional Encoder Representations from Transformers) model [30]. DistilBERT reduces the size of BERT by approximately 40%, making it more efficient in terms of memory and computational resources while retaining about 97% of BERT's performance on language understanding benchmarks.

DistilBERT achieves this efficiency through knowledge distillation [31], where a smaller student model learns to mimic the behavior of a larger teacher model. This process involves training the student model to reproduce the outputs of the teacher model, effectively capturing the essential knowledge in a more compact form without the need for extensive mathematical computations during inference.

The architecture of DistilBERT retains the Transformer-based design [32] but reduces the number of layers from 12 to 6. Despite this reduction, it maintains the ability to capture complex contextual relationships within the text through self-attention mechanisms. The self-attention mechanism allows the model to weigh the importance of different words in a sequence, enabling it to understand the context and nuances of language effectively. The architecture of DistilBERT can be seen in Fig. 3.

By integrating DistilBERT embeddings into the model, It leverages rich contextual representations of the input text, which enhances the performance of the spam detection task. This approach provides a balance between computational efficiency and model accuracy, making it suitable for applications requiring quick response times without significant loss in performance.

For detailed information on the mathematical formulations and training objectives of DistilBERT, readers are referred to Sanh et al. [19] and the foundational works on Transformers by Vaswani et al. [32].

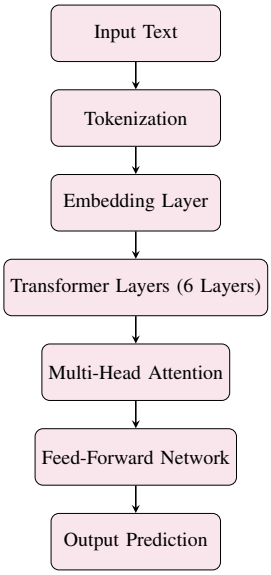


Fig. 3. Architecture of DistilBERT.

D. SVM Model Selection

1) Support Vector Machine: This study focuses on using Support Vector Machines (SVM) to filter spam in the SMS dataset. SVMs are supervised learning models used for regression analysis and classification. Gaye et al. (2021) [33] found that the SVM works by choosing the best hyperplane that separates the data into different classes. The main goal is to maximize the margin—the gap between the hyperplane and the nearest data points of each class—which can be either hard or soft. This separation challenge is transformed into a quadratic programming problem, allowing for the optimal hyperplane to be found efficiently.

This transformation is pivotal as it enables the SVM model to effectively handle linearly inseparable cases through the introduction of slack variables for soft margin optimization and the employment of kernel functions. Kernel functions, such as polynomial, radial basis function (RBF), and sigmoid, allow SVM to operate in high-dimensional spaces, facilitating the classification of complex datasets [34].

For the task of SMS spam filtering, the application of SVM is particularly promising due to its ability to discern between spam and legitimate messages with high precision. By constructing a feature vector from the SMS dataset and applying an appropriate kernel function, SVM can effectively classify

messages, leveraging the textual and contextual differences between spam and non-spam SMS. This capability is further evidenced by recent studies, which have demonstrated SVM's superior performance in text classification tasks compared to other machine learning algorithms [35] [36].

Furthermore, the adaptability of SVM in handling various types of data makes it an ideal choice for this study. By fine-tuning the SVM parameters, including the regularization parameter (C) and the kernel parameters, it can optimize the model to achieve maximum accuracy in spam detection. This optimization process is crucial for adapting the SVM model to the specific characteristics of the SMS dataset, thereby ensuring the effectiveness of the spam filtering solution.

2) AdaBoost: This study implements the ensemble classifier method AdaBoost for comparison analysis. AdaBoost is a powerful machine learning technique that combines multiple weak classifiers to create a robust, highly accurate classifier. It is simple to implement and relatively insensitive to noise in the data, but it can be affected by specific types of noise, such as class imbalance or outliers.

The following equation describes how each training instance's weight is updated by AdaBoost:

$$D_{t+1}(i) = \frac{D_t(i) \exp(-\alpha_t y_i h_t(X_i))}{Z_t} \tag{1}$$

In this equation, $D_t(i)$ represents the weight of the i-th training instance at iteration t, and α_t denotes the weight of the classifier. The exponential term adjusts the weight based on whether the prediction $h_t(X_i)$ matches the true label y_i. The normalization factor Z_t ensures that all weights sum to one, enabling the model to focus more on incorrectly classified instances [37].

In this study, AdaBoost with SVM is used as a comparison method to evaluate the performance of the proposed SVM-DistilBERT-based model and to assess the impact of lemmatization in classifying SMS spam messages.

3) eXtreme Gradient Boosting (XGBoost): XGBoost was employed in this study for comparative analysis alongside other models to evaluate the impact of lemmatization. XGBoost, or "Extreme Gradient Boosting", is a powerful and efficient machine learning algorithm built on the gradient boosting framework. Its high performance and speed make it popular for various supervised learning tasks. This algorithm is known for its scalability, sparsity awareness, and considerations for data compression, sharding, and cache-aware access [38].

These features enable XGBoost to efficiently manage large datasets with billions of entries, using fewer computational resources than many other systems [39]. In this study, it serves as a benchmark to understand how lemmatization affects model performance relative to other methods.

4) Voting Classifier: In this study, several machine learning models were combined with a voting classifier to create a reliable SMS spam detection system. The classifier combined Support Vector Machine (SVM), Random Forest, Gradient Boosting, Logistic Regression, and K-Nearest Neighbors into a single predictive model. The goal was to enhance the system's overall performance by using the advantages of each particular model.

The key to building an efficient SMS spam detection system is to balance the advantages of different machine learning models with each one's drawbacks. The ensemble approach seeks to use each model's robustness by combining these various models into a single voting classifier, producing a forecast that is more accurate and dependable. Every model makes a distinct contribution to the classifier; some are better at managing enormous datasets or offering interpretability, while others are better at handling high-dimensional data. Combining these models guarantees a more balanced approach to categorization that can handle the subtleties of SMS data with better accuracy while also improving the system's overall performance.

Support Vector Machine are very effective in a high dimensional data spaces and it is robust against outliers which is very good in handling noisy environments [40]. However, SVM also has its drawbacks that it faces scalability issues and is computationally intensive when handling a large datasets [41].

Random Forest(RF) can be integrated to help solve to address SVM drawbacks as they are very efficient in managing large datasets that leads to better generalization [41]. Random Forest is also very good in handling the missing data and conducting variable selection, however Random Forest may struggle on interpretability and imbalanced datasets [42] [43].

To add more strength to the ensemble, Logistic Regression were added to the Voting Classifier, that is known for it's simplicity and interpretability. It is very effective against binary classification problems and it is widely used for social sciences/medical field because of its interpretable and clear coefficients [44]. Logistic Regression can reduce the potential bias by handling the categorical predictor and continuous variables and also can effectively control confounding variables [45]. However, logistic regression has its drawbacks which is sensitive to outliers [46] and also has the assumption that there is a linear relationship between the predictors and the log-odds of the outcome that will effect on the limitation on its effectiveness for nonlinear boundaries [47].

On the other hand, Gradient Boosting model strength lies on it's high predictive accuracy and it's ability to adapt to the ensemble, especially when managing noisy data and multiple features [48] [49]. Gradient Boosting complements very good with the versatile capabilities of logistic regression and the robustness of Random Forest [50].

K-Nearest neighbor (KNN) contributes to the model because it's simple and effective to perform well in classification task, especially on how it groups the data based on the similarity. The flexibility of K-Neares neighbor (KNN) by leveraging different distance metrics improves its adaptability to different kinds of data [51]. When K-Nearest Neighbor (KNN) pairs with a structured models like Gradient Boosting and Random Forest, the combined model will perform better in handling complex data scenario [52].

The final output is generated by averaging the predictions made by each model in an ensemble technique. The voting classifier produces a more balanced and dependable detection

system, which integrates the outputs from SVM, Random Forest, Logistic Regression, Gradient Boosting, and K-nearest neighbors.

Using this method, the study shows that properly adjusted voting classifiers may greatly increase the precision and dependability of an SMS spam detection system.

E. Hyperparameter Optimization Using Optuna

In this study, Optuna is employed for hyperparameter optimization across various machine learning models for text classification, including XGBoost, AdaBoost, and Voting Classifiers with multiple base learners. To enhance readability and reduce complexity, standardized hyperparameter optimization across models were applied. For both XGBoost and AdaBoost, This study optimized the maximum number of features in the TF-IDF vectorizer, *max_features* $\in \{1000, 2000, 3000, 4000, 5000\}$, as well as the number of estimators, $n_{\text{estimators}} \in \{50, 100, 150, 200\}$, and the learning rate.

For XGBoost, additional parameters such as the maximum tree depth, *max_depth* $\in [3, 10]$, and the subsampling ratio, *subsample* $\in [0.5, 1.0]$, were optimized. Class imbalance was addressed using the *scale_pos_weight* parameter. In the Voting Classifier ensemble, shared hyperparameters across its constituent models were optimized to ensure consistency. The classifiers included SVC and Logistic Regression, where the regularization parameter C was optimized over a logarithmic scale. Additionally, Random Forest and Gradient Boosting classifiers were tuned for the number of estimators, with Random Forest also having an optimized maximum depth, and K-Nearest Neighbors varying in the number of neighbors.

When incorporating DistilBERT embeddings, the shared hyperparameters were optimized to maintain consistency across models. Stratified K-Fold cross-validation with $k = 5$ were employed, optimizing for metrics such as accuracy and ROC AUC. This systematic approach with Optuna enhanced model performance while reducing complexity and improving clarity in the hyperparameter optimization strategies.

F. Comparing Performance Evaluation

To evaluate the performance of the tested models, this study employ a technique called stratified k-fold cross-validation. Stratified K-fold cross-validation is an improved variant of k-fold cross-validation that is primarily used to ensure that the dataset's folds have similar class label distributions while maintaining the distribution of different classes [53]. With this method, over-fitting is reduced in datasets with imbalanced classes, unlike the regular k-fold cross validation, it can produce folds with skewd distribution of class labels in unbalanced datasets which may lead inaccurate performance measures.

After the integrated model is evaluated, the data is divided into five sections. Four of the segments are utilized to train the model, and the remaining one is used for testing. The aim of this assessment is to evaluate the model's differentiate capability across classes, with a specific focus on how well it can detect positive cases based on the ROC AUC score, Precision, Recall, F1-Score, and Accuracy.

G. Evaluation Measures

To provide different insights for the performance of classification model that were tested, this study includes different metrics such as Precision, Recall, F1-Score, ROC AUC Score and the Accuracy.

1) Precision: It is a statistical measures that evaluates how well a model predicts the favorable outcomes. It indicates the percentage of correctly predicted positive instances out of from all cases that were predicted positive. The notation for precision is denoted as in Eq. 2.

Mathematical Definition:

$$\text{Precision} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Positives (FP)}} \quad (2)$$

2) Recall: The proportion of accurately predicted positive observations to all of the observations made during the actual class is known as recall.

Mathematical Definition:

$$\text{Recall} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Negatives (FN)}} \quad (3)$$

3) F1 score: The harmonic mean of Precision and Recall is the F1 score. It is helpful when attempting to achieve a balance between recall and precision.

Mathematical Definition:

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

4) ROC AUC Score: A performance metric for classification issues at different threshold settings is the ROC (Receiver Operating Characteristic) AUC (Area Under the Curve) score. The degree or measure of separability is represented by AUC, and ROC is a probability curve. It indicates the degree to which the model can discriminate between classes.

Mathematical Definition: Plotting TPR (True Positive Rate, sometimes called Recall) against FPR (False Positive Rate) yields the ROC curve. The area under this curve, or AUC score, has the following mathematical definition:

$$\text{AUC} = \int_0^1 \text{TPR}(\text{FPR})\, d(\text{FPR}) \quad (5)$$

True Positive Rate (TPR) is defined as:

$$\text{TPR} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Negatives (FN)}} \quad (6)$$

False Positive Rate (FPR) is defined as:

$$\text{FPR} = \frac{\text{False Positives (FP)}}{\text{False Positives (FP)} + \text{True Negatives (TN)}} \quad (7)$$

The AUC score falls between 0 and 1. An AUC of 1 indicates a perfect prediction model; an AUC of 0.5 indicates

a random prediction model. Better model performance is indicated by values nearer 1. More specifically, because it offers a thorough assessment of model performance across all classification thresholds, AUC is an important metric when assessing models on unbalanced datasets.

IV. Results and Analysis

The results in Table III and Table IV summarize various methods for SMS spam classification, including SVM-TF (Support Vector Machine with Term Frequency-Inverse Document Frequency), SVM-TF-Bi (SVM with TF-IDF and bi-grams), SVM-TF-Bi-Ada (SVM with TF-IDF Bi-gram and Adaboost), SVM-TF-Bi-XGB (SVM with TF-IDF Bi-gram and XGBoost), SVM-TF-Bi-Vote (SVM with TF-IDF Bi-gram and Voting Classifier), and SVM-DistilBERT-Vote (SVM with DistilBERT embeddings and Voting Classifier), where the "-Lem" suffix indicates the use of lemmatization, and performance is evaluated using the ROC AUC (Receiver Operating Characteristic Area Under Curve) metric.

TABLE III. Performance Comparison of Different Models: Models without Lemmatization

Model	ROC AUC	Precision	Recall	F1-Score	Accuracy
SVM-TF	0.9931	0.9878	0.8835	0.9327	0.9829
SVM-TF-Bi	0.9927	0.9719	0.8821	0.9248	0.9808
SVM-TF-Bi-Ada	0.9903	0.9984	0.8541	0.9206	0.9803
SVM-TF-Bi-XGB	0.9855	0.9387	0.8983	0.9179	0.9785
SVM-TF-Bi-Vote	0.9923	0.9984	0.8674	0.9283	0.9821
SVM-DistilBERT-Vote	0.9996	0.9973	0.9752	0.9861	0.9961

TABLE IV. Performance Comparison of Different Models: Models with Lemmatization

Model	ROC AUC	Precision	Recall	F1-Score	Accuracy
SVM-TF	0.9913	0.9855	0.9049	0.9433	0.9855
SVM-TF-Bi	0.9916	0.9856	0.9129	0.9477	0.9865
SVM-TF-Bi-Ada	0.9809	0.9803	0.7925	0.8764	0.9700
SVM-TF-Bi-XGB	0.9840	0.9512	0.8809	0.9145	0.9779
SVM-TF-Bi-Vote	0.9937	0.9925	0.8888	0.9376	0.9842
SVM-DistilBERT-Vote	0.9995	0.9951	0.9828	0.9878	0.9968

Table V compares the performance of this research with various previous studies on SMS spam classification, highlighting the differences in methods, accuracy, and datasets used. While traditional approaches such as TF-IDF with Random Forest [55] and XGBoost [59] reported accuracies of 97.50% and 97.64%, respectively, other methods like a hybrid system using K-Means SVM [56] and a Voting Classifier approach [57] achieved slightly higher accuracies, ranging from 98.8% to 98.93%. In contrast, this research, which employs an SVM DistilBERT model integrated with a Voting Classifier, achieves a superior accuracy of 99.6

The performance of various machine learning models on the SMS spam detection task was systematically evaluated. The results, summarized in Table III and Table IV, provide insights into how each model performed under two different preprocessing conditions: with and without the application of lemmatization. Lemmatization improves SMS spam identification by minimizing feature space redundancy, standardizing morphological variations (e.g. "running", "runs", and "ran" become "run"), and boosting generalization. For instance, a sample spam message, "Congrats! You've won a prize", is normalized to "congratulate! you win prize", allowing the algorithm to recognize spam-related phrases more accurately.

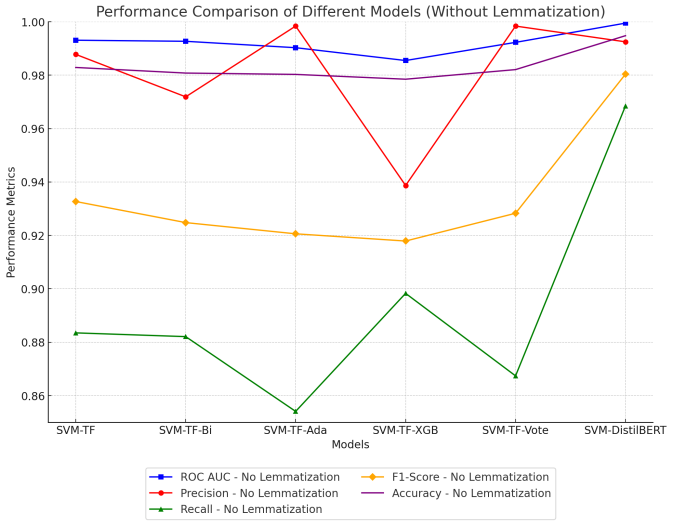


Fig. 4. Performance comparison of different models (without lemmatization).

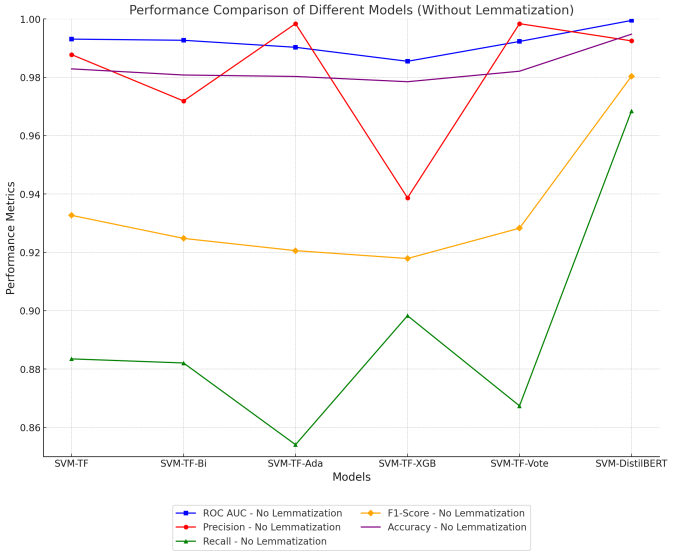


Fig. 5. Performance comparison of different models (with lemmatization).

This preprocessing step is especially beneficial for simpler models such as SVM-TF and SVM-TF-Bi, as evidenced by their higher recall and precision scores (Table IV). By emphasizing semantic meaning over lexical differences, lemmatization enhances detection accuracy and contributes to more effective spam filtering.

Fig. 5 and Fig. 4 showcase the performance metrics for six different models: SVM with Term Frequency (TF), SVM with TF and Bigrams (TF-Bi), SVM with TF and Bigram AdaBoost (TF-Bi-Ada), SVM with TF Bigram XGBoost (TF-Bi-XGB), SVM with TF Bigram and Voting Classifier (TF-Bi-Vote), and SVM with DistilBERT embeddings enhanced with Voting Classifier (SVM-DistilBERT-Vote). The key observation here is the effect of lemmatization on the models' performance.

Without lemmatization (Fig. 4), the ROC AUC remains consistently high across all models, with minor variations.

TABLE V. SUMMARY OF DIFFERENT METHODS IN CLASSIFYING SMS SPAM MESSAGES

Title and Reference	Dataset	Methods	Accuracy
SMS Spam Classification Using Machine Learning Techniques [54]	UCI Machine Learning Repository	SVM	98.797%
SMS Spam Message Detection using Term Frequency-Inverse Document Frequency and Random Forest Algorithm [55]	UCI Machine Learning Repository	TF-IDF with Random Forest	97.50%
Hybrid SMS Spam Filtering System Using Machine Learning Techniques [56]	UCI Machine Learning Repository	K-Means SVM	98.8%
A Robust System For Message Filtering Using An Ensemble Machine Learning Supervised Approach [57]	6000 Messages Data, 1000 Messages are spam	Voting Classifier	98.93%
Semi-supervised novelty detection with one class SVM for SMS spam detection [58]	747 spam, 4827 non-spam messages	One class SVM	98%
Relevant SMS Spam Feature Selection Using Wrapper Approach and XGBoost Algorithm [59]	UCI Machine Learning Repository	XGBoost Classifier	97.64%
This Research	UCI Machine Learning Repository	SVM DistilBERT with Voting Classifier	99.6%

However, precision shows a significant drop for the SVM-TF-Ada model, indicating that this model might be struggling with false positives when lemmatization is not applied. Recall for the same model also dips notably, which could suggest that the model is less sensitive to actual spam messages without the normalization that lemmatization provides.

In contrast, with lemmatization applied (Fig. 5), the performance of the SVM-TF-Bi-Ada model sees a marked improvement in recall, indicating better detection of spam messages. The F1-Score, which balances precision and recall, reflects these changes, showing a more consistent performance across the models when lemmatization is used.

Interestingly, the SVM with DistilBERT embeddings integrated with Voting Classifier consistently shows high performance across all metrics, with and without lemmatization, suggesting that this model is robust to variations in text preprocessing. This robustness can likely be attributed to the sophisticated nature of the DistilBERT embeddings, which capture contextual information effectively even in raw, non-lemmatized text.

Overall, these results suggest that while lemmatization generally aids in improving recall and precision for certain models, particularly ensemble methods like AdaBoost and Voting Classifier, models leveraging advanced embeddings like DistilBERT are less dependent on such preprocessing steps. Therefore, the choice of preprocessing should be carefully considered depending on the model being used, with lemmatization being more crucial for traditional machine learning approaches.

1) Performance without Lemmatization: The SVM-DistilBERT-Vote model demonstrated superior performance across all evaluation metrics, positioning itself as the leading model in this task. Specifically, it achieved an ROC AUC of 0.9996, indicating near-perfect discrimination between spam and non-spam messages. The model also recorded a Precision of 0.9973, which reflects its high ability to correctly identify spam messages without including false positives. The Recall score of 0.9752 shows that the model effectively identified the majority of actual spam messages. This balance between high Precision and high Recall resulted in an F1-Score of 0.9861, underscoring the model's effectiveness in maintaining a low rate of both false positives and false negatives. The high Accuracy of 0.9961 further supports these findings, indicating that the model correctly classified a vast majority of messages.

Comparatively, other models, such as SVM-TF and various ensemble methods (SVM-TF-Bi-Vote, SVM-TF-Bi-XGB), also performed well but with some noticeable differences. For instance, the SVM-TF model achieved a Recall of 0.8835, lower than that of SVM-DistilBERT-Vote, suggesting that it missed more spam messages. Despite this, the SVM-TF model's Precision remained high at 0.9878, resulting in an F1-Score of 0.9327. While this score is robust, the model's lower Recall indicates a higher likelihood of misclassifying spam messages as non-spam, which could be critical in certain applications. The ensemble methods, while effective, exhibited similar trends, with generally strong Precision but lower Recall compared to SVM-DistilBERT-Vote, indicating a potential trade-off in these models between false positives and false negatives.

2) Performance with Lemmatization: The application of lemmatization yielded varying impacts across the different models, with the SVM-DistilBERT-Vote model once again demonstrating the highest performance. After lemmatization, the SVM-DistilBERT-Vote model maintained an ROC AUC of 0.9995, with only a slight reduction from the non-lemmatized version, which suggests that lemmatization had little effect on the model's ability to distinguish between classes. However, its Recall improved to 0.9828, leading to an F1-Score of 0.9878, slightly higher than without lemmatization. This improvement in Recall indicates that lemmatization helped the model better identify spam messages, making it even more reliable for practical use.

Other models, particularly those based on TF-IDF vectorization, showed more pronounced improvements with lemmatization. The SVM-TF-Bi model, for instance, experienced a notable increase in Recall from 0.8821 to 0.9129, which contributed to a rise in its F1-Score from 0.9248 to 0.9477. This suggests that lemmatization improved the model's ability to capture the semantic essence of the text, thereby reducing the number of missed spam messages. The enhancement in feature

representation due to lemmatization is likely responsible for this improvement.

However, not all models benefited from lemmatization. The SVM-TF-Bi-Ada model, in particular, saw a decline in performance with lemmatization, as evidenced by its decreased Recall (0.7925) and F1-Score (0.8764). This decline suggests that lemmatization may have disrupted the feature space that this ensemble method relies on, reducing its effectiveness in distinguishing between spam and non-spam messages. Such a decrease in performance highlights the importance of considering the model architecture when applying preprocessing techniques like lemmatization.

The variation in lemmatization's effect on models may arise from ensemble approaches such as AdaBoost, which depend on feature diversity that lemmatization might diminish, while simpler vectorization models gain from a less complex feature space.

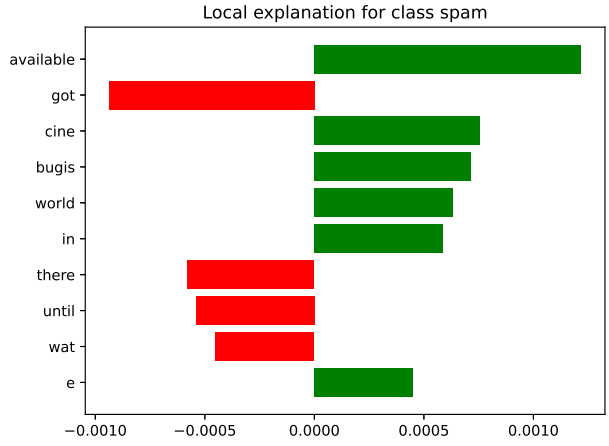


Fig. 6. Lime local variable explanation.

3) Explainable AI Using LIME: Fig. 6 presents a visual representation of explainable AI, generated using a tool called LIME (Local Interpretable Model-agnostic Explanations). This tool provides insights into how predictions are made by machine learning models through local explanations. LIME works by perturbing the input data—making slight alterations—and then assessing the impact of these modifications on the model's predictions.

In text classification tasks, such as the one illustrated in the figure, LIME identifies which words in a message have the most significant effect on the model's prediction. To enhance the interpretability of the model's decision-making process, it visualizes each word's contribution, highlighting those that increase or decrease the likelihood of the message being classified as spam.

For example, the word *"available"* has a contribution value of approximately **0.0010**, indicating a strong positive influence toward spam classification. On the other hand, *"got"* has a contribution of around **-0.0008**, meaning it significantly reduces the likelihood of the message being labeled as spam.

While certain words such as *"cine"* and *"bugis"* also contribute positively with values of **0.0006** and **0.0004** respectively, words like *"until"* and *"wat"* have smaller negative contributions, each near **-0.0004**. This numerical breakdown allows for a clearer understanding of which specific terms influence the spam classification and by how much, ensuring transparency in the model's decision-making process.

V. Conclusion

The study found that lemmatization often improves SMS spam detection performance, particularly in models that use TF-IDF vectorization. Lemmatization improves the model's ability to generalize and focus on message semantics by minimizing feature space redundancy and normalizing morphological variances. Models such as SVM-TF and SVM-TF-Bi showed considerable gains in recall and precision after lemmatization (Table IV), emphasizing its importance in increasing detection accuracy.

However, the impact of lemmatization is not uniform across all models. While models like SVM-TF-Bi showed enhanced performance with lemmatization, certain ensemble models, such as SVM-TF-Bi-Ada, experienced a decline, particularly in Recall and F1-Score. This suggests that the benefits of lemmatization are dependent on the specific model architecture and that its application should be considered carefully based on the characteristics of the model and the intended use case.

Overall, the findings underscore the importance of selecting the right preprocessing techniques in conjunction with the appropriate machine learning model to achieve optimal performance in text classification tasks. The variability in the effects of lemmatization across different models suggests that a one-size-fits-all approach may not be effective, and careful experimentation and analysis are necessary to determine the best preprocessing and modeling strategy for a given task.

Future works will be focusing on the different dataset other than the UCI Machine learning SMS Spam dataset that is more recent. Since this research is focusing on the SVM Centric to detect SMS Spam Detection, other methods that is more poweful while maintaing less computational cost still remains a challenge to address. Furthermore, synonym replacement in this study relied on WordNet without considering contextual similarity. Integrating models like BERT in the future could ensure replacements better align with sentence context, improving the quality of data augmentation.

Acknowledgment

The authors would like to express their sincere gratitude to King Abdulaziz University for the financial support provided through their scholarship program, which made this journal article possible. This support has been instrumental in enabling the research and completion of this work.

References

[1] Truecaller Insights. (2022) Truecaller insights 2022 us spam & scam report. Accessed: Insert Access Date. [Online]. Available: https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report

[2] S. Abdulhamid, M. S. A. Latiff, H. Chiroma, O. Osho, G. Abdul-Salaam, A. I. Abubakar, and T. Herawan, "A review on mobile sms spam filtering techniques," *IEEE Access*, vol. 5, pp. 15 650–15 666, 2017.

[3] A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti, and M. Alazab, "A comprehensive survey for intelligent spam email detection," *IEEE Access*, vol. 7, pp. 168 261–168 295, 2019.

[4] S. Rao, A. Verma, and T. Bhatia, "A review on social spam detection: Challenges, open issues, and future directions," *Expert Syst. Appl.*, vol. 186, p. 115742, 2021.

[5] T. Xia, "A constant time complexity spam detection algorithm for boosting throughput on rule-based filtering systems," *IEEE Access*, vol. 8, pp. 82 653–82 661, 2020.

[6] A. P. Rodrigues, R. Fernandes, A. A, A. B, A. Shetty, A. K, K. Lakshmanna, and R. M. Shafi, "Real-time twitter spam detection and sentiment analysis using machine learning and deep learning techniques," *Computational intelligence and neuroscience*, vol. 2022, p. 5211949, 2022, retraction published Comput Intell Neurosci. 2023 Oct 11;2023:9810910. [Online]. Available: https://doi.org/10.1155/2022/5211949

[7] H. Jain and R. K. Maurya, "A review of sms spam detection using features selection," *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, pp. 101–106, 2022.

[8] K. Zainal and M. Z. Jali, "A review of feature extraction optimization in sms spam messages classification," pp. 158–170, 2016.

[9] L. Zhang, "A new feature selection using dynamic interaction," *Pattern Analysis and Applications*, vol. 24, pp. 203–215, 2020.

[10] D. Bhusal, R. Shin, A. A. Shewale, M. K. M. Veerabhadran, M. Clifford, S. Rampazzi, and N. Rastogi, "Sok: Modeling explainability in security analytics for interpretability, trustworthiness, and usability," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ser. ARES '23. New York, NY, USA: Association for Computing Machinery, 2023. [Online]. Available: https://doi.org/10.1145/3600160.3600193

[11] C. Oswald, S. E. Simon, and A. Bhattacharya, "Spotspam: Intention analysis–driven sms spam detection using bert embeddings," *ACM Trans. Web*, vol. 16, no. 3, Sep. 2022. [Online]. Available: https://doi.org/10.1145/3538491

[12] T. Akiba, S. Sano, T. Yanase, T. Ohta, and M. Koyama, "Optuna: A next-generation hyperparameter optimization framework," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2019.

[13] M. T. Ribeiro, S. Singh, and C. Guestrin, ""why should i trust you?": Explaining the predictions of any classifier," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 1135–1144. [Online]. Available: https://doi.org/10.1145/2939672.2939778

[14] W. S. Noble, "What is a support vector machine?" *Nature biotechnology*, vol. 24, no. 12, pp. 1565–1567, 2006.

[15] D. A. Pisner and D. M. Schnyer, "Chapter 6 - support vector machine," in *Machine Learning*, A. Mechelli and S. Vieira, Eds. Academic Press, 2020, pp. 101–121. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128157398000067

[16] S. D. Gupta, S. Saha, and S. K. Das, "Sms spam detection using machine learning," *Journal of Physics: Conference Series*, vol. 1797, no. 1, p. 012017, feb 2021. [Online]. Available: https://dx.doi.org/10.1088/1742-6596/1797/1/012017

[17] D. Jalal Mussa and N. G. M. Jameel, "Relevant sms spam feature selection using wrapper approach and xgboost algorithm," *KJAR*, vol. 4, no. 2, pp. 110–120, Nov. 2019.

[18] T. Singh, T. A. Kumar, and P. G. Shambharkar, "Enhancing spam detection on sms performance using several machine learning classification models," in *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2022, pp. 1472–1478.

[19] V. Sanh, L. Debut, J. Chaumond, and T. Wolf, "Distilbert, a distilled version of bert: smaller, faster, cheaper and lighter," 2020. [Online]. Available: https://arxiv.org/abs/1910.01108

[20] T. A. Almeida, J. M. G. Hidalgo, and A. Yamakami, "Contributions to the study of sms spam filtering: new collection and results," in *ACM Symposium on Document Engineering*, 2011. [Online]. Available: https://api.semanticscholar.org/CorpusID:13871930

[21] S. J. Delany, M. Buckley, and D. Greene, "Sms spam filtering: Methods and data," *Expert Systems with Applications*, vol. 39, no. 10, pp. 9899–9908, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417412002977

[22] I. Akhmetov, A. Pak, I. Ualiyeva, and A. Gelbukh, "Highly language-independent word lemmatization using a machine-learning classifier," *Computación y Sistemas*, vol. 24, no. 3, pp. 1353–1364, 2020.

[23] S. Yerima and A. Bashar, "Semi-supervised novelty detection with one class svm for sms spam detection," *2022 29th International Conference on Systems, Signals and Image Processing (IWSSIP)*, vol. CFP2255E-ART, pp. 1–4, 2022.

[24] T. S. Guzella and W. M. Caminhas, "A review of machine learning approaches to spam filtering," *Expert Systems with Applications*, vol. 36, no. 7, pp. 10 206–10 222, 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S095741740900181X

[25] V. Metsis, I. Androutsopoulos, and G. Paliouras, "Spam filtering with naive bayes - which naive bayes?" 01 2006.

[26] O. Chapelle, P. Haffner, and V. Vapnik, "Support vector machines for histogram-based image classification," *IEEE Transactions on Neural Networks*, vol. 10, no. 5, pp. 1055–1064, 1999.

[27] T. Almeida and J. Gómez Hidalgo, "SMS Spam Collection: A Public Set of SMS Labeled Messages," https://archive.ics.uci.edu/ml/datasets/sms+spam+collection, 2011, accessed: [25 November 2023].

[28] O. Abayomi-Alli, S. Misra, and A. Abayomi-Alli, "A deep learning method for automatic sms spam classification: Performance of learning algorithms on indigenous dataset," *Concurrency and Computation: Practice and Experience*, vol. 34, 2022.

[29] P. Joseph and S. Y. Yerima, "A comparative study of word embedding techniques for sms spam detection," in *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2022, pp. 149–155.

[30] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," 2019. [Online]. Available: https://arxiv.org/abs/1810.04805

[31] G. Hinton, O. Vinyals, and J. Dean, "Distilling the knowledge in a neural network," 2015. [Online]. Available: https://arxiv.org/abs/1503.02531

[32] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. Kaiser, and I. Polosukhin, "Attention is all you need," 2023. [Online]. Available: https://arxiv.org/abs/1706.03762

[33] B. Gaye, D. Zhang, and A. Wulamu, "Improvement of support vector machine algorithm in big data background," *Mathematical Problems in Engineering*, vol. 2021, p. 5594899, 2021. [Online]. Available: https://doi.org/10.1155/2021/5594899

[34] A. Tharwat, "Parameter investigation of support vector machine classifier with kernel functions," *Knowledge and Information Systems*, pp. 1–34, 2019.

[35] H. Lee and S. Kang, "Word embedding method of sms messages for spam message filtering," *2019 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 1–4, 2019.

[36] C. Wang, Q. Li, T. Ren, X. Wang, and G. Guo, "High efficiency spam filtering: A manifold learning-based approach," *Mathematical Problems in Engineering*, 2021.

[37] M. Gupta, A. Bakliwal, S. Agarwal, and P. Mehndiratta, "A comparative study of spam sms detection using machine learning classifiers," in *2018 eleventh international conference on contemporary computing (IC3)*. IEEE, 2018, pp. 1–7.

[38] N. Ghatasheh, I. Altaharwa, and K. Aldebei, "Modified genetic algorithm for feature selection and hyper parameter optimization: case of xgboost in spam prediction," *IEEE Access*, vol. 10, pp. 84 365–84 383, 2022.

[39] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 785–794. [Online]. Available: https://doi.org/10.1145/2939672.2939785

[40] A. V. Messem, "Support vector machines: A robust prediction method with applications in bioinformatics," *Handbook of Statistics*, 2020.

[41] M. Singla and K. K. Shukla, "Robust statistics-based support vector machine and its variants: a survey," *Neural Computing and Applications*, vol. 32, pp. 11 173 – 11 194, 2019.

[42] T. Zhu, "Analysis on the applicability of the random forest," *Journal of Physics: Conference Series*, vol. 1607, 2020.

[43] M. N. Wright and I. König, "Splitting on categorical predictors in random forests," *PeerJ*, vol. 7, 2019.

[44] N. Gilbert, "Logistic regression," *Analyzing Tabular Data*, 2022.

[45] H. Nayebi, "Logistic regression analysis," *Advanced Statistics for Testing Assumed Casual Relationships*, 2020.

[46] I. A. I. Ahmed and W. Cheng, "The performance of robust methods in logistic regression model," *Open Journal of Statistics*, 2020.

[47] G. Zeng, "Logistic regression without intercept," *Asian Journal of Probability and Statistics*, 2022.

[48] C. Bentéjac, A. Csörgo, and G. Martínez-Muñoz, "A comparative analysis of gradient boosting algorithms," *Artificial Intelligence Review*, vol. 54, pp. 1937–1967, 2020. [Online]. Available: https://consensus.app/papers/analysis-gradient-boosting-algorithms-bentjac/c3be7a8bb964590488d56f7b829a39ab/?utm_source=chatgpt

[49] A. Ustimenko, L. Prokhorenkova, and A. Malinin, "Uncertainty in gradient boosting via ensembles," *ArXiv*, vol. abs/2006.10562, 2020. [Online]. Available: https://consensus.app/papers/uncertainty-gradient-boosting-ensembles-ustimenko/dbda713e90385394afce8d98dc7ac077/?utm_source=chatgpt

[50] D. Schalk, B. Bischl, and D. Rugamer, "Accelerated componentwise gradient boosting using efficient data representation and momentum-based optimization," *ArXiv*, vol. abs/2110.03513, 2021. [Online]. Available: https://consensus.app/papers/accelerated-componentwise-gradient-boosting-using-schalk/03898648792956a8811614558f4b9abe/?utm_source=chatgpt

[51] S. Zhang, "Challenges in knn classification," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, pp. 4663–4675, 2021.

[52] A. Shokrzade, M. Ramezani, F. Tab, and M. A. Mohammad, "A novel extreme learning machine based knn classification method for dealing with big data," *Expert Syst. Appl.*, vol. 183, p. 115293, 2021.

[53] J. A. Sáez and J. L. Romero-Béjar, "Impact of regressand stratification in dataset shift caused by cross-validation," *Mathematics*, 2022. [Online]. Available: https://consensus.app/papers/impact-regressand-stratification-dataset-shift-caused-sez/b32921947c5753ed9fb8bd1090b79fc4/?utm_source=chatgpt

[54] T. Jain, P. Garg, N. Chalil, A. Sinha, V. K. Verma, and R. Gupta, "Sms spam classification using machine learning techniques," in *2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2022, pp. 273–279.

[55] N. N. Amir Sjarif, N. F. Mohd Azmi, S. Chuprat, H. M. Sarkan, Y. Yahya, and S. M. Sam, "Sms spam message detection using term frequency-inverse document frequency and random forest algorithm," *Procedia Computer Science*, vol. 161, pp. 509–515, 2019, the Fifth Information Systems International Conference, 23-24 July 2019, Surabaya, Indonesia. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919318617

[56] H. Baaqeel and R. Zagrouba, "Hybrid sms spam filtering system using machine learning techniques," in *2020 21st International Arab Conference on Information Technology (ACIT)*, 2020, pp. 1–8.

[57] A. Mahabub, M. Innat, and M. Faruque, "A robust system for message filtering using an ensemble machine learning supervised approach," *ICIC Express Letters*, vol. 10, pp. 805–811, 07 2019.

[58] S. Yerima and A. Bashar, "Semi-supervised novelty detection with one class svm for sms spam detection," *2022 29th International Conference on Systems, Signals and Image Processing (IWSSIP)*, vol. CFP2255E-ART, pp. 1–4, 2022.

[59] D. Mussa and N. M. Jameel, "Relevant sms spam feature selection using wrapper approach and xgboost algorithm," *Kurdistan Journal of Applied Research*, vol. 4, pp. 110–120, 11 2019.

A Machine Learning Approach to pH Monitoring: Mango Leaf Colorimetry in Aquaculture

Hajar Rastegari[1], Romi Fadilah Rahmat[2], Farhad Nadi[3]
Higher Institution Center of Excellence (HICoE)-Institute of Tropical Aquaculture and Fisheries,
Universiti Malaysia Terengganu, 21030 Kuala Nerus, Terengganu, Malaysia[1]
Department of Information Technology-Faculty of Computer Science and Information Technology,
University of Sumatera Utara Medan, North Sumatra, Indonesia[2]
School of Information Technology, UNITAR International University, 47301 Kelana Jaya, Selangor, Malaysia[3]
Center for Innovation and Technology Adoption (CITA), UNITAR International University,
47301 Kelana Jaya, Selangor, Malaysia[3]

***Abstract*—Maintaining optimal water quality is crucial for successful aquaculture. This necessitates careful management of various water quality parameters, including pH levels within their ideal range. There is growing interest in creating affordable optical pH sensors that provide accurate readings across a wide range of pH values. Development of sensors that are both accurate and cost-effective remains a challenge. To this end, this study demonstrates the use of machine learning with mango leaf extract as a colorimetric indicator to achieve accurate and cost-effective pH estimation for aquaculture practices. Mango leaf was utilized as the pH indicator, covering a range from 1 to 13. RGB color extraction and Exif data were used for image analysis to extract relevant features. The XGBoost algorithm, optimized through stepwise hyperparameter tuning with early stopping, was used to train three different models on this dataset to predict pH values. Three classification models, namely Y3, Y5, and Y13, were trained with 3, 5, and 13 output classes, respectively. The overall precision achieved by each model was 0.94, 0.85, and 0.72, respectively. This demonstrates the potential of this approach for developing a user-friendly yet cost-effective sensor for pH detection applicable in aquaculture practices. The proposed method could help aquaculture farmers an affordable and intelligent smartphone-based pH detection tool, enhancing water quality management while reducing the need for expensive instruments and eliminating the need for additional costly and time-consuming experimental work, thereby contributing to the sustainability of aquaculture practices.**

***Keywords*—Aquaculture; machine learning; XGboost; water quality; sustainable aquaculture practices; water quality monitoring; mango leaf extract**

I. Introduction

Water quality is a pivotal factor in aquaculture, exerting significant influence on fish growth, survival, and reproduction [1], [2], [3]. Precise and consistent monitoring of water quality parameters is essential for effective aquaculture management, aiding in disease prevention, treatment, and overall productivity [2]. To maintain optimal water conditions, various physical, chemical, and biological treatments are applied to aquaculture pond [3]. Key water quality parameters, including temperature, dissolved oxygen, salinity, and pH, provide valuable insights into aquaculture system health and performance [4], [5]. The primary challenge with traditional water quality assessment methods is their lack of cost-effectiveness and the significant labour they require. This highlights the need for more innovative monitoring solutions. Although technological advancements like the Internet of Things (IoT) and artificial intelligence have enabled real-time monitoring and analysis of water quality [6], the high cost of sensors remains a major barrier to the widespread adoption of these modern technologies [7].

Several studies have highlighted that pH is a crucial parameter for assessing water quality and plays a fundamental role in aquatic ecosystems. It has been reported that abnormal pH levels can negatively impact the health of aquatic organisms and the overall quality of water [8], [9]. Therefore, maintaining optimal pH levels is essential for successful aquaculture practices. However, research consistently shows that the ideal pH range varies among fish species, as detailed in Table I, which presents the acceptable pH ranges for different aquatic species.

Colorimetric methods are simpler, more cost-effective, and capable of providing realtime results, making them a promising solution for pH measurement in various fields, such as environmental monitoring [10], [11], [12], [13]. In aquaculture, colorimetric pH sensors demonstrated continuous, in-situ monitor-ing, which allows for early detection of pH fluctuations and enables prompt corrective actions [14]. This study aims to advance the development of more efficient and effective aquaculture practices by addressing the limitations of traditional water quality monitoring techniques and leveraging the benefits of colorimetric pH sensors.

Supervised learning is a subfield of machine learning algorithms that trains models, f, on la-belled data. This data comprises feature vectors, x, and their corresponding labels, y. The primary objective is to minimize a loss function, denoted by $L(f)$, which quantifies the discrepancy between the predicted labels, $f(x)$, and the true labels, y [23].

Ensemble learning is a subcategory of supervised learning algorithms that aims to construct a robust learner, F, by combining multiple weaker learners, fi. A prominent example of ensemble learning is XGBoost, which utilizes decision trees as base learners. These decision trees recursively partition the feature space based on specific decision rules, ultimately predicting a class or a continuous value [24]. XGBoost operates in

TABLE I. OPTIMAL RANGE OF PH VALUES AS REPORTED IN LITERATURE

Description	Lower Range	Upper Range	Reference
Optimal pH range for nile tilapia is between 5 and 8.	5	8	[15]
Efficient nitrification activity in aquaculture biofilters 7.0 9.0			
Reproduction and infectivity of c. Irritans.	6	9	[16]
C. Irritans can survive in pH 5-10 in aquaculture.	5	10	[16]
PH ranged from 7.4 to 9.6 in eutrophic aquaculture ponds.	7.4	9.6	[8]
pH range 6-8 commonly acceptable in aquaculture.	6	8	[17]
pH ranges vary based on species, but generally 6.5-9.0.	6.5	9.0	[18]
Optimal pH for most aquaculture species is 7.0-8.5.	7.0	8.5	[18]
pH levels between 7.51 and 8.00 maintained in aquaculture.	7.51	8.00	[19]
Atlantic salmon embryos have lower lethal limits around pH 3.0-4.0.	3.0	4.0	[20]
Silver catfish juveniles survive in pH range of 4.0-9.0.	4.0	9.0	[21]
pH range in aquaculture: 6.5-9.0 suggested, optimal range varies by species.	6.5	9.0	[22]
Results suggest that 8.0–8.5 is the best pH range for survival and growth of the larvae of the silver catfish (rhamdia quelen) larvae	8.0	8.5	[22]

an iterative manner, gradually building an ensemble of decision trees. Each subsequent tree, f_i, focuses on rectifying the errors made by its predecessors using a technique called gradient boosting. Mathematically, this translates to minimizing $L(f)$ by strategically adding trees that target the residuals of the existing ensemble, $F_{i-1}(x)$. This approach enables XGBoost to effectively handle intricate feature relationships and achieve significant minimization of the loss function, $L(f)$.

II. BACKGROUND

Traditionally, pH measurement has relied on physical sensors, both analog and digital [25]. Despite their precision, these sensors necessitate frequent calibration to maintain accuracy, which can be expensive and time-consuming. Coupled with manual operation, this has prompted a search for more affordable and user-friendly alternatives. Recent advancements have facilitated the integration of digital pH sensors into IoT systems for continuous water quality monitoring [26], [25], [27]. While these solutions are suitable for larger aquaculture operations, their high implementation costs often preclude their adoption by smaller farms seeking economical options. An alternative approach to pH measurement involves pH test strips, a traditional and cost-effective method for assessing water quality in aquaculture [28], [29]. While less precise than sensor-based methods, their simplicity, affordability, and portability make them valuable tools in various applications. However, relying on visual color comparisons with a reference chart can introduce subjectivity and potential inaccuracies. Furthermore, the presence of other water constituents may interfere with test strip accuracy [30], [31]. Despite these limitations, the ease of use and absence of calibration requirements make pH test strips an economical option, particularly for small-scale farms with limited resources.

To mitigate the subjectivity inherent in interpreting pH test strip colors, researchers have explored the use of machine learning models to enhance the accuracy of pH measurements derived from paper strips [32], [33], [34]. Concurrently, the development of novel reagents for pH determination remains an active research area. These innovative reagents, when integrated with smartphone or machine learning-based methodologies, hold the potential to significantly improve pH measurement accuracy. A novel method for directly measuring the pH of airborne particles or droplets has been developed, combining pH indicator paper with RGB-based colorimetric analysis. This approach established a linear correlation between RGB values and pH, surpassing the accuracy and applicability of previous models. Hydrion® Brilliant pH dip stciks (lot no. 3110, Sigma-Aldrich), with their wide pH detection range and resistance to interference, were deemed optimal for analyzing ambient aerosols. Initial findings suggest that aerosol pH can be estimated with an uncertainty of 0.5 units or less, casting doubt on the reliability of traditional pH color charts and emphasizing the need for in situ calibration of pH papers using standardized pH buffers [11].

A smartphone-based colorimetric analysis technique employing a pH-sensitive photonic gel was reported. The gel exhibited color variations corresponding to different pH levels, which were captured and analyzed using a smartphone camera and image processing algorithms. This method demonstrated accurate real-time pH measurement, suggesting its potential applications in environmental monitoring and medical diagnostics [35].

A smartphone-based colorimetric method was developed for detecting enzyme-substrate reactions using pH-responsive gold nanoparticle assemblies. The pH-induced color changes in the gold nanoparticles, resulting from enzyme-substrate interactions, were captured and analyzed using a smartphone. This method offers a simple, cost-effective, and portable platform for monitoring enzyme-substrate reactions in various fields such as biochemistry and environmental science [36].

Traditionally, pH measurement in aquaculture has relied on physical sensors and pH test strips, which provide accurate results but often suffer from portability and usability constraints. In contrast, smartphone-based approaches, utilizing colorimetric changes and sophisticated image processing, offer high precision, portability, and user-friendliness, making them suitable for remote and real-time monitoring. However, these methods may necessitate specific reagents and con-trolled conditions for optimal performance. This research underscores the potential for developing cost-effective and user-friendly smartphone-based pH detection systems with broader applications.

III. MATERIALS AND METHODS

A. Chemicals

Ortho-Phosphoric acid (85-88%) and sodium hydroxide (99%) were purchased from R & M Chemicals. All chemicals were of analytical grade and used as received without further purification. Distilled water was used in all experiments. Green

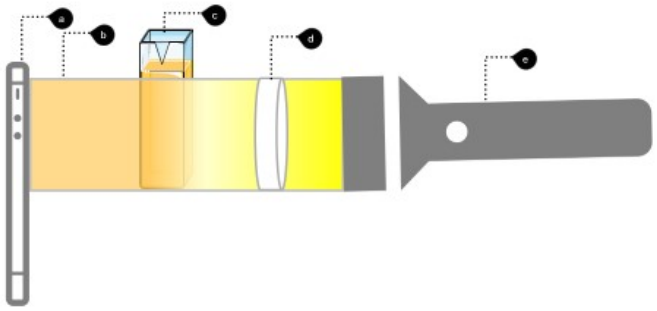


Fig. 1. Schematic illustration of the smartphone colorimetric sensors data gathering. (a) smart phone, (b) PVC pipe of, (c) Cuvette containing sample solution, (d) light diffuser that is a one-centimeter-thick hot glue, (e) torch light as the source of light.

mango leaves were collected from apple mango trees in Kuala Nerus, Terengganu, in November and December 2023.

B. Sample Preparation for Colorimetric Studies

Mango leaves powder was prepared by thoroughly washing the leaves with tap water, followed by three additional rinses with distilled water. The washed leaves were then dried in an air oven at 65°C for 48 h. After drying, the leaves were ground and sieved to obtain a powder with a particle size of 120 µm. To prepare standard solutions covering a pH range from 1 to 13, a sequential dilution process was conducted. This process involved diluting stock solutions of 1M H3PO4 and 1M NaOH with distilled water. The dilution ratios were exactly adjusted to achieve the desired pH levels for each standard solution. For colorimetric studies, 40 mL of each standard solution was mixed with 0.1 g of mango leaves powder. The mixture was manually shaken for 1 min at room temperature and then centrifuged at 8000 rpm for 15 min. The supernatants were removed and filtered using a Nylon syringe filter with a pore size of 0.22 µm. The filtered samples were then transferred to cuvettes for colorimetric analysis.

C. Dataset

Seven different smartphones were used to capture three sets of photographs for each sample with pH values ranging from 1 to 13. A simple photography setup, as illustrated in Fig. 1, was employed for image acquisition. The apparatus consisted of a commonly available 1-inch PVC pipe (Fig. 1(b)) designed to produce consistent images. A $22cm$ long polyethylene pipe with a $4.5cm$ inner diameter was used for the setup. A white LED flashlight (Eveready LC1L2A) was placed at one end of the pipe to illuminate the samples (Fig. 1(e)). To position the samples, a hole was created $7cm$ from the light source. A $0.5cm$ thick layer of translucent hot melt glue was applied inside the pipe to evenly distribute the light (Fig. 1(d)). The smartphone camera was positioned at the opposite end of the pipe to capture images of the samples (Fig. 1(a)). All photographs were taken of samples placed in standard spectrophotometer cuvettes with dimensions of $4.5cm$ height, $3.5mL$ capacity, and an optical range of $190-2500nm$ (Fig. 1(c)).

Image files were renamed to accurately reflect sample type details and subsequently transferred to a computer system.

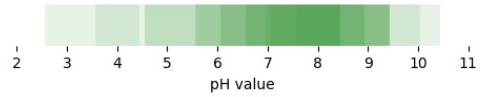


Fig. 2. Heat map chart of suitable pH ranges in aquaculture, as reported in the literature.

iPhone images were converted to JPG format post-transfer. Image boundaries were then delineated using the VIA annotation tool [37].

A dataset of 819 images was initially collected, reduced to 817 images after excluding two due to incorrect labeling. A Python script was developed to extract dominant colors within annotated regions of interest from each image. This process involved applying K-Means clustering with K=1 to determine the predominant color within the annotated regions of the image.

In addition to the dominant color's RGB value, Exif metadata was extracted from each image and integrated into the dataset. Feature engineering was applied to create additional features, such as average image intensity (mean of RGB values) and grayscale values calculated using,

$$0.299R + 0.587G + 0.114B,$$

The red-to-green ratio was calculated and added as an additional feature to the dataset. Subsequently, RGB values were converted to XYZ, HSL, and LAB color spaces using the Python colormath library.

D. pH Class Construction

The original dataset contained a discrete target variable, pH, with 13 distinct classes, forming a 13-class classification problem (Y13). To create datasets with reduced class numbers, a label binarization process was applied. The pH values were grouped into three and five classes for the Y3 and Y5 datasets, respectively. These new datasets represent multi-class classification problems with reduced cardinality. Table II outlines the binning criteria used to transform the original 13 classes into the desired number of classes.

TABLE II. CLASSIFICATION SCENARIOS

Scenario	Label	pH low	pH high
Y3	Acidic	1	3
	Neutral	4	6
	Basic	7	13
Y5	Lethal Acidic	1	3
	Acidic	4	5
	Neutral	6	9
	Basic	9	10
	Lethal Basic	11	13

Fig. 2 presents a heat-map generated from Table I data that was used as the reference points for determining class boundaries. Colour intensity within the heat-map indicates the frequency with which a pH range was reported as optimal in the literature. These ranges were used as a reference to define pH class boundaries for the Y3 and Y5 datasets.

E. XGBoost Classifier

The XGBoost was selected as it offers a compelling alternative to complex deep learning mod-els, particularly for tabular data problems, due to its practicality, robustness, and effectiveness (Harrison, 2023). This algorithm belongs to a family of Ensemble learning, a meta-algorithmic framework that amalgamates multiple base models to enhance predictive accuracy and robustness, has witnessed substantial growth in recent years. Within this domain, boosting has gained recognition for its effectiveness as a sequential approach where models are iteratively developed to correct the errors of their predecessors. Among boosting algorithms, XGBoost stands out as a leading option, known for its computational efficiency, scalability, and superior predictive accuracy. Unlike traditional gradient boosting methods, XGBoost introduces key enhancements such as regularization, optimized tree construction, and robust handling of missing data. The primary objective of XGBoost is to minimize a loss function that includes both a differentiable error component and a regularization term, which helps prevent over-fitting. This approach is mathematically represented as:

$$L(\theta) = \Sigma_{i=1}^{n} l(y_i, \hat{y}_i) + \Omega(\theta)$$

The algorithm iteratively builds decision trees, with each tree refining the predictions made by the previous ensemble. XGBoost accelerates the training process by utilizing techniques such as approximation, weighted quantile sketches, and columnar storage. Furthermore, it incorporates a regularized objective function that includes both L1 and L2 regularization, which helps prevent overfitting and enhances generalization. XGBoost's ability to efficiently handle missing values, along with its parallel computing capabilities, has solidified its dominance in various machine learning competitions and real-world applications.

F. Hyperparameter Tuning

Hyperparameter tuning was performed utilizing a stepwise approach with Hyperopt. This method iteratively explores the space of possible hyperparameter values. In each iteration, a configuration is drawn from the search space, an XGBoost model is trained with those parameters, and the model's performance is evaluated using a chosen metric. This information is then used by Hyperopt to update its internal model of the search space, prioritizing regions that are more likely to contain high-performing configurations. This process continues until a stopping criterion, such as a maximum number of iterations, is met. The main advantage of this approach is its faster execution time compared to other methods. Table III shows the value of the hyper parameters for each classification scenario.

TABLE III. THE HYPER PARAMETER VALUES AS THE RESULT OF HYPERPARAMETER TUNING FOR EACH SCENARIO

Parameter	Y3	Y5	Y13
max_depth	4	8	5
min_child_weight	0.69	0.44	0.22
subsample	0.87	0.92	0.67
colsample_bytree	0.53	0.72	0.96
reg_alpha	0.59	0.89	0.47
reg_lambda	4.57	1.75	8.64
gamma	0.00	0.01	0.00
learning rate	0.52	0.27	0.48

IV. METHODOLOGY

As previously described, three distinct classification scenarios, labeled Y3, Y5, and Y13, were established. To optimize model performance, hyper-parameter tuning with early stopping was implemented for each scenario. The identified optimal parameters were subsequently employed to train respective models. A comprehensive evaluation of these models was undertaken, en-compassing precision, recall, F1-score, and support metrics. To provide a visual representation of model performance, a variety of diagnostic plots were generated. These included confusion matrix heat-maps to visualize classification accuracy, prediction error charts to identify patterns in mis-classifications, classification charts to assess overall performance, and AUC-ROC curves to evaluate the model's ability to discriminate between positive and negative classes.

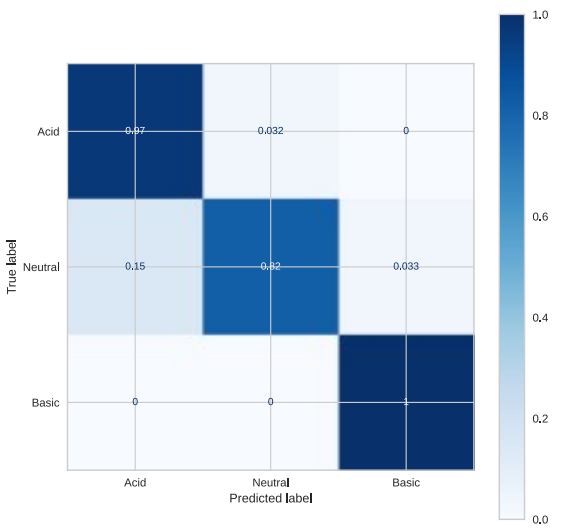
V. RESULTS

Fig. 3 presents the confusion matrices for the three scenarios. The results indicate that model performance generally improved as the number of classes decreased. In the Y3 scenario, the model achieved perfect classification of all Basic samples. Similarly, all samples in the "lethal acidic" category were correctly classified in the Y5 scenario. A common trend emerged, demonstrating superior model performance for samples at the extreme ends of the class spectrum. Conversely, classification accuracy tended to diminish for samples in the intermediate classes, a pattern particularly evident in the Y13 scenario.

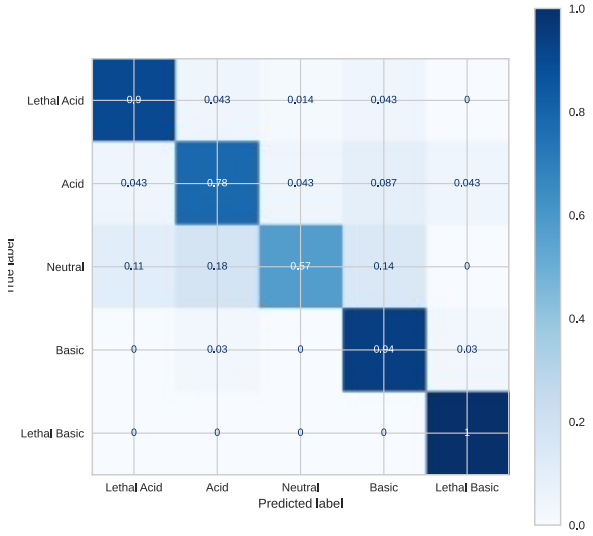
Fig. 4 illustrates the class prediction error profiles for the three classification models using stacked bar charts. Each bar represents a true class, segmented into stacked bars indicating the predicted classes. This visualization provides insights into the types of errors made by the models.

In the Y3 and Y5 scenarios shown in Fig. 4a and Fig. 4b respectively, the models demonstrated relatively strong performance, with most observations correctly classified within their respective true classes. However, the Y13 (show in Fig. 4c) model exhibited a more pronounced error pattern. The stacked bars for pH 9 and pH 5 classes were notably taller than others, indicating higher rates of mis-classification for these categories. This suggests potential class overlap, where instances of pH 9 might share similar feature characteristics with other classes, leading to confusion during the classification process. Additionally, the model might have been underrepresented in training data for these classes, contributing to lower classification accuracy. These findings highlight the challenges inherent in multi-class classification tasks, where class boundaries can be less distinct and model performance is influenced by factors such as data quality and feature engineering.

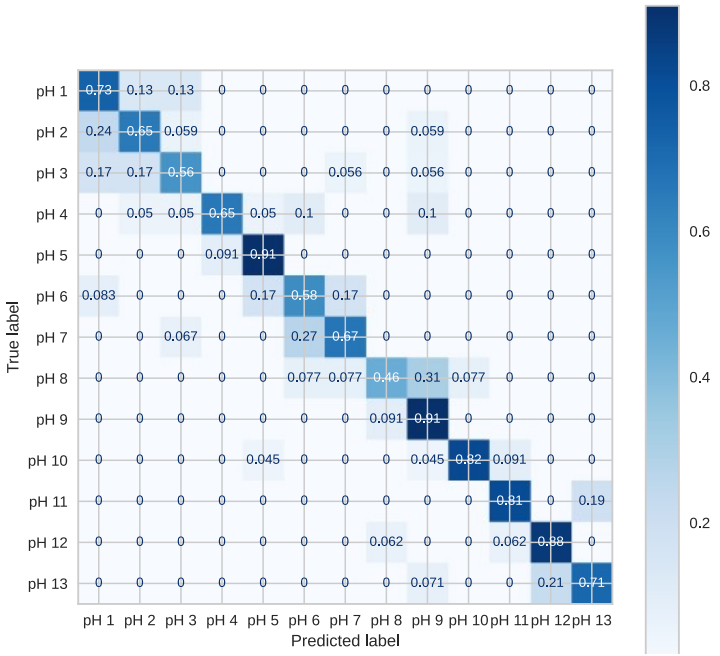
Fig. 5 presents a heatmap visualization of key classification metrics computed on a per-class basis. The heatmap encapsulates four critical performance indicators: precision, recall, F1-score, and support. Support represents the number of instances within each class, providing a measure of class distribution. Precision quantifies the accuracy of positive predictions, essentially the proportion of correctly predicted positive instances among all predicted positives. Recall, conversely, assesses a model's ability to identify all relevant instances, calculated as the ratio of correctly predicted positive instances to the total



(a) Y3



(b) Y5



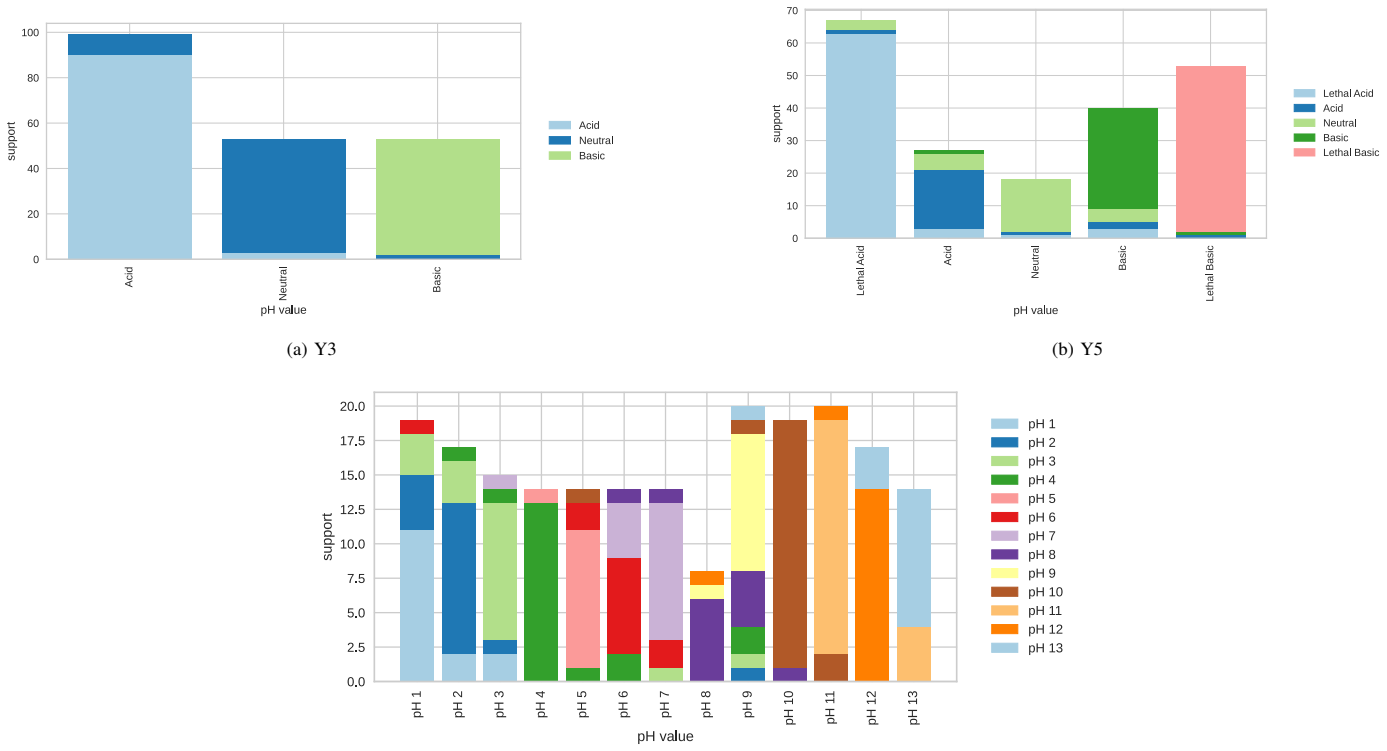
(c) Y13

Fig. 3. Confusion matrices.

number of actual positive instances. The F1-score, a harmonic mean of precision and recall, offers a balanced evaluation of a model's performance, providing a single metric that considers both precision and recall. This metric ranges from 0 to 1, with higher values indicating superior performance. A weighted average of the F1-scores across all classes is commonly employed to compare the overall effectiveness of different classification models.

Referring to Fig. 5c we can observe that while several classes demonstrated robust classification capabilities, as indicated by F1-scores exceeding 0.7, a subset of classes exhibited suboptimal performance. These classes with lower F1-scores suggest potential challenges in accurately identifying and classifying instances within these categories, warranting further investigation into factors such as class imbalance, data quality, or model complexity.

The original model, i.e. Y13 model, exhibited variable performance across classes, with several notably lower F1-scores. While the distribution of instances across classes appeared balanced, as indicated by the support column in the classification report, the intrinsic challenge of the problem became apparent. The data, primarily composed of images with subtle variations in shades of yellow, presented a complex classification task. The model's difficulties in distinguishing



(a) Y3

(b) Y5

(c) Y13

Fig. 4. Class prediction errors.

be-tween these closely related visual features, coupled with the limited discriminative power of the available features, likely contributed to the sub-optimal performance. These findings suggest that enhancing feature engineering or exploring more sophisticated image processing techniques might be necessary to improve classification accuracy for Y13 scenario.

The Y3 and Y3 scenario exhibit notably higher average F1-scores compared to the original thirteen-class model. This suggests that consolidating the original classes into fewer categories has led to improved classification performance. The Y3 model, in particular, demonstrates consistently strong performance across all classes, with F1-scores above 0.88. The Y5 model also shows promising results, with three classes achieving F1-scores above 0.7. These findings imply that the complexity introduced by the thirteen-class model might have hindered its ability to accurately discriminate between closely related classes. By reducing the number of classes, the models were able to focus on more distinct categorical boundaries, resulting in enhanced classification accuracy.

The ROC AUC curves, as shown in Fig. 6, provide valuable insights into the discriminative power of the models across different class scenarios. The Y3 model (see Fig. 6a) exhibits exceptional performance, with all classes achieving AUC values close to 1. This indicates an outstanding ability to differentiate between the three classes. While the Neutral class in Y3 shows a slightly lower AUC of 0.94 compared to the other two classes, the overall performance remains exceptionally high. The same is true for the Y5 (see Fig. 6b) model as it has shown comparable performance with the Y3 model.

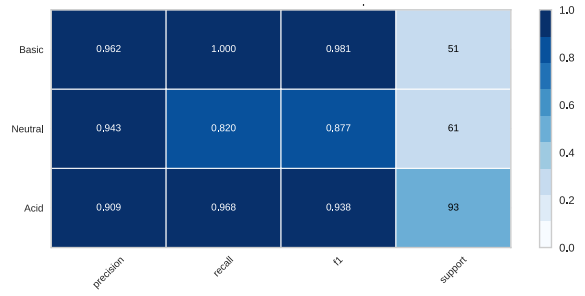
In contrast, the Y13 model (see Fig. 6c) presents a more complex picture. While the macro and micro average AUC values of 0.96 are still commendable, the individual class performance varies. Classes “pH 6” and “pH 3” show notably lower AUC values, suggesting challenges in distinguishing these classes from others. This aligns with the previously discussed difficulties in classifying closely related shades of yellow.

Overall, the ROC AUC analysis reinforces the findings from the F1-score evaluation. The Y3 model demonstrates superior discriminative power, likely due to the increased class separability. The Y13 model, while showing good overall performance, struggles with certain classes, emphasizing the impact of feature similarity and the potential limitations of the current feature set.

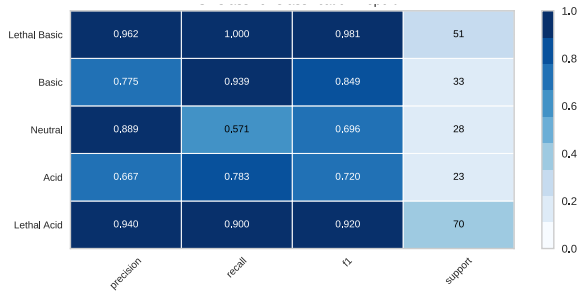
These results further support the conclusion that refining feature engineering or exploring more advanced image processing techniques could be crucial for improving the performance of the thirteen-class model.

This research evaluated the feasibility of developing a cost-effective smartphone-based pH detection system for aquaculture. While commercial pH sensors provide precise measurements, their high cost limits their adoption by small-scale farmers.

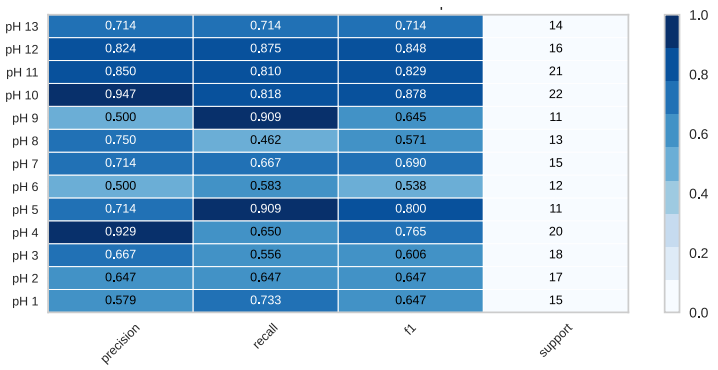
To address this gap, we developed a method using readily available materials like mango leaves, smartphones, and simple



(a) Y3



(b) Y5



(c) Y13

Fig. 5. Classification report.

photography equipment. Our results demonstrate that while models like Y13 may not achieve the precision of commercial sensors, models Y3 and Y5 can effectively estimate pH ranges. This level of accuracy aligns with the practical needs of most aquaculture farmers, as precise pH values are often less critical than maintaining pH within specific ranges (see Table I).

Our proposed method offers a low-cost, accessible alternative to traditional pH monitoring. By reducing reliance on expensive equipment, it has the potential to improve water quality management in aquaculture. However, to ensure reliable results, farmers should conduct multiple tests and consider factors such as water change frequency and potential water treatment measures.

VI. Conclusion

This study successfully demonstrated the potential of a smartphone-based sensor for pH monitoring in aquaculture settings. By integrating the colorimetric properties of mango leaf extract with advanced image processing and machine learning techniques, we developed a predictive model for pH levels. This approach offers a sustainable and economically viable alternative to traditional pH sensors.

The use of a natural indicator aligns with eco-friendly aquaculture practices while the smartphone platform enhances accessibility. Farmers can potentially utilize this device for regular water quality assessments, enabling proactive pond management.

While the initial results are promising, further research is imperative to improve the model's precision and reliability under diverse environmental conditions. Extensive field trials are necessary to validate the sensor's effectiveness in real-world aquaculture scenarios. Overcoming these challenges is crucial for transforming the technology into a practical and indispensable tool for aquaculture practitioners.

Ultimately, the development of cost-effective and user-friendly water quality monitoring solutions is essential for the sustainable growth of the aquaculture industry. This research represents a significant step towards achieving this goal. By providing farmers with data-driven insights into water quality, we can enhance the overall health and productivity of aquaculture systems while minimizing environmental impact.

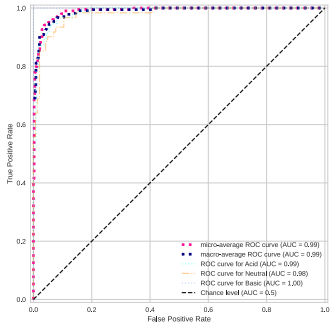
Acknowledgment

The authors would like to thank the Research Management Office (RMO) at Universiti Malaysia Terengganu, for the financial support of this research through Talent and Publication Enhancement-Research grant 2023 (UMT/TAPE-RG/55497)

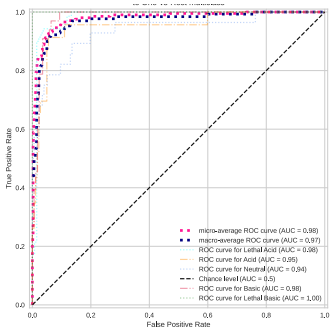
References

[1] N. Abdullah, A. S. Chowdhury, M. M. Hossain, O. Dutta, and J. Uddin, "Analysis of aquaculture for cultivating different types of fish," in *Applied Informatics for Industry 4.0*. Chapman and Hall/CRC, 2023, pp. 83–96.

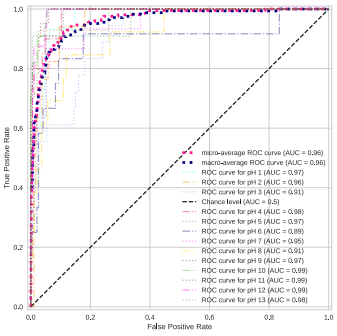
[2] P. Lindholm-Lehto, "Water quality monitoring in recirculating aquaculture systems," *Aquaculture, Fish and Fisheries*, vol. 3, no. 2, pp. 113–131, Apr. 2023. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/aff2.102



(a) Y3



(b) Y5



(c) Y13

Fig. 6. Receiver Operating Characteristic (ROC) to One-vs Rest runtime.

[3] T. Y. Wei, E. S. Tindik, C. F. Fui, H. Haviluddin, and M. H. A. Hijazi, "Automated water quality monitoring and regression-based forecasting system for aquaculture," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 1, pp. 570–579, Feb. 2023. [Online]. Available: https://beei.org/index.php/EEI/article/view/4464

[4] D. Kültz, "213Abiotic parameters," in *A Primer of Ecological Aquaculture*. Oxford University Press, 09 2022. [Online]. Available: https://doi.org/10.1093/oso/9780198850229.003.0016

[5] P. C. Lindholm-Lehto, "Water quality monitoring in recirculating aquaculture systems," *Aquaculture, fish and fisheries*, vol. 3, no. 2, pp. 113–131, 2023.

[6] . Flura, M. Moniruzzaman, M. A. Alam, M. H. Rashid, M. H. Rahman, M. A. Rahman, and Y. Mahmud, "An Assessment of the Water Quality Factors: A Case of Hilsa Fishery River Areas," *Asian Journal of Fisheries and Aquatic Research*, pp. 30–47, Oct. 2022. [Online]. Available: https://journalajfar.com/index.php/AJFAR/article/view/486

[7] H. Rastegari, F. Nadi, S. S. Lam, M. Ikhwanuddin, N. A. Kasan, R. F. Rahmat, and W. A. W. Mahari, "Internet of Things in aquaculture: A review of the challenges and potential solutions based on current and future trends," *Smart Agricultural Technology*, vol. 4, p. 100187, Aug. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2772375523000175

[8] J. A. Hargreaves, L. D. Sheely, and F. S. To, "A Control System to Simulate Diel pH Fluctuation in Eutrophic Aquaculture Ponds," *Journal of the World Aquaculture Society*, vol. 31, no. 3, pp. 390–402, Sep. 2000. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1111/j.1749-7345.2000.tb00889.x

[9] N. Mohamed Ramli, C. Giatsis, F. Md Yusoff, J. Verreth, and M. Verdegem, "Resistance and resilience of small-scale recirculating aquaculture systems (RAS) with or without algae to pH perturbation," *PLOS ONE*, vol. 13, no. 4, p. e0195862, Apr. 2018. [Online]. Available: https://dx.plos.org/10.1371/journal.pone.0195862

[10] L. Di Costanzo and B. Panunzi, "Visual pH Sensors: From a Chemical Perspective to New Bioengineered Materials," *Molecules*, vol. 26, no. 10, p. 2952, may 2021. [Online]. Available: https://www.mdpi.com/1420-3049/26/10/2952

[11] G. Li, H. Su, N. Ma, G. Zheng, U. Kuhn, M. Li, T. Klimach, U. Pöschl, and Y. Cheng, "Multifactor colorimetric analysis on pH-indicator papers: an optimized approach for direct determination of ambient aerosol pH," *Atmospheric Measurement Techniques*, vol. 13, no. 11, pp. 6053–6065, nov 2020. [Online]. Available: https://amt.copernicus.org/articles/13/6053/2020/

[12] K. Vizarova, I. Vajova, N. Krivonakova, R. Tino, Z. Takac, S. Vodny, and S. Katuscak, "Regression Analysis of Orthogonal, Cylindrical and Multivariable Color Parameters for Colorimetric Surface pH Measurement of Materials," *Molecules*, vol. 26, no. 12, p. 3682, jun 2021. [Online]. Available: https://www.mdpi.com/1420-3049/26/12/3682

[13] W. X. C. S. W. X. W. L. K. Q. Y. M. L. X. X. J. Z. C. X. Y., "pH-Sensitive Dye-Based Nanobioplatform for Colorimetric Detection of Heterogeneous Circulating Tumor Cells," *ACS Sensors*, vol. 6, no. 5, pp. 1925–1932, may 2021. [Online]. Available: https://pubs.acs.org/doi/10.1021/acssensors.1c00314

[14] H. Chen, F. Ding, Z. Zhou, X. He, and J. Shen, "FRET-based sensor for visualizing pH variation with colorimetric/ratiometric strategy and application for bioimaging in living cells, bacteria and zebrafish," *The Analyst*, vol. 145, no. 12, pp. 4283–4294, 2020. [Online]. Available: https://xlink.rsc.org/?DOI=D0AN00841A

[15] Y.-J. Wang, T. Yang, and H.-J. Kim, "pH Dynamics in Aquaponic Systems: Implications for Plant and Fish Crop Productivity and Yield," *Sustainability*, vol. 15, no. 9, p. 7137, apr 2023. [Online]. Available: https://www.mdpi.com/2071-1050/15/9/7137

[16] L. Zhou, J. Huang, Y. Jiang, J. Kong, X. Xie, and F. Yin, "pH Regulates the Formation and Hatching of *Cryptocaryon irritans* Tomonts, Which Affects Cryptocaryoniasis Occurrence in *Larimichthys crocea* Aquaculture," *Applied and Environmental Microbiology*, vol. 88, no. 7, pp. e00 058–22, apr 2022. [Online]. Available: https://journals.asm.org/doi/10.1128/aem.00058-22

[17] E. D. Chang, R. M. Town, S. F. Owen, C. Hogstrand, and N. R. Bury, "Effect of Water pH on the Uptake of Acidic (Ibuprofen) and Basic (Propranolol) Drugs in a Fish Gill Cell Culture Model," *Environmental Science & Technology*, vol. 55, no. 10, pp. 6848–6856, may 2021. [Online]. Available: https://pubs.acs.org/doi/10.1021/acs.est.0c06803

[18] J. R. Bowman and J. E. Lannan, "Evaluation of Soil pH-Percent Base Saturation Relationships for Use in Estimating the Lime Requirements of Earthen Aquaculture Ponds," *Journal of the World Aquaculture Society*, vol. 26, no. 2, pp. 172–182, jun 1995. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1111/j.1749-7345.1995.tb00241.x

[19] C. M. McGraw, C. E. Cornwall, M. R. Reid, K. I. Currie, C. D. Hepburn, P. Boyd, C. L. Hurd, and K. A. Hunter, "An automated pH-controlled culture system for laboratory-based ocean acidification experiments," *Limnology and Oceanography: Methods*, vol. 8, no. 12, pp. 686–694, dec 2010. [Online]. Available: https://aslopubs.onlinelibrary.wiley.com/doi/10.4319/lom.2010.8.0686

[20] P. G. Daye and E. T. Garside, "Lower lethal levels of pH for embryos and alevins of Atlantic salmon, *Salmo salar* L." *Canadian Journal of Zoology*, vol. 55, no. 9, pp. 1504–1508, sep 1977. [Online]. Available: http://www.nrcresearchpress.com/doi/10.1139/z77-194

[21] L. S. D. Andrade, R. L. B. D. Andrade, A. G. Becker, L. V. Rossato, J. F. D. Rocha, and B. Baldisserotto, "Interaction of Water Alkalinity and Stocking Density on Survival and Growth of Silver Catfish, *Rhamdia quelen* , Juveniles," *Journal of the World Aquaculture*

Society, vol. 38, no. 3, pp. 454–458, sep 2007. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1111/j.1749-7345.2007.00118.x

[22] J. Lopes, L. Silva, and B. Baldisserotto, "Survival and growth of silver catfish larvae exposed to different water pH," *Aquaculture International*, vol. 9, no. 1, pp. 73–80, 2001. [Online]. Available: http://link.springer.com/10.1023/A:1012512211898

[23] L. Takahashi, Keisuke; Takahashi, "Supervised Machine Learning," in *Materials Informatics and Catalysts Informatics*. Singapore: Springer Nature Singapore, 2024, pp. 191–226. [Online]. Available: $https://link.springer.com/10.1007/978-981-97-0217-6_8$

[24] L. Vanneschi and S. Silva, "Ensemble Methods," in *Lectures on Intelligent Systems*. Cham: Springer International Publishing, 2023, pp. 283–288, series Title: Natural Computing Series. [Online]. Available: $https://link.springer.com/10.1007/978-3-031-17922-8_11$

[25] G. Aryotejo, P. W. Adi, and E. A. Sarwoko, "Water quality monitoring with an early warning system for enhancing the shrimp aquaculture production," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 2, p. 1042, may 2024. [Online]. Available: https://ijeecs.iaescore.com/index.php/IJEECS/article/view/35583

[26] F. Akhter, H. R. Siddiquei, M. E. E. Alahi, K. P. Jayasundera, and S. C. Mukhopadhyay, "An IoT-Enabled Portable Water Quality Monitoring System With MWCNT/PDMS Multifunctional Sensor for Agricultural Applications," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14 307–14 316, aug 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9390294/

[27] M. Singh, K. S. Sahoo, and A. Nayyar, "Sustainable IoT Solution for Freshwater Aquaculture Management," *IEEE Sensors Journal*, vol. 22, no. 16, pp. 16 563–16 572, aug 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9827934/

[28] K. Devarayan, D. Anandakumar Muthurani, G. Kannusamy, A. Theivasigamani, Y. Palanisamy, G. Mohan, M. Sukumaran, E. U. Siluvai John, R. Marimuthu, and H. Anjappan, "On-site colorimetric determination of pH in brackish water aquaculture," *Pigment & Resin Technology*, may 2024. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/PRT-11-2023-0099/full/html

[29] A. Jain, S. Wadhawan, V. Kumar, and S. K. Mehta, "pH-Sensing Strips Based on Biologically Synthesized Ly-MgO Nanoparticles," *ACS Omega*, vol. 4, no. 26, pp. 21 647–21 657, dec 2019. [Online]. Available: https://pubs.acs.org/doi/10.1021/acsomega.9b01306

[30] S. Borsci, P. Buckle, J. Huddy, Z. Alaestante, Z. Ni, and G. B. Hanna, "Usability study of pH strips for nasogastric tube placement," *PLOS ONE*, vol. 12, no. 11, p. e0189013, nov 2017. [Online]. Available: https://dx.plos.org/10.1371/journal.pone.0189013

[31] N. A. Metheny, E. M. Gunn, C. S. Rubbelke, T. F. Quillen, U. R. Ezekiel, and K. L. Meert, "Effect of pH Test-Strip Characteristics on Accuracy of Readings," *Critical Care Nurse*, vol. 37, no. 3, pp. 50–58, jun 2017. [Online]. Available: https://aacnjournals.org/ccnonline/article/37/3/50/3578/Effect-of-pH-TestStrip-Characteristics-on-Accuracy

[32] S. D. Kim, Y. Koo, and Y. Yun, "A Smartphone-Based Automatic Measurement Method for Colorimetric pH Detection Using a Color Adaptation Algorithm," *Sensors*, vol. 17, no. 7, p. 1604, jul 2017. [Online]. Available: https://www.mdpi.com/1424-8220/17/7/1604

[33] A. Mutlu, A. Y. Mutlu, V. Kılıç, V. Kilic, G. K. Özdemir, G. K. Özdemir, A. Bayram, A. Bayram, N. Horzum, N. Horzum, M. Solmaz, and M. E. Solmaz, "Smartphone-based colorimetric detection via machine learning," *Analyst*, 2017.

[34] E. V. Woodburn, K. D. Long, and B. T. Cunningham, "Analysis of Paper-Based Colorimetric Assays With a Smartphone Spectrometer," *IEEE Sensors Journal*, vol. 19, no. 2, pp. 508–514, jan 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8494768/

[35] H. Park, Y. G. Koh, and W. Lee, "Smartphone-based colorimetric analysis of structural colors from pH-responsive photonic gel," *Sensors and Actuators B: Chemical*, vol. 345, p. 130359, oct 2021. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0925400521009278

[36] L. Zou, C. Mai, M. Li, and Y. Lai, "Smartphone-assisted colorimetric sensing of enzyme-substrate system using pH-responsive gold nanoparticle assembly," *Analytica Chimica Acta*, vol. 1178, p. 338804, sep 2021. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0003267021006309

[37] A. Dutta and A. Zisserman, "The VIA Annotation Software for Images, Audio and Video," in *Proceedings of the 27th ACM International Conference on Multimedia*, ser. MM '19. New York, NY, USA: ACM, 2019, event-place: Nice, France. [Online]. Available: https://doi.org/10.1145/3343031.3350535

Unveiling Hidden Variables in Adversarial Attack Transferability on Pre-Trained Models for COVID-19 Diagnosis

Dua'a Akhtom[1], Manmeet Mahinderjit Singh[2]*, Chew XinYing[3]
School of Computer Sciences, Universiti Sains Malaysia, Gelugor, Pulau Pinang 11700, Malaysia[1]
Universiti Sains Malaysia, Gelugor, Pulau Pinang 11700, Malaysia[2,3]

***Abstract*—Adversarial attacks represent a significant threat to the robustness and reliability of deep learning models, particularly in high-stakes domains such as medical diagnostics. Advanced Persistent Threat (APT) attacks, characterized by their stealth, complexity, and persistence, exploit adversarial examples to undermine the integrity of AI-driven healthcare systems, posing severe risks to their operational security. This study examines the transferability of adversarial attacks across pre-trained models deployed for COVID-19 diagnosis. Using two prominent convolutional neural networks (CNNs), ResNet50 and EfficientNet-B0, this study explores critical factors that influence the transferability of adversarial perturbations, a vulnerability that could be strategically exploited by APT attackers. By investigating the roles of model architecture, pre-training dataset characteristics, and adversarial attack mechanisms, this research provides valuable insights into the propagation of adversarial examples in medical imaging. Experimental results demonstrate that specific model architectures exhibit varying levels of susceptibility to adversarial transferability. ResNet50, with its deeper layers and residual connections, displayed enhanced robustness against adversarial perturbations, whereas EfficientNet-B0, due to its distinct feature extraction strategy, was more vulnerable to perturbations crafted using ResNet50's gradients. These findings underscore the influence of architectural design on a model's resilience to adversarial attacks. By advancing the understanding of adversarial robustness in medical AI applications, this study offers actionable guidelines for mitigating the risks associated with adversarial examples and emerging threats, such as APT attacks, in real-world healthcare scenarios.**

***Keywords*—Adversarial attack; advanced persistent threat; pre-trained model; robust DL; transferable attack**

I. Introduction

The application of deep learning (DL) in medical imaging has transformed the landscape of disease diagnosis, offering unprecedented accuracy and efficiency. Particularly, the remarkable diagnostic capabilities of pre-trained DL models such as ResNet50 and EfficientNet-B0 have significantly enhanced disease detection from X-ray images in the medical field [1], [2], [3], [4]. These models excel particularly due to their DL architectures that effectively capture complex features, thus improving predictive accuracy in clinical settings. A critical advantage of employing these pre-trained models lies in their capability to function effectively even with limited labelled medical datasets. Through transfer learning, they can be fine-tuned using relatively smaller datasets, which is especially beneficial in scenarios where comprehensive medical annotations are scarce or costly to obtain.

Despite their successes, these models are notably sensitive to adversarial attacks—a form of manipulation where subtle modifications are made to input data to mislead models into making incorrect predictions [5], [6]. This vulnerability is further compounded by the transferability property, where adversarial examples crafted for one model can deceive another [7]. The risk becomes even more pronounced with the emergence of Advanced Persistent Threat (APT) attacks, which are stealthy, complex, and persistent cyber threats aimed at disrupting or stealing information from targeted systems [22]. In this context, adversarial examples serve as a strategic tool for APT attackers to manipulate DL models in healthcare, thereby undermining the integrity of AI-driven diagnostics [23]. The efficacy of such attacks has been demonstrated in various domains, particularly in the medical field, where the high stakes of misdiagnosis or overlooking critical patient conditions can lead to severe consequences [8], [9].

Several studies across various domains have highlighted the efficacy of such attacks on DL models, demonstrating that models can be misled by carefully perturbed inputs. Among the plethora of attack methods, the Projected Gradient Descent (PGD) [10] and Fast Gradient Sign Method (FGSM) [6] are particularly noteworthy due to their simplicity and effectiveness. In the medical field, this sensitivity poses a unique risk as it could lead to misdiagnosis or overlook critical patient conditions, emphasizing the need for models to be both accurate and robust. In this context, robustness in DL models refers to their ability to maintain performance and make correct predictions despite the presence of adversarial perturbations in their inputs. Studies focused on improving model robustness often explore techniques such as adversarial training [11], where models are trained with adversarial examples to learn to resist them. Other techniques include gradient masking [12] to obscure the model's gradients and using defensive distillation to train models that are inherently more robust. Research has shown varying levels of success with these defenses, highlighting the need for continuous exploration of more robust solutions. However, despite these defensive strategies significantly enhancing the robustness of DL models, their effectiveness tends to diminish against unfamiliar attacks. In this realm, prior research has predominantly concentrated on assessing robustness by examining vulnerabilities to Gaussian Noise, out-of-distribution scenarios, and shortcut learning [13], [14], [15]. Yet, there has been a lack of focus on evaluations against

*Corresponding authors.

adversarial examples. Specifically, there is a gap in assessing how reliably pre-trained models perform against transferable adversarial images originating from different models. This study is primarily guided by two questions: How vulnerable are pre-trained DL models, employed in medical imaging, to adversarial attacks, particularly those that are designed to be transferable between models? And, what strategies can be implemented to enhance the robustness of these models against such sophisticated threats? Correspondingly, the objectives of this research are to investigate the transferability of non-targeted attacks by generating and analyzing adversarial images using two different attack methods (FGSM and PGD) across two pre-trained networks that have been fine-tuned on medical imagery. This research provides a thorough assessment of the susceptibility of widely-used pre-trained models to transferable adversarial attacks, thereby highlighting critical security vulnerabilities within DL applications in the medical field. By conducting this comprehensive vulnerability assessment, the study illuminates areas where current models are prone to compromise, guiding future enhancements in both model design and application. Furthermore, the findings of this research contribute significantly to the broader understanding of the effectiveness of current defensive strategies against adversarial attacks. This evaluation is crucial for developing more robust defensive mechanisms that can effectively protect DL systems in high-stakes environments such as healthcare.

The implications of our findings are profound, impacting the deployment of DL models within healthcare settings. Through our meticulous examination of model vulnerabilities and robustness, this work not only enhances the reliability of automated disease diagnostics but also ensures the protection of sensitive medical data against malicious cyber activities.

A. Transferability of Adversarial Examples: An Overview

In examining the existing literature, the concept of transferability was first discussed in [5], where Szegedy et al. explored the ability of adversarial samples to transfer across models using the same data set as depicted in Fig. 1. Subsequently, Goodfellow et al. in [6] noted that transferable images closely corresponded with model weights, and that models tended to learn similar weights for similar tasks. However, their findings in [16] indicated that this pattern does not hold for models based on ImageNet. It has been shown in [17] that models trained on the same tasks share portions of subspaces, which facilitates transferability.

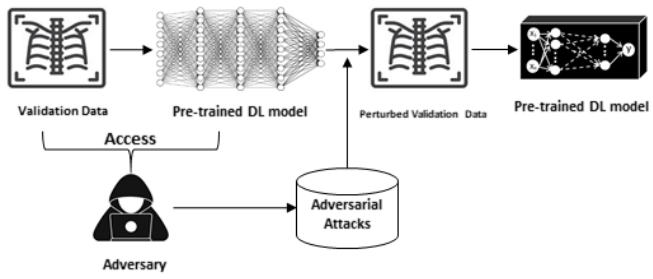


Fig. 1. Transferability of adversarial attack.

Further research into the vulnerability of DL systems in medical image analysis has shown that pre-training dramatically increases the transferability of adversarial examples, even across differing architectures. However, variations in training data and model architecture significantly decrease the success of these attacks, emphasizing the need for careful consideration of these elements in security-critical applications [18]. The remainder of this paper is organized as follows: Section II delves into the methodology employed to generate and evaluate adversarial attacks on the discussed DL models. Section III presents a detailed account of the results obtained from these evaluations, showcasing the vulnerabilities and performance metrics under various adversarial conditions. Section IV discusses the implications of these findings, offering insights into the robustness of the models. Finally, Section V suggests avenues for future research, underscoring the critical need for continuous improvements in the security of AI systems within the field of medical imaging.

II. Study Design

A. Target Architecture

To assess the robustness of pre-trained models against adversarial attacks, two prominent architectures are selected that have demonstrated exceptional effectiveness in medical diagnostics through X-ray imaging:

- Residual Networks (ResNet) [19]: Known for their ability to be deeply layered without the degradation in performance typically seen in traditional deep networks, ResNets employ an identity mapping layer that adds the output of previous layers to subsequent ones, enabling effective learning in deeper architectures.
- EfficientNet-B0 [20]: This model represents a scalable approach to convolutional networks that balances network depth, width, and resolution, which has been shown to achieve superior performance. The scaling method, based on an efficient compound coefficient, allows the model to systematically adjust to varied data complexities and resource allocations.

B. Adversarial Examples Generation

Two adversarial techniques are employed to generate examples designed to probe and expose vulnerabilities within these architectures:

- Fast Gradient Sign Method (FGSM): As one of the simplest yet effective adversarial attacks, FGSM [6] perturbs images by adding noise derived from the sign of the gradient of the loss function with respect to the input image as illustrated by Eq. 1, scaled by a small factor ϵ. This method challenges the model's resilience to slight but targeted data modifications.

$$x' = x + \varepsilon \cdot \text{sign}(\nabla_x J(\theta, x, y)) \tag{1}$$

- Projected Gradient Descent (PGD): An iterative method that builds upon FGSM by taking multiple small steps in the direction of the gradient [10], each time projecting back to the epsilon-constrained perturbation space as shown by Eq. 2. This attack tests the model's robustness across a series of incremental

yet adversarial modifications, offering insights into its defensive capabilities.

$$\tilde{X}_{N+1} = \text{Clip}_{X,\varepsilon}\left\{\tilde{X}_N + \alpha \cdot \text{sign}(\nabla_X J(\tilde{X}_N, y))\right\} \quad (2)$$

C. Dataset and Model Configuration

In this study, two distinct X-ray image datasets were utilized. The first dataset included samples labeled as COVID-19 and Normal, while the second dataset contained images categorized as Pneumonia and Normal, sourced from Kaggel [21]. To address class imbalance, a balanced subset of 5,259 images was extracted from the COVID-19 dataset, with 2,631 COVID-19 cases and 2,628 Normal cases. Similarly, the Pneumonia dataset was balanced by selecting 1,344 images of Pneumonia cases and 1,341 Normal cases for model fine-tuning.

The COVID-19 dataset was used to train and fine-tune ResNet50 and EfficientNet-B0 models. As illustrated in Fig. 2, ResNet50 was initially trained and fine-tuned on the COVID-19 dataset to serve as a baseline model for generating adversarial examples. In parallel, the EfficientNet-B0 model was also trained on the same dataset to evaluate the transferability and impact of adversarial attacks across different model architectures. Additionally, the EfficientNet-B0 model was fine-tuned on the Pneumonia dataset to further assess the transferability of attacks across datasets with differing characteristics. Adversarial examples were generated using two common adversarial attack methods: FGSM and PGD. These methods were applied to the fine-tuned ResNet50 model. The perturbations were varied across three epsilon values — 0.01, 0.05, and 0.1 — to create adversarial examples that tested the models at different levels of attack intensity. This approach allowed the investigation of both models' robustness under increasing adversarial perturbations and the impact of different attack magnitudes on model performance. Fig. 3 shows the impact of applying FGSM attack on covid sample with different values of perturbations.

D. Evaluation Metrics and Scenarios

The effectiveness of the adversarial examples was assessed through several rigorous scenarios:

- Intra-model evaluation on ResNet50: Testing the generated adversarial examples on the same model from which they were derived highlights the internal robustness of the model against self-generated threats.
- Cross-model transferability to EfficientNet-B0: This test evaluates how adversarial examples designed for one model affect another, providing a measure of the adaptability and generalizability of defensive mechanisms across different architectures.
- Cross-dataset and model adaptability: By testing on a variant of the EfficientNet-B0 model fine-tuned on a different medical dataset, this step assesses the robustness and generalizability of the models across medical conditions, which is crucial for real-world application.

Performance metrics such as accuracy and AUC-ROC are used to quantify the models' diagnostic accuracy and robustness under adversarial conditions, effectively highlighting potential vulnerabilities and areas for improvement in AI applications in medical imaging.

III. Results

The resulting adversarial examples were evaluated on the same ResNet50 model to assess intra-model resilience and on EfficientNet-B0 models fine-tuned on either COVID-19 or pneumonia datasets to explore inter-model transferability.

A. Intra-model Robustness of ResNet50

The adversarial attacks generated against the ResNet50 model provided significant insights into its robustness, quantitatively summarized by robustness scores calculated for both true positive and true negative predictions across different perturbation levels.

1) FGSM attack: As shown in Table I, at lower perturbation levels ($\epsilon = 0.01$), ResNet50 displayed robust performance with an accuracy of 91.56%, indicating effective handling of slight perturbations. However, as the perturbation magnitude increased, we observed a pronounced drop in model accuracy (68.36% for $\epsilon = 0.05$ and 50.62% for $\epsilon = 0.1$), suggesting a substantial degradation in model discrimination capability. The robustness scores for true positives remained high at 0.9934, reflecting the model's resilience in correctly identifying positive cases. However, the true negatives robustness score of 0.4818 indicates significant vulnerability in correctly rejecting non-conditions at higher perturbations.

TABLE I. ResNet50 Trained on COVID-19 Attacked by FGSM Attack

ε	TP	FN	FP	TN	Accuracy
0.01	2581	50	394	2234	0.9156
0.05	2629	2	1661	964	0.6836
0.1	2631	0	2597	31	0.5062

2) PGD attack: As illustrated in Table II, this model exhibited higher resilience to PGD attacks at lower perturbations (96.08% accuracy at $\epsilon = 0.01$), likely due to PGD's iterative nature allowing the model to better adapt to gradual changes. However, similar to FGSM, increased perturbation levels led to a considerable decrease in performance (accuracy of 55.22% at $\epsilon = 0.1$). The robustness scores for true positives under PGD attacks were lower (0.7504) compared to FGSM, reflecting a balanced decline in performance across both positive and negative classifications, with true negatives achieving a robustness score of 0.6715. These results underscore that while ResNet50 can manage lower intensity adversarial attacks, its vulnerability escalates with increased perturbation magnitude, especially under FGSM's more disruptive approach.

TABLE II. ResNet50 Trained on COVID-19 Attacked by PGD Attack

ε	TP	FN	FP	TN	Accuracy
0.01	2161	52	78	1024	0.9608
0.05	1122	8	331	759	0.8473
0.1	2624	7	2348	280	0.5522

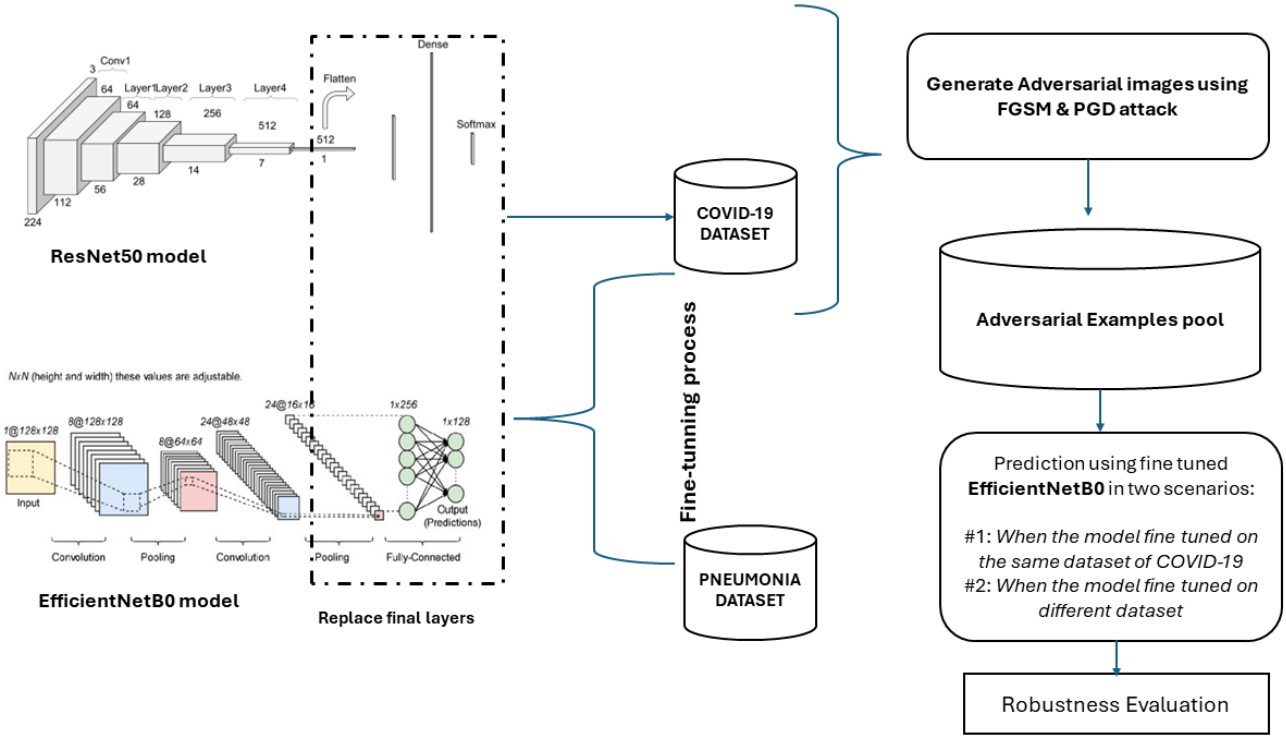


Fig. 2. Schematic diagram of robustness evaluation against transferable adversarial examples.

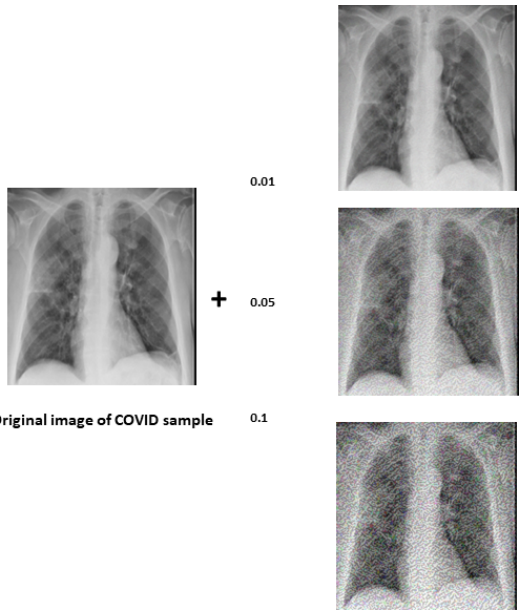


Fig. 3. Generation of adversarial COVID example using FGSM attack.

B. Inter-model Transferability to EfficientNet-B0

The evaluation of adversarial examples on EfficientNet-B0 model trained on different dataset highlighted critical aspects of model transferability and dataset-specific robustness.

- EfficientNet-B0 trained on COVID-19: The FGSM and PGD attacks at low perturbation levels ($\epsilon = 0.01$) resulted in relatively high accuracies (95.03% for PGD and 79.18% for FGSM) as shown in Tables III and IV, suggesting that EfficientNet-B0 can effectively handle adversarial examples when the training and attack contexts are aligned. However, the robustness scores provide additional insight:
  - TP robustness score decreased from 0.95 to 0.60 as ϵ increased from 0.01 to 0.1.
  - TN robustness score showed a more significant decline from 0.85 to 0.30 across the same range of perturbations.

  These numbers indicate that while the model maintains a moderate ability to correctly identify positive cases, its capability to correctly reject negative cases is substantially compromised as perturbations intensify.
- EfficientNet-B0 trained on pneumonia: This configuration demonstrated poor performance across all perturbation levels for both FGSM and PGD attacks, with overall accuracies and robustness scores deteriorating to around 50% or lower as illustrated in Tables V and VI. The specific robustness scores further highlight the challenges:
  - TP robustness score consistently remained below 0.50 across all levels of perturbation.
  - TN robustness score was particularly low, hovering around 0.40, even at lower perturbations.

  The consistently low robustness scores, especially for TN, underscore the substantial vulnerabilities of the

EfficientNet-B0 model to adversarial attacks when trained on pneumonia images as evidenced in Fig. 4 and 5. The performance remains near random classification levels at varying perturbation levels for both types of attacks, illustrating the model's difficulty in maintaining accuracy under adversarial conditions.

TABLE III. EFFICIENTNET-B0 TRAINED ON COVID-19 ATTACKED BY PGD ATTACK

ε	TP	FN	FP	TN	Accuracy
0.01	2213	0	166	936	0.9503
0.05	1130	0	1090	0	0.509
0.1	2631	0	2628	0	0.5003

TABLE IV. EFFICIENTNET-B0 TRAINED ON COVID-19 ATTACKED BY FGSM ATTACK

ε	TP	FN	FP	TN	Accuracy
0.01	2631	0	1095	1533	0.7918
0.05	2631	0	2625	0	0.5006
0.1	2631	0	2628	0	0.5003

TABLE V. EFFICIENTNET-B0 TRAINED ON PNEUMONIA ATTACKED BY PGD ATTACK

ε	TP	FN	FP	TN	Accuracy
0.01	0	2213	73	1029	0.3104
0.05	0	1130	0	1190	0.5129
0.1	0	2631	0	2628	0.4997

TABLE VI. EFFICIENTNET-B0 TRAINED ON PNEUMONIA ATTACKED BY FGSM ATTACK

ε	TP	FN	FP	TN	Accuracy
0.01	0	2443	93	2326	0.4789
0.05	0	2631	0	2625	0.4994
0.1	0	2631	0	2628	0.4997

C. Intra-model Robustness of ResNet50 and FGSM vs. PGD impact

The evaluation of FGSM and PGD attacks on the ResNet50 model revealed critical insights into the differential impacts of these adversarial methods. FGSM, due to its one-step, maximal perturbation approach, tends to exploit the gradients of the model aggressively. This leads to significant changes in the input space that are not necessarily optimal but are sufficient to disrupt the model's performance drastically at higher perturbation levels. FGSM's strategy of applying a large, uniform adjustment to the input image often results in more pronounced errors in model predictions because it forces the model to respond to an abrupt deviation from the learned data distribution.

In contrast, PGD's iterative nature, involving multiple smaller steps with adjustments, allows the model more room to adapt to changes, resulting in a less steep decline in performance as perturbation increases. This iterative refinement helps in exploring a more effective adversarial path that, while potent, typically leads to less dramatic performance degradations compared to FGSM.

IV. DISCUSSION

A. Transferability and Architecture Impact on EfficientNet-B0 vs. ResNet50

When comparing the impact of the same adversarial examples on EfficientNet-B0 and ResNet50, both trained on the COVID-19 dataset, a notable difference in their vulnerability to attacks was observed. Despite being trained under similar conditions, EfficientNet-B0 generally exhibited more susceptibility to adversarial perturbations than ResNet50. Several factors contribute to this observed difference:

- Architectural differences: EfficientNet-B0 and ResNet50 differ significantly in their architecture. EfficientNet-B0 is designed to systematically scale width, depth, and resolution with a compound coefficient, which could potentially expose it to different sensitivities in processing adversarial inputs compared to ResNet50. The latter's architecture, with residual connections and deeper layers, might inherently provide better resilience against abrupt changes in input data, enabling it to maintain performance under adversarial conditions better.

- Transferability issues: The concept of transferability of adversarial examples across models posits that adversarial examples effective against one model may not necessarily perform the same against another due to differences in model architecture, even if the training data is the same. This is evident in the discrepancies in model performance under attack. EfficientNet-B0's structure may lead to different feature extraction and prioritization, making it less robust to perturbations designed based on the gradient information of ResNet50.

- Adversarial sensitivity: The sensitivity of each model to adversarial examples also depends on the specific ways each architecture processes inputs and learns features. EfficientNet-B0's variance in handling input features might make it inherently more vulnerable to certain types of adversarial noise that ResNet50 can resist better due to its architectural robustness and perhaps different learning dynamics.

  These findings highlight the complex interplay between model architecture, training dataset, and the nature of adversarial attacks in determining the robustness of DL models. FGSM's aggressive perturbation strategy disproportionately affects model performance compared to PGD, underscoring the need for defensive strategies that can address sudden, large-scale input distortions. Additionally, the difference in the impact of adversarial examples on EfficientNet-B0 compared to ResNet50 despite similar training conditions underscores the importance of considering architectural characteristics when developing and deploying models in adversarial environments. This emphasizes the necessity for tailored defensive mechanisms that account for specific architectural vulnerabilities to enhance the security and reliability of models in critical applications like medical imaging.

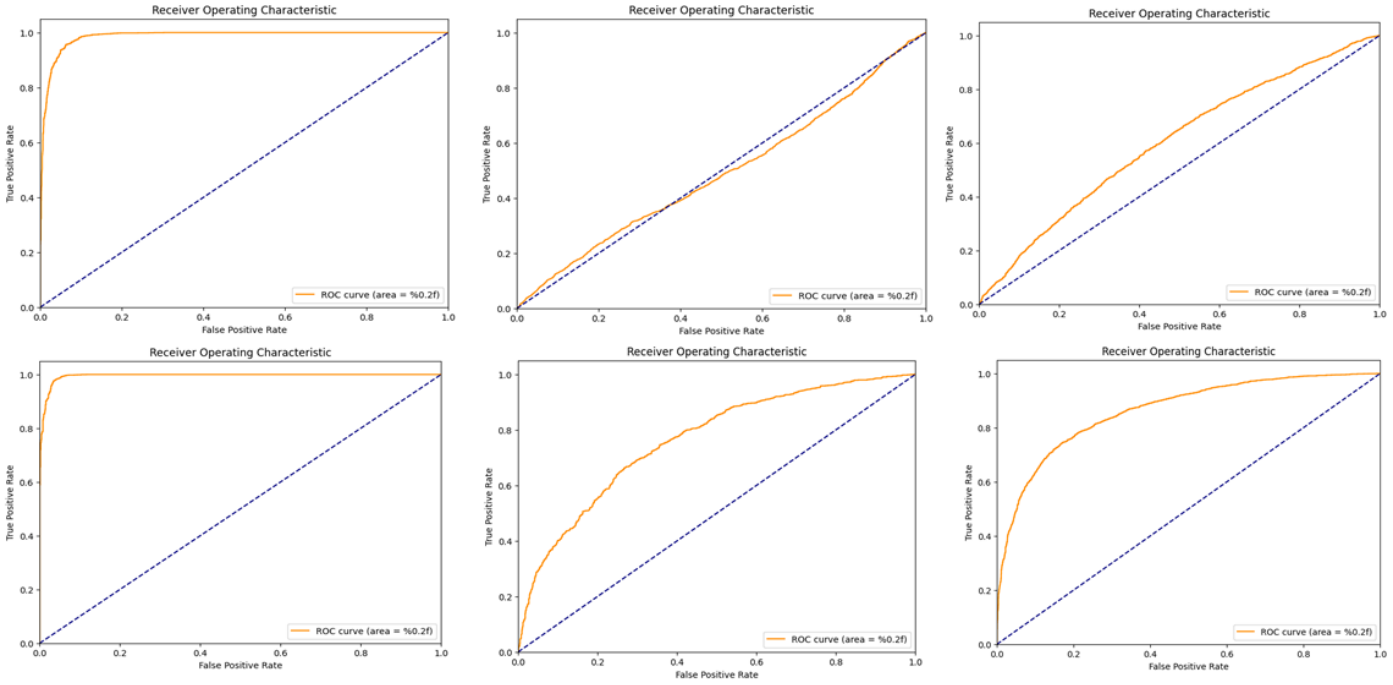


Fig. 4. ROC curves of EfficientNet-B0 model fine-tuned on COVID-19 dataset for both FGSM (Top row) and PGD (Second row) with perturbation values 0.01, 0.05, 0.1 (from left to right).

V. Future Research Directions

The insights garnered from our investigation underscore the urgent need to enhance the robustness and security of AI systems utilized in medical imaging. In pursuit of this goal, this study proposes several critical areas of future research:

- Architectural Innovations: The findings reveal diverse responses to adversarial perturbations by models such as ResNet50 and EfficientNet-B0, indicating a need for tailored architectural enhancements. Future studies should focus on optimizing DL architectures to bolster their resilience. This could include integrating architectural features that inherently improve defenses against adversarial inputs, such as attention mechanisms or dynamic routing layers, which may provide more robust recognition capabilities under adversarial conditions.
- Cross-Condition Robustness Testing: The variability in model performance under adversarial attacks across different medical conditions highlights a significant gap in current research. Investigating the transferability of adversarial examples across a variety of medical imaging datasets, especially those with different pathologies, is essential. This research will be invaluable in revealing model limitations and aiding in the design of AI systems that maintain high levels of accuracy and reliability across various clinical scenarios.
- Real-Time Adversarial Detection and Mitigation: To maintain trust and ensure the reliability of medical AI applications, it is crucial to develop systems capable of detecting and mitigating adversarial attacks in real time. Future work should explore the integration of real-time anomaly detection systems within AI diagnostics frameworks. These systems could act as critical safeguards, providing an additional layer of security by actively monitoring and responding to potential adversarial threats during clinical decision-making processes.

By addressing these areas, future research will significantly advance the development of medical imaging AI systems that are not only accurate but also resilient to sophisticated adversarial threats, ultimately enhancing patient safety and trust in AI-driven diagnostics.

Conclusion

This study underscores the significant vulnerabilities of pre-trained DL models in medical imaging to adversarial attacks, highlighting crucial areas for improvement in model robustness and security. Our examination of ResNet50 and EfficientNet-B0 using adversarial examples generated through FGSM and PGD revealed that the inherent architectural characteristics of these models influence their resilience to such attacks. While ResNet50 showed relative resilience at lower perturbations, EfficientNet-B0 displayed a marked decline in performance as perturbation levels increased, especially when faced with adversarial examples from a condition different from the training data.

The findings emphasize the importance of developing robust defense strategies that enhance the security and reliability

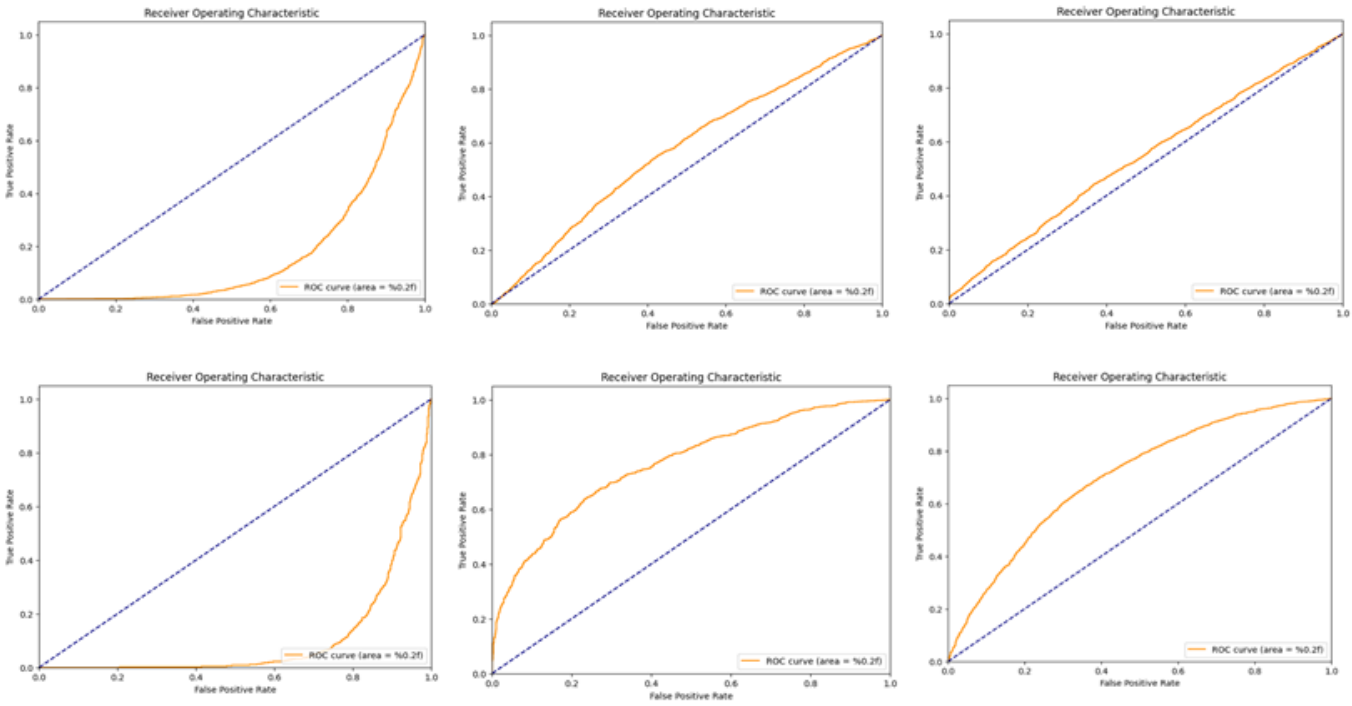


Fig. 5. ROC curves of EfficientNet-B0 model fine-tuned on pneumonia dataset for both FGSM (Top row) and PGD (Second row) with perturbation values 0.01, 0.05, 0.1 (from left to right).

of medical imaging AI systems. Implementing adversarial training, exploring architectural modifications, and enhancing model training protocols are critical steps toward mitigating the impact of adversarial attacks. Additionally, our study highlights the need for ongoing research into the transferability of adversarial attacks across different medical conditions, ensuring that AI tools in healthcare remain dependable under adversarial conditions.

By focusing on these aspects, the medical imaging community can advance toward deploying AI systems that are not only accurate but also resilient to the sophisticated threats posed by adversarial attacks, ultimately safeguarding patient outcomes and trust in AI-driven diagnostic processes.

ACKNOWLEDGMENT

The authors would like to thank The Ministry of Higher Education Malaysia supports this work under the Fundamental Research Grant Scheme, project Code FRGS/1/2020/ICT07/USM/02/2.

REFERENCES

[1] V. Ravi, V. Acharya, and M. Alazab, "A multichannel EfficientNet deep learning-based stacking ensemble approach for lung disease detection using chest X-ray images," *Cluster Comput.*, vol. 26, pp. 1181–1203, 2023. Available: https://link.springer.com/10.1007/s10586-022-03664-6. doi: 10.1007/s10586-022-03664-6.

[2] M. A. Talukder, M. A. Layek, M. Kazi, M. A. Uddin, and S. Aryal, "Empowering COVID-19 detection: Optimizing performance through fine-tuned EfficientNet deep learning architecture," *Computers in Biology and Medicine*, vol. 168, Art. no. 107789, 2024. Available: https://linkinghub.elsevier.com/retrieve/pii/S0010482523012544. doi: 10.1016/j.compbiomed.2023.107789.

[3] M. Nawaz, T. Nazir, J. Baili, M. A. Khan, Y. J. Kim, and J. H. Cha, "CXray-EffDet: Chest disease detection and classification from X-ray images using the EfficientDet model," *Diagnostics*, vol. 13, Art. no. 248, 2023. Available: https://www.mdpi.com/2075-4418/13/2/248. doi: 10.3390/diagnostics13020248.

[4] G. Srivastava, A. Chauhan, M. Jangid, and S. Chaurasia, "CoviXNet: A novel and efficient deep learning model for detection of COVID-19 using chest X-ray images," *Biomedical Signal Processing and Control*, vol. 78, Art. no. 103848, 2022. Available: https://linkinghub.elsevier.com/retrieve/pii/S1746809422003597. doi: 10.1016/j.bspc.2022.103848.

[5] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing properties of neural networks," *arXiv*, 2013. Available: https://arxiv.org/abs/1312.6199. doi: 10.48550/ARXIV.1312.6199.

[6] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," *arXiv*, 2014. Available: https://arxiv.org/abs/1412.6572. doi: 10.48550/ARXIV.1412.6572.

[7] F. Waseda, S. Nishikawa, T.-N. Le, H. H. Nguyen, and I. Echizen, "Closer look at the transferability of adversarial examples: How they fool different models differently," *arXiv*, 2021. Available: https://arxiv.org/abs/2112.14337. doi: 10.48550/ARXIV.2112.14337.

[8] U. Ozbulak, A. Van Messem, and W. De Neve, "Impact of adversarial examples on deep learning models for biomedical image segmentation," in *Proc. Medical Image Computing and Computer Assisted Intervention–MICCAI 2019: 22nd International Conference*, Shenzhen, China, Oct. 13–17, 2019, vol. 2, pp. 300–308. Springer.

[9] I. Bankole-Hameed, A. Parikh, and J. Harguess, "Exploring the effect of adversarial attacks on deep learning architectures for X-ray data," in *Proc. 2022 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, Washington, DC, USA, 2022, pp. 1–9. Available: https://ieeexplore.ieee.org/document/10092220. doi: 10.1109/AIPR57179.2022.10092220.

[10] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," *arXiv*, 2017. Available: https://arxiv.org/abs/1706.06083. doi: 10.48550/ARXIV.1706.06083.

[11] C. Eleftheriadis, A. Symeonidis, and P. Katsaros, "Adversarial robustness improvement for deep neural networks," *Machine Vision and Applications*, vol. 35, no. 3, Art. no. 35, 2024. Available: https://link.springer.com/10.1007/s00138-024-01519-1. doi: 10.1007/s00138-024-01519-1.

[12] X. Ma, L. Jiang, H. Huang, Z. Weng, J. Bailey, and Y.-G. Jiang, "Imbalanced gradients: a subtle cause of overestimated adversarial robustness," *Machine Learning*, vol. 113, no. 5, pp. 2301–2326, 2024. Available: https://link.springer.com/10.1007/s10994-023-06328-7. doi: 10.1007/s10994-023-06328-7.

[13] D. Juodelyte, Y. Lu, A. Jiménez-Sánchez, S. Bottazzi, E. Ferrante, and V. Cheplygina, "Source matters: Source dataset impact on model robustness in medical imaging," *arXiv*, 2024. Available: https://arxiv.org/abs/2403.04484. doi: 10.48550/ARXIV.2403.04484.

[14] O. M. Velarde, C. Lin, S. Eskreis-Winkler, and L. C. Parra, "Robustness of deep networks for mammography: Replication across public datasets," *Journal of Imaging Informatics in Medicine*, vol. 37, no. 2, pp. 536–546, 2024. Available: https://doi.org/10.1007/s10278-023-00943-5. doi: 10.1007/s10278-023-00943-5.

[15] J. Jiang, X. Jiang, L. Xu, Y. Zhang, Y. Zheng, and D. Kong, "Noise-robustness test for ultrasound breast nodule neural network models as medical devices," *Frontiers in Oncology*, vol. 13, 2023. Available: https://doi.org/10.3389/fonc.2023.1177225. doi: 10.3389/fonc.2023.1177225.

[16] Y. Liu, X. Chen, C. Liu, and D. Song, "Delving into transferable adversarial examples and black-box attacks," *arXiv*, 2016. Available: https://arxiv.org/abs/1611.02770. doi: 10.48550/ARXIV.1611.02770.

[17] F. Tramèr, N. Papernot, I. Goodfellow, D. Boneh, and P. McDaniel, "The space of transferable adversarial examples," *arXiv*, 2017. Available: https://arxiv.org/abs/1704.03453. doi: 10.48550/ARXIV.1704.03453.

[18] G. Bortsova et al., "Adversarial attack vulnerability of medical image analysis systems: Unexplored factors," *Medical Image Analysis*, vol. 73, 2021, Art. no. 102141. Available: https://linkinghub.elsevier.com/retrieve/pii/S1361841521001870. doi: 10.1016/j.media.2021.102141.

[19] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, 2016, pp. 770–778.

[20] M. Tan and Q. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," in *Proc. International Conference on Machine Learning*, PMLR, 2019, pp. 6105–6114.

[21] KUMC, "COVID-19 Radiography Database," Kaggle, [Online]. Available: https://www.kaggle.com/datasets/kumcs2004/covid-19-radiography-database

[22] A. Sharma, B. B. Gupta, A. K. Singh, and V. K. Saraswat, "Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 7, pp. 9355–9381, 2023.

[23] V. C. Sharmila, S. Aswin, B. M. Vadivel, and S. Vinutha, "Advanced Persistent Threat Assessment," in *Proc. International Conference on Data & Information Sciences*, Springer, 2023, pp. 383–394.

Image Information Hiding Processing Based on Deep Neural Network Algorithm

Zhe Zhang[1,*]
School of Computer Science and Technology, Nanyang Normal University, Nanyang, Henan, 473061, China[1]

***Abstract*—In order to more effectively hide and extract image information, a deep neural network-based algorithm and computer-aided image information hiding method is proposed. The hardware design of the system includes the selection of the main control chip, the design of the parallel processing structure, and the design of the Ethernet communication circuit; Software design includes an image information hiding module, an image information extraction module, and a carrier image processing module. The operation of the image information processing system based on the reversible information hiding algorithm is realized through the system hardware and software design. The experimental results show that the carrier image processing degree of the design system is much higher than that of the traditional system, and the maximum value can reach 91%, indicating that the carrier image processing performance of the design system is better. The scheme proposed in this paper can improve the security of secret information while ensuring the quality of dense image. Follow-up studies will continue to explore the combination of adversarial learning and various traditional embedding algorithms to further improve the concealment of graph-hiding algorithms.**

Keywords*—Image information hiding; neural networks; system design; image acquisition; information processing

I. INTRODUCTION

With the development of technology, people have entered the era of networking, informatization, and intelligence, and correspondingly, the requirements for various industries are also increasing. Visual information is the most direct carrier of human information, and images are the main manifestation of visual information. Images are an effective description of objective objects, mainly including their texture distribution, morphology, etc. Continuous image sequences also contain information such as the motion characteristics of objects. The combination of these information is an important basis for determining the category of objects. Therefore, image information processing has become an important research direction in the field of information processing today, and many scholars and experts have conducted in-depth research on it and achieved certain results [1-2]. At present, with the continuous improvement of the Internet and chip level, intelligent communication devices have become an important part of people's work and life, and also brought a variety of information security risks, such as personal sensitive information leakage caused by the low security transmission of information. Therefore, the research in the field of information security is of great significance. Information hiding technology is an important component of the field of information security. It mainly embeds secret information into multimedia carriers through information hiding algorithms, and the recipient extracts the secret information from the carrier through extraction algorithms [3]. Due to the insensitivity to modifications and pixel redundancy of images, they are currently widely used as hidden carriers and one of the main research directions.

In recent years, optoelectronic technology and integrated circuits have developed rapidly. Image information processing systems, which use image sensors as information acquisition methods and embedded hardware as acquisition and information processing units, have been widely applied in fields such as agriculture, military, transportation, and industry [4]. Traditional image information processing systems mainly use image sensors to obtain image information. Due to the small field of view angle of the sensors, low resolution, and limited information transmission, the image resolution is reduced, and there is significant distortion, which cannot clearly distinguish the details of the imaging target in the image. The development of network information technology has led to frequent leakage of image information, posing information risks. Traditional image steganography algorithms often rely on manually designed distortion cost functions, which are complex and highly specific. Once features are discovered, they will completely lose their security advantages, resulting in high maintenance costs for traditional image steganography algorithms. The main principle of traditional image steganography algorithms is to calculate the impact of each pixel modification on overall distortion, in order to find the optimal embedding position, reduce the modification of the carrier image by secret information, and achieve the goal of confusing the public [5]. Common methods include statistical histogram steganography and dual communication code steganography. The difference between these two types of algorithms lies in the different ways in which redundant information is filtered. Combined with the visual difference vulnerability of adjacent colors in the same color gamut of the human eye, the modification of the carrier image can be ignored when observed by the human eye. The former achieves steganography by transforming the image pixel matrix into redundant statistics that can be filtered out by histograms in different transformation domains; The latter uses the adjoint error correction code mechanism in reverse to define the encrypted carrier as a disturbed channel. Through the communication code error correction mechanism, the encrypted carrier is corrected back to the original carrier to extract secret messages. However, these schemes all have obvious specificity features. With the increasing maturity of deep learning technology in recent years, the above algorithms have limited ability to resist data-driven deep steganalysis [6].

*Corresponding author

II. LITERATURE REVIEW

Advancements in information technology and hardware have led to remarkable increases in computer processing capabilities. Consequently, deep learning, which heavily relies on substantial computing power, has garnered significant attention in research circles. Convolutional Neural Networks (CNNs) have emerged as a prominent tool in machine vision, yielding impressive achievements and widespread adoption in various applications [7]. Object detection serves as the cornerstone for a multitude of advanced visual tasks, including image semantic segmentation, instance segmentation, image annotation, and video comprehension. Its importance cannot be overstated, as it lays the groundwork for complex visual tasks like image scene recognition and content comprehension. Moreover, it plays a pivotal role in constructing image retrieval systems, facial recognition, object identification, pedestrian detection, video surveillance, and facilitating advancements in autonomous driving technology [8]. Information hiding technology is a method of hiding secret information in multimedia information. Images are the most suitable data carrier for information hiding. The main methods of information hiding include digital watermarking technology, steganography, etc. Information hiding can be divided into lossy information hiding and reversible information hiding techniques, with the difference being whether the receiving end can recover the carrier without distortion. Lossy information hiding technology can be applied to copyright protection scenarios of multimedia data, and the receiver cannot fully recover the carrier after extracting secret data. Reversible information hiding can be applied to the illegal tampering of multimedia data, which can verify its integrity and restore it without loss, such as medical diagnostic information. After extracting secret information at the receiving end, the carrier can be restored without distortion.

Lai et al. proposed method, a generative image steganalysis algorithm is introduced, leveraging a focused feedback residual convolutional neural network. This approach enables the simultaneous detection and extraction of concealed information within images. Initially, a preprocessing network, comprising multiple convolutional layers and two novel focus modules, is employed to preprocess candidate stego images, producing enhanced feature maps. Subsequently, these enhanced feature maps are fed into both the classification network and the reconstruction network [9]. Khan, A. A. and others introduced a steganography technique utilizing the least significant bit (LSB) method to conceal secret data within an original image. Initially, lightweight stream encryption cryptography encrypts the confidential information within the cover image, safeguarding it throughout transmission from source to destination. The encrypted cover data is then embedded into the carrier of the steganographic image, employing the LSB technique for transmission [10]. Jun, M. et al. introduced an innovative dual-stream convolutional neural network tailored for single image dehazing. This network architecture comprises two distinct flows: the spatial information feature flow and the high-level semantic feature flow. The spatial information feature flow focuses on retaining intricate details within the dehazed image, while the high-level semantic feature flow specializes in extracting multi-scale structural features from the dehazed image [11].

Image encryption and information hiding are research directions for protecting information security. Cryptography ensures the security of data content through encryption. Information hiding technology verifies the integrity of multimedia data by embedding secret data. The reversible information hiding of encrypted images can play a dual role in ensuring information security during data processing. Encryption protects the content of image data, while embedded secret data can monitor whether multimedia data has been tampered with during transmission after decryption, verify its integrity, and achieve lossless recovery of the original carrier. It can be applied in scenarios such as remote medical diagnosis, encrypted data annotation in cloud environments, and digital forensics in the judiciary. In order to solve the problems existing in traditional systems, the author designs a reversible image information hiding system, applies reversible information hiding algorithms to image information processing systems, improves image processing speed and transmission speed, and ensures the security of image information processing.

III. METHOD

A. Hardware Design of Image Information Processing System

The system hardware mainly includes the selection of the main control chip, the design of parallel processing structure, and the design of Ethernet communication circuit. The specific design process is as follows:

1) Selection of main control chip: The main control chip adopts an FPGA chip, which is the core of image information processing and has the advantages of fast processing speed, simple operation structure, and large amount of data involved. The performance of the FPGA chip determines the effectiveness of image information processing. After research and comparison, it was found that the XC5VLX110T chip produced by Xilix Company was chosen. The XC5VLX110T chip has 110000 equivalent logic units, 16 transceivers, 64 DSP48E logic chips, 5328Kb ARM, and six clocks [12].

2) Parallel processing architecture design: Parallel processing is mainly implemented by buses, therefore, the design of parallel processing architecture mainly involves designing bus interfaces. The system bus interface connection diagram is shown in Fig. 1.

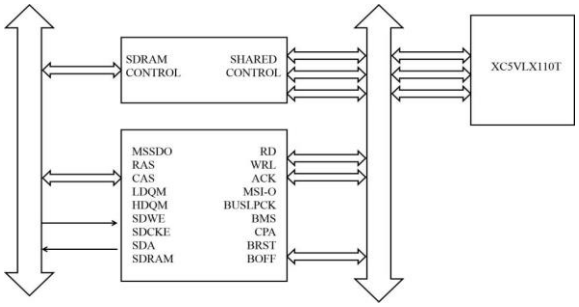


Fig. 1. Bus interface connection diagram.

The bus interface has multiple pins, as defined in Table I.

TABLE I. DEFINITION OF BUS PINS

grouping	types	Describe
External port bus control	I/O	Burst
	O	Host space chip selection signal
	O	Memory selection
	I/O	Response
External port arbitration	I	Revoke
	O	Bus lock indication
	I/O	Kernel Access Priority
	I	Host bus grant
External port DMA/Flyby	I	DMA request pin
	O	I/O read
	O	I/O device output enable
	O	I/O write

3) Ethernet communication circuit design: The image information processing system requires good network communication support. In order to design an Ethernet communication circuit, the independent interface of the processor needs to be connected to the Ethernet transceiver, and the IEEE802.3 network transmission protocol needs to be set. The circuit should be set to work mode to ensure the normal operation of the image information processing system.

The design diagram of the Ethernet communication circuit is shown in Fig. 2.

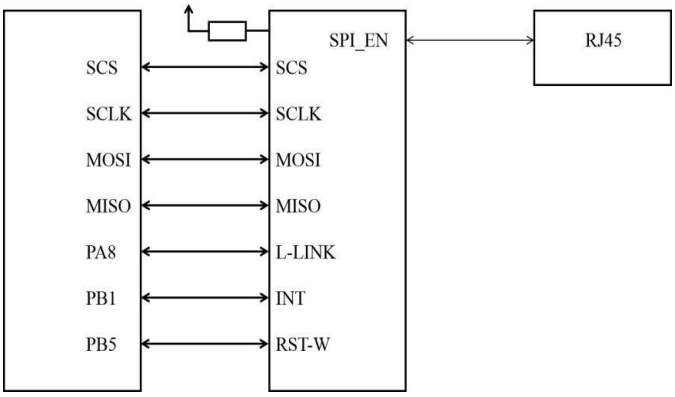


Fig. 2. Ethernet communication circuit design diagram.

The above process has completed the design of the system hardware, providing hardware support for the following system software design.

B. Software Design of Image Information Processing System

The system software mainly includes an image information hiding module, an image information extraction module, and a carrier image processing module. The specific design process is as follows:

1) Image information hiding module: The image information hiding module mainly uses reversible information hiding algorithms to hide image information, achieving the goal of protecting image information. Firstly, the carrier image is divided into non overlapping blocks, with a block size of 2 × 2. Secondly, each image block is processed sequentially, paying attention to hiding image information. The specific steps for hiding image information are as follows:

Step 1: Generate a reference matrix of 256 x 256 based on n x n matrix blocks, with n optional values including 4, 8, 16, and 32.

Step 2: The image block mainly consists of 4 pixels, denoted as $C(i,j)$, $C(i,j+1)$, $C(i+1,j)$, and $C(i+1,j+1)$. Construct them into three pixel pairs and convert them into planar coordinate points, denoted as $P_1(C(i,j),\ C(i,j+1))$, $P_2(C(i,j),\ C(i+1,j))$, and $P_3(C(i,j),\ C(i+1,j+1))$. Among them: $C(i,j)$ represents the pixels of the carrier image; $C(i,j+1)$, $C(i+1,j)$, and $C(i+1,j+1)$ represent the pixels obtained by interpolation calculation.

Step 3: Convert the reference matrix into a planar region, map P_1, P_2, and P_3 to the reference matrix, and find the corresponding coordinate positions.

Step 4: Scan in the left and right directions with P_1 as the center in the reference matrix. Form a pixel group G with n scanned pixels, convert their information into hidden information using decimal, find the corresponding position in G, replace the vertical coordinate of P_1 point, and complete the information hiding of P_1 point.

Step 5: Process P_2 and P_3 information according to the method in Step 4, and complete the hiding of P_2 and P_3 information.

Step 6: Repeat steps 2 to 5 until all image information is hidden.

2) Image information extraction module: Based on the hidden images mentioned above, embed a decoding program to extract image information. The specific process is shown below.

The decoding program refers to the decoding algorithm of reversible information hiding algorithms, which converts hidden information into raw information and extracts it [13-14]. Under normal circumstances, only personnel with image ownership rights can have decoding programs, and outsiders cannot extract image information. This can greatly ensure the security of image information and avoid the harm caused by image information leakage. The decoding key is mainly represented by k_1 and k_2, and the image information extraction process is shown in Fig. 3.

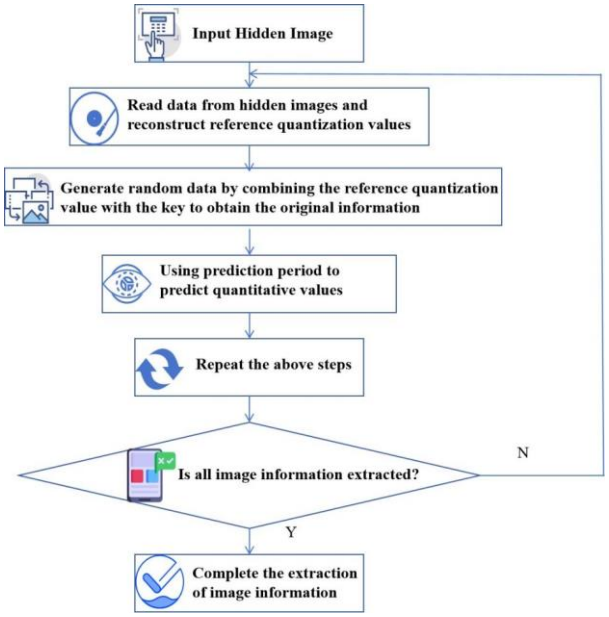


Fig. 3. Image information extraction process diagram.

3) Carrier image processing module: After extracting image information, it is necessary to process the carrier image, which is the inverse process of image information hiding. The specific program is shown in Fig. 4.

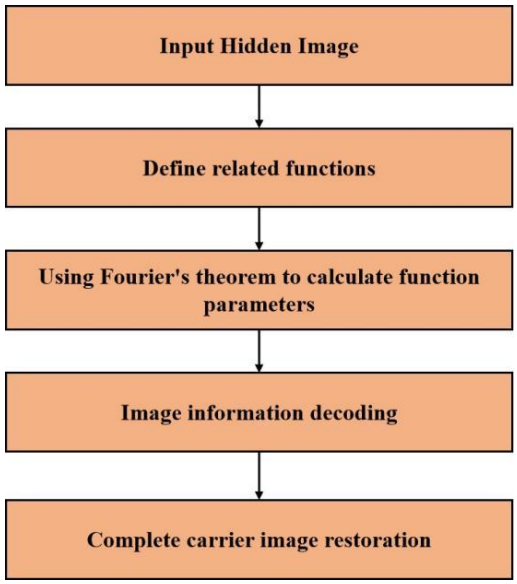


Fig. 4. Carrier image processing program diagram.

The carrier image processing function is represented as:

$$H = \sum_{i=1}^{n} \alpha k_1 * \beta k_2 \quad (1)$$

In the formula α, β represents the carrier image processing parameters.

Through the design of the hardware and software of the above system, the operation of an image information processing system based on reversible information hiding algorithm has been achieved, providing more effective support for image information security.

C. Similarity of Semantic Information

By applying probability functions to analyze the similarity of semantic information between images, propose image and semantic sets for a given query image.

The representation method for image sets:

$$I = \{I_1, \ I_2, \ \cdots I_n\} \quad (2)$$

The representation method of semantic sets:

$$X = \{x_1, \ x_2, \ \cdots x_m\} \quad (3)$$

Based on the given set expansion analysis, when the image I_i has semantic x_j, it can be represented by $x_j(I_i) \in \{0, \ 1\}$. In order to further clarify the similarity between the two images, it is necessary to measure the distance between the indicator functions. There is a relationship where the decrease in this value leads to an increase in similarity. The categories of natural semantic information are diverse and have significant uncertainty, so even with the same semantics, there may be multiple categories. Considering this situation, a probability based semantic level information similarity method is adopted. Assuming that I_i has semantic x_j, it is represented by $p = (x_j(I_i) = 1|I_i)$. This can further clarify the semantic labels of the image, specifically:

$$x_j: \ max_{x_j} p = (x_j(I_i) = 1|I_i) \quad (4)$$

The query image I_q maintains a relatively independent relationship with the dataset image I_i. Under this condition, there is $p = (I_q, \ I_i|x_j) = p(I_q|x_j)(I_i|x_j)$. Based on the image I_q and I_i, the correlation features of the image can be obtained through joint probability, which can be expressed as follows:

$$p = (I_q I_i) = \sum_{x_j \in X} p(I_q, \ I_i|x_j) = \sum_{x_j \in X} p(I_q|x_j)\, p(I_i|x_j) p(x_j) \quad (5)$$

In addition, considering the development needs of scalability, a matrix $\Lambda = I \times X$ is introduced to conduct calculations and analysis, exploring the correlation between two images. If the joint distribution of the images exceeds the cutoff threshold t, it is reasonable to indicate that there is correlation between the two images:

$$\Lambda = (I_q I_i) = p(I_q I_i) \geq t \quad (6)$$

On the contrary, it indicates that the two are not related. By applying the probability function of semantics between images, it is possible to effectively determine the semantic correlation of images. If the threshold is exceeded, it indicates significant semantic correlation, otherwise there is no significant correlation [15].

D. System Implementation Process

Write a reversible image information hiding system using callable functions to achieve image information hiding processing. The image information hiding system based on reversibility uses FIFO memory to collect image information, applies grayscale stretching processing to the image, threshold segmentation processing to the image after stretching processing, and uses ARM processor to hide image

information through reversible information hiding algorithm. After reverse operation, the hidden image information is extracted and output to achieve image information processing in the image information processing system [16].

E. Data Communication Module

The image data transmission is achieved through a data communication module, which can achieve multi chip communication. The data communication of the image information processing system is achieved through Ethernet data transmission interface and high-speed serial interface. The data communication module utilizes PCI interface to achieve information exchange between the image information processing system and the computer. The PCI interface is the data exchange and control center of the system hardware, which receives commands and data from the image information processing system and various device drivers through the communication interface module. The communication interface module completes the coordination work of various modules in the system, achieving system image information processing. The PCI communication interface module sends the collected image information and system processed data to a general-purpose PC using the PCI bus, and selects PLX's PCI9030 as the interface chip of the communication data module [17].

IV. Results and Discussion

A. Experimental Analysis

The experiment mainly uses Ethernet communication, and in order to ensure the smooth progress of the experiment, the experimental network is tested. After testing, the changes in Ethernet traffic are shown in Fig. 5. The significant changes in traffic indicate that Ethernet communication is normal and effective.

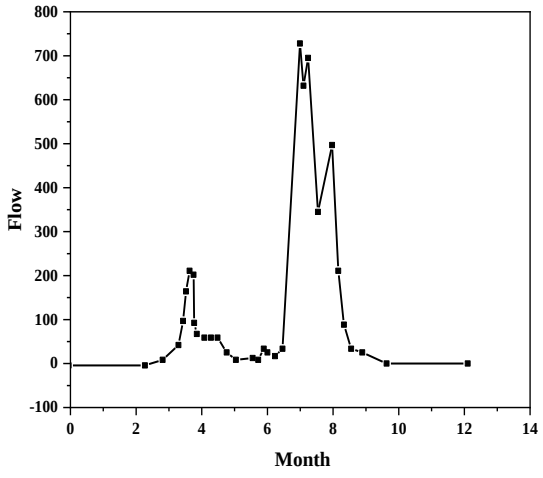


Fig. 5. Changes in Ethernet traffic.

B. Analysis of Experimental Results

The comparison of carrier image processing levels obtained through experiments is shown in Table II.

TABLE II. Comparison of Carrier Image Processing Levels %

Number of experiments	Traditional systems	design system
10	45	66
20	40	68
30	41	67
40	39	70
50	50	72
60	50	73
70	53	76
80	50	78
90	39	88
100	41	91

As shown in Table II, the carrier image processing level of the designed system is much higher than that of traditional systems, with a maximum value of 91%, indicating that the carrier image processing performance of the designed system is better [18]. The experimental results show that compared with traditional image information processing systems, the image information processing system designed by the author greatly improves the processing performance of carrier images, fully demonstrating that the designed image information processing system has better processing effects.

V. Conclusion

The author proposes an image information hiding processing based on deep neural network algorithms. Image information processing is an extremely important part of the field of image processing. The proposed solution can improve the security of secret information while ensuring the quality of encrypted images. Design a reversible image information hiding system and apply the reversible information hiding algorithm to the image information processing system. Through experimental results, it has been verified that using this system to process image information can achieve high image information processing efficiency at a lower cost, and has good processing performance, which can be applied to practical processing requirements of different types of image information.

References

[1] Liu X .Analysis on the Development of Cigarette Packaging in the Era of Intelligence[J]. Electronic Research and Applications, 2023, 7(3):1-6.

[2] Ballesteros, M. , & Garro, G. . (2022). A model and a numerical scheme for the description of distribution and abundance of individuals. Journal of Mathematical Biology, 85(4), 1-37.

[3] FengXU, XiaopengYANG, & YiZHAO. (2022). Beamspace mimo radar tensor modeling and 2-d doa estimation. Journal of Signal Processing, 38(1), 1-8.

[4] Liu, D. , Chen, N. , Song, Y. , Song, X. , Sun, J. , & Tan, C. , et al. (2023). Mechanical and heat transfer properties of aln/cu joints based on nanosecond laser-induced metallization. Journal of the European Ceramic Society, 43(5), 1897-1903.

[5] Zhou, L. , Zhigao, L. U. , You, W. , & Fang, X. . (2023). Reversible data hiding using a transformer predictor and an adaptive embedding

strategy. Frontiers of Information Technology & Electronic Engineering, 24(8), 1143-1155.

[6] Zhang, Q. , Jiang, N. , Zhang, Y. , Li, A. , Xiong, H. , & Hu, G. , et al. (2024). On-chip spiking neural networks based on add-drop ring microresonators and electrically reconfigurable phase-change material photonic switches. Photonics Research, 12(4), 755.

[7] LI Shanhai, WU Yanxiong, WANG Bei, XU Yan, & LIU Yulong. (2022). Prediction of enterprise growth in information technology listed campanies based on ga-bp network. Journal of Systems Science and Mathematical Sciences, 42(4), 854-866.

[8] Gupta, S. , & Garg, N. K. . (2023). Data hiding in the optimal keyframes using circular shifting and mutation operations for improvement in imperceptibility. International Journal of Information and Computer Security, 20(1/2), 158.

[9] Lai, Z. , Zhu, X. , & Wu, J. . (2022). Generative focused feedback residual networks for image steganalysis and hidden information reconstruction. Applied Soft Computing, 39(1), 14-27.

[10] Khan, A. A. , Shaikh, A. A. , Cheikhrouhou, O. , Laghari, A. A. , Rashid, M. , & Shafiq, M. , et al. (2022). Img-forensics: multimedia-enabled information hiding investigation using convolutional neural network. IET image processing,13(11), 3543-3554.

[11] Jun, M. , Yuanyuan, L. , Huahua, L. , & You, M. . (2022). Single-image dehazing based on two-stream convolutional neural network. Journal of Artificial Intelligence Technology (English), 82(3), 3459-3484.

[12] Sahin, M. E. . (2023). Image processing and machine learning-based bone fracture detection and classification using x-ray images. International Journal of Imaging Systems and Technology, 33(3), 853-865.

[13] Nagai, S. , & Tomioka, A. . (2022). Information needs of adolescent with cancer who returning to social life. Journal of AYA Oncology Alliance, 2(1), 8-15.

[14] Guy, T. S. , & Edwards, K. . (2022). Military-civilian cardiothoracic surgery affiliations: a potential solution for low clinical volume in military medical facilities. The Annals of thoracic surgery, 114(3), 625.

[15] Jayasekara, S. , Karunasekera, S. , & Harwood, A. . (2022). Optimizing checkpoint-based fault-tolerance in distributed stream processing systems: theory to practice. Software: Practice and Experience, 52(1), 296-315.

[16] Lilian, H. , Yi, S. , Jianhong, X. , & Linyu, W. . (2022). Image encryption based on a novel memristive chaotic system,grain-128a algorithm and dynamic pixel masking. Systems Engineering and Electronic Technology: English Version, 33(3), 17.

[17] Gao, Z. , Deng, Z. , Zhang, L. , Gao, X. , An, Y. , & Wang, A. , et al. (2024). 10 gb/s classical secure key distribution based on temporal steganography and private chaotic phase scrambling. Photonics Research, 12(2), 321.

[18] Rahman, Z. , Yi, X. , Billah, M. , Sumi, M. , & Anwar, A. . (2022). Enhancing aes using chaos and logistic map-based key generation technique for securing iot-based smart home. Electronics, 11(7), 1083.

Intelligent Digital Virtual Clothing Display System Based on LDA Mathematical Model

Zhao Wu*[1], Qingyuan He[2]
Fashion Design and Technology, Wuhan College of Foreign Languages and Foreign Affairs, Wuhan, Hubei, 430083, China[1, 2]

***Abstract*—In order to understand the intelligent digital virtual clothing display system based on mathematical models, the author proposes a research on an intelligent digital virtual clothing display system based on LDA mathematical models. The author first analyzes the realization of clothing matching function, and selects the cooperation between human skin color and clothing field as the influencing factors of clothing color matching and style matching based on expert knowledge and historical experience. Secondly, based on the different characteristics of different skin tones and the knowledge of clothing color matching, a set of clothing matching recommendation plans is presented to recommend suitable colors for users to refer to. Additionally, clothing style recommendations and choices are set, divided into upper and lower clothing, allowing users to choose more independently, the system itself also provides certain reference matching knowledge. Finally, the clothing matching rules were converted into computer image data, through analysis of the current market and existing research results, it was decided to implement a clothing matching display system based on VR technology, while providing recommended clothing matching solutions, a three-dimensional space was constructed to display clothing, allowing users to watch the effects of clothing matching according to their own choices, provide a new way for users in the clothing industry who have this demand.**

Keywords*—Mathematical model; virtual technology; clothing display

I. Introduction

With the continuous and rapid development of society, meeting people's daily clothing needs is becoming increasingly important. Clothing matching not only refers to the matching of clothes themselves, but also needs to be selected based on the appearance characteristics of the wearer. It is also necessary to consider the occasion of the wearer to match different clothes, in order to provide suggestions for clothing matching. The matching effect of clothing is a Visualization display. Under the fashion trend of clothing fashion from top to bottom, the four major international fashion weeks are a very important platform, which can gather the eyes of manufacturers, consumers and suppliers to display clothing with seasonal fashion trends and drive the economic development of the clothing industry. However, due to the significant amount of time, space, money, and energy consumed in hosting it once, there are many difficulties and limitations.

The rapid development of multimedia technology and computer science technology has provided excellent technical support for the practical application of virtual fitting. The mature application of virtual reality technology in many fields has prompted more researchers to conduct research on this technology. At present, virtual reality technology has been applied in all aspects of the social economy and has strong expressive power and realism. Clothing matching is an important way of expressing culture and art, with a strong artistic atmosphere and a combination of innovative matching and cultural connotations. This study analyzed the digital display design of a clothing matching display platform, and used virtual reality technology to complete the design of the virtual clothing display platform scene. Its interactive function can also be completed using the Unity3D engine. The main value of this research achievement lies in using virtual reality technology and clothing display platforms as carriers to demonstrate different ways of clothing matching. Applying virtual reality technology to the display of new clothing styles can reflect stronger interactivity and fun, and also enable users to better understand and match clothing. At present, with the rapid development of virtual reality technology, research and development work based on user actual needs is also constantly deepening. Starting from the current development status of the clothing industry, how to integrate virtual reality technology with modern clothing trends has become a focus of attention [1-2].

II. Literature Review

The LDA model (Latent Dirichlet Allocation, LDA) is essentially a Bag-of-words model, it believes that a document is composed of a group of words, and there is no sequential relationship between words. The LDA model presents the themes of each document in the document set in the form of a general distribution. After analyzing some documents and extracting their themes (distribution), topic clustering or text classification can be performed based on the topic distribution. At present, the application of LDA model is very extensive, and the specific value of LDA model has been realized in multiple domain modules. In 2022, scholars Zhang, X. D. F., and others proposed an SS-LDA model for short text analysis [3]. In the field of clothing matching, Tian, F. et al. used LDA models to analyze virtual clothing display systems and combined them with SVM algorithms to obtain color designs for clothing matching [4].

Virtual Reality (VR) is a major branch of computer simulation, which refers to the formation of a three-dimensional virtual world through computer simulation. It can simulate people's senses such as sight, hearing, and touch, allowing them to see content in the three-dimensional real space more accurately and without obstacles. The images displayed by virtual reality technology have a strong sense of

*Corresponding author: Zhao Wu

authenticity and immersion, which can make people immersive. The practical application of virtual reality technology needs to go through three stages: The first stage is the three-dimensional digital simulation process, which presents the content that can be represented by VR in the form of digital simulation, which is also more realistic; The second stage is the interaction between humans and the environment through writing script programs; The third stage is to integrate the first two processes, and finally create a comprehensive virtual reality environment to complete the interactive experience. The tools and software used can be roughly divided into three types:（1) The typical development method of scenario modeling software is 3DStudio Max; (2) The typical development mode of Model figure management software is Zbrush; (3) The typical development method of script development management software is the Unity3D engine, which is mainly designed and programmed in C language. The data is stored in Extensible Markup Language (XML) documents [5-6].

The author mainly analyzes the virtual fitting mechanism based on virtual reality technology, the network clothing display technology based on object Panorama, the design and implementation of clothing display system, and finally establishes a more complete virtual VR clothing display system.

III. METHODS

A. Virtual Fitting Function

Adopting a case-driven virtual fitting mechanism, using case-based reasoning to obtain clothing display cases that best match the user's physical characteristics and personalized display of clothing. First, define the characteristic parameters of people and clothing, and then collect clothing cases and form a case database. After inputting the user's body shape characteristic parameters, retrieve the clothing display cases that best match the user's body shape characteristics through the case reasoning mechanism in the case database, and obtain personalized clothing display effects that match the user's body shape characteristics. Regarding case search, searches for the closest case (the clothing display instance that best fits the user's body shape) by calculating similarity, and designs an instance retrieval algorithm based on similarity calculation. The calculation steps mainly consist of two parts: parameter weight calculation and similarity calculation.

In the process of image matching and image search, the virtual fitting mechanism has shown good adaptability. Compared with global characteristics, local characteristics do not have close connections, therefore, even if there are defects in the graphics, it will not have a negative impact on the coordination between other features. Analysis and research on local feature extraction algorithms have shown that they exhibit strong robustness and can effectively eliminate the possibility of partial interference, enabling the smooth completion of feature extraction work. In terms of the current situation where images can be locally obtained, even if the scale remains unchanged, the use of feature transformation algorithms is still relatively common. In terms of rotation interference, brightness interference, light noise influence, and other aspects, its robustness is also high. In addition, the advantages of high efficiency and scalability are also evident. The calculation process of body shape parameters is shown in Fig. 1 [7-8].

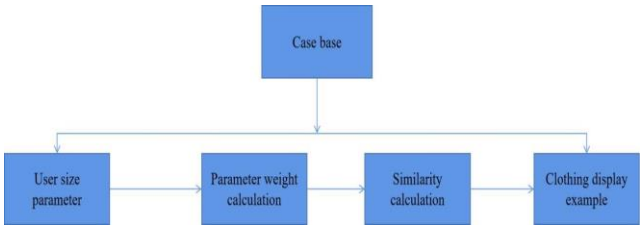


Fig. 1. Calculation of body shape parameters.

B. Panorama Display

In order to meet the new demand for clothing presentation in the clothing matching platform and according to the defects in the current virtual reality clothing presentation methods, the author selects the clothing presentation method based on the object Panorama, and the general process is as follows: Firstly, complete the image collection, secondly, splice the collected images, and finally use virtual reality technology to present the overall effect of the clothing. This process needs to input human organ data first, establish a basic Model figure, and then establish a complete set of Mannequin according to the human characteristics of different age groups (such as children, women, and the elderly), and carry out clothing matching in the virtual reality platform to show the clothing matching characteristics of different types of people. This clothing display method has the advantages of real-time and interactivity, allowing viewers to naturally and dynamically observe the overall display effect of clothing from various angles, making consumers more confident in choosing clothing and enhancing their shopping desire. The image display process is shown in Fig. 2.

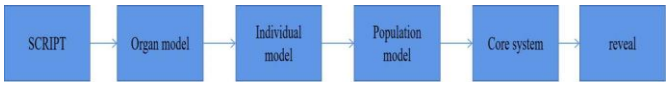


Fig. 2. Image display process.

In the process of detecting image signals of clothing and presenting their characteristics, the application range of global feature extraction calculation is large, and the main characteristics can be divided into three types: One of them is the appearance characteristics, which is to extract the external contour shape of the clothing and determine its style characteristics. For example, through convolution calculation, the target contour shape can be obtained. Then, the initial shape is processed to eliminate the influence parts outside the target contour shape line, and a feature matrix can be obtained. Finally, the target graphic area is effectively extracted. The second is the surface texture characteristics, which extract various textures that appear on the surface of clothing images to determine the fabric characteristics. The third is color characteristics, which use color information to achieve identification purposes. When expressing color characteristics, color histograms are an effective way. After defining commonly used color spaces, calculate each pixel in the clothing image to form a correct understanding of color distribution, and have outstanding advantages in robustness [9-10].

IV. Experiments and Analysis

A. Clothing Matching Scheme Display Design

1) Analysis of clothing matching factors: The author chooses to analyze and organize the knowledge based on traditional clothing matching expert knowledge and historical experience, and obtain corresponding clothing matching rules for the clothing matching recommendation scheme in the system. The clothing matching recommendations formed through expert knowledge have strong professionalism and are easy to use. The VR system is not limited by time and space, allowing users to apply clothing matching knowledge from a more intuitive perspective and see the display effect after matching. Experts recommend personalized clothing by analyzing the user's own skin color, hair color, pupil color, and other physical signs to find the most suitable color range for clothing. Then, according to different body shapes, choose the appropriate clothing outline shape, and judge the clothing style based on the environment. This determines the main color and fabric selection, and finally matches the entire set of clothing. After in-depth analysis, it is found that in order to achieve a beautiful and appropriate effect in clothing, it is necessary to consider three factors: the wearer's own physical characteristics, environment, and matching rules.

The characteristic of the virtual scene and display model designed in this system is that there is no difference in time and space in the virtual scene, and there is no consideration of time and place factors; the female human body modeled through Maya is a thin body with a standard Y-shape, with black hair and pupil colors. Therefore, the appearance of the above factors cannot be changed, so only the skin color of the human body is considered in this system. And considering that there are many and complex details involved in clothing matching, the principle of "minimum system" will be adopted in the clothing matching rules to reduce some details and focus on analyzing and exploring the selection factors.

Based on the analysis and consideration of various factors mentioned above, when designing clothing matching rules, the author chooses skin color in individual characteristics and the clothing occasions in TPO dressing rules as factors that affect clothing matching. Clothing is no longer a separate individual, and users' needs and characteristics are reflected in the attributes of clothing products. Skin color and dressing occasion are the influencing factors of clothing color, while dressing occasion is the influencing factor of clothing style, according to the application of matching rules, the color and style of clothing are influenced by skin color and the occasion in which the clothing is worn, thus obtaining a complete display rule for clothing matching [11-12] as shown in Fig. 3.

Fig. 3. Relationship between clothing factors.

2) Analysis of human skin color factors: Due to differences in innate skin color genes, living environment, and daily sun protection, adults have various skin types. Some have snow-white skin tones, while others have dark and yellowish skin tones. These differences can lead to different visual effects when choosing clothing of the same color. This is whether traditional clothing is suitable for one's temperament. Through the classification of different skin colors, the characteristics of their skin colors are analyzed, and the clothing color matching methods suitable for different skin colors are obtained to make the matching reasonable, highlight the advantages of human skin color, improve the bad skin color, and bring good mental outlook.

The author uses the skin color classification method of the twelve season color theory, in which the human skin color is divided into twelve types: Light spring, warm spring, pure spring, light summer, soft summer, cold summer, warm autumn, soft autumn, deep autumn, pure winter, cold winter, and deep winter. According to the spring, summer, autumn, and winter seasons, it is divided into four modules to elaborate on different skin color characteristics [13-14]. Spring is a season of recovery and vitality for all things. The colors of spring are warm, soft and light, giving people a soft and comfortable feeling. The overall skin color of the spring type is soft, as shown in Table I, summarizing the three skin color characteristics of the spring type.

TABLE I. Classification Characteristics of Spring Skin Tone

Skin color name	characteristic
Light spring type	With a clear skin tone and a hint of cream
Pure spring type	Skin tone that leans towards natural tones, mostly with light ivory skin tone
Warm Spring Type	The skin is relatively thin and transparent, with a darker warm tone compared to the light spring type

Summer brings with it the feeling of vibrant pink lotus growth under the white sunlight. So the overall skin tone of the summer style is a medium brightness skin tone with a pink tone. Table II analyzes the different characteristics of summer skin tone, which can better grasp skin tone.

TABLE II. CLASSIFICATION CHARACTERISTICS OF SUMMER SKIN TONE

Skin color name	Characteristic
Light summer type	A pink and tender skin with a light pink tone, compared to other summer styles, its brightness is lower
Soft summer type	Medium to light skin tone, with a rose pink complexion with a hint of gray tone
Cold summer type	A clear waxy yellow or rose pink color indicates a low purity cyan tone in the skin tone

Autumn is the season of falling leaves, so the main color tone of the autumn type skin is yellow, and the overall skin texture is not clear and transparent, with a slight sense of heaviness. Table III provides a brief description of the skin color characteristics of the autumn type.

TABLE III. CLASSIFICATION CHARACTERISTICS OF AUTUMN SKIN TONE

Skin color name	Characteristic
Soft autumn type	The face is light yellow, and the skin color is textured, not clear and transparent
Warm Autumn Type	With a golden tone, it is a yellow skin with high brightness
Late autumn type	The deep orange color of yellow is darker and lower in purity in late autumn compared to warm autumn

The color sensation brought by winter is a cool and harsh winter with cold white as the main tone, and the overall characteristic of winter skin tone is a bias towards cyan skin tone. Table IV provides a description of the characteristics of winter skin tone.

TABLE IV. CLASSIFICATION CHARACTERISTICS OF WINTER SKIN TONE

Skin color name	Characteristic
Net winter type	With a green background tone, a pale and light turquoise complexion, the overall color of the skin is white in tone
Frozen type	The skin tone ranges from cyan white to turquoise brown, but overall the skin tone has a higher brightness and is brighter
Deep winter type	Dark yellow skin with lighter purity ranging from dark wheat to turquoise brown

B. Analysis of Dressing Occasion Factors

In the TPO matching rule, it is required that when choosing clothing and considering its specific style, people should ensure that the clothing and its specific style are coordinated and consistent with the time, place, and occasion of the clothing, producing a harmonious and matching effect. In social life, according to the different Role people play, when going in and out on different occasions, the user's clothing reflects the wearer's purpose expectations, different clothing will leave different impressions on others, and clothing styles and colors play a certain role in expressing the user's clothing purpose.

Based on the analysis of the significant characteristics and purposes of different dressing occasions in real life, it is decided to divide their dressing occasions into five scenarios for further analysis and exploration:

- Leisure occasions: Places where leisure activities can take place, such as entertainment, shopping, and home activities. In these occasions, people are in a relaxed state, pursuing freedom, comfort, convenience, and an unrestrained state [15-16].
- Sports occasions: The awareness of national sports to strengthen the body is strengthened. More and more people choose to carry out sports activities in the gym or outdoor sports venues. According to different sports methods, different clothes are selected to match sports, so that clothing can play an auxiliary role and bring comfort to the wearer.
- Workplace: Work is a social occasion that occupies a significant portion of people's daily lives. Wearing classic and formal clothing can leave a good impression on the wearer.
- Banquet Occasion: In banquets and other occasions, people often dress with a purpose in mind, and the appearance of the clothing represents a spiritual outlook that the wearer wants to showcase. Wearing bright and luxurious clothing is the first choice for gatherings.
- Resort: The resort itself indicates that people are happy and comfortable in this occasion, without any constraints. The main design concept is strong, showcasing the beautiful and generous state of the wearer.

1) Color matching rules: By combining colors, better visual effects can be achieved. The rational use of color matching rules can be applied to clothing matching to achieve harmonious effects. Colors can be divided into two categories: Colored and achromatic. Achromatic refers to neutral colors, which are commonly referred to as black, white, and gray; Colorfulness is composed of three major attributes of color: Hue, brightness, and purity, among which brightness and purity together constitute hue.

According to the three attributes of colors, hue refers to the appearance of different colors, composed of three primary colors: Red, yellow, and blue. It is divided by the wavelength of light. In daily life, the most common basic colors are "red, orange, yellow, green, blue, and purple".

C. Clothing Color Matching Design

Clothing color can give the most intuitive visual impression in the overall combination of clothing. By combining users' skin color choices and the occasion of

clothing wearing, using reasonable color combinations can fully demonstrate personalized clothing style and taste. In clothing matching, fully grasp the purity, brightness, and hue attributes of colors, cleverly blend and match colors to display good visual effects [17].

1) Clothing style matching design: The style of clothing refers to the style and shape of clothing, which is generally divided into upper and lower clothing for separate matching. In the classification of upper clothing, there are T-shirts, vests, shirts, pullovers, suits, jackets, vests, polo shirts, etc, in the classification of bottoms, there are pants, casual pants, straight pants, cropped pants, shorts, short skirts, long skirts, one step skirts, pleated skirts, puffy skirts, and so on. Different clothing styles bring different visual experiences to people.

According to the style characteristics and overall shape effect of the clothing style, when the clothing is suitable for the atmosphere of the occasion, it is considered as the suitable style type for wearing in the occasion.

The combination of upper and lower clothing styles can generate a variety of matching styles. Combining the visual effect of the outer contour of clothing styles, by analyzing the main clothing occasions in daily life, Table V recommends two sets of clothing styles for each of the five selected clothing occasions.

TABLE V. RECOMMENDED STYLES FOR DIFFERENT DRESSING OCCASIONS

Dressing occasions	Style Recommendation	Main Features
leisure time	T-shirt, jeans, jacket, wide leg pants	The style is loose and comfortable, with a simple design that does not emphasize the waistline
motion	Vest, Leggings, sports sweater, culottes	Lightweight and vibrant, with a variety of close fitting styles to protect the body
work	Suit set, shirt, one step skirt	Formal, classic cut, smooth lines, and streamlined styling
banquet	Fish tail dress, short dress	Lightweight and elegant, with strong characteristics and personality, the style and style are exaggerated, highlighting the figure
spend one's holidays	Dresses, short tops, hot pants	The characteristics of clothing styles are comfortable, natural, lightweight, and simple in style

2) Overall clothing matching plan: The overall matching scheme of clothing is to determine the optimal color range of clothing based on the skin color characteristics selected by the user. The theme color and style of clothing are determined for different dressing occasions, and the clothing matching rules are designed to obtain the suitable clothing matching recommendation scheme in the design system.

The design concept of this set of clothing matching is to first determine the color range of the clothing top based on the twelve determined skin color classifications, and compare the relationship between cold and warm tones and brightness purity. Then, according to different dressing occasions, the theme color is selected, and the color of the lower garment is selected. Finally, the color matching of the entire set of clothing is completed. The recommended style combinations are only influenced by the factors of the dressing occasion, so in the previous section, the style combinations have been completed.

The matching design of clothing colors is only based on qualitative semantic descriptions, and in order to apply it in computer mode, it is necessary to quantify it. The most commonly used RGB mode is to mix and overlay different proportions of red, green, and blue colors to generate different colors, similar to pigment mixing and color matching in painting. The famous Pantone clothing color card uses RGB mode to represent different colors. However, according to the previous analysis of clothing color matching, the matching rule recommended by experts is to match colors based on the three attributes of colors, and the color generation principle of HSB mode is more suitable for the transformation of the author's matching method to express different colors [18].

In HSB color mode, there are three attribute sliders: hue, which is the hue ring, and complete colors are represented as a 360 degree hue wheel; the range value of purity is 0-100%, with increasing purity and the purest color expression; the range value of brightness is also 0-100%, with increasing brightness and reaching the brightest color.

In order to achieve the recommended scheme for clothing color in the system, it is necessary to convert the RGB values of conventional colors into HSB values. Based on these three attributes, the matching rules can be applied to effectively obtain the recommended scheme for clothing matching. The following are the conversion formulas for the two modes, as shown in Eq. (1) - Eq. (3).

$$H=\begin{bmatrix} 60\times((G-B)/\Delta\times \mathrm{mod}), C_{\max}=R \\ 60\times(\frac{(B-R)}{\Delta}+2), C_{\max}=G \\ 60\times(\frac{(\mathrm{R}-\mathrm{G})}{\Delta}+4)\ ,\ \mathrm{C}_{\max}=\mathrm{B} \end{bmatrix} \quad (1)$$

$$s=\begin{bmatrix} 0, C_{\max}=0 \\ \frac{\Delta}{C_{\max}}, C_{\max}\neq 0 \end{bmatrix} \quad (2)$$

$$\mathrm{B}=\mathrm{C}_{\max} \quad (3)$$

Correctly convert the clothing colors in the Pantone color card into hue, brightness, and purity values, and convert the semantic descriptions of twelve human skin tones and clothing occasions into their HSB mode color tone matching values

and hue matching values. Based on the clothing matching rules obtained in the previous text, the use case for determining a set of clothing matching is presented here;

Based on the user's choice of pure spring skin color, the recommended clothing color range is high brightness, high purity, and color values without cold or warm tones. The numerical range converted into computer HSB mode is: Brightness value 70% -100%, purity value 70% -100%.

Choose a banquet occasion for dressing. Based on the requirements of the theme color, which is bright and eye-catching, choose a red hue value of 0 degrees here. According to the method of contrasting colors in color matching, the lower garment can be matched with color values within the range of 0 degrees and 120 degrees, or neutral colors without warm or cold tones can be selected as a match, such as black. This completes the color recommendation for the entire set of clothing for subsequent clothing matching displays.

Translate the clothing matching rules into different numerical ranges for the three major attributes in computer HSB mode, and determine that the color HSB value within the numerical range is the color recommended for matching. If it is not within the numerical range, it is not recommended. Based on this, a case study of clothing color matching required in the system is formed [19-20].

ACKNOWLEDGMENT

Key research project of Wuhan Vocational College of Foreign Languages and Foreign Affairs, Research on the Application of digital Virtual Technology of Clothing in the development Mode of Product Innovation Studio in Higher Vocational Colleges, (Project number: 2023WYZDKY02)

V. CONCLUSION

By analyzing the clothing matching experience in expert knowledge, combined with the characteristics of the system, selecting factors related to human skin color and dressing occasions for analysis, and combining color matching rules to determine the color matching of clothing; Combining TPO matching rules to match clothing styles, comprehensively completing clothing matching recommendation schemes, and applying them to the implementation of clothing matching functions in the system.

REFERENCES

[1] Zhang, X. , & Dong, F. . (2021). How virtual social capital affects behavioral intention of sustainable clothing consumption pattern in developing economies? a case study of china. Resources Conservation and Recycling, 170(3), 105616.

[2] Chen, T. , Yang, E. K. , & Lee, Y. . (2021). Development of virtual up-cycling fashion design based on 3-dimensional digital clothing technology. The Research Journal of the Costume Culture, 29(3), 374-387.

[3] Zhang, X. D. F. . (2021). How virtual social capital affects behavioral intention of sustainable clothing consumption pattern in developing economies? a case study of china. Resources, Conservation and Recycling, 170(1)14.

[4] Tian, F. . (2021). Immersive 5g virtual reality visualization display system based on big-data digital city technology. Mathematical Problems in Engineering, 2021(3), 1-9.

[5] Liu, JingjunMcCool, BenjaminJohnson, J. R.Rangnekar, NeelDaoutidis, ProdromosTsapatsis, Michael. (2021). Mathematical modeling and parameter estimation of mfi membranes for para/ortho-xylene separation. AIChE Journal, 67(6)14.

[6] Fei, X. . (2021). An lda based model for semantic annotation of web english educational resources. Journal of intelligent & fuzzy systems: Applications in Engineering and Technology, 40(2)14

[7] Arev, I. , Arev, B. P. , Krstonoi, V. , Janev, M. , & Atanackovi, T. M. . (2021). Modeling the rheological properties of four commercially available composite core build-up materials:. Polymers and Polymer Composites, 29(7), 931-938.

[8] Franco, P. , Sanchez, M. T. , & Nalda, E. . (2021). Mathematical models for the dimensional accuracy of products generated by additive manufacturing - sciencedirect. Advances in Mathematics for Industry 4.0, 3(6)1-388..

[9] Ma, Q. , Sun, C. , Cui, B. , & Jin, X. . (2021). A novel model for anomaly detection in network traffic based on kernel support vector machine. Computers & Security, 104(2), 102215.

[10] Meng, Q. , & Xiong, H. . (2021). A doctor recommendation based on graph computing and lda topic model. International Journal of Computational Intelligence Systems, 14(1), 808.

[11] Seong-Taek, P. , & Chang, L. . (2022). A study on topic models using lda and word2vec in travel route recommendation: focus on convergence travel and tours reviews. Personal and ubiquitous computing14(2), 26.

[12] Zhang, Z. , Hosaka, T. , Yamashita, H. , & Goto, M. . (2021). A study on recommender system considering diversity of items based on lda. Asian journal of management science and applications14(1), 6.

[13] Galib, S. M. S. , Islam, S. M. R. , & Rahman, M. A. . (2021). A multiple linear regression model approach for two-class fnir data classification. Iran Journal of Computer Science14(1), 4.

[14] Sun, Y. , Zhuang, J. , & Wentzcovitch, R. M. . (2022). Thermodynamics of spin crossover in ferropericlase: an improved lda + usc calculation. Electronic Structure, 4(1), 014008 (10pp).

[15] Amiri, V. , & Nakagawa, K. . (2021). Using a linear discriminant analysis (lda)-based nomenclature system and self-organizing maps (som) for spatiotemporal assessment of groundwater quality in a coastal aquifer. Journal of Hydrology, 603, 127082-.

[16] Zheng, Y. . (2021). Research and application of lda model in movies images based on the visual effects of computer images. Journal of Physics: Conference Series, 1952(2), 022060 (7pp).

[17] Liu, X. , Gao, Y. , Cao, Z. , & Sun, G. . (2021). Lda-based topic mining of microblog comments. Journal of Physics Conference Series, 1757(1), 012118.

[18] Zhao, C. , Cao, G. , Ding, H. , Zhang, Y. , & Hou, H. . (2021). Research on intelligent recognition and control device of aviation line number. Journal of Physics: Conference Series, 1754(1), 012099 (7pp).

[19] MD Nardo, Madonna, M. , Gallo, M. , & Murino, T. . (2020). A risk assessment proposal through system dynamics. Xinan Jiaotong Daxue Xuebao/Journal of Southwest Jiaotong University.

[20] Bentkowska, U. , Zarba, L. , Stanislawa Bazan-Socha, Mrukowicz, M. , Bazan, J. G. , & Socha, J. . (2022). Interval modelling in optimization of k-nn classifiers for large number of attributes in data sets on an example of dna microarrays. International Journal of Intelligent Systems, 37(6), 3334-3372.

Enhancing Alzheimer's Detection: Leveraging ADNI Data and Large Language Models for High-Accuracy Diagnosis

Hassan Almalki[1], Alaa O. Khadidos[2], Nawaf Alhebaishi[3]
Department of Information Technology, College of Technology for Communications and Information, Jeddah, Saudi Arabia[1]
Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia[2, 3]
Center of Research Excellence in Artificial Intelligence and Data Science, King Abdulaziz University, Jeddah, Saudi Arabia[2]

***Abstract*—Alzheimer's disease (AD), the most common type of dementia, is expected to affect 152 million people by 2050, emphasizing the importance of early diagnosis. This study uses the Alzheimer's Disease Neuroimaging Initiative (ADNI) dataset, combining cognitive tests, biomarkers, demographic details, and genetic data to build predictive models. Using large language models (LLMs), specifically ChatGPT 3.5, we achieved high classification accuracy, with ROC AUC values of 0.98 for cognitively normal (CN) individuals, 0.99 for dementia, and 0.98 for mild cognitive impairment (MCI). These findings show that LLMs can handle complex data quickly and accurately. By focusing on numerical and text-based data instead of just imaging, this method provides a cost-effective and accessible option for diagnosing AD. Adding genetic information improves the predictions, reflecting the important role of genetics in AD risk. This study highlights the potential of combining different types of data with advanced machine learning and LSTM to improve early AD diagnosis. Future research should explore more ways to combine data and test different machine learning models to further enhance diagnostic tools.**

***Keywords*—Alzheimer; dementia; LLMs; ChatGPT; LSTM**

I. Introduction

Alzheimer's disease (AD), the most common form of dementia, accounts for 60–80% of all dementia cases and is expected to become even more prevalent as populations age [1-7]. By 2050, it is estimated that 152 million people worldwide will be living with Alzheimer's and other forms of dementia [1]. AD is particularly significant among non-communicable diseases, which together account for approximately 70% of global deaths [8-10]. The disease primarily affects older adults, impairing memory, behaviour, and reasoning abilities [11, 12].

To improve the health and quality of life for older adults, it is increasingly important to develop effective treatments for AD [13-15]. Although several biomarkers for early diagnosis have been identified [4], accurate diagnosis still partly relies on clinical criteria, which can take up to six months as symptoms gradually become apparent [16, 17]. Even when symptoms are clear enough for a confirmed diagnosis, AD remains incurable [10, 18, 19].

The Global Deterioration Scale [20] outlines symptoms such as decreased work performance, increased forgetfulness, and frequent disorientation during the mild cognitive impairment (MCI) stage. MCI is characterized by a prolonged period of decline that can last for around seven years [18]. This has led medical professionals to focus on establishing criteria for early diagnosis to slow or potentially prevent disease progression [14, 18].

Current medical practices for diagnosing AD can be time-consuming. As a result, researchers are increasingly exploring approaches that combine medicine with computer science, particularly deep learning, to develop methods for earlier and more accurate diagnoses. This interdisciplinary focus has become a key area of ongoing research.

Various approaches have been employed to diagnose Alzheimer's disease (AD) as early as possible. These include skeleton-based human action evaluation [18], 3D CNN-based classification of sMRI and MD-DTI images to detect brain changes [8, 9, 19], and speech analysis [15, 17]. Monitoring dementia progression using 2D and 3D imaging techniques has become a sophisticated method, utilizing advanced medical imaging to track changes in brain structure and function over time [2, 7, 19, 21, 22]. Additionally, it is crucial to determine whether cognitive measures identified as predictive in research cohorts are also applicable in clinical memory clinics [2, 13, 23-25].

This study aimed to identify the most effective measures for predicting future AD dementia in clinical settings where expensive biomarkers may not be widely available. Early detection of AD severity is critical [5, 14, 19, 26, 27]. While neuroimaging and computer-assisted diagnostic tools can detect AD in its early stages, these methods often lack high accuracy [11]. Techniques like Computed Tomography (CT), Positron Emission Tomography (PET), and Magnetic Resonance Imaging (MRI) significantly contribute to diagnosing brain disorders [28].

Advancements in medical imaging, supported by computer-aided diagnostic research, have greatly improved the ability to monitor and predict dementia progression. 2D and 3D imaging techniques play an essential role, offering a comprehensive view through structural, functional, and molecular imaging. These advances continue to improve our understanding and management of this complex condition, providing hope for better patient outcomes.

However, several challenges persist. Advanced imaging techniques such as MRI and PET are expensive, making routine monitoring financially difficult for many patients. Access to high-quality imaging facilities is often limited, particularly in rural or underserved areas. Additionally, technical limitations such as resolution and sensitivity may prevent the detection of small or early brain changes. Imaging data can also be affected by noise and artifacts, complicating interpretation. Health-related concerns include exposure to ionizing radiation from PET and CT scans, especially with repeated use, and discomfort or anxiety during MRI scans, particularly for patients with claustrophobia.

From a technical perspective, the large volume of data generated by 3D imaging requires robust data management and analysis systems, along with advanced computational tools and expertise for handling and interpreting big data. While these imaging techniques provide valuable insights, their limitations underscore the importance of a balanced approach.

Recent advancements have also identified blood-based biomarkers that can assist in monitoring dementia progression. These tests are less invasive than cerebrospinal fluid (CSF) tests and more practical for regular use. Key biomarkers include Amyloid Beta (Aβ), Tau Proteins, and Neurofilament Light Chain (NfL). Cognitive tests remain essential for assessing cognitive functions and tracking changes over time. Commonly used tests include the Mini-Mental State Examination (MMSE), Montreal Cognitive Assessment (MoCA), Clock Drawing Test, Alzheimer's Disease Assessment Scale-Cognitive Subscale (ADAS-Cog), and neuropsychological testing. This paper consists of literature review, methodology, results, discussion and conclusion, where every section highlights related information.

II. Literature Review

Alzheimer's disease (AD) is a neurological disorder that progressively worsens over time. It is typically divided into three main stages, with the early stage being particularly important [29]. One challenge with Alzheimer's treatments is their limited effectiveness, especially during the disease's typical eight-year progression [29].

In the early stage, daily activities gradually become more difficult. The most common signs include short-term memory loss and trouble learning new things [12, 29]. Other symptoms may include low energy, a sad mood, and a lack of interest or motivation [30]. Notably, individuals diagnosed with mild cognitive impairment (MCI) are at a significantly higher risk of developing AD [29]. In many cases, MCI is classified as the early stage of AD [31].

Researchers have also observed that difficulties with language—such as trouble pronouncing or remembering complex words—alongside challenges in performing daily tasks, may serve as early indicators of AD [29, 31, 32]. These findings suggest that there are more affordable diagnostic tools for detecting dementia than costly imaging techniques. Many studies have applied statistical analysis alongside other types of data (excluding imaging) to explore alternative methods for diagnosing Alzheimer's disease (AD). For instance, human action evaluation has shown potential applications in areas such as assisted living, physical rehabilitation, sports activity scoring, and skills training [18]. This approach can also be applied to AD by using sequences of 3D skeletal joint data to assess the severity of the disease in patients. For example, Yu et al. [18] utilized a two-task graph convolutional network to analyze skeleton data for tasks involving abnormality detection and quality evaluation. Their method, evaluated using the UI-PRMD dataset, demonstrated accurate abnormality detection.

Taghvaei et al. [33] applied statistical analysis to investigate the relationship between white matter hyperintensities (WMH) tract disconnection and cognitive performance. Their study highlighted the significant role of demographic factors, such as education level, age, and sex, in influencing the relationship between WM tracts and cognitive scores. Similarly, Raj et al. [1, 34] emphasized the importance of genetics, which contributes to approximately 70% of the overall risk for AD. They introduced a system that combines text mining and machine learning to identify and prioritize candidate genes for AD, categorizing them into three association classes with corresponding weights.

Another cost-effective method for predicting AD involves analyzing patients' speech patterns [35]. Many studies have focused on acoustic and syntactic analysis of speech. For example, Haj Zargarbashi and Bagher [17] employed statistical and neural methods to classify audio signals into dementia and control groups, achieving an accuracy of 83.6%. Similarly, Vincze et al. [36] analyzed specific utterances using deep learning models, with and without demographic data, and found no significant differences between the models. Colla et al. [37] used large language models alongside N-grams and perplexity metrics to predict potential AD with an accuracy of 84%. Gómez-Zaragoza et al. [15] provided empirical evidence that punctuation and pauses in speech could reveal early signs of AD. A comprehensive review by [38] highlighted the high potential for deep learning to be utilized with medical data in future research.

Cai et al. [35] examined methods for detecting AD through speech analysis by transcribing audio into text and extracting audio features using the WavLM model. They tested pre-trained models and Graph Neural Networks (GNNs) with the DementiaBank Pitt dataset and applied fine-tuning techniques such as data augmentation (e.g., synonym replacement and GPT-based augmentation). Wang et al. [39] also used pre-trained language models with fine-tuning methods, achieving up to 89% accuracy. Finally, blood tests have shown promise in detecting AD. Certain biomarkers in blood may indicate the potential presence of the disease. Kim and Lee [40] demonstrated that complex interactions among blood proteins could predict the likelihood of AD development.

Several gaps have been identified in Alzheimer's disease (AD) research. For example, while the ADNI dataset has been extensively used in studies focusing on MRI images [29], it has only been partially utilized. Most studies have concentrated solely on MRI images, overlooking the wealth of other information in the dataset that could enhance the analysis of AD. A recent systematic literature review by Singh et al. [41] found that the majority of AD studies used ADNI and deep learning methods, a trend confirmed by Alwuthaynani et al. [2],

but with an exclusive focus on MRI data. Similarly, Essemlali et al. [42] highlighted that one of the key challenges in dementia prediction lies in distinguishing between MCI and AD, as well as between NC (normal cognition) and MCI. These are among the most difficult classification tasks and often require additional data, such as multi-modality or genetic information, to improve predictions.

This study leverages the powerful classification capabilities of large language models (LLMs), such as ChatGPT, to classify dementia stages. There is a notable lack of research utilizing LLMs with non-imaging data from the ADNI dataset to address classification problems. For instance, Agbavor and Liang [43] demonstrated that GPT-3 embeddings significantly improved Alzheimer's detection accuracy from spontaneous speech, outperforming traditional methods based on acoustic features. They used models such as support vector classifiers and logistic regression, achieving high classification performance. Another study [44] combined imaging and phenotype data from the ADNI dataset with LLMs, achieving state-of-the-art performance in classifying Alzheimer's and various stages of cognitive impairment. This highlights the effectiveness of integrating LLMs with diverse data types.

However, as discussed, this study focuses on utilizing LLMs with textual and numerical data rather than imaging data. This approach aims to provide a cost-effective solution suitable for clinical settings and requiring less computational power. The methodology is informed by the work of Feng et al. [44], excluding imaging data, to create a more accessible and efficient model for AD classification.

III. METHODOLOGY

A. ADNI Dataset

This study utilized the ADNI dataset due to its extensive use in recent research and its comprehensive collection of data necessary to achieve the goals of this study. The ADNI dataset, available at adni.loni.ucla.edu, has been widely referenced in studies related to Alzheimer's detection [41, 45].

The ADNI project was launched in 2003 by the National Institute on Aging (NIA), the Food and Drug Administration (FDA), the National Institute of Biomedical Imaging and Bioengineering (NIBIB), private non-profit organizations, and pharmaceutical companies [41, 45]. Its original purpose was to determine whether the combination of genetic, neuroimaging, biomarker, clinical, and neuropsychological data could be used to predict Alzheimer's disease.

The ADNI dataset is renowned for its longitudinal design, capturing data at multiple time points. Images and other data are collected at baseline and then at intervals of 6 months, 12 months, 24 months, and 48 months [42]. Several versions of the dataset, including ADNI2 and ADNI-Go, have been developed to expand its scope.

B. Feature Set

In addition to demographic data, such as sex, age, gender, and race, which have been shown to significantly contribute to predicting the clinical status of individuals [36], this study incorporates a variety of other features for analysis. Cognitive tests play a central role in assessing various aspects of memory, language, and executive function. These include the Mini-Mental State Examination (MMSE), a widely used measure of cognitive function, and the Montreal Cognitive Assessment (MOCA), another standard cognitive measure. The study also utilizes scores from the Rey Auditory Verbal Learning Test (RAVLT), including immediate recall, learning, forgetting, and percentage of forgetting, which assess different dimensions of memory. Other cognitive tests include the Logical Memory Delayed Recall test (LDELTOTAL), the Digit Span test (DIGITSCOR), which measures attention and working memory, and the Trail Making Test Part B (TRABSCOR), which evaluates executive function. The Functional Activities Questionnaire (FAQ) is also included to assess daily living capabilities.

Biomarkers represent another crucial component of the analysis. The Apolipoprotein E (APOE4) genotype, strongly associated with Alzheimer's disease risk, is used alongside imaging biomarkers from PET scans, including tracers such as FDG, PIB, AV45, and FBB. Additionally, cerebrospinal fluid protein levels of amyloid-beta (ABETA), tau (TAU), and phosphorylated tau (PTAU) are examined for their role in the disease's progression.

Clinical and diagnostic scores also contribute significantly to the analysis. These include the Clinical Dementia Rating – Sum of Boxes (CDRSB), which evaluates cognitive and functional performance, and various subscales from the Alzheimer's Disease Assessment Scale (ADAS), such as ADAS11, ADAS13, and ADASQ4. Reports of cognitive function from both patients and their study partners are included, with patient-reported scores covering memory, language, visuospatial ability, planning, organization, divided attention, and overall cognitive function. Study partner-reported scores assess the same domains, providing additional perspectives on cognitive performance.

Baseline data for all these measures are also incorporated to analyze changes over time. Baseline values for clinical scores such as CDRSB, ADAS, and MMSE, as well as cognitive tests like RAVLT, Logical Memory, and FAQ, are included. Baseline levels of biomarkers, such as ABETA, TAU, and PTAU, are also considered. Patient- and study partner-reported cognitive scores at baseline offer further context for tracking progression. Temporal variables, such as the number of years or months since the baseline visit, are included to provide additional detail about the timing of data collection.

In summary, the features included in this study's prediction models encompass cognitive assessments, genetic information, biomarkers, demographic data, and clinical details. These measures provide a comprehensive dataset for early detection of dementia, offering insights into cognitive decline and associated risk factors. By integrating this diverse set of features, the study aims to improve the accuracy and practicality of predictive models for Alzheimer's disease [27, 46, 47].

C. Models

Shah and Shah [12] explored the use of machine learning (ML) algorithms, particularly convolutional neural networks (CNNs), for the early diagnosis of Alzheimer's disease (AD)

through the analysis of medical imaging data, such as MRI scans and biomarkers. Their study compared various ML algorithms, including k-nearest neighbor (KNN) and support vector machines (SVM), and highlighted the superior accuracy and reliability of CNNs in detecting AD. The deep learning capabilities of CNNs enable them to extract subtle features from medical images, making them particularly effective for this application. Shah and Shah [12] demonstrated that CNNs outperformed other algorithms due to their deep architecture, which can handle complex data and identify patterns that simpler models may miss.

However, the authors also noted several challenges in using CNNs for AD diagnosis. These include the need for large, well-curated datasets, as CNN models are prone to overfitting when trained on small or imbalanced datasets. Additionally, they emphasized the importance of transparency and interpretability in ML models, especially in medical applications where clinicians need to understand the rationale behind a diagnosis. Despite these challenges, CNN-based models were identified as the most effective for early detection of AD, particularly when applied to MRI scans and biomarker data.

While Shah and Shah [12] provided a thorough investigation into the use of ML and deep learning methods for early AD detection, their work predominantly focused on image-based data, such as MRI scans. They did not explore the application of these methods to other types of data, such as textual or numerical information, nor did they consider the potential of large language models (LLMs). LLMs, with their ability to process both structured and unstructured text, could provide valuable insights and significantly enhance prediction models for AD. Additionally, the study did not examine the use of Long Short-Term Memory (LSTM) networks, which are particularly effective for analyzing sequential data, such as time-series health records or longitudinal datasets.

Building on their work, this study proposes the integration of both LSTM networks and LLMs alongside traditional machine learning methods to develop cost-effective and accurate prediction solutions for AD. By focusing on non-image data, such as cognitive assessments, biomarkers, and clinical records, this approach aims to expand the scope of predictive models and offer accessible diagnostic tools for clinical settings.

1) LSTM: Long Short-Term Memory (LSTM) networks are a specialized type of recurrent neural network (RNN) designed to learn and retain long-term dependencies in sequential data. They are particularly well-suited for tasks involving time-series or sequential data due to their unique architecture, which includes memory cells and gating mechanisms (input, output, and forget gates) to control the flow of information. This capability makes LSTM networks highly effective in addressing the vanishing gradient problem, a common challenge in traditional RNNs.

In this study, LSTM networks are employed to process clinical and biomarker data from the ADNI dataset. The input features, which consist of textual and numerical data, are well-suited to LSTM's architecture. The model begins with an input layer that accepts the data features, followed by one or more LSTM layers that process the sequences of observations. The final dense layer produces the output, classifying the stages of Alzheimer's disease based on the processed data. By leveraging LSTM's ability to handle sequences effectively, this study aims to improve classification accuracy for Alzheimer's diagnosis. Additionally, LSTM networks are prioritized due to their demonstrated effectiveness in managing textual and numerical data, which are key components of the ADNI dataset. The following equations illustrate the core functionality of LSTM networks in classification tasks:

The forget gate controls which information from the previous cell state (C_{t-1}) should be carried forward to the current cell state (C_t).

$$f_t=\sigma(W_f \cdot[h_{t-1}, x_t] + b_f)$$

Where f_t is the forget gate's activation vector; W_f and b_f are the weight matrix and bias for the forget gate; h_{t-1} is the previous hidden state; x_t is the current input and σ is the sigmoid activation function [48]. Input Gate [49] represented as follows:

$$i_t=\sigma(W_i\cdot[h_{t-1}, x_t] + b_i)$$

$$\dot{C}_t =tanh\ (W_C \cdot[h_{t-1}, x_t] + b_C)$$

where i_t is the input gate's activation vector; $\dot{C}_t$ is the candidate cell state, representing new information; and W_i, W_C b_i, b_C are the weight matrices and biases for the input gate and cell state.

Meanwhile; Cell State Update is implemented as follows

$$C_t=f_t*C_{t-1}+i_t* \dot{C}_t$$

And the output gate [50] is implemented as follows

$$o_t=\sigma(W_o\cdot[h_{t-1}, x_t]+b_o)$$

$$h_t=o_t*tanh(C_t)$$

where o_t is the output gate's activation vector; h_t is the current hidden state (which also serves as the output for classification).

The classification layer is implemented using this formula [51]:

$$y=softmax(W_y\cdot h_t+by)$$

where y is the predicted class probabilities; W_y and by are the weight matrix and bias for the classification layer.

finally; Loss Function for Classification (Cross-Entropy) [52] is presented by

$$L= -\sum_{i=1}^{N} y_i\ log(y'_i)$$

Where: y_i is the true label; y'_i is the predicted probability for class and N is the number of classes.

At each time step, the LSTM updates the cell state and hidden state using the forget, input, and output gates. The final hidden state after processing the entire sequence is passed to the classification layer, where the class probabilities are calculated. The loss function is used to optimize the model by comparing the predicted output with the actual labels. This process allows the LSTM to classify sequential data effectively.

2) Few-Shot: Few-shot learning is a machine learning technique that enables models to perform tasks with minimal examples or training data. Unlike traditional machine learning methods, which rely on large datasets and extensive training, few-shot learning allows for adaptability and flexibility with significantly reduced training overhead. This approach is particularly useful for large language models (LLMs) like OpenAI's ChatGPT-3.5-turbo, as it enables the model to learn effectively from a limited number of examples. The primary advantage of few-shot learning is its ability to achieve accurate predictions with less effort in data preparation and model training.

In this study, few-shot learning was applied to classify Alzheimer's disease stages using examples from the ADNI dataset. The process began by defining a small set of examples representing the desired outcomes: "CN" (cognitively normal), "Dementia," and "MCI" (mild cognitive impairment). A sample of 10 examples was provided, reflecting various cases in the dataset, including instances with missing values across specific groups of features. Next, a prompt was constructed to include these examples and the task to be performed, guiding the model toward the desired predictions. The model then used this context to generate predictions, which were subsequently extracted to retrieve the relevant outputs. This streamlined process demonstrates the efficiency of few-shot learning in handling limited data while maintaining accurate and meaningful results.

IV. Results

A. Demographic

The ADNI dataset contains numerous cases categorized under each stage of dementia. These cases include multiple rows for the same patient, corresponding to different visits over time. The distribution of cases across the stages of dementia is illustrated in Fig. 1. As shown, the majority of patients are at the MCI stage, followed by those at the CN stage, highlighting the prevalence of MCI cases in the dataset.

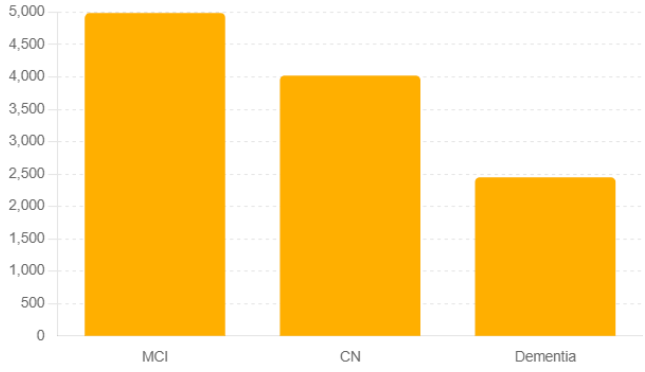


Fig. 1. Patients'stage in ADNI dataset.

The demographic data available in the ADNI dataset is presented in Fig. 2. The data shows a balanced distribution in terms of gender. However, there is an imbalance in race, with the white population significantly outnumbering other racial groups. The age range of participants spans from 55 to 90 years.

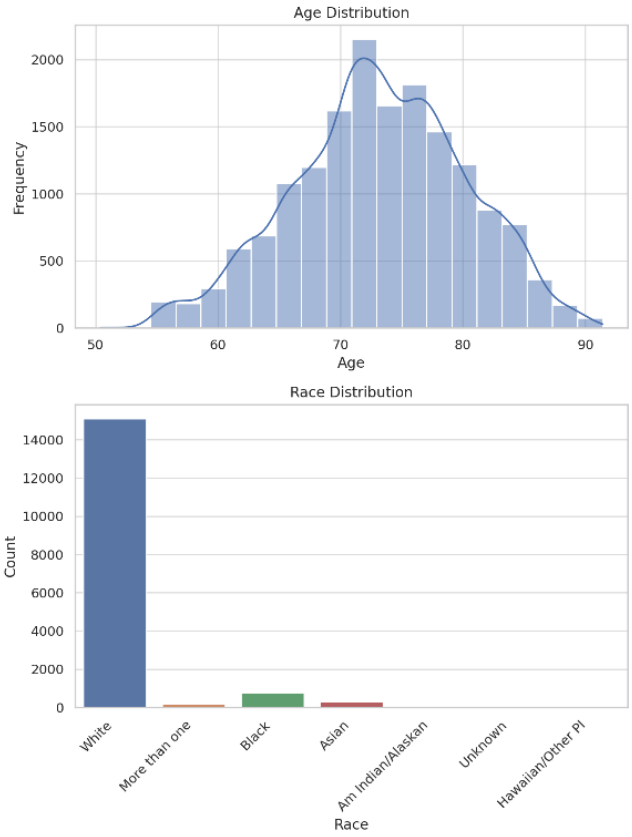


Fig. 2. Demographics related statistics.

B. Feature Selection and Machine learning Methods' Prediction

To identify the most important features for predicting the diagnosis label (DX), three approaches were implemented: (a) Correlation Analysis to examine relationships between features and DX, (b) Random Forest Feature Importance to rank features by their predictive significance, and (c) Recursive Feature Elimination (RFE) to select the most relevant features based on model performance.

The Correlation Analysis revealed that the features most strongly correlated with DX are: CDRSB (Cognitive Dementia Rating – Sum of Boxes) with a correlation of 0.751, EcogSPTotal (Total score of Everyday Cognition, Study Partner version) at 0.735, EcogSPMem (Everyday Cognition, Study Partner Memory score) at 0.732, FAQ (Functional Activities Questionnaire) at 0.730, and ADAS13 (Alzheimer's Disease Assessment Scale, 13-item) at 0.725. These results indicate that cognitive and functional assessments are highly correlated with Alzheimer's diagnosis. Using Random Forest Feature Importance, the top features for predicting DX were identified as EcogSPTotal (20.28%), ADAS13 (18.84%), ADAS11 (16.54%), EcogSPMem (12.64%), and EcogSPOrgan (9.45%). These findings reinforce the importance of cognitive and functional assessments in predicting Alzheimer's.

With Recursive Feature Elimination (RFE), the same top five features were selected: EcogSPTotal, EcogSPMem, ADAS13, ADAS11, and EcogSPOrgan. A Random Forest Classifier trained using only these features achieved an average

cross-validation accuracy of 38.75% (standard deviation: 0.89%) and a test accuracy of 39%. Class 2 (Dementia) was predicted with the highest recall (63%), but precision and recall for Class 0 (Cognitively Normal) and Class 1 (MCI) were low. The macro-average F1-score was 0.32, highlighting significant confusion between classes, particularly between Cognitively Normal and MCI.

To address these limitations, several strategies were explored. Class Imbalance Handling techniques, such as oversampling, undersampling, and class-weighted models, improved the weighted F1-score slightly to 0.37, with Class 2 (Dementia) achieving 63% recall. However, confusion between Cognitively Normal and MCI persisted. Feature Engineering was then applied, creating interaction features by combining cognitive scores and biomarkers. This approach marginally increased the overall accuracy to 40%, with a recall of 66% for Class 2. While improvements in classifying Cognitively Normal and MCI cases were observed, misclassification between MCI and Dementia remained significant.

Next, Advanced Models were tested, including Gradient Boosting and Support Vector Machines (SVM). Gradient Boosting achieved an overall accuracy of 43%, with Class 2 (Dementia) recall at 92%. However, predictions for Class 0 (Cognitively Normal) and Class 1 (MCI) were poor, with F1-scores close to zero. Similarly, SVM performed slightly better with an overall accuracy of 45% and a recall of 99% for Class 2, but almost no correct predictions for Classes 0 and 1. Both models struggled with class imbalance, favoring Dementia at the expense of distinguishing other classes.

Finally, Ensemble Modeling was implemented, leveraging techniques like Voting Classifiers (combining Random Forest, Gradient Boosting, and SVM), Stacking Classifiers (training multiple models and using their predictions as inputs for a meta-model), and Bagging (aggregating predictions from models trained on different data subsets). These ensemble methods aim to balance predictive performance across classes and address the challenges of class imbalance and overlapping features. Further evaluation and refinement of these approaches are ongoing to improve the overall diagnostic accuracy and robustness of the model.

1) Voting classifier results: The model achieved an overall accuracy of 43%, with Class 2 (Dementia) having the highest recall at 90%. However, performance for Class 0 (Cognitively Normal) and Class 1 (MCI) was poor, with F1-scores of approximately 0.09 and 0.05, respectively. The macro-average F1-score was 0.24, highlighting that the model disproportionately favors Dementia while struggling to accurately classify Cognitively Normal and MCI cases. Significant confusion remains between the classes, with many CN and MCI cases misclassified as Dementia.

2) Stacking classifier results: The model achieved an overall accuracy of 45%, matching the performance of the Voting Classifier. However, the results reveal a significant bias, as Class 2 (Dementia) was the only class predicted, with a recall of 100%. Both Class 0 (Cognitively Normal) and Class 1 (MCI) had 0% recall and precision, indicating that no cases from these classes were correctly identified. The macro-average F1-score was 0.21, underscoring the model's heavy bias toward Dementia and its inability to distinguish between Cognitively Normal and MCI cases. All instances of CN and MCI were misclassified as Dementia.

3) Bagging: Using Bagging with the Random Forest model, which inherently trains on different subsets of data, the overall accuracy achieved was 41%. Class 2 (Dementia) had a recall of 73%, while Class 0 (Cognitively Normal) and Class 1 (MCI) showed lower recall and F1-scores. The macro-average F1-score was 0.31, indicating a moderate improvement in balancing predictions across classes compared to previous classifiers. Bagging demonstrated better differentiation between classes than the Voting and Stacking classifiers, though significant misclassifications remained between Cognitively Normal, MCI, and Dementia. Notably, Bagging performed slightly better in predicting minority classes.

In summary, the Voting Classifier achieved an accuracy of 43% but was heavily biased toward predicting Dementia, performing poorly on other classes. The Stacking Classifier achieved a slightly higher accuracy of 45%, but it failed to classify Cognitively Normal and MCI cases, predicting only Dementia. Bagging, with an accuracy of 41%, showed improved balance across the classes compared to Voting and Stacking but continued to struggle with distinguishing between Cognitively Normal and MCI cases.

Among the ensemble methods, Bagging demonstrated better overall balance in classifying multiple categories, although limitations remained. To further enhance performance, future work could focus on advanced feature engineering, fine-tuning model hyperparameters, or exploring other sophisticated techniques to address the challenges in distinguishing between these diagnostic categories.

C. Advanced Analyses

To further improve model performance, particularly in distinguishing between the different diagnostic classes (Cognitively Normal, MCI, and Dementia), several advanced techniques could be employed. Automated machine learning (AutoML) tools, such as TPOT, can automate the process of testing a range of algorithms and hyperparameter configurations, helping to identify the best model without requiring manual experimentation.

In this study, an AutoML framework was used to automatically test multiple models and optimize their hyperparameters. The results from the TPOT AutoML run provided valuable insights into the model selection and tuning process. The internal cross-validation (CV) accuracy, which TPOT uses to evaluate different pipelines during its evolutionary search, stabilized at approximately 47.7% across most generations. The final best pipeline achieved an internal CV score of 47.78%, indicating the highest performance based on TPOT's cross-validation evaluation.

TPOT selected the ExtraTreesClassifier as the best model. This ensemble method, similar to Random Forest, reduces variance by averaging predictions across multiple decision trees, often resulting in more stable outcomes. The

ExtraTreesClassifier was identified as the optimal model with the following key parameters:

- Bootstrap: True (bootstrap sampling was used).
- Criterion: Gini (used for measuring the quality of a split).
- Max features: 0.8 (80% of the features are considered when looking for the best split).
- Min samples leaf: 17 (minimum number of samples required to be at a leaf node).
- Min samples split: 5 (minimum number of samples required to split an internal node).
- n_estimators: 100 (number of trees in the forest).

The test set accuracy was 43.6%, meaning the final model achieved 43.6% accuracy on unseen data. While consistent with the performance of other models tested, this accuracy highlights the challenges in distinguishing between the diagnostic categories (Cognitively Normal, MCI, and Dementia). The consistency of accuracy between 43% and 45% across different models suggests that the feature set may require further refinement or that the inherent complexity of differentiating between these classes, particularly between Cognitively Normal and MCI, remains a significant challenge.

Since focusing on the top five features did not result in substantial improvements in accuracy, a new approach was tested by including DX_bl (the baseline diagnosis) as a key feature for predicting the final diagnosis (DX). This approach is logical, as the baseline diagnosis likely correlates strongly with the final diagnosis, and transitions between diagnostic categories (e.g., from MCI to Dementia) over time can provide valuable insights. Using a Random Forest model with DX_bl as a feature, the accuracy improved significantly to 83%, demonstrating that DX_bl is a strong predictor of the final diagnosis.

The model's performance metrics for each class are as follows:

Class 0 (Cognitively Normal - CN):

Precision: 89% (89% of cases predicted as CN are correct).

Recall: 92% (92% of actual CN cases were correctly identified).

F1-Score: 91% (indicating strong and balanced performance for this class).

Class 1 (MCI):

Precision: 100% (all predicted MCI cases were correct).

Recall: 51% (only 51% of actual MCI cases were identified correctly).

F1-Score: 67% (highlighting an imbalance, as many MCI cases are misclassified).

Class 2 (Dementia):

Precision: 75% (75% of Dementia predictions were correct).

Recall: 93% (93% of actual Dementia cases were identified).

F1-Score: 83% (indicating strong performance for this class).

The Macro Average F1-Score, which gives equal weight to each class, was 80%, showing good overall performance but highlighting some imbalance in the prediction of MCI. The Weighted Average F1-Score, which accounts for the number of instances in each class, was 82%, reflecting the model's strong performance for the larger classes (CN and Dementia).

Cognitively Normal (CN) and Dementia cases are well predicted, with high precision and recall. However, MCI remains the most challenging class for the model to classify, with high precision but low recall. This indicates that many MCI cases are misclassified as either CN or Dementia. While DX_bl is a highly predictive feature for the final diagnosis, the model still struggles to effectively differentiate MCI from the other categories.

D. Baseline Data Analysis and Prediction

Baseline data analysis can provide valuable insights and contribute to improving predictions. Among the diagnostic groups, Cognitively Normal (CN) and Alzheimer's Disease (AD) dominate the baseline dementia diagnoses. This analysis specifically compares these two groups with respect to key variables, such as CDRSB (Cognitive Dementia Rating Sum of Boxes) and PTAU_bl (Phosphorylated Tau at baseline). Using the Mann-Whitney U test, a non-parametric test suitable for comparing two independent samples, the following results were obtained:

CDRSB: The p-value was effectively 0, indicating a highly significant difference in cognitive scores between the CN and AD groups.

PTAU_bl: The p-value was 0.0001, also showing a highly significant difference in phosphorylated tau levels between the two groups. These findings suggest that both cognitive scores (CDRSB) and biomarker levels (PTAU_bl) are significantly different between CN and AD groups, consistent with established Alzheimer's research. The Mann-Whitney U test for ABETA levels yielded a p-value of <0.0001, further confirming a significant difference between CN and AD groups. This result aligns with the well-documented role of amyloid-beta in Alzheimer's disease pathology. Similarly, for MMSE (Mini-Mental State Examination), the p-value was <0.0001, indicating that AD participants had significantly lower MMSE scores, reflecting more severe cognitive impairment. The same was observed for MOCA (Montreal Cognitive Assessment), where the p-value was 0.0001, demonstrating a significant difference in MOCA scores between CN and AD groups.

The analysis of neuroimaging biomarkers, such as FDG (Fluorodeoxyglucose PET) and AV45 (Amyloid PET), also revealed significant differences. The p-value for FDG PET was 0.0001, indicating that brain glucose metabolism, as measured by FDG PET, is significantly lower in individuals with AD. Similarly, AV45 PET, which measures amyloid accumulation, showed a p-value of 0.0001, confirming higher amyloid levels

in the AD group. These findings underscore the significant differences in neuroimaging biomarkers between CN and AD groups.

Regarding the APOE4 genotype distribution, the results highlight the strong association between APOE4 and Alzheimer's risk. Among individuals with AD, 47.7% had one copy of the APOE4 allele, 21.2% had two copies, and 31.1% had no copies. In contrast, among CN individuals, 72.6% had no copies, 25.4% had one copy, and only 2% had two copies. These distributions confirm the well-established link between APOE4 and increased Alzheimer's risk, with individuals carrying one or two APOE4 alleles being significantly more likely to develop the disease.

Examining the impact of APOE4 status on biomarkers and cognitive scores provides additional insights into how this genetic risk factor influences Alzheimer's pathology. Individuals without APOE4 alleles had the highest average ABETA levels (990), while those with two alleles had the lowest (521), consistent with APOE4's role in promoting amyloid accumulation. Similarly, TAU and PTAU levels were progressively higher in individuals with more APOE4 alleles. Those with two alleles had the highest TAU (363) and PTAU (35), reflecting greater neurofibrillary pathology. Cognitive function, as measured by MMSE, decreased with the number of APOE4 alleles, with individuals carrying two alleles having the lowest average MMSE score (24.5). The CDRSB score, indicating cognitive impairment, increased with the number of APOE4 alleles.

These findings demonstrate that APOE4 is strongly associated with greater amyloid and tau pathology and more severe cognitive decline. The relationship between APOE4 status, biomarkers, and cognitive scores underscores the genetic influence on Alzheimer's disease progression.

E. Neural Network Prediction Models

The results of the models developed in this study, particularly the LSTM model, were evaluated using the ADNI dataset. Performance metrics included accuracy, precision, recall, and F1-score. The model achieved a Validation Loss of 0.369 and a Validation Accuracy of 84.5%, with an overall Accuracy of 84.5%. A detailed classification report is presented in Table I, while the confusion matrix is illustrated in Fig. 3, providing further insights into the model's performance across diagnostic categories.

TABLE I. PERFORMANCE MATRIX FOR LSTM-BASED MODEL

	precision	Recall	F1-score
CN	0.84	0.81	0.83
Dementia	0.79	0.80	0.80
MCI	0.86	0.87	0.87
Accuracy	0.84		
macro avg.	.83	.83	.83
Weighted avg	0.84	0.84	.84

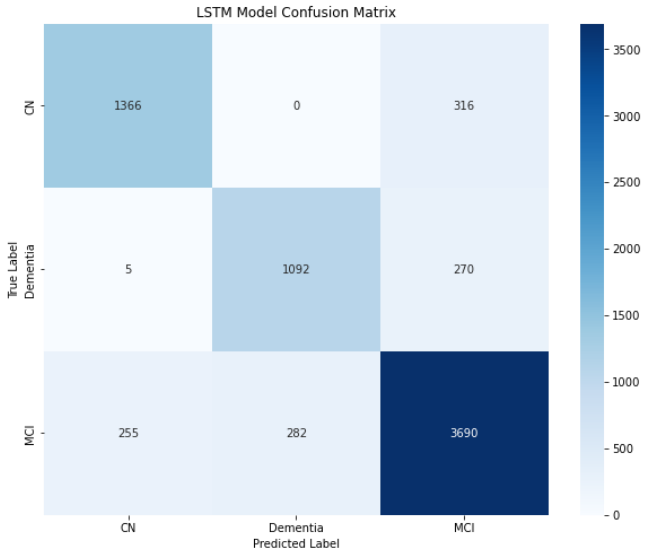


Fig. 3. Confusion matrix for LSTM-based model.

It was observed that the features illustrated in Fig. 4 contribute significantly more to predicting Alzheimer's disease compared to other features. Among these, MMSE_bl (baseline Mini-Mental State Examination) and MMSE_fu (follow-up Mini-Mental State Examination) showed the greatest contribution, highlighting their critical role in the predictive model.

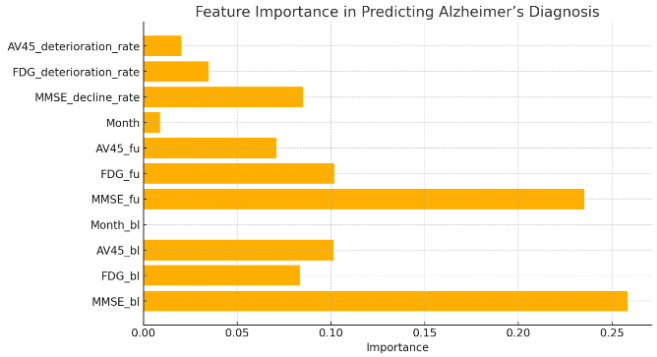


Fig. 4. The important features in predicting Alzheimer.

Additional models were explored using baseline information, including Gradient Boosting and Support Vector Machine (SVM). The Gradient Boosting model achieved an impressive 96% accuracy on the test set, with perfect precision, recall, and F1-scores for both the Cognitively Normal (CN) and Alzheimer's Disease (AD) groups. Similarly, the SVM classifier performed exceptionally well, achieving 95% accuracy on the test set and perfect scores across all performance metrics. These results demonstrate the strong predictive capabilities of both models when using baseline data.

F. Evaluating Model Performance Longitudinally

To assess longitudinal performance, the model's ability to predict changes in cognitive scores, imaging biomarkers, or diagnoses over time was evaluated. This involved two main aspects:

Predicting Cognitive Decline: The model was used to predict future cognitive scores based on baseline data and observed longitudinal trends.

Evaluating Model Stability: The model's predictive accuracy was tested across multiple visits for the same individuals to determine its consistency over time.

The analysis began with visualizing interactions among key features, followed by evaluating longitudinal performance. A heatmap (Fig. 5) illustrates the correlations between key features. Notably, the MMSE Decline Rate is negatively correlated with both MMSE at Baseline and FDG (Fluorodeoxyglucose PET), indicating that as cognitive function declines, brain metabolism also tends to decrease. In contrast, AV45 (Amyloid PET) shows a weaker correlation with other features, highlighting its specific role in amyloid accumulation, which is less directly tied to immediate cognitive decline. These findings underscore the nuanced relationships between cognitive decline, biomarkers, and brain function over time.

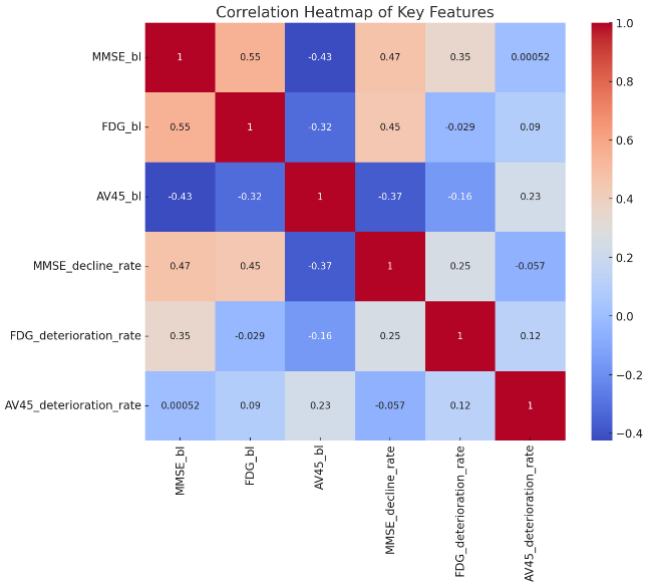


Fig. 5. Correlation of heatmap of key features (baseline features).

The model's ability to predict cognitive decline, such as changes in MMSE scores over time, was evaluated using baseline data. The assessment focused on how well the model predicts cognitive decline across multiple visits. A linear regression model, which used baseline features including MMSE, FDG, and AV45, achieved a Mean Squared Error (MSE) of approximately 0.01. This indicates that the model performed reasonably well in predicting cognitive decline over time. The low error suggests the model has potential for forecasting Alzheimer's progression, though further refinement and validation on larger datasets could improve its accuracy and robustness.

When a more advanced regression method, such as Gradient Boosting, was applied to refine the longitudinal model, it achieved an MSE of 0.0121. While the Gradient Boosting model captured some patterns in the data, its slightly higher MSE suggests that the simpler linear regression model performed better for this specific task.

Fig. 6 visualizes the relationship between predicted and actual MMSE decline rates. The scatter plot includes a red dashed line representing ideal predictions, where predicted values perfectly match the actual values. Most predictions were reasonably close to the actual values, with some variability, which is expected in longitudinal predictions. These findings demonstrate the model's promise in predicting cognitive decline over time while highlighting areas for further improvement in longitudinal performance. The same analysis used to predict cognitive decline was applied to forecast imaging deterioration over time, focusing on FDG (glucose metabolism) and AV45 (amyloid accumulation). Baseline features such as FDG_bl, AV45_bl, and MMSE_bl were utilized to predict changes in FDG and AV45 over time. Gradient Boosting Regression was employed for both tasks, demonstrating strong performance in predicting longitudinal imaging changes.

For FDG deterioration rate prediction, the model achieved a Mean Squared Error (MSE) of 0.000006, indicating excellent accuracy in forecasting changes in glucose metabolism over time. Similarly, for AV45 deterioration rate prediction, the MSE was 0.000028, showing the model's effectiveness in predicting changes in amyloid accumulation. These low error rates suggest that the model performs well for both imaging biomarkers, making it a valuable tool for tracking Alzheimer's progression longitudinally. Visualization of the results further supports the model's effectiveness. In Fig. 7, the scatter plot illustrates the predicted vs. actual FDG deterioration rates, with most points closely aligned with the ideal prediction line (red dashed line), indicating strong predictive performance. Similarly, Fig. 8 shows the predicted vs. actual AV45 deterioration rates, with most points clustering near the ideal line, demonstrating the model's capability to accurately forecast amyloid accumulation changes.

Overall, the models effectively predict longitudinal changes in both FDG and AV45 imaging biomarkers, which are critical for monitoring Alzheimer's disease progression over time. These results highlight the utility of Gradient Boosting Regression in capturing complex patterns in imaging data.

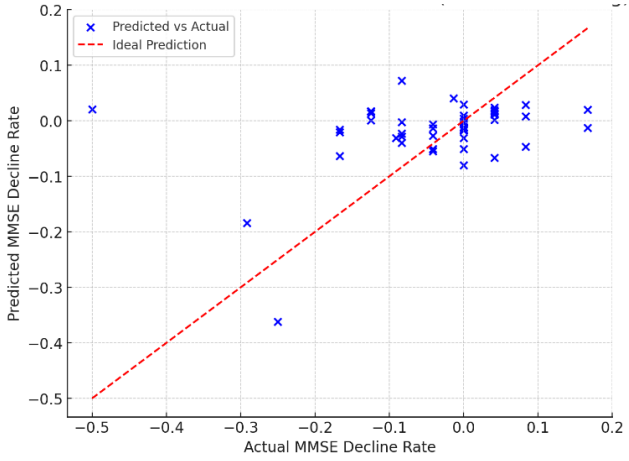


Fig. 6. Predicted vs. Actual MMSE Decline Rate (Gradient Boosting).

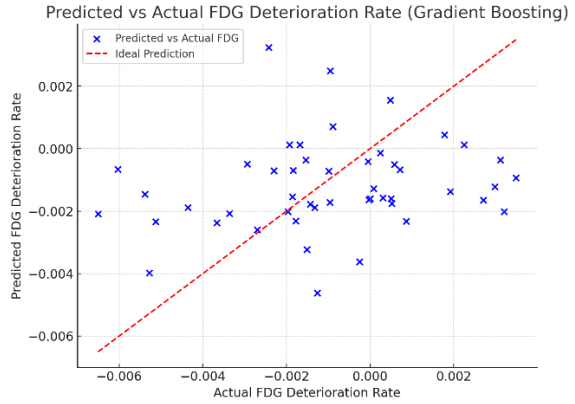


Fig. 7. Predicted vs. Actual FDG Deterioration Rate (using Gradient Boosting).

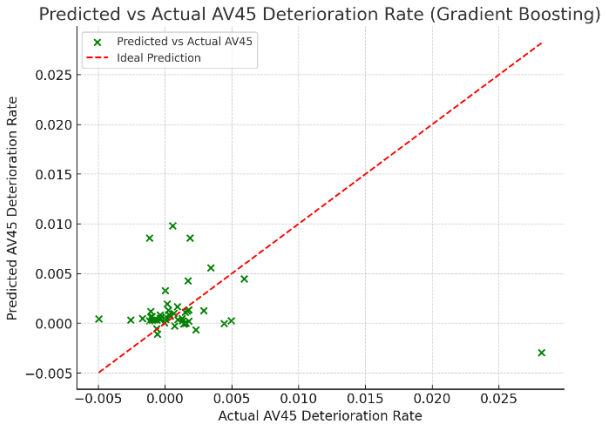


Fig. 8. Predicted vs. Actual AV45 Deterioration Rate (using Gradient Boosting).

We explored additional derived features by combining cognitive scores and biomarkers to create new indicators of Alzheimer's progression. Investigating interactions between longitudinal features and temporal patterns revealed deeper insights into disease progression. These derived features were designed to capture more complex relationships between cognitive and biomarker data. The newly created features included:

MMSE_TAU Interaction: A combination of baseline MMSE and FDG values to assess the relationship between cognitive function and brain metabolism.

ABETA_TAU Ratio: A ratio of amyloid (AV45) to glucose metabolism (FDG) to highlight the balance between amyloid accumulation and metabolic activity.

Combined Decline Rate: The sum of MMSE and FDG deterioration rates, providing a measure of overall cognitive and metabolic decline.

Using cross-validation, the performance of models with these derived features was evaluated. The Random Forest model achieved an accuracy of 97.46%, slightly outperforming the other models. The Gradient Boosting model achieved an accuracy of 96.83%, while the Support Vector Machine (SVM) reached 96.21%. All three models demonstrated strong predictive performance, with Random Forest showing a marginal advantage. These results highlight the potential of derived features in enhancing model performance by capturing intricate relationships between cognitive and biomarker data. This approach emphasizes the value of feature engineering in advancing the predictive capabilities of machine learning models for Alzheimer's progression.

G. *Few-shot LLMs*

Regarding the results of the experiment with few-shot training, we employed Large Language Models (LLMs), specifically ChatGPT 3.5, instead of LSTM models. The results demonstrated a significant improvement over LSTM, with the following performance metrics: Accuracy: 0.97, Precision: 0.97, Recall: 0.97, and F1-Score: 0.97. The confusion matrix is presented in Fig. 4. To evaluate the diagnostic performance of the model, we used Receiver Operating Characteristic (ROC) curves for various clinical conditions, as shown in Fig. 9. The ROC curve provides a graphical representation of the model's ability to discriminate between diagnostic categories by plotting the true positive rate (sensitivity) against the false positive rate (1-specificity) across different threshold settings. The model demonstrated excellent discriminatory ability across all diagnostic categories. The Area Under the Curve (AUC) for the ROC of Cognitively Normal (CN) subjects was 0.98, indicating a high level of accuracy in distinguishing CN individuals from those with cognitive impairment. Similarly, the ROC curve for dementia yielded an AUC of 0.99, reflecting outstanding performance in identifying subjects with dementia. For Mild Cognitive Impairment (MCI), the ROC curve achieved an AUC of 0.98, signifying robust capability in differentiating MCI from other conditions.

The high AUC values for CN, dementia, and MCI underscore the exceptional performance of our model in correctly classifying individuals into their respective diagnostic categories. These findings highlight the potential of our approach in supporting early and accurate diagnosis of Alzheimer's disease and related cognitive disorders. The results demonstrate that few-shot training with LLMs like ChatGPT 3.5 can provide significant advancements in diagnostic modeling, offering reliable and efficient tools for clinical applications.

V. Discussion

The ADNI dataset is regularly updated as more participants engage in studies on dementia progression. This work utilized the latest version of the dataset, published in 2024, which includes detailed information on assessments conducted during each patient visit. It was observed that machine learning models achieved high accuracy when predicting the baseline dementia stage using baseline information. However, their performance declined when tasked with predicting the dementia stage for each subsequent visit, highlighting the challenges associated with longitudinal predictions. When exploring neural networks and deep learning, the results of this study underscore the significant potential of integrating numerical and textual data from the ADNI dataset to develop highly accurate predictive models for Alzheimer's disease and related cognitive disorders. By leveraging the extensive cognitive assessments, biomarkers, and demographic data available in ADNI, our approach illustrates how comprehensive datasets can enhance diagnostic

accuracy. The inclusion of varied data types enables a multifaceted analysis, which is essential for understanding the complex progression of Alzheimer's disease. This integrative approach not only improves model performance but also provides deeper insights into the factors driving cognitive decline, reinforcing the value of holistic data utilization in Alzheimer's research.

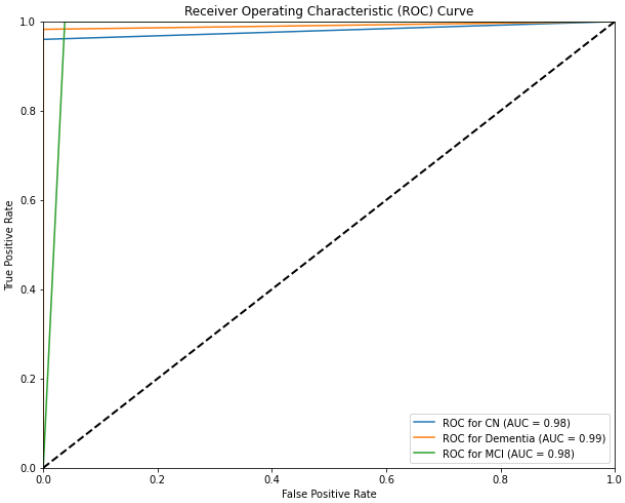


Fig. 9. ROC for the ChatGPT 3.5 after been few-shot training.

In the introduction, we highlighted the projected increase in Alzheimer's disease prevalence, with estimates suggesting that 152 million people globally will be affected by 2050. This alarming trend underscores the urgent need for effective diagnostic tools that facilitate early detection and intervention. The current study addresses this need by leveraging the extensive ADNI dataset, which includes diverse data such as cognitive test scores (e.g., MMSE, RAVLT), biomarker levels (e.g., amyloid-beta, tau proteins), and demographic information (e.g., age, gender, race, education). These features have been shown to significantly contribute to predicting clinical status, as noted by Banerjee (2020) and Tian et al. (2023).

The literature review emphasized the limitations of relying solely on imaging techniques for Alzheimer's diagnosis, such as the high cost and limited accessibility of MRI and PET scans. Previous studies, such as Balakrishnan et al. (2023), predominantly focused on MRI images, underutilizing the full spectrum of data available in ADNI. Our study addresses this gap by integrating numerical and textual data, offering a more holistic and cost-effective approach to Alzheimer's diagnosis. This aligns with findings by Feng et al. (2023), who demonstrated the efficacy of combining imaging and phenotype data with large language models (LLMs).

The application of LLMs, such as ChatGPT 3.5, significantly improved classification performance in this study. LLMs enable rapid processing and analysis of large datasets, achieving high accuracy in classification tasks. Our findings show that LLMs can accurately distinguish between cognitively normal individuals, those with mild cognitive impairment (MCI), and those with dementia. Specifically, the ROC curves for cognitively normal (CN) subjects, dementia, and MCI exhibited AUC values of 0.98, 0.99, and 0.98, respectively. These high AUC values highlight the robustness of LLMs in classifying different stages of cognitive impairment, thereby supporting early and precise diagnoses.

Genetics, a significant contributor to Alzheimer's disease risk (accounting for approximately 70% of overall risk), was also incorporated into our predictive models, as suggested by Raj et al. (2024). The importance of genetic data is underscored in this study, complementing other features. Furthermore, the literature review highlighted the effectiveness of speech analysis and text mining in detecting Alzheimer's disease. Studies by Agbavor and Liang (2022) and Colla et al. (2022) demonstrated the utility of LLMs in analyzing spontaneous speech and text data, aligning with our approach of utilizing LLMs to process numerical and textual data from ADNI.

The contribution of this work lies in demonstrating that LLMs provide not only a rapid and effective approach to classification tasks but also maintain high accuracy, making them valuable tools in clinical settings. This study fills a critical gap in existing research by focusing on the integration of textual and numerical data from ADNI, rather than relying solely on imaging data. By doing so, we offer a cost-effective alternative that reduces dependence on expensive and less accessible imaging techniques. The ability to utilize readily available data to achieve reliable diagnostic outcomes represents a significant advancement, paving the way for more accessible and scalable solutions in Alzheimer's disease detection.

Future research can expand the scope of Alzheimer's prediction beyond image analysis by incorporating a broader range of patient data, such as clinical notes, genetic information, and cognitive test results. This approach has the potential to lead to more comprehensive and accurate prediction models, facilitating earlier detection and enabling more personalized treatment strategies for patients with Alzheimer's disease.

In conclusion, this study highlights the transformative potential of LLMs in utilizing diverse datasets to enhance diagnostic accuracy for Alzheimer's disease. By integrating cognitive assessments, biomarkers, demographic data, and genetic information, our approach offers a comprehensive and efficient diagnostic tool. The findings emphasize the importance of multi-modal data integration and advanced machine learning techniques in addressing the growing challenge of Alzheimer's disease diagnosis and management.

VI. CONCLUSION

This study demonstrates the significant potential of integrating numerical and textual data from the Alzheimer's Disease Neuroimaging Initiative (ADNI) dataset to develop highly accurate predictive models for Alzheimer's disease and related cognitive disorders. By leveraging a comprehensive range of features, including cognitive assessments, biomarkers, demographic information, and genetic data, this approach provides a robust and holistic method for early diagnosis.

The findings underscore the utility of large language models (LLMs), such as ChatGPT 3.5, in processing and analyzing complex datasets. LLMs exhibited exceptional performance in classification tasks, achieving high accuracy rates and rapid processing times. Specifically, the ROC curves for cognitively

normal (CN) subjects, dementia, and mild cognitive impairment (MCI) yielded AUC values of 0.98, 0.99, and 0.98, respectively. These results highlight the efficacy of LLMs in distinguishing between different stages of cognitive impairment, thereby supporting early and precise diagnosis.

This study addresses a critical gap in existing research by focusing on the integration of numerical and textual data rather than relying solely on imaging data. This approach provides a cost-effective alternative, reducing dependence on expensive and less accessible imaging techniques. Utilizing readily available data to achieve reliable diagnostic outcomes represents a significant advancement, paving the way for more accessible and scalable solutions for Alzheimer's disease detection. Additionally, the inclusion of genetic information aligns with findings from previous studies that emphasize the importance of understanding the genetic basis of Alzheimer's disease. By incorporating diverse data types, the proposed models offer a more comprehensive analysis, improving prediction accuracy and supporting targeted interventions.

The transformative potential of combining multi-modal data with advanced machine learning techniques is a key contribution of this work. Integrating ADNI's rich dataset with LLMs offers a promising approach to enhancing diagnostic accuracy and efficiency. Beyond Alzheimer's disease, this work provides a framework for leveraging diverse datasets to address other complex medical conditions. Future research should focus on further integrating various data types and exploring advanced machine learning models to enhance diagnostic capabilities and improve patient outcomes.

REFERENCES

[1] S. Raj, A. Vishnoi, and A. Srivastava, "Classify Alzheimer genes association using Naïve Bayes algorithm," *Human Gene*, 2024, Art no. 201309, doi: https://doi.org/10.1016/j.humgen.2024.201309.

[2] M. Alwuthaynani, M, Z. Abdallah, S, and R. Santos-Rodriguez, "Transfer Learning and Class Decomposition for Detecting the Cognitive Decline of Alzheimer Disease," *arXiv*, 2023, doi: 10.48550/arXiv.2301.13504.

[3] K. Ong, Tzu-iunn *et al.*, "Evidence-empowered transfer learning for Alzheimer's disease," *techrxiv*, 2023, doi: 10.36227/techrxiv.22199635.v1.

[4] A. Aviles-Rivero, I, C. Runkel, N. Papadakis, Z. Kourtzi, and C.-B. Schönlieb, "Multi-Modal Hypergraph Diffusion Network With Dual Prior For Alzheimer Classification," presented at the 25th International Conference on Medical Image Computing and Computer Assisted Intervention – MICCAI, Singapore, Singapore, 2022.

[5] M. Memon, Hammad "Early Stage Alzheimer's Disease Diagnosis Method," presented at the 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 2019.

[6] G. Lee, K. Nho, B. Kang, K.-A. Sohn, and D. Kim, "predicting Alzheimer's disease progression using multi-modal deep learning approach," *Scientific Report*, vol. 2019, no. 9, 2019, doi: https://doi.org/10.1038/s41598-018-37769-z.

[7] K. Aderghal, A. Khvostikov, A. Krylov, J. Benois-Pineau, K. Afdel, and G. Catheline, "Classification of alzheimer disease on imaging modalities with deep cnns using cross-modal transfer learning," presented at the 2018 IEEE 31st International Symposium on Computer-Based Medical Systems (CBMS, 2018

[8] A. Khvostikov, K. Aderghal, J. Benois-Pineau, A. Krylov, and G. Catheline, "3D CNN-based classification using sMRI and MD-DTI images for Alzheimer disease studies," *ArXiv*, 2018.

[9] G. Awate, "Detection of Alzheimers Disease from MRI using Convolutional Neural Networks, Exploring Transfer Learning And BellCNN," *ArXiv*, vol. abs/1901.10231, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:59336290.

[10] Y. Gao, H. Huang, and L. Zhang, "Predicting Alzheimer's Disease Using 3DMgNet," *arXiv e-prints*, p. arXiv:2201.04370, 2022.

[11] M. Fareed, Muhammad, Sadiq *et al.*, "ADD-Net: An Effective Deep Learning Model for Early Detection of Alzheimer Disease in MRI Scans," *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3204395.

[12] S. Shah and M. Shah, "The Effects of Machine Learning Algorithms in Magnetic Resonance Imaging (MRI), and Biomarkers on Early Detection of Alzheimer's Disease," *Advances in Biomarker Sciences and Technology*, 2024, doi: https://doi.org/10.1016/j.abst.2024.08.004.

[13] P. Cao, X. Shan, D. Zhao, M. Huang, and O. Zaiane, "Sparse shared structure based multi-task learning for MRI based cognitive performance prediction of Alzheimer's disease," *Pattern Recognition*, vol. 72 no. 2017, pp. 219–235, 2017.

[14] M. El-Yacoubi, A, S. Garcia-Salicetti, C. Kahindo, A. Rigaud, S, and V. Cristancho-Lacroix, "From aging to early-stage Alzheimer's: uncovering handwriting multimodal behaviors by semi-supervised learning and sequential representation learning," *Pattern Recognition*, vol. 86, pp. 112–133, 2019.

[15] L. ı. Go´mez-Zaragoza´, S. Wills, C. Tejedor-Garcia, J. Mar´ın-Morales, M. Alcan˜iz, and H. Strik, "Alzheimer Disease Classification through ASR-based Transcriptions: Exploring the Impact of Punctuation and Pauses," presented at the Interspeech 2023, Dublin, Ireland, 2023.

[16] B. Dubois *et al.*, "Research criteria for the diagnosis of Alzheimer's disease: revising the NINCDS-ADRDA criteria," *Lancet Neurol*, vol. 6, no. 8, pp. 734–746, 2007.

[17] S. Haj Zargarbashi, Soroush and B. Bagher, "A Multi-Modal Feature Embedding Approach to Diagnose Alzheimer Disease from Spoken Language," *arXiv*, 2019.

[18] B. Yu, X, B, Y. Liu, K. Chan, C, C, Q. Yang, and X. Wang, "Skeleton-based human action evaluation using graph convolutional network for monitoring Alzheimer's progression," *Pattern Recognition*, vol. 119, p. 108095, 2021, doi: https://doi.org/10.1016/j.patcog.2021.108095.

[19] S. Doering *et al.*, "Deconstructing pathological tau by biological process in early stages of Alzheimer disease: a method for quantifying tau spatial spread in neuroimaging," *eBioMedicine*, 2024, doi: https://doi.org/10.1016/j.ebiom.2024.105080.

[20] B. Reisberg, S. Ferris, H, M. de Leon, J, and T. Crook, "The global deterioration scale for assessment of primary degenerative dementia," *Am. J. Psychiatry*, 1982.

[21] D. Agarwal, M. Berbís, Álvaro, A. Luna, V. Lipari, J. Ballester, Brito, and I. de la Torre-Díez, "Automated Medical Diagnosis of Alzheimer´s Disease Using an Efficient Net Convolutional Neural Network," *Journal of Medical Systems*, 2023, doi: https://doi.org/10.1007/s10916-023-01941-4.

[22] F. Alghamedy, H, M. Shafiq, L. Liu, A. Yasin, R. Khan, Ali, and H. Mohammed, Sobahi, "Machine Learning-Based Multimodel Computing for Medical Imaging for Classification and Detection of Alzheimer Disease," *Computational Intelligence and Neuroscience*, 2022, doi: https://doi.org/10.1155/2022/9211477.

[23] A. Beck, G. Emery, and R. Greenberg, *Anxiety Disorders and Phobias. A Cognitive Perspective*. New York: Basic Books, 1985.

[24] L. Chen, S. Ho, S, and M. Lwin, O "A meta-analysis of factors predicting cyberbullying perpetration and victimization: From the social cognitive and media effects approach," *New Media & Society*, vol. 19, no. 8, pp. 1-20, 2017.

[25] M. Eysenck, W and M. Keane, T, *Cognitive psychology: A student's handbook (6th ed.)*. New York: Psychology Press, 2010.

[26] E. Nichols and T. Vos, "The estimation of the global prevalence of dementia from 1990–2019 and forecasted prevalence through 2050: An analysis for the global burden of disease (GBD) study 2019," *Alzheimer's Dementia*, vol. 17, no. 10, pp. e105–e125, 2021.

[27] E. Goetzl, J, "Current Developments in Alzheimer's Disease: Developments in Alzheimer's Disease," *The American Journal of Medicine*, 2024, doi: https://doi.org/10.1016/j.amjmed.2024.08.019.

[28] A. Tufail, B, Y. Ma, -K, and Q. Zhang, -N, "Binary classification of Alzheimer's disease using sMRI imaging modality and deep learning," *J. Digit. Imag.*, vol. 33, no. 5, pp. 1073–1090, 2020.

[29] N. Balakrishnan, Bini, P. Sreeja, S, and J. Panackal, Jose, "Alzheimer's Disease Diagnosis using Machine Learning: A Review," *International Journal of Engineering Trends and Technology*, vol. 71, no. 3, pp. 120-129, 2023, doi: https://doi.org/10.14445/22315381/IJETT-V71I3P213.

[30] T. Tuan, Anh, T. Pham, Bao, J. Kim, Young, and J. Tavares, Manuel, R, S, "Alzheimer's diagnosis using deep learning in segmenting and classifying 3D brain MR images," *Int J Neurosci.*, vol. 132, no. 7, pp. 689-698, 2022, doi: 10.1080/00207454.2020.1835900.

[31] M. Dyrba *et al.*, "Robust Automated Detection of Microstructural White Matter Degeneration in Alzheimer's Disease Using Machine Learning Classification of Multicenter DTI Data," *Plos One*, vol. 8, no. 5, 2013, doi: 10.1371/journal.pone.0064925.

[32] J. Liu, M. Li, Y. Luo, S. Yang, W. Li, and Y. Bi, "Alzheimer's Disease Detection Using Depthwise Separable Convolutional Neural Networks," *Computer Methods and Programs in Biomedicine*, vol. 203, 2021, doi: https://doi.org/10.1016/j.cmpb.2021.106032.

[33] M. Taghvaei *et al.*, "Impact of white matter hyperintensities on structural connectivity and cognition in cognitively intact ADNI participants," *Neurobiology of Aging*, vol. 135, no. 2024, pp. 79-90, 2024, doi: https://doi.org/10.1016/j.neurobiolaging.2023.10.012.

[34] D. Hernández, S. Schlicht, Morgan , J. Clarke, Elli, M. Daniszewski, and C. Karch, M, "Generation of a gene-corrected human isogenic iPSC line from an Alzheimer's disease iPSC line carrying the PSEN1 H163R mutation," *Stem Cell Research*, vol. 79, 2024, Art no. 103495, doi: https://doi.org/10.1016/j.scr.2024.103495.

[35] H. Cai *et al.*, "Exploring Multimodal Approaches for Alzheimer's Disease Detection Using Patient Speech Transcript and Audio Data," *arXiv*, 2023, doi: https://doi.org/10.48550/arXiv.2307.02514.

[36] V. Vincze *et al.*, "Linguistic Parameters of Spontaneous Speech for Identifying Mild Cognitive Impairment and Alzheimer Disease," *Computational Linguistics*, vol. 48, no. 1, 2022, doi: https://doi.org/10.1162/COLI.a.00428.

[37] D. Colla, M. Delsanto, M. Agosto, B. Vitiello, and D. Radicioni, P, "Semantic coherence markers: The contribution of perplexity metric," *Artificial Intelligence in Medicine*, vol. 134, no. 102393, 2022, doi: https://doi.org/10.1016/j.artmed.2022.102393.

[38] A. Esteva *et al.*, "A guide to deep learning in healthcare," *Nature Medicine*, vol. 25, no. 1, pp. 24-29, 2019, doi: 10.1038/s41591-018-0316-z.

[39] Y. Wang *et al.*, "Exploiting prompt learning with pre-trained language models for Alzheimer's Disease detection," *arXiv*, 2023, doi: https://doi.org/10.48550/arXiv.2210.16539.

[40] Y. Kim and H. Lee, "PINNet: a deep neural network with pathway prior knowledge for Alzheimer's disease," *Front. Aging Neurosci.*, vol. 15, 2023, doi: https://doi.org/10.3389/fnagi.2023.1126156.

[41] N. Singh, D. Patteshwari, N. Soni, and A. Kapoor, "Automated detection of Alzheimer disease using MRI images and deep neural networks- A review," *arXiv:2209.11282* 2022, doi: https://doi.org/10.48550/arXiv.2209.11282.

[42] A. Essemlali, E. St-Onge, M. Descoteaux, and P.-M. Jodoin, "Understanding Alzheimer disease's structural connectivity through explainable AI," presented at the Machine Learning Research, 2020.

[43] F. Agbavor and H. Liang, "Predicting dementia from spontaneous speech using large language models," *PLOS Digital Health* vol. 1, no. 12, 2022, Art no. e0000168, doi: https://doi.org/10.1371/journal.pdig.0000168.

[44] Y. Feng, J. Wang, X. Gu, X. Xu, and M. Zhang, "Large language models improve Alzheimer's disease diagnosis using multi-modality data," *arXiv:2305.19280* 2023, doi: https://doi.org/10.48550/arXiv.2305.19280.

[45] H. Musto, D. Stamate, I. Pu, and D. Stahl, "Predicting Alzheimer's Disease Diagnosis Risk over Time with Survival Machine Learning on the ADNI Cohort," *arXiv*, 2023, doi: https://doi.org/10.48550/arXiv.2306.10326.

[46] A. Banerjee, "Machine Learning for Health: Personalized Models for Forecasting of Alzheimer Disease Progression," Master, Department of Computing, Imperial College London, London, UK, 1, 2020.

[47] G. Tian, J. Hanfelt, J. Lah, J, and B. Risk, "Mixture of regressions with multivariate responses for discovering subtypes in Alzheimer's biomarkers with detection limits," *arXiv*, 2023, doi: 10.48550/arXiv.2303.00715.

[48] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997, doi: https://doi.org/10.1162/neco.1997.9.8.1735.

[49] K. Greff, R. Srivastava, Kumar , J. Koutník, B. Steunebrink, R, and J. Schmidhuber, "LSTM: A Search Space Odyssey," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 28, no. 10, pp. 2222-2232, 2017.

[50] F. Gers, A, J. Schmidhuber, and F. Cummins, "Learning to forget: continual prediction with LSTM," presented at the Ninth International Conference on Artificial Neural Networks ICANN 99, Edinburgh, UK, 2000.

[51] I. Goodfellow, Y. Bengio, and A. Courville, "Chapter 6: Sequence Modeling," in *Deep Learning*: MIT Press, 2016.

[52] C. Bishop, M, "Chapter 4: Classification and Loss Functions," in *Pattern Recognition and Machine Learning*: Springer, 2006.

Visual Recognition and Localization of Industrial Robots Based on SLAM Algorithm

Wei Cui[1]*, Yuefan Zhao[2], Litao Sun[3]
Department of Electrical Engineering, Hebei Institute of Mechanical and Electrical Technology, Hebei 054000, China[1, 3]
Department of Mechanical Engineering, Hebei Institute of Mechanical and Electrical Technology, Hebei 054000, China[2]

Abstract—The front-end feature matching module of traditional SLAM systems is characterized by sparse or dense feature points, it is difficult to generate accurate camera trajectory and scene reconstruction results, in response to this problem, the author studied a fast reconstruction algorithm for any path based on V-SLAM, by using improved feature matching algorithms to accurately match feature points, the accuracy of scene sparse reconstruction and camera trajectory recovery has been improved, the backend optimization thread adopts segmented optimization matching to reduce the computational burden of reconstruction, and the performance of the V-SLAM system was improved through parallel processing, the matching results and camera trajectory error comparison results showed that the improved V-SLAM algorithm can quickly recover camera trajectory and scene reconstruction, with the development of multi-sensor collaborative coupling and multi view fusion technology, the V-SLAM method proposed by the author can add virtual 3D objects to real scenes, and the V-SLAM system can extract feature points in the screen in real-time and detect planar objects in the scene, ensure that multiple virtual objects in the scene meet geometric consistency with the actual scene, in the experiment, two objects were added to the virtual scene, users can interactively scale objects and add them without being affected by camera movements, ensuring consistency between objects and the real scene.

Keywords—SLAM algorithm; industrial robot; visual recognition; location

I. INTRODUCTION

The positioning and map creation of mobile robots are hot research topics in the field of robotics, and are also important links in navigation. There are already some practical solutions for autonomous localization of robots in known environments and map creation of known robot positions [1]. However, in many environments, robots cannot use global positioning systems for localization, and obtaining a map of the robot's working environment in advance is also difficult, or even impossible. At this point, the robot needs to create a map in a completely unknown environment with its own position uncertain, and simultaneously use the map for autonomous positioning and navigation, as well as positioning and mapping [2]. Assuming that the robot is moving in a completely unknown environment, executing control commands and observing the characteristics of the environment, both the control and observation quantities will be affected by noise interference, SLAM is the restoration of robot path and environmental feature information from a series of noisy variables. If the path of the robot is determined (such as GPS positioning), then it is a problem of building a map, where the position of the target in the environment is estimated using an independent filter; When the robot's path is unknown, the robot's path is related to the error of the map, so, the state information and map information of the robot must be estimated simultaneously. The SLAM problem includes four basic aspects: (1) How to describe the environment, the representation method of environmental maps; (2) How to obtain environmental information, robots roam the environment and record sensor perception data, which involves the problem of robot localization and environmental feature extraction; (3) How to represent the obtained environmental information and update the map based on the environmental information requires addressing the description and processing methods of uncertain information; (4) Develop stable and reliable SLAM methods. The SLAM algorithm has many important attributes that affect the uncertainty in map features and robot position estimation, including the convergence of state estimation, the data consistency of the estimation process, and the computational complexity of updating the state covariance matrix. Convergence of state estimation: As the number of observations increases, in order to reduce the uncertainty of map estimation to a limited range, the convergence of state estimation must be maintained. Firstly, the accuracy of the map is related to the position accuracy of the robot when the first environmental feature is observed, so it is necessary to ensure the convergence of the state matrix when the first environmental feature is observed [3-4]; Secondly, the update of the state covariance matrix after each measurement must be convergent relative to the matrix before the update [5]; Finally, in extreme cases, as the number of observations increases, the feature estimation becomes completely correlated. As long as these are ensured, the relationship between map features is completely determined. Consistency of data association: Data association is the key to data fusion. In the SLAM process, data association mainly completes two tasks: Detection of new environmental features and feature matching. If the data association is not accurate, it will lead to filter divergence, which has a particularly prominent impact on EKF based methods. In order to maintain the consistency of SLAM, it is necessary to update the state covariance matrix. The observation of the environment is relative to robots, so any errors in robot estimation are related to errors in map estimation. In the absence of information about the robot's position and its environmental characteristics, in order to keep the error of system state estimation within a limited range, it is necessary to maintain the consistency of state estimation. Therefore, it is necessary to update the covariance matrix between the robot states and environmental features in real-time. The scene perception effect of traditional SLAM relies on

*Corresponding Author.

radar or laser sensors and is easily affected by acquisition noise, so sometimes the scene reconstruction and perception effect are not ideal. When the scene contains objects with too single or too complex features, inter frame feature matching is too sparse or too dense, uneven allocation, and affects scene perception, bringing additional computational pressure to backend scene optimization [6]. The author uses visual sensors as the main sensing device to estimate the camera position and the V of the environment in which it is located_ SLAM (Vision based SLAM) group technology, by improving the matching algorithm and backend optimization strategy of SLAM front-end threads, V-SLAM has good scalability, flexibility, and can be applied to large-scale scene perception. The improved V-SLAM can add virtual objects to the scene in real-time, providing users with an intuitive and real-time visual experience, expressing AR effects, and obtaining real-time device parameters and posture determination play an important role in the SLAM system. The global positioning system (GPS) can greatly reduce its positioning accuracy in indoor environments or when signals are severely obstructed; Placing sensors that receive signals in specific indoor environments can obtain rich data and greatly improve positioning accuracy, but it requires pre-arranged usage scenarios and does not have good flexibility and adaptability; Lidar systems are difficult to popularize due to their high cost. V-SLAM has significant advantages in scenario adaptability, scalability, and low cost [7]. V-SLAM has natural advantages in augmented reality positioning solutions, the improved V-SLAM proposed by the author can add virtual objects while constructing the three-dimensional scene of the environment, allowing users to add selected objects to the perception scene. Currently, there are many types of SLAM algorithms, ORB- SLAM (OKVIS, viorbvins- SLAM)、DTAM (dense tracking and mapping) and LSD-SLAM (large scale direct monocular SLAM). ORB-SLAM is a SLAM algorithm based on keyframe BA, using the PTAM (pickuptruck access method) system framework. ORB SLAM uses ORB feature points for matching to improve the accuracy of bundle adjustment. DTAMLo and LSD-SLAM7 solve for motion by directly comparing pixel colors between images, these two local pixel based SLAMs have good reconstruction performance in noisy environments. They can restore 3D scenes in real-time, but LSD SLAM can only restore depth maps of semi dense scenes; Due to the need for DTAM to process the depth information of each pixel to establish a dense map, the computational complexity is high and the scene perception efficiency is low. By constructing a feature transformation network, which is composed of multiple similar affine transformation, the author matches feature points to improve the matching accuracy and efficiency, thus reducing the calculation time of front-end threads [8-9]. Fig. 1 is the flow chart of the overall visual SLAM.

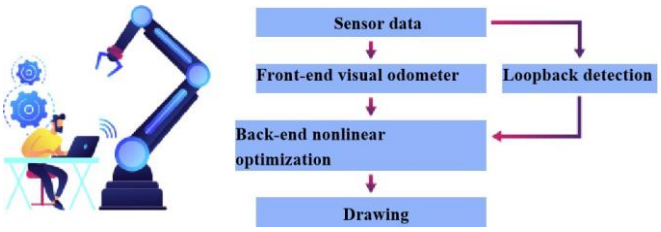


Fig. 1. Overall visual SLAM flowchart.

II. METHODS

The V-SLAM system mainly includes front-end and back-end threads, among which the front-end threads mainly pass through visual sensors such as cameras, input the acquired data into the SLAM system for initialization, put the SLAM system into tracking state, and output real-time camera pose and scene point cloud; The backend thread mainly optimizes the thread, and there may be pose deviation or scale drift during camera motion or scene switching, resulting in error accumulation, when the error accumulates to a certain extent, it will cause the algorithm module to stop working, the backend thread uses scene loop detection to correct the drift phenomenon that occurs during the camera movement process, the author uses local or global optimization to reduce the error accumulation of SLAM system [10].

A. Front End Thread Design for V-SLAM

The SLAM system initializes the system by detecting a certain number of feature points and enters camera tracking mode, the tracking stage mainly includes motion between images and scenes, image feature extraction, feature matching, and reconstruction from 2D images to 3D scenes. Visual sensors are used in unknown environments, perceiving the surrounding environment by capturing continuous environmental images, while constructing a scene using a three-dimensional sparse point cloud, with the world coordinate system feature point X; Projection to the image coordinate system, which includes the transformation from the world coordinate system to the camera coordinate system and the transformation from the camera coordinate system to the imaging coordinate system. In the world coordinate system, the feature points Xn of the environment [11-12]. The motion parameter during the shooting process in three-dimensional coordinates $[x_n, y_n, z_n]^T$ can be expressed as $C_1,...,C_i,...,C_n$, each camera motion parameter contains 3x3 camera rotation matrix Rn and position offset pn. Convert the feature point Xn in the world coordinate system to the camera's local coordinate system as shown in Eq. (1):

$$\begin{bmatrix} x_{cn} \\ y_{cn} \\ z_{cn} \end{bmatrix} = R_n \left(\begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} - p_n \right) \tag{1}$$

The camera projects the 3D point $[x_{cn}, y_{cn}, z_{cn}]^T$ in the camera coordinate system to the image point $[x, y]^T$ in the 2D coordinate system through perspective changes:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \left[\frac{F_x x_{cn}}{z_{cn}} + c_x, \frac{F_y y_{cn}}{z_{cn}} + c_y \right]^T \tag{2}$$

Among them, c_x, c_y represent the position of the lens optical center in the image, F_x, F_y represents the focal length

of the image along the x and y axes, and (x, y) represents the pixel position.

The environmental structure feature points in the world coordinate system are projected onto the image coordinate system, and each frame of the image input to the camera sensor is used for feature extraction and feature point matching between adjacent frames, feature point extraction and matching provide the data required for SLAM algorithm processing, which is related to the quality of camera path reconstruction and the accuracy of scene perception. High precision feature point matching algorithms are beneficial for reducing error accumulation during camera motion [13].

In order to generate accurate camera paths and high-quality scene perception, the V-SLAM system requires continuous feature point matching between hundreds or even thousands of frames of images. The feature matching algorithm proposed by the author ensures global optimization and has a certain degree of robustness through efficient region matching; At the same time, it also has good matching performance in scenes with fewer feature points or scenes where the captured image is blurry due to strong shaking of the lens [14-15].

The camera obtains consecutive frames $I_1,...,I_i,...,I_n$, using the image of the region where a feature point is located in frame Ii as a template, adjacent frame image I_{i+1} represents the image to be matched, and $W(I_i)$ represents the total change in the i-th frame image:

$$v_m = \max_{s \in N(m)} |I_i(m) - I_i(s)| \tag{3}$$

$$W(I_i) = \sum_{m \in I_i} |v_m| \tag{4}$$

Among them, the maximum difference between pixel point m and its adjacent eight pixels N (m) is taken as the variation of m. Traditional image matching algorithms first extract feature points from two consecutive frames of images, calculate the distance between feature points, and use threshold feature points as matching feature points between the detected image frames. The matching algorithm proposed by the author considers that the continuous frame images taken by the camera have little change, and a feature point image in the image frame Ii is mapped to the next frame image I_{i+1} through a certain affine transformation [16].

B. VSLAM Backend Thread Optimization

In the V-SLAM system, bundle adjustment is the core task of backend optimization. In order to reduce the cumulative error of the SLAM system, the backend threads of the SLAM system include local bundle adjustment (LBA) and global bundle adjustment (GBA) 24. LBA mainly optimizes the local scenes and camera keyframes generated during the process, while GBA optimizes all image frames and landmark pose features. The author proposes an improved LBA and segmented GBA optimization strategy. Once a new keyframe is added in the scene, LBA optimization is triggered, the feature points and camera trajectories of the current keyframe and previous frames within a certain time range are processed using improved segmented GBA [17-18].

In traditional SLAM systems, the key frame count for LBA optimization is 70-85, with a maximum of 100 frames, there is a significant consumption of redundant storage in system computing and storage. When the V-SLAM system processes captured video clips, when the visible two-dimensional feature points in a certain image frame meet the set values, they are labeled and added to the keyframe set. In local scenes, LBA optimizes the visible feature points in these keyframes. The traditional LBA optimization method involves the appearance of optimized 3D feature points in newly added keyframes, resulting in repeated optimization of visible feature points and keyframes in the scene, resulting in a large amount of redundant computation and memory consumption, greatly reducing the efficiency of SLAM backend processing threads. In the process of generating local environment, when high-precision local scene landmarks are detected, the author defines them as fixed landmarks, which can be used as reference landmarks to make other keyframes or scenes reference their positions to estimate coordinates. The same visible feature point does not need to be optimized multiple times, as the accumulation of system errors reduces the accuracy of camera trajectory and landmark coordinates. The backend system records the number of optimizations for visible feature points in each keyframe, when the point has been optimized 10 times, it is marked as a reference landmark, and LBA will no longer optimize the landmark and can estimate the camera pose of the current frame using this point. If there are visible reference landmarks in the newly added keyframes, LBA will no longer optimize them, thereby reducing the number of visible points for local optimization. For large scenes with many keyframes, when the keyframes exceed 120, the average keyframes in local LBA optimization range from 50 to 65, reducing the computational burden of the system and improving the efficiency and accuracy of local BA optimization.

In the backend optimization of V-SLAM system, GBA optimizes all global keyframes and visible feature points, resulting in high computational complexity and memory consumption, the number of optimizations far exceeds that of LBA. For the accumulation of errors in GBA optimization, the author proposes a segmented optimization to gradually eliminate error accumulation, each continuous frame calculates a set of motion variables, the relative error of continuous image frames is relatively small, and only needs to be calculated at the connection between segments, compared with traditional GBA optimization, the performance is improved to a certain extent, and the processing efficiency is improved to a certain extent. The relative pose of each consecutive keyframe remains unchanged during optimization, only visible landmarks between segments are optimized, experimental data shows that the improved backend optimization strategy has good real-time performance and high efficiency in processing camera trajectory optimization in large scenes. At the same time, in augmented reality applications, the system detects that a plane in a real-time scene is considered a homography plane that can add objects, manually adding a 3D model to the scene can provide users with a more intuitive visual experience [19].

III. Experimental Results

The author proposes a fast scene reconstruction algorithm based on improved V-SLAM, which includes parallel front-end and back-end threads, and is deployed and implemented on a personal PC, the hardware configuration is IntelCorei584002.8GHz CPU, 8GB memory, NVIDIAGTX1050Ti graphics card, OS is ubuntu16.04, and input video image resolution is 640x480. In the V-SLAM system, the front-end tracking thread projects real-world 3D points onto the 2D points of the current frame to solve the camera pose transformation, it is necessary to determine the position or offset of a feature point in the next frame. The author proposes a region matching algorithm for inter frame feature point matching to minimize errors and reduce computational pressure on backend optimization threads. Select an area with many or dense feature points, perform template affine transformation through the transformation network to match the next frame, select ROI in the region of interest in the image, and input ROI into the transformation network through certain amplification or reduction of ROI, the transformation network performs affine transformation on ROI until a transformation maximally matches a region of the next frame image, so that the feature points in the region can be matched. Good performance can also be achieved in cases of camera shake and rapid rotation, and the use of transform networks reduces the burden on the SLAM system and improves its real-time performance.

The algorithm proposed by the author was tested in offices and large indoor scenes, during the experimental shooting, the camera experienced some shaking and rapid movement, the algorithm combined RGB images and depth images for real-time processing to reconstruct a sparse 3D point cloud of the scene, the sparse reconstructed 3D point cloud was displayed in blue, the newly added 3D point cloud at the current frame in the scene is displayed in red, and the yellow trajectory represents the reconstructed camera motion trajectory. V-SLAM performs sparse reconstruction on two types of indoor environments, and the shooting data of the two scenes are shown in Table I. The SLAM method proposed by the author has good reconstruction results for large factory buildings, with the yellow trajectory being the camera shooting path trajectory.

TABLE I. Scene Information of Offices and Large Factories

Scenario Type	Track length/m	Time 1 second	Average Movement Speed/(m/s)
Office Scenarios	21.460	88.0	0.250
Large factory buildings	40.051	173.2	0.240

In terms of backend optimization, the main focus is on optimizing camera trajectories, including camera loop detection, local or global BA optimization, and scene map expansion. The author adopts a segmented optimization approach, marking feature points with optimized values reaching a certain threshold as reference landmarks without further processing, reducing the computational complexity of the system and improving real-time data processing capabilities. In the experiment, the camera trajectory was saved to a CameraTrajectory file and compared with the actual trajectory on the ground, absolute trajectory error (ATE) was used for comparison, and ATE was used to compare the SLAM system based on keyframes, as shown in Table II.

TABLE II. Path Absolute Error Analysis

Scenario Type	ATE /m			
	ORB-SLAM	PTAM	ISD-SLAM	Ours
Office Scenarios	0.100	0.745	0.874	0.096
Large factory buildings	0.121	0.727	0.895	0.104

Preprocessing was performed on each frame of the image, and a timestamp was used to compare the estimated camera pose with the actual camera pose, as shown in Fig. 2, compare the results of the error between the real trajectory and the optimized camera trajectory in the office small scene environment, by calculating the difference between camera poses in each segment, the absolute translation error is 0.09623. When estimating errors in large factory buildings, the backend optimization thread of the system performs well, as shown in Fig. 3, the actual trajectory and camera trajectory only deviate to a certain extent in local areas, while the other parts almost overlap. The absolute translation error in larger scenes is 0.10448. Root mean square error (RMSE) is also used to evaluate backend thread optimization performance, as shown in Table III. By comparing the performance parameters of various SLAM systems in the same scenario, the algorithm proposed by the author can more accurately process deep data and meet the real-time requirements of V-SLAM systems.

TABLE III. Comparison of Root Mean Square Error of Absolute Path for Key Frames of Different Algorithms

Scenario Type	RMSE /m			
	ORB-SLAM	PTAM	ISD-SLAM	Ours
Office Scenarios	0.034	-	0.385	0.030
Large factory buildings	0.381	0.332	0.356	0.327

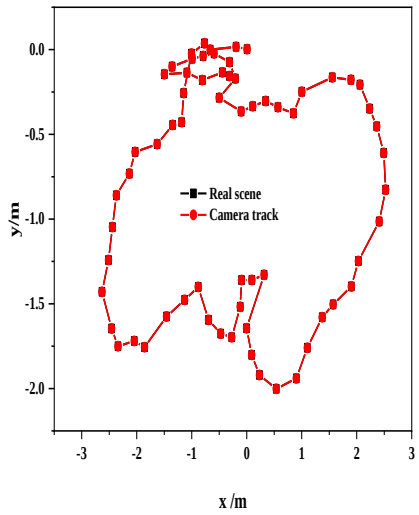


Fig. 2. Comparison of camera errors in office environments.

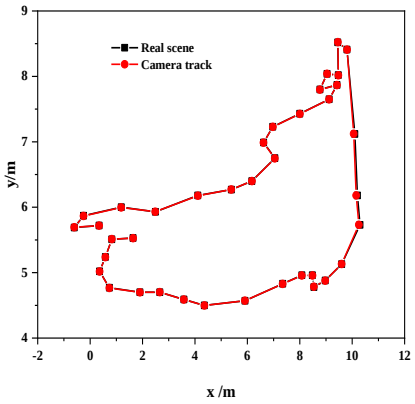


Fig. 3. Error comparison of camera trajectories in large factory environment.

The V-SLAM method proposed by the author can add virtual 3D objects to real scenes. The V-SLAM system can extract feature points from the screen in real-time and detect scene plane objects, ensuring that multiple virtual objects in the scene meet geometric consistency with the actual scene. In the experiment, two objects were added to the virtual scene, users can interactively scale objects and add them without being affected by camera movements, ensuring consistency between objects and the real scene [20].

IV. Conclusion

SLAM technology has been a research and application hotspot in recent years, applied in fields such as scene reconstruction, perception, digital city construction, VR/AR applications, drone driving, robotics, etc. SLAM includes LSDSLAM, ORBSLAM, Mono SLAM, etc. Simultaneous Location and Map Building (SLAM) plays an important role in the fields of computer vision and robotics, and also provides basic technical support for VR/AR applications. When facing scenes with relatively single or complex features, the front-end feature matching module of traditional SLAM systems is difficult to generate accurate camera trajectory and scene reconstruction results due to the sparsity or density of feature points. The author proposes an improved algorithm for arbitrary path scene reconstruction based on visual SLAM, the front-end thread uses Hessian matrix to extract and match the image features, and applies affine transformation to the region of interest to identify the feature points of adjacent frames to improve the matching efficiency, thereby reducing the original error of camera track and scene reconstruction; The backend optimization thread reduces the number of marker points to optimize the number of feature points, and uses local and global BA (bundle adjustment) methods to segment and optimize the camera motion trajectory, reducing system errors and improving the efficiency of camera trajectory optimization. The proposed method can add 3D objects in real-time to the scene. The experimental results show that the improved visual SLAM algorithm has better real-time performance than traditional SLAM algorithms.

Acknowledgment

The paper is the output of R&D Platform Special of Xingtai Technology Innovation Center for Intelligent Sensing and control of mechanical and electrical equipments.

References

[1] Chen, L. , Jin, S. , & Xia, Z. . (2021). Towards a robust visual place recognition in large-scale vslam scenarios based on a deep distance learning. Sensors, 21(1), 310.

[2] Srithar, S. , Priyadharsini, M. , Sharmila, F. M. , & Rajan, R. . (2021). Yolov3 supervised machine learning framework for real-time object detection and localization. Journal of Physics: Conference Series, 1916(1), 012032 (7pp).

[3] Salim, M. Z. , Abboud, A. J. , & Yildirim, R. . (2022). A visual cryptography-based watermarking approach for the detection and localization of image forgery. Electronics, 11(1), 136-.

[4] Schubert, S. , Neubert, P. , & Protzel, P. . (2021). Graph-based non-linear least squares optimization for visual place recognition in changing environments. IEEE Robotics and Automation Letters, 6(2), 811-818.

[5] Lu, F. , Chen, B. , Zhou, X. D. , & Song, D. . (2021). Sta-vpr: spatio-temporal alignment for visual place recognition. IEEE Robotics and Automation Letters, PP(99), 1-1.

[6] Molloy, T. L. , Fischer, T. , Milford, M. J. , & Nair, G. N. . (2021). Intelligent reference curation for visual place recognition via bayesian selective fusion. IEEE Robotics and Automation Letters, 6(2), 588-595.

[7] Hu, H. , Wang, H. , Liu, Z. , & Chen, W. . (2021). Domain-invariant similarity activation map metric learning for retrieval-based long-term visual localization. IEEE/CAA Journal of Automatica Sinica, PP(99), 1-16.

[8] He, D. , Chuang, H. M. , Chen, J. , Li, J. , & Namiki, A. . (2021). Real-time visual feedback control of multi-camera uav. Journal of Robotics and Mechatronics, 33(2), 263-273.

[9] Wan, G. , Wang, G. , Xing, K. , Fan, Y. , & Yi, T. . (2021). Robot visual measurement and grasping strategy for roughcastings:. International Journal of Advanced Robotic Systems, 18(2), 715-720.

[10] Awwad, A. . (2021). Visual emotion-aware cloud localization user experience framework based on mobile location services. International Journal of Interactive Mobile Technologies (iJIM), 15(14), 140.

[11] Torii, A. , Taira, H. , Sivic, J. , Pollefeys, M. , Okutomi, M. , & Pajdla, T. , et al. (2021). Are large-scale 3d models really necessary for accurate visual localization?. IEEE transactions on pattern analysis and machine intelligence, 43(3), 814-829.

[12] Beuth, F. , Kowerko, D. , & Hamker, F. H. . (2021). Contrasting attentional processing in visual search, object recognition, and complex tasks. Journal of Vision, 21(9), 2753-.

[13] Chen, J. , Takashima, R. , Guo, X. , Zhang, Z. , & Hancock, E. R. . (2021). Multimodal fusion for indoor sound source localization. Pattern Recognition, 115(3), 107906.

[14] Liang, J. , Zhang, J. , Pan, B. , Xu, S. , & Zhang, X. . (2021). Visual reconstruction and localization-based robust robotic 6-dof grasping in the wild. IEEE Access, PP(99), 1-1.

[15] Mahapatra, S. , & Sahu, S. . (2021). Integrating resonant recognition model and stockwell transform for localization of hotspots in tubulin. IEEE transactions on nanobioscience, 20(3), 345-353.

[16] Nguyen, T. H. , Nguyen, T. M. , & Xie, L. . (2021). Range-focused fusion of camera-imu-uwb for accurate and drift-reduced localization. IEEE Robotics and Automation Letters, PP(99), 1-1.

[17] M Servières, Renaudin, V. , Dupuis, A. , & Antigny, N. . (2021). Visual and visual-inertial slam: state of the art, classification, and experimental benchmarking. Journal of Sensors, 2021(1), 1-26.

[18] Zhao, W. , Panerati, J. , & Schoellig, A. P. . (2021). Learning-based bias correction for time difference of arrival ultra-wideband localization of resource-constrained mobile robots. IEEE Robotics and Automation Letters, PP(99), 1-1.

[19] Yang, M. , & Li, Y. . (2021). Design of intelligent safety protection robot based on global position system and machine vision. Journal of Physics: Conference Series, 1883(1), 012146 (6pp).

[20] Ali, R. , Liu, R. , He, Y. , Nayyar, A. , & Qureshi, B. . (2021). Systematic review of dynamic multi-object identification and localization: techniques and technologies. IEEE Access, PP(99), 1-1.

Optimizing Threat Intelligence Strategies for Cybersecurity Awareness Using MADM and Hybrid GraphNet-Bipolar Fuzzy Rough Sets

Qian Zhang
Shaanxi Police College,
Xi'an, Shaanxi, 710021, China

***Abstract*—Advanced threat detection systems are needed more than ever as cyber-attacks become more advanced. A novel cybersecurity model uses Bipolar Fuzzy Rough Sets, Graph Neural Networks, and dense network (BFRGD-Net) architectures to identify threats with unmatched accuracy and speed. The approach optimizes threat detection using Dynamic Range Realignment, anomaly-driven feature enhancement, and a hybrid feature selection strategy on a comprehensive Texas dataset of 66 months of real-world network activity. With 97.8% accuracy, 97.5% F1-score, and 98.3% AUC, BFRGD-Net sets new standards in the field. Threat Detection Sensitivity shows the model's capacity to find uncommon, high-severity threats, while Balanced Risk Detection Efficiency provides fast, accurate threat detection. The model has strong correlations and the highest statistical metrics scores compared to other techniques. Extensive simulations demonstrate the model's capacity to discern threat levels, attack kinds, and response techniques. BFRGD-Net revolutionizes cybersecurity by seamlessly merging cutting-edge machine learning with specific insights. Its advanced threat detection and classification engine reduces false negatives and enables proactive critical infrastructure protection in real-time. The model's adaptability to various attack situations makes it vital for cybersecurity resilience in a digital environment.**

***Keywords*—Cybersecurity awareness; threat intelligence; MADM framework; BFRGD-Net; hybrid model; deep learning**

I. Introduction

Advancements in technology have raised cybersecurity risks such as unauthorized access, malware attacks, phishing, and DoS [1]. Over 900 million malware executables existed in 2024, compared to 50 million in 2010 [2]. Annual cybercrime costs firms, individuals, and governments $400 billion. Due to data breaches and security incidents, essential systems and data require cybersecurity. Modernizing security helps companies avoid losses and adapt to shifting threats. Cybersecurity shields data, programs, networks, and systems against cyberattacks and unauthorized access [2]. Security for networks, applications, data, and operations. Data-driven cybersecurity solutions complement firewalls, antivirus, and intrusion detection. To improve threat detection, machine learning (ML) may find hidden patterns and irregularities. Cybersecurity machine learning is part of AI-powered decision-making and threat identification. Attackers' expertise in exploiting connected technologies is leading to more complex cyber threats [3]. From 2015 to 2022, cybersecurity and machine learning gained popularity from 30 to over 70 [3]. ML increases complex dataset analysis, security, and incident response. Traditional security measures, such as user authentication, cryptographic systems, and firewalls, need human setup and maintenance, making them less effective as threats evolve [4] Thus, machine learning and data analytics-based adaptive and automated systems discover new risks and provide robust protection.

Cybersecurity situational awareness (SA) involves collecting, evaluating, and interpreting information from several sources to manage risks [5]. SA, created for military usage, is currently utilized in cybersecurity to understand activities. Real-time vulnerability and network traffic analysis may prevent attacks. SA frameworks integrate data from several sources, including network traffic and vulnerability assessments, to provide a comprehensive security picture [5]. SA predicts and detects cyberattacks using many data sources. Many situational awareness methods manually gather and analyze data. Despite advancements in data fusion and machine learning, human participation remains vital [6]. Our fully automated systems must use the Common Vulnerability Scoring System to monitor and evaluate network parts for vulnerabilities and security risks.

Company cybersecurity awareness initiatives may raise security awareness and share responsibilities. A frequent cybersecurity risk is the human component since workers are the weakest link in the security chain [7]. Security-focused workplaces prevent errors and social engineering. Cyberattacks may harm reputation, legal obligations, consumer confidence, and money. Secure solutions must address technology and humans. As more people use the internet, hackers target browsers. Using browser vulnerabilities, attackers may get access to devices and steal sensitive data [8]. Covert downloads from reputable websites spread 22 million malware types in 2022. User data must be protected from browser-based attacks using security, notably automated threat detection. Cybersecurity requires flexibility. To resist growing threats, cybersecurity defenses must adapt to new attack methods [9]. Machine learning and situational awareness automate danger detection in this essay. Multi-domain threat detection is improved by diverse data sources and new techniques. Main contributions of this research.

1) The BFRGD-Net framework is introduced to enhance threat intelligence, integrating BFRS, GNN, and DenseNet architectures to improve Cyber Secu-

rity Awareness Programs. This advanced approach facilitates accurate threat detection by identifying intricate patterns in network traffic, hence enhancing the precision and dependability of threat intelligence techniques.

2) The study introduces innovative preprocessing techniques, including HTS and CBSA, that substantially improve data quality and model resilience in support of cyber security awareness. By mitigating data imbalance and noise, these solutions enable threat intelligence tactics to react to emerging cyber threats, hence enhancing the efficacy of awareness programs.
3) Hybrid Feature Selection for Enhanced Threat Identification: The use of a hybrid feature selection methodology that integrates Statistical-Driven Filtering, Redundancy Aggregation, and ODAS guarantees the prioritization of the most pertinent and significant characteristics. This enhancement improves threat detection, making it a substantial tool for advancing Cyber Security Awareness Programs.
4) The research introduces new metrics—TDS, AIS, and BRDE—that provide a more thorough assessment of threat detection efficacy. These metrics are designed to assess the model's capacity to recognize significant risks and optimize detection efficiency, aiding in the identification of the most effective tactics for improving cybersecurity awareness.
5) Exhibiting Enhanced Threat Detection to Guide Awareness Initiatives: Comprehensive assessments indicate that BFRGD-Net routinely surpasses current models, demonstrating superior capability in detecting diverse attack types and categorizing threat severity levels. This performance highlights the framework's capacity to enhance Cyber Security Awareness Programs via the provision of actionable and timely threat information.

The remaining structure of the paper: Section 2 discussed the review of relevant literature. The proposed method structure is described in detail in Section 3. The simulations and their accompanying discussion are detailed in Section 4. The last section concludes with a discussion of future work.

II. Related Work

Threat intelligence and cybersecurity awareness initiatives have been improved using machine learning and decision-making frameworks. The NIST cybersecurity lifecycle consists of five steps: Identify, Protect, Detect, Respond, and Recover, offering a systematic threat management strategy [10]. However, many studies disregard lifecycle-wide techniques and concentrate on one or two processes. One threat intelligence technique in Software-Defined Networking (SDN) uses a Support Vector Machine (SVM) to discover attack scenarios and analyze vulnerabilities [11]. Another method uses K-Nearest Neighbors (KNN) to categorize IoT network traffic by risk level [12]. These strategies emphasize identification without incorporating threat intelligence throughout the lifecycle.

Threat detection is improved via machine learning. An anomaly-based intrusion detection system (IDS) increased prediction accuracy by using Recurrent Neural Networks (RNNs) to identify unexpected network patterns [13]. A Multiclass Support Vector Machine (SVM) was used to categorize network abnormalities in real-time, successfully distinguishing attack types [14]. Due to obsolete datasets, many methods fail to identify new threats. Users learn to recognize and react to cyber dangers via cybersecurity awareness programs. Static material in traditional systems may not be adequate for developing threats [15]. A dynamic strategy using Graph Neural Networks (GNNs) was suggested to update cybersecurity training material depending on current threat information [16]. Using Convolutional Neural Networks (CNNs), another application created interactive training simulations [17]. These strategies increased training but did not integrate live threat intelligence data. Cybersecurity methods are evaluated using MADM frameworks. One method assessed intrusion detection trade-offs using Decision Trees (DT) based on accuracy and reaction time [18]. Analytical Hierarchy Process (AHP) and Logistic Regression (LR) were used to prioritize threat response techniques and evaluate their influence on security [19]. Although effective, MADM approaches are seldom used to improve awareness training.

Deep learning-fuzzy logic hybrid models can handle cybersecurity uncertainty. LSTM networks and Fuzzy C-Means clustering were utilized to identify Advanced Persistent Threats (APTs) using fuzzy logic to handle imprecise data [20]. A study used Deep Belief Networks (DBN) and Fuzzy Inference Systems (FIS) to improve network anomaly classification accuracy under uncertainty [21]. Fuzzy rough set techniques have been used in cybersecurity research, notably for uncertain decision-making. Bipolar Fuzzy Rough Sets (BFRS) add bipolar information to fuzzy logic for more sophisticated decision-making. In the study, BFRS using Random Forest (RF) classifiers improved phishing attack detection rates by addressing uncertainty in approaches [22]. BFRS and Neuro-Fuzzy Systems (NFS) were combined to enhance threat categorization and protect against zero-day attacks [23]. Merging Bipolar Fuzzy C-Means (BFCM) clustering with BFRS may enhance network traffic anomaly detection and reduce false positives [24].

Cybersecurity hybrid models and decision-making frameworks are difficult to integrate. Many frameworks lack thorough integration of situational awareness technologies and threat intelligence methodologies, and obsolete datasets hinder innovative threat detection. The summarized view of the literature is shown in Table I.

TABLE I. Summarized Literature Review

Ref	Method Used	Objective Achieved	Limitations
[10], [11]	SVM, KNN	Detection of attack scenarios and classification of network flows in SDN and IoT environments based on risk levels.	Focuses mainly on identification without fully integrating the complete threat lifecycle.
[12], [13]	RNN, Multiclass SVM	Anomaly detection and real-time classification of network anomalies, improving prediction accuracy by leveraging historical data.	Relies on outdated datasets, limiting the ability to detect emerging threats.
[14], [15]	GNN, CNN	Dynamic modeling of relationships between cybersecurity events for adaptive training and creating interactive simulations for better user engagement.	Lacks full integration with live threat intelligence data, limiting real-time adaptability.
[16], [17]	Decision Trees, AHP, Logistic Regression	Evaluation of intrusion detection configurations and prioritization of threat response strategies based on various criteria (e.g., accuracy, cost).	Rarely applied to evaluating cybersecurity awareness programs' effectiveness.
[18], [19]	LSTM, Fuzzy C-Means, DBN, FIS	Detection of Advanced Persistent Threats and classification of network anomalies under uncertain conditions.	High computational cost and limited adaptability to novel attack types.
[20], [21], [22]	BFRS, Random Forest, Neuro-Fuzzy Systems, BFCM	Detection of phishing attacks, adaptive threat classification, and enhanced anomaly detection using Bipolar Fuzzy Rough Sets.	May require continuous retraining, with increased sensitivity potentially leading to higher false-positive rates.

A. Challenges and the Need for BFRGD-Net

Cybersecurity threat identification is complicated by uneven datasets, dynamic attack patterns, and real-time reaction. These issues demand a model that can manage uncertainty, rapidly interpret complicated data linkages, and react to changing threats. The BFRGD-Net framework was created around these factors. It uses BFRS, GNNs, and DenseNet to provide a resilient, adaptable solution.

1) Suitability of BFRGD-Net for cybersecurity challenges:

- Bipolar Fuzzy Rough Sets clearly accommodate for ambiguous patterns by separating confidence and uncertainty, making the model more accurate in finding anomalies with confusing features.
- Relational Insights: GNNs capture source-destination dependencies and flow correlations, which are essential for threat categorization.
- DenseNet's layered architecture efficiently propagates and reuses features, allowing it to analyze high-dimensional data without duplicate calculations.
- Balanced Detect: BFRGD-Net balances feature significance and class distributions in cybersecurity datasets using hybrid feature selection (Statistical-Driven Filtering, RRFA, ODAS) and advanced preprocessing (CBSA, HTS).

2) Existing technique limitations:

- Traditional models like SVM and KNN struggle with huge, unbalanced datasets and cannot identify high-severity, low-frequency threats.
- CNNs and LSTMs ignore network traffic related relationships in favor of spatial or temporal patterns.
- Fuzzy logic can manage uncertainty, but hybrid systems like BFRGD-Net give scalability and real-time flexibility.
- Old dataset models cannot adapt to new attack vectors, limiting their real-world usefulness. However, BFRGD-Net's superior preprocessing and dynamic feature selection enable stable performance in changing settings.

BFRS, GNN, and DenseNet in the BFRGD-Net architecture overcome these restrictions, enabling great sensitivity to uncommon threats, real-time efficiency, and flexibility to varied attack scenarios. These traits make BFRGD-Net ideal for current cybersecurity applications, assuring its relevance and efficacy in solving problems.

III. Proposed Method

To improve threat classification accuracy and resilience, the proposed cybersecurity threat detection framework uses modern Deep learning and statistical analysis methodologies. The hybrid architecture, BFRGD-NeT, uses Bipolar Fuzzy Rough Sets (BFRS) and a GNN-DenseNet model to leverage GNNs' relational learning and DenseNet's feature reuse. Data is preprocessed using Dynamic Range Realignment and Perturbation-Weighted Outlier Filtering to ensure quality and correct feature imbalance. A Hybrid Feature Selection technique using Statistical-Driven Filtering and Optimization-Driven Adaptive Selection identifies the most relevant features for classification after preprocessing. Feature transformation improves model training data representation using Scaled Differential Encoding and Exponential Scaling Modulation. Using its capacity to manage ambiguity and relational data, the BFRGD-NeT model classifies threats. Using Adaptive Learning Rate Adjustment, model hyperparameters are fine-tuned for best performance. The proposed framework is shown in Figure 1 and afterwards, each module is explained in detail.

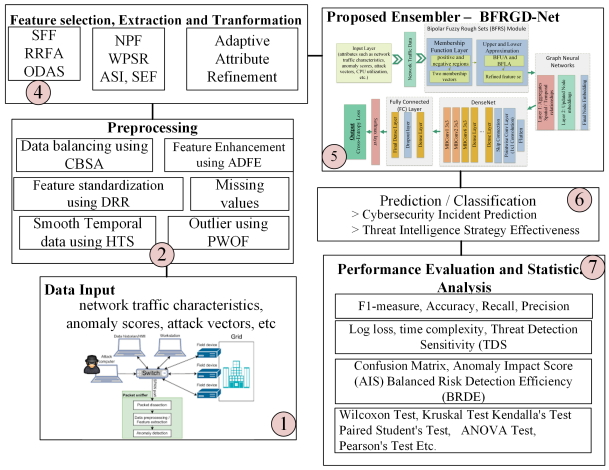


Fig. 1. Proposed system framework.

A. Dataset Description

This research utilized real-world Texas network traffic and cybersecurity activities. Over 66 months, from January 2018 to July 2024, the study collects hourly network events, user behaviors, and system states in an active corporate network infrastructure [23]. Financial companies, healthcare providers, and educational institutions in the area provided vital cybersecurity information for the dataset. These firms follow strong compliance standards to protect data. From low-level abnormalities to high-severity threats, the data shows how cyber dangers evolve. In Texas, a technological and industrial powerhouse, network connections, user behaviors, and worldwide cyberattack vectors are abundant. Information from local threat intelligence feeds was included in the dataset to make it more realistic and depict these firms' cybersecurity environment. This dataset provides a complete picture of regional cybersecurity issues by merging numerous data sources and using threat information from internal and external systems. It presents a solid framework for designing and testing advanced threat intelligence tactics to improve cybersecurity awareness and response. The dataset's imbalance, caused by real-world network traffic and attack events, properly depicts current cybersecurity systems' situations. The dataset characteristics are listed in Table II.

B. Data Preprocessing Steps

The dataset underwent preprocessing using many innovative strategies to enhance its appropriateness for machine

TABLE II. DATASET FEATURES OVERVIEW

S.No	Features	Short Description
1	Source IP	IP address of the source device or user.
2	Destination IP	IP address of the target device or server.
3	Source Port	Port number used by the source device for communication.
4	Destination Port	Port number used by the destination device.
5	Protocol Type	Type of protocol used for communication (TCP, UDP, etc.).
6	Flow Duration	Total duration of the network flow.
7	Packet Size	Size of the transmitted packets during the communication.
8	Flow Bytes/s	Rate of bytes transmitted per second.
9	Flow Packets/s	Rate of packets transmitted per second.
10	Total Forward Packets	Total number of packets sent by the source.
11	...	...
18	Anomaly Score	A score indicating the abnormality level of the traffic.
19	Attack Vector	The method or entry point used by the attack.
20	Botnet Family	Family of botnet detected in network traffic.
21	Anomaly Severity Index	Derived feature measuring anomaly severity.
22	CPU Utilization	CPU usage percentage during traffic transmission.
23	Memory Utilization	Memory usage percentage during the flow.
24	Label	Indicate whether the traffic is normal or an attack.

learning [24][25]. The first phase was Dynamic Range Realignment (DRR), used to normalize feature values according to their dynamic range while preserving variability. The transition is articulated as:

$$y_{adjusted} = \frac{y - \min(y)}{\max(y) - \min(y)} + \beta \cdot \left(\frac{\xi(y)}{\psi(y)} \right) \tag{1}$$

β is a weighting factor, $\xi(y)$ is the standard deviation, and $\psi(y)$ is the feature mean. Features with different scales are modified while keeping their relative dispersion using this method. To reduce noise and preserve trends across time, Hierarchical Temporal Smoothing (HTS) was employed to smooth temporal data across periods. Smoothing involves:

$$y_{smooth} = \frac{1}{h} \sum_{k=1}^{h} (y_{t-k} + y_{t+k}) + \theta \cdot \sum_{l=1}^{n} u_l \cdot y_{t-l} \tag{2}$$

where h represents short-term window size, θ adjusts long-term trend, and u_l weights temporal distances. This successfully captures short-term and long-term tendencies. Perturbation-Weighted Outlier Filtering (PWOF) was created to handle outliers. The following rule filtered outliers:

$$y_{filtered} = \begin{cases} y & \text{if } |y - \text{median}(y)| \leq \zeta \cdot \xi(y) \\ \text{median}(y) & \text{otherwise} \end{cases} \tag{3}$$

where ζ is the threshold determining outlier sensitivity, and $\xi(y)$ is the standard deviation. This method ensures that extreme values are moderated without affecting the general distribution of the feature. To handle class imbalance, *Cluster-Based Synthetic Amplification (CBSA)* was applied, generating synthetic samples for underrepresented classes based on clustering. The synthetic sample generation is governed by:

$$y_{synth} = y_g + \lambda \cdot (y_g - y_h) \tag{4}$$

where y_g is the cluster centroid, y_h is an adjacent point, and λ regulates synthetic amplification. This generates realistic new data points to balance the collection. In conclusion, *Anomaly-Driven Feature Enhancement (ADFE)* was used to enhance important features, particularly surrounding identified assaults. Enhancement calculation is done using the following equation:

$$y_{enhanced} = y \cdot \left(1 + \omega \cdot \frac{1}{1 + e^{-\phi(t - t_{event})}} \right) \tag{5}$$

ω indicates the amplification factor, ϕ adjusts temporal effect, and t_{event} represents the closest attack timestamp. This technique emphasizes anomaly-related characteristics as needed. These preprocessing processes balance, normalize and filter the dataset while keeping temporal and anomaly-based information needed for robust model performance.

C. Hybrid Feature Selection Process

This research uses a hybrid feature selection procedure that combines innovative strategies to maximize relevance and reduce duplication [26]. First, Statistical-Driven Feature Filtering (SFF) assesses feature variance and class separability contribution. For dataset imbalances, SFF dynamically weights feature importance by class distribution, unlike previous approaches. The significance score for feature h is determined as:

$$W_h = \frac{\zeta_h}{\eta_h} \cdot \frac{1}{1 + e^{-\mu(T_h - \bar{T})}} \tag{6}$$

ζ_h and η_h represent the feature's standard deviation and mean, T_h represents its correlation with the target label, and μ regulates the score's sensitivity This prioritizes high-variance, class-separable characteristics. To reduce feature redundancy, Redundancy-Reduced Feature Aggregation (RRFA) was created. This technique penalizes feature content redundancy by measuring overlap. The aggregate score for feature pairs (h_i, h_j) is:

$$V_{h_i,h_j} = \frac{|S_{h_i,h_j}|}{1 + \phi \cdot |S_{h_i,h_j}|} \tag{7}$$

Where S_{h_i,h_j} represents the correlation between features, and ϕ penalizes highly correlated features, preserving only the most representative ones from each correlated collection. Next, the Optimization-Driven Adaptive Selector (ODAS) approach is used. The cost function in ODAS repeatedly adjusts feature weights depending on predicted accuracy while punishing needless complexity. The cost function is:

$$\mathcal{F} = \sum_{h=1}^{m} v_h \cdot R(h) + \theta \cdot \sum_{j=1}^{m} v_j^2 \tag{8}$$

where v_h is feature weight, $R(h)$ is error contribution, and θ is regularization parameter. This refines choices by deleting low-performance model characteristics. SFF, RRFA, and ODAS are combined to keep just the most important, non-redundant features in the hybrid feature selection approach. This method optimizes features for prediction performance and simplicity.

D. Derived Attribute Transformation

This work proposed a unique approach called *Derived Attribute Transformation (DAT)* to create new characteristics from existing ones, therefore improving the dataset's capacity to capture intricate interactions. The first derived feature, *Normalized Packet Flow (NPF)*, integrates forward and backward packet counts normalized by flow time, articulated as:

$$\text{NPF} = \frac{(P_{\text{forward}} + P_{\text{backward}})}{\text{Flow Duration}} \tag{9}$$

This function captures a network flow's communication strength. Computed as weighted packet size ratio (WPSR), another attribute balances forward and backward packet sizes relative to flow bytes:

$$\text{WPSR} = \frac{\text{Forward Packet Size} \cdot \text{Flow Bytes}}{\text{Backward Packet Size} + \epsilon} \tag{10}$$

Using IDS alerts and reputation score, a crucial function Anomaly Severity Index (ASI) increases the anomaly score:

$$\text{ASI} = \text{Anomaly Score} \cdot (1 + \log(1 + \text{IDS Alerts})) \cdot \left(\frac{100 - \text{Reputation Score}}{100}\right) \tag{11}$$

This underscores the importance of reputation and IDS alerts in the identification of hazards. The *Session Efficiency Factor (SEF)* is a metric that integrates system resource utilization and session activity.

$$\text{SEF} = \frac{\text{Active Duration}}{\text{Idle Duration} + \epsilon} \cdot \left(\frac{\text{CPU Utilization}}{\text{Memory Utilization} + \epsilon}\right) \tag{12}$$

Lastly, Dynamic Threat Potential (DTP) figures out risk based on how bad an attack is and how many hosts have been hacked:

$$\text{DTP} = (\text{Attack Severity} \cdot \log(1 + \text{Compromised Hosts})) \cdot \frac{1}{1 + e^{-\gamma \cdot (\text{Attack Vector})}} \tag{13}$$

The newly created features, produced by the DAT method, provide enhanced insights into network activity, hence improving model performance for predictive analysis.

E. Adaptive Attribute Refinement (AAR)

A new method of transformation called Adaptive Attribute Refinement (AAR) is suggested in this research. The goal of this approach is to dynamically modify feature values according to how they affect the distribution of the whole dataset so that important patterns are highlighted and noise is reduced [26]. When characteristics change substantially between classes or time intervals, the AAR process uses an adaptive scaling technique to account for this. In the first stage of transformation, known as Dynamic Weight Adjustment (DWA), the statistical variance and impact of each feature on class separability are used to weigh the value of each feature. The feature y transformation is defined as:

$$y_{\text{adj}} = y \cdot \left(1 + \kappa \cdot \frac{|y - \nu_y|}{\tau_y}\right) \tag{14}$$

where ν_y is the feature mean, τ_y is the standard deviation, and κ is an adaptive scaling factor based on the feature distribution. This emphasizes outliers and major deviations by weighing data further from the mean. The next stage, Contextual Recalibration (CR), refines the converted feature depending on its temporal or category context. In datasets with characteristics that respond differently under different situations (e.g., events), this is beneficial. The recalibration process:

$$y_{\text{rec}} = y_{\text{adj}} \cdot \frac{1}{1 + e^{-\lambda \cdot (D_t - \bar{D})}} \tag{15}$$

λ is a sensitivity factor, D_t is the feature's contextual score at the time (t), and $\bar{D}$ is the dataset's average contextual score This adjusts features depending on their situation or class relevance. Finally, the Smooth Variance Reduction (SVR) stage reduces noise while maintaining essential trends. This stage maintains the converted feature's variability by smoothing severe variations. Transformation is modulated by:

$$y_{\text{smooth}} = \frac{y_{\text{rec}}}{1 + \theta \cdot \rho_{\text{local}}} \tag{16}$$

θ is a tuning parameter, and ρ_{local} is the local variance within a preset window of neighboring values. Short-term spikes are reduced but long-term patterns are maintained. The integrated Adaptive Attribute Refinement (AAR) technique produces a robust transformation process that improves the model's crucial pattern detection, noise reduction, and context-aware dataset refinement. This technique dynamically adapts each feature depending on its importance to the task, improving model accuracy and resilience.

This work uses BFRGD-Net, a unique classification model that combines Bipolar Fuzzy Rough Sets (BFRS) with GNN-DenseNet. This hybrid model benefits from Bipolar Fuzzy Rough Sets (BFRS) for uncertainty and interpretability, Graph Neural Networks (GNNs) for relational learning, and DenseNet for feature propagation and reuse. This layered structure is ideal for high-dimensional, complicated data like cybersecurity threats, where local and global interactions are crucial to threat identification.

F. Classification using BFRGD-Net

An improved method for handling uncertainty is presented by the Bipolar Fuzzy Rough Sets (BFRS) [27] framework, which describes the dataset using positive and negative areas. Positive associations represent certainty, while negative connections capture doubt. The proposed layered archictecutre is shown in Figure 2.

This is of the utmost importance in the field of cybersecurity since irregularities often manifest in unpredictable data patterns. The membership functions, both positive and negative, are defined by the BFRS method as:

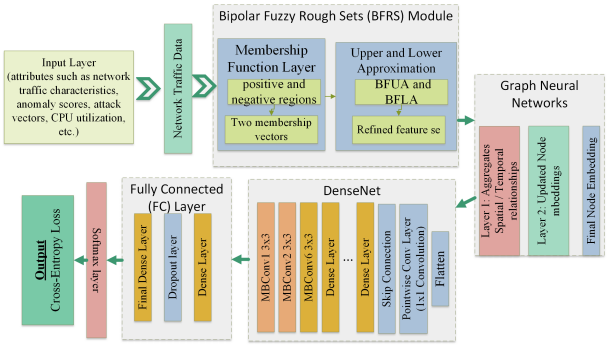


Fig. 2. Proposed BFRGD-Net architecture.

$$P(Z) = \{z \in U \mid \nu_1(z) \geq \alpha\}, \quad N(Z) = \{z \in U \mid \nu_2(z) \leq \beta\} \tag{17}$$

In this instance, $P(Z)$ and $N(Z)$ denote the positive and negative areas, respectively, while $\nu_1(z)$ and $\nu_2(z)$ signify the membership functions for the positive and negative classes. Additionally, α and β represent the thresholds that delineate the certainty and uncertainty regions. The Bipolar Fuzzy Upper Approximation (BFUA) and Bipolar Fuzzy Lower Approximation (BFLA) of a set Z are defined as follows:

$$\text{BFUA}(Z) = \sup_{z \in U} \left(\min\left(\nu_1(z), 1 - \nu_2(z)\right)\right) \tag{18}$$

$$\text{BFLA}(Z) = \inf_{z \in U} \left(\max\left(\nu_1(z), 1 - \nu_2(z)\right)\right) \tag{19}$$

These approximations improve the model's capacity to identify ambiguous data points, aiding in the identification of indistinct cybersecurity risks that display obscure patterns. The Graph Neural Network (GNN) component captures relational connections in graph-structured data, including network traffic and system logs. In Graph Neural Networks (GNNs), each node $g_i^{(l)}$ at layer l consolidates information from its adjacent nodes to enhance its feature representation in the subsequent layer. The propagation rule for a Graph Neural Network layer is delineated as follows:

$$g_i^{(l+1)} = \sigma\left(W^{(l)} \cdot \sum_{j \in \mathcal{N}(i)} \frac{1}{\sqrt{d_i d_j}} g_j^{(l)} + b^{(l)}\right) \tag{20}$$

$g_i^{(l+1)}$ is the updated node feature for node i at layer $l+1$, $W^{(l)}$ is the weight matrix for layer l, d_i and d_j are the degrees of nodes i and j, and σ is the activation function $\frac{1}{\sqrt{d_i d_j}}$ normalizes node connections, enabling balanced information aggregation from nearby nodes. In the cybersecurity dataset, the model may capture local (node-level) and global (graph-level) interactions.

The DenseNet design tightly connects each layer to every other layer feed-forward for optimal feature reuse. This propagates previous layer feature maps without losing critical information, which is vital for deep model performance. The DenseNet l-th layer output is computed as:

$$x^{(l)} = T_l\left(\left[x^{(0)}, x^{(1)}, \ldots, x^{(l-1)}\right]\right) \tag{21}$$

T_l is the transformation (e.g., batch normalization, ReLU, convolution) performed to the concatenated input from all preceding layers $[x^{(0)}, x^{(1)}, \ldots, x^{(l-1)}]$. The model can capture complex cybersecurity data relationships by effectively propagating information by concatenating feature maps. This reduces feature extraction parameters. DenseNet transition layers pool feature maps to reduce dimensionality while preserving crucial information. Transition layer outputs are calculated as:

$$S(x) = \text{BN}\left(\text{ReLU}\left(\text{Conv}(x)\right)\right) \tag{22}$$

where $S(x)$ is transition layer output, BN is batch normalization, $ReLU$ is activation function, and $Conv$ is input feature map convolution. The model stays small and economical without losing performance with this operation. A fully connected layer and softmax function complete the classification stage after GNN-DenseNet processing. Class probabilities for each cybersecurity threat are calculated using learning attributes. Definition of softmax:

$$\hat{y}_k = \frac{e^{o_k}}{\sum_{j=1}^{C} e^{o_j}} \tag{23}$$

The predicted probability for class k is $\hat{y}_k$, the logit output is o_k, and the total number of classes is C. Cybersecurity risks may be accurately classified using the softmax function's probability distribution across all classes. BFRGD-Net training uses cross-entropy loss, which is ideal for multi-class classification problems like threat detection. The cross-entropy loss $\mathcal{L}$ is computed as:

$$\mathcal{L} = -\sum_{k=1}^{C} y_k \log(\hat{y}_k) \tag{24}$$

y_k is the actual label for class k; $\hat{y}_k$ is the projected probability for class k. This loss function motivates the model to provide greater probability for the proper class and penalizes erroneous projections.

Bipolar Fuzzy Rough Sets (BFRS), Graph Neural Networks (GNNs), and DenseNet form the BFRGD-Net architecture, which detects cybersecurity risks effectively. BFRS improves the model's uncertainty handling, GNN layers capture network traffic relational relationships, and DenseNet optimizes feature reuse. With the softmax classification layer and cross-entropy loss function, the model can reliably identify many cybersecurity risks while being computationally efficient. That makes BFRGD-Net ideal for real-time threat identification in complicated cybersecurity contexts.

Algorithm 1 BFRGD-Net Framework

Require: Preprocessed input features $\mathbf{X}$, true labels $\mathbf{Y}$, learning rate η, number of GNN layers L_g, number of Dense blocks L_d, batch size B, number of epochs E
Ensure: Predicted class probabilities $\hat{\mathbf{Y}}$
Step 1: Input Layer
Initialize the input layer with feature vector $\mathbf{X}$
Step 2: Bipolar Fuzzy Rough Sets (BFRS) Module
Calculate positive and negative membership functions for $\mathbf{X}$
Compute Bipolar Fuzzy Upper Approximation (BFUA) and Lower Approximation (BFLA)
Update input features based on BFUA and BFLA
Step 3: Graph Neural Network (GNN) Layers
for $l = 1$ to L_g **do**
    Perform graph convolution on node features using neighbors
    Apply degree normalization and ReLU activation
end for
Step 4: DenseNet Module
for $d = 1$ to L_d **do**
    Perform convolution, batch normalization, and ReLU activation in Dense Block d
    Concatenate output with input features for feature reuse
    if Transition Layer is required **then**
        Apply batch normalization, ReLU activation, and average pooling
    end if
end for
Step 5: Fully Connected Layer
Flatten the output from the DenseNet module
Pass through a dense layer with ReLU activation
Optionally apply dropout for regularization
Step 6: Output Layer
Use a final dense layer to map features to the number of classes
Apply the softmax activation function to get class probabilities $\hat{\mathbf{Y}}$
Step 7: Loss Function and Backpropagation
Compute the cross-entropy loss between $\mathbf{Y}$ and $\hat{\mathbf{Y}}$
Update model parameters using the Adam optimizer with learning rate η
Step 8: Training Loop
for epoch $= 1$ to E **do**
    for each batch of size B **do**
        Forward pass: Perform Steps 1 to 6
        Compute loss and perform backpropagation (Step 7)
        Update parameters
    end for
end for
Return Predicted class probabilities $\hat{\mathbf{Y}}$

G. Role of Bipolar Fuzzy Rough Sets in BFRGD-Net

The BFRGD-Net architecture relies on Bipolar Fuzzy Rough Sets (BFRS) to deal cybersecurity dataset uncertainty and ambiguity. BFRS clearly separates confidence from uncertainty by dividing the dataset into positive and negative areas. This method assures accurate categorization, even when data points overlap or are unclear.

The BFRS module refines data representations using BFUA and BFLA. BFUA finds the largest collection of class members, whereas BFLA finds the most specific. These estimates help the framework manage imprecise and partial data. The BFUA and BFLA are defined mathematically:

$$\text{BFUA}(Z) = \sup_{z \in U} \left(\min \left(\nu_1(z), 1 - \nu_2(z) \right) \right) \tag{25}$$

$$\text{BFLA}(Z) = \inf_{z \in U} \left(\max \left(\nu_1(z), 1 - \nu_2(z) \right) \right) \tag{26}$$

$\nu_1(z)$ and $\nu_2(z)$ are the membership functions for positive and negative classes, respectively, and Z is the dataset.

BFRS improves the model's unusual and ambiguous threat classification by using these approximations. Cybersecurity requires this capability because high-severity anomalies can resemble regular data. In addition to uncertainty managing, BFRS improves model decision-making interpretability, revealing threat identification and classification. In real-world applications where transparency is as crucial as accuracy, interpretability is a major benefit.

H. Performance Evaluation Metrics

To evaluate the BFRGD-Net model for cybersecurity threat detection, metrics like accuracy, precision, recall, and F1-score are used to evaluate correctness, true positives, and precision-recall balance [28]. However, cybersecurity requires identifying uncommon and significant threats, thus we offer three unique metrics: Threat Detection Sensitivity (TDS), Anomaly Impact Score (AIS), and Balanced Risk Detection Efficiency. Threat Detection Sensitivity (TDS) weights low-frequency, high-severity events that dataset imbalances ignore to assess the model's capacity to identify infrequent, high-impact threats. We compute TDS as:

$$\text{TDS} = \frac{\sum_{j=1}^{M} \left(v_j \cdot \frac{A_j}{A_j + B_j} \right)}{\sum_{j=1}^{M} v_j} \tag{27}$$

where v_j represents threat class weight based on severity and frequency, A_j represents true positives, and B_j represents false negatives. This statistic prioritizes infrequent but significant threats, boosting the model's sensitivity to high-risk cybersecurity events. The Anomaly Impact Score (AIS) calculates real-time detection system operating expenses for false positives and negatives. AIS weighs the real-world effect of false positives and missing detections against the advantages of true positives. We define AIS as:

$$\text{AIS} = \frac{\sum_{j=1}^{M} \left(\frac{A_j}{A_j + C_j + \rho \cdot B_j} \right)}{M} \tag{28}$$

ρ penalizes false negatives, especially in high-impact circumstances, whereas A_j represents genuine positives, C_j false positives, and B_j false negatives for class j. This enhances real positive detection while lowering false positives and undiscovered threats. Finally, Balanced Risk Detection Efficiency (BRDE) evaluates the model's real-time detection accuracy and operating efficiency. To respond quickly, cybersecurity models must effectively identify threats with minimal latency. These two elements are balanced in BRDE:

$$\text{BRDE} = \frac{\sum_{j=1}^{M} \left(\frac{A_j}{A_j + C_j + B_j} \cdot \frac{1}{1 + \theta \cdot D_j} \right)}{M} \tag{29}$$

where D_j is the detection time for class j and θ is a scaling factor that accounts for detection speed. This measure penalizes longer detection durations to keep the model efficient in real-time threat detection when speed and accuracy are critical. While accuracy, precision, recall, and F1-score give a broad evaluation of model performance, TDS, AIS, and BRDE provide key insights into the model's capacity to manage infrequent threats, balance operational effects, and retain efficiency. These new measurements address cybersecurity problems, making BFRGD-Net reliable and practical for real-world deployments where speed and accuracy are crucial.

IV. Simulation Results

To assess the proposed BFRGD-NeT framework, extensive simulations were run on a Dell Core i7 12th Gen system with an 8-core CPU and 32 GB RAM. Python and SPYDER IDE were used for simulation setup and execution. The framework has three essential modules, and hyperparameters for each module were carefully tweaked throughout studies to produce the best outcomes. To assure data quality, dynamic

parameters like the outlier filtering threshold were set to 0.15, and feature scaling factors were modified for each dataset in the preprocessing module. To balance feature relevance and redundancy, the feature selection module used Statistical-Driven Filtering and Adaptive Selector with 0.6 optimization weight. For the classification module, the Adam optimizer was used with a learning rate of 0.0005, batch size of 32, and dropout rates of 0.3 to avoid overfitting. The attention processes were also tuned to recognize complicated threat patterns. These setups improved detection accuracy and processing performance across circumstances.

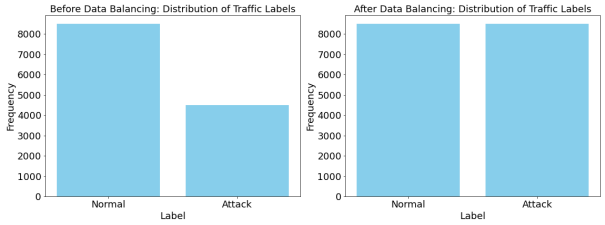


Fig. 3. Label distribution before and after data balancing.

Figure 3 illustrates cybersecurity dataset traffic label distribution before and after data balancing. On the left side of the graphic, the original data distribution shows a large imbalance between "Normal" and "Attack" labels, with 8500 normal traffic and 1500 attack traffic. Machine learning methods may bias forecasts toward typical traffic due to this imbalance. After balancing, the data distribution is shown on the right. This updated distribution equalizes "Normal" and "Attack" to 8500 occurrences each. The machine learning model will train on this balanced dataset, treating all groups equally, boosting attack detection, and lowering false negatives. This illustrates how data balancing improves cybersecurity model robustness and accuracy for recognizing normal and attack traffic by showing the before-and-after comparison.

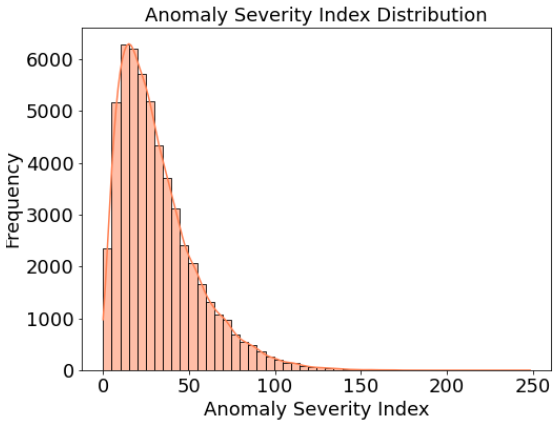


Fig. 4. Anomaly severity index distribution.

Figure 4 shows the distribution of the Anomaly Severity Index in the dataset, indicating the frequency of various severity levels. The Anomaly Severity Index is on the x-axis and frequency is on the y-axis. The histogram and KDE line show data distribution, with peaks suggesting shared severity. Right-skewed distributions indicate that lower-severity anomalies are more prevalent. The KDE line smoothes the probability distribution, simplifying data interpretation. This chart shows how successfully the system handles different threat levels.

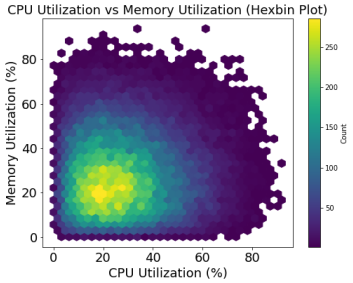


Fig. 5. CPU-Memory connection.

A hexbin plot in Figure 5 shows the dataset's CPU-Memory connection. Each hexagonal bin's color indicates the number of observations in that bin, representing data point density. Data points are denser in darker hues, whereas lighter colors indicate fewer observations. Analyzing the hexbin plot reveals CPU and memory consumption trends. Dark hexagon clusters may represent average CPU and memory use during system operation, whereas lighter hexagons may show outlier behaviors. This visualization helps uncover CPU and memory consumption correlations and unexpected or dispersed patterns that may suggest system abnormalities or performance issues. It helps analyze system performance and identify unexpected CPU and memory utilization patterns.

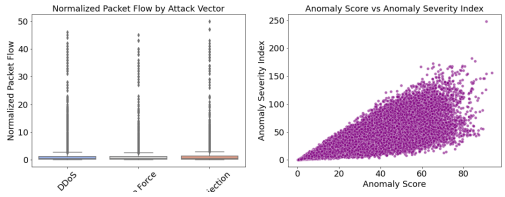


Fig. 6. Normalized packet flow by attack vector and anomaly score vs. severity index.

Figure 6 shows cybersecurity concerns from network traffic patterns and abnormalities. The left boxplot shows Normalized Packet Flow by Attack Vector, displaying packet flow rates by attack type. It displays the median, quartiles, and outliers for each attack vector to assist identify malicious from benign traffic behavior. This graphic shows which attack vectors substantially affect network traffic. The scatter figure on the right demonstrates how the Anomaly Score and Anomaly Severity Index correspond with threat severity. Higher anomaly scores indicate greater hazards, helping determine danger levels based on network activity.

A correlation heatmap of the cybersecurity dataset characteristics is shown in Figure 7. Each column represents the correlation coefficient between two attributes, ranging from -1 to 1, where darker hues indicate stronger linear relationships. Blue denotes negative correlations, while red indicates positive correlations. Values near 0 suggest no linear association, whereas values closer to ±1 indicate strong correlations. For example, packet size and flow bytes per second may exhibit significant positive correlations (close to 0.9), suggesting that

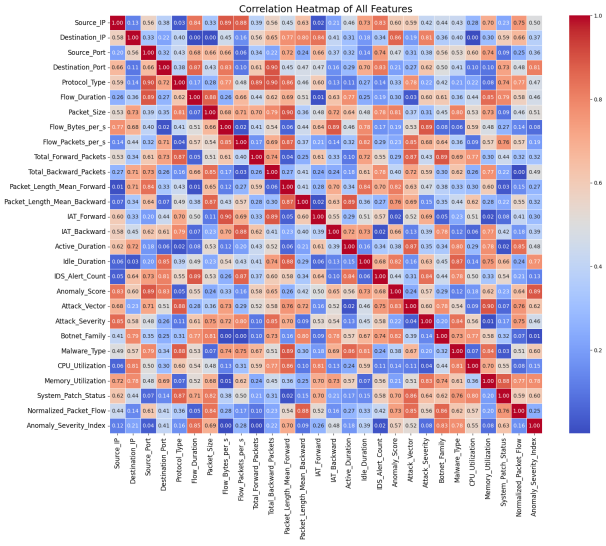


Fig. 7. Correlation heatmap of features.

larger packets carry more data. This heatmap helps identify patterns that guide feature selection and detect multicollinearity, aiding in feature engineering and model development.

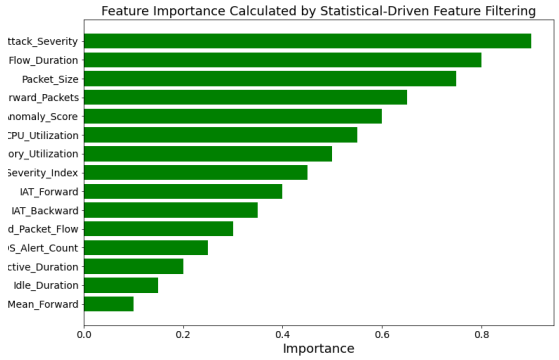


Fig. 8. Feature significance calculated by statistical-driven feature filtering.

Figure 8 displays the Statistical-Driven Feature Filtering estimates of feature significance. The bar plot scores 15 characteristics by relevance from 0.1 to 0.9. Important characteristics are at the top of the decreasing list. The graphic shows which characteristics classify cybersecurity risks in the dataset most. Features like Attack Severity and Flow Duration had higher significance values (0.9 and 0.8, respectively), suggesting they are significant in identifying normal from harmful activity. Packet Length Mean Forward and Idle Duration have lower significance values, indicating they contribute less to categorization. This figure also shows how feature importance affects the model's cybersecurity threat detection. This knowledge may assist choose features that improve model accuracy and reduce computing complexity.

Figures 9, 10, and 11 for the model's Threat Severity, Attack Type, and Cybersecurity Strategy Effectiveness Each figure's confusion matrix shows how effectively the model classifies jobs, with diagonal components indicating accurate classifications and off-diagonal parts not. Confusing "No

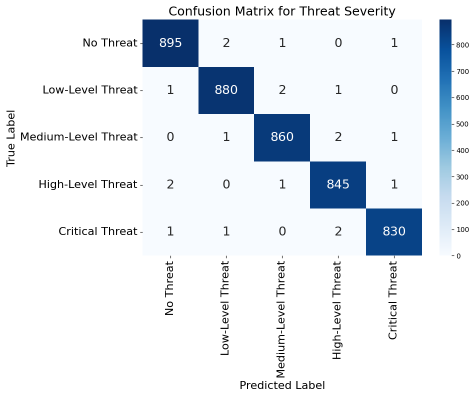


Fig. 9. Threat severity confusion matrix.

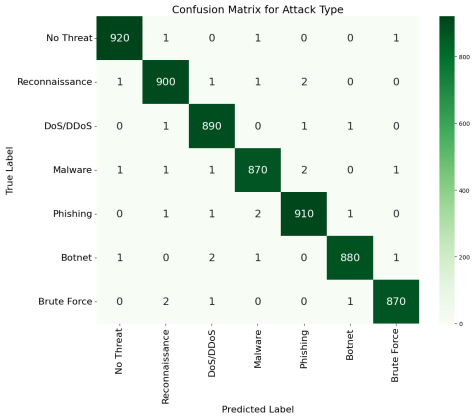


Fig. 10. Attack type identification confusion matrix.

Threat" to "Critical Threat." Most occurrences are likely categorized by the strong diagonal alignment. Few misclassifications occur around danger levels, showing the model can compare severity levels across categories. It can evaluate cybersecurity incident criticality. Figure 10 shows reconnaissance, DoS/DDoS, malware, phishing, botnet, plus brute force. The confusion matrix shows the model notices diagonal assaults. Comparing attack types is challenging since few misclassifications occur. The matrix proves the model properly classifies cyber dangers. Figure 11 displays the model's "No Action Required" to "Optimal Effectiveness." In the confusion matrix, most diagonal predictions are accurate across all effectiveness levels. Minimal off-diagonal values suggest the model seldom mixes categories, demonstrating cybersecurity assessment accuracy. Here are the model's cybersecurity risk, attack, and defense categories. The model's durability and real-time threat detection and response improve cybersecurity operational decision-making with little misclassification across all three activities.

Table III compares cybersecurity threat detection classification methods based on Accuracy, Log Loss, F1-Score, AUC, Recall, Precision, Balanced Precision Index (BPI), and Fault Detection Variability Coefficient. The table shows the efficacy of each strategy, with BFRGD-NeT winning all criteria. BFRGD-NeT has the greatest accuracy (97.8%) and F1-Score (97.5%), suggesting its robustness in determining threat levels. With the lowest Log Loss (0.071), the BFRGD-NeT model

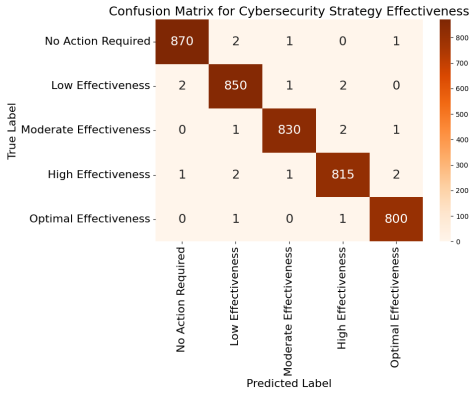


Fig. 11. Cybersecurity strategy effectiveness confusion matrix.

TABLE III. CLASSIFICATION RESULTS OF DIFFERENT TECHNIQUES

Techniques	Accuracy (%)	Log Loss	F1-Score (%)	AUC (%)	Recall (%)	Precision (%)	BPI (%)	FDVC (%)
CNN [14]	87.8	0.271	87.2	88.6	87.0	86.8	79.5	71.2
Decision Trees [16]	83.1	0.342	81.5	84.2	82.8	81.6	74.1	65.9
GNN [14]	90.1	0.255	89.4	90.8	89.0	88.7	82.9	74.6
DBN [21]	85.5	0.298	84.7	86.4	84.1	83.9	76.3	68.4
SVM [10]	85.1	0.309	83.8	85.9	83.3	82.7	76.0	67.0
BFRS [20]	86.5	0.285	85.1	87.3	85.4	84.8	78.0	69.8
KNN [11]	83.6	0.332	82.3	84.5	82.0	81.5	73.7	65.4
LSTM [18]	84.2	0.325	82.9	85.3	83.6	82.3	75.7	67.5
Proposed BFRGD-NeT	97.8	0.071	97.5	98.3	97.6	97.4	94.2	88.7

predicts more accurately than other techniques. Other models like GNN and CNN perform well but fall short of the proposed strategy, notably in BPI and FDVC, which imply balanced prediction accuracy and fault detection consistency. Traditional Decision Trees and KNN have poorer accuracy, F1-Score, and AUC values, demonstrating they cannot handle complicated cybersecurity threat data. The table shows that the BFRGD-NeT model is best for real-time threat detection due to its excellent classification performance.

TABLE IV. STATISTICAL ANALYSIS OF CLASSIFICATION METHODS (F-STATISTIC & P-VALUE)

Statistical Method	ANOVA	Student's T-test	Pearson Correlation (r)	Kendall's Tau (τ)	Chi-Square (χ^2)
CNN [14]	6.98	0.020	0.88	0.75	7.92
Decision Trees [16]	4.89	0.043	0.61	0.57	6.18
GNN [14]	7.56	0.014	0.84	0.72	8.63
DBN [21]	6.45	0.017	0.78	0.71	7.45
SVM [10]	5.67	0.029	0.70	0.64	6.88
BFRS [20]	7.12	0.021	0.81	0.69	7.58
KNN [11]	5.12	0.036	0.62	0.58	6.33
LSTM [18]	5.22	0.031	0.65	0.59	6.54
Proposed BFRGD-NeT	**8.93**	**0.007**	**0.94**	**0.81**	**9.92**

Table IV compares cybersecurity threat detection categorization approaches using statistical tests including ANOVA, Student's T-test, Pearson Correlation (r), Kendall's Tau (τ), and Chi-Square (χ^2). Decision Trees, KNN, SVM, CNN, GNN, and DBN perform differently, as seen in the table. The BFRGD-NeT technique classifies cybersecurity risks with the greatest statistical values across all parameters, demonstrating its consistency, correlation, and robustness. ANOVA and Chi-Square scores for BFRGD-NeT are greater than other approaches, indicating a more statistically significant difference between predictions. BFRGD-NeT's Pearson Correlation (0.94) and Kendall's Tau (0.81) reflect greater correlations and rank correlation with outcomes, improving prediction. Decision Trees and KNN have poorer statistical results, indicating their inability to handle complicated cybersecurity data. Table IV shows that BFRGD-NeT produces more accurate threat categorization than standard and deep learning approaches.

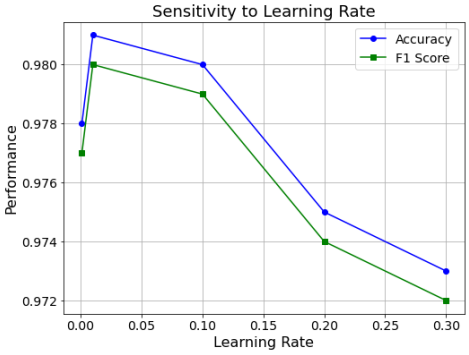


Fig. 12. Sensitivity to learning rate.

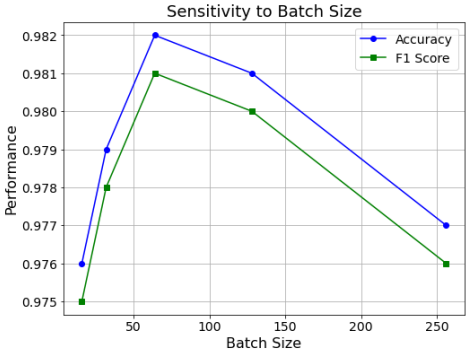


Fig. 13. Sensitivity to batch size.

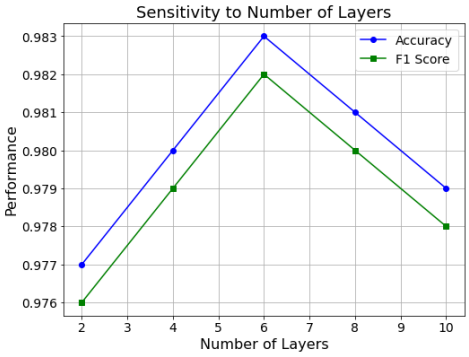


Fig. 14. Sensitivity to number of layers.

This model's sensitivity analysis shows how learning rate, batch size, and layer count impact its performance in Figure 12, 13 and 14. The figure shows the sensitivity to learning rate, batch size, and number of layers, with accuracy and F1-score displayed in each subplot. In the plots, the model regu-

larly achieves excellent accuracy and F1-scores close to 98%, however hyperparameters vary somewhat. These variations show that appropriate learning rates or batch sizes improve outcomes, helping to optimize the model.

V. Conclusion

In cybersecurity threat detection, the BFRGD-Net framework outperforms standard models in accuracy, F1-score, and AUC. It captures local interdependence and global traffic patterns to solve difficult cybersecurity data problems using BFRS, GNN, and DenseNet. A comprehensive hybrid feature selection approach and sophisticated preprocessing methods like HTS and CBSA have improved data quality and feature relevance, improving classification performance. Novel metrics TDS, AIS, and BRDE show how the system can effectively detect uncommon, high-severity threats in real time while retaining operational efficiency. Statistical research shows the model's consistency and resilience, making it suitable for cybersecurity situations that need accurate and quick threat detection. The findings are encouraging, but further study is required to improve the framework. Data sources, adjust the model for ICS and IoT networks and optimize hyperparameters to enhance performance. This work enhances threat detection and develops scalable, adaptive algorithms to react to the quickly changing cyber threat environment, enabling more proactive and robust security systems.

For cybersecurity dataset uncertainty management, Bipolar Fuzzy Rough Sets (BFRS) in the BFRGD-Net architecture are effective. Future work will include dynamic thresholds for positive and negative areas and investigate context-aware modifications to BFRS. These improvements improve the model's capacity to distinguish complex, dynamic threat patterns, making it more applicable in real-world cybersecurity settings.

VI. Practical Implications of Theoretical Results

Real-world cybersecurity applications benefit from BFRGD-Net framework theoretical findings. The model is ideal for dynamic and high-risk contexts because it can manage skewed datasets, identify infrequent but crucial threats, and adapt to changing assault patterns.

- **Critical Infrastructure Protection:** The framework protects electricity grids, healthcare systems, and transportation networks against undiscovered cybersecurity attacks, which might have serious effects.
- **Proactive Threat Mitigation:** This research offered unique metrics including Threat Detection Sensitivity (TDS) and Anomaly Impact Score (AIS) to prioritize and mitigate cybersecurity threats. These measurements help organisations prioritise the biggest dangers and allocate resources more strategically.
- **Scalable, Real-Time Performance:** BFRS, GNNs, and DenseNet are used in BFRGD-Net's architecture to ensure computational efficiency and scalability, making it suitable for real-time systems like industrial control systems (ICS) and IoT networks.

The suggested framework may improve cybersecurity measures in many applications by combining theoretical and practical contributions. These practical advantages demonstrate the theoretical conclusions' relevance and application to cybersecurity issues.

References

[1] M. A. I. Mallick and R. Nath, *Navigating the cybersecurity landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments*, World Scientific News, vol. 190, no. 1, pp. 1-69, 2024.

[2] S. Razaulla, C. Fachkha, C. Markarian, A. Gawanmeh, W. Mansoor, B. C. Fung, and C. Assi, *The age of ransomware: A survey on the evolution, taxonomy, and research directions*, IEEE Access, vol. 11, pp. 40698-40723, 2023.

[3] S. Abdelkader, J. Amissah, S. Kinga, G. Mugerwa, E. Emmanuel, D. E. A. Mansour, *Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks*, Results in Engineering, p. 102647, 2024.

[4] F. N. U. Jimmy, *Cybersecurity vulnerabilities and remediation through cloud security tools*, Journal of Artificial Intelligence General Science (JAIGS), vol. 2, no. 1, pp. 129-171, 2024.

[5] H. J. Ofte and S. Katsikas, *Understanding situation awareness in SOCs, a systematic literature review*, Computers & Security, vol. 126, p. 103069, 2023.

[6] A. A. Almazroi, F. S. Alsubaei, N. Ayub, and N. Z. Jhanjhi, *Inclusive smart cities: IoT-cloud solutions for enhanced energy analytics and safety*, International Journal of Advanced Computer Science & Applications, vol. 15, no. 5, 2024.

[7] S. Chaudhary, V. Gkioulos, and S. Katsikas, *Developing metrics to assess the effectiveness of cybersecurity awareness program*, Journal of Cybersecurity, vol. 8, no. 1, p. tyac006, 2022.

[8] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, *A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions*, Electronics, vol. 12, no. 6, p. 1333, 2023.

[9] M. Thakur, *Cybersecurity threats and countermeasures in the digital age*, Journal of Applied Science and Education (JASE), vol. 4, no. 1, pp. 1-20, 2024.

[10] M. Aslam, D. Ye, A. Tariq, M. Asad, M. Hanif, D. Ndzi, and S. F. Jilani, *Adaptive machine learning-based distributed denial-of-service attacks detection and mitigation system for SDN-enabled IoT*, Sensors, vol. 22, no. 7, p. 2697, 2022.

[11] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, *Towards a machine learning-based framework for DDoS attack detection in software-defined IoT (SD-IoT) networks*, Engineering Applications of Artificial Intelligence, vol. 123, p. 106432, 2023.

[12] M. Memarzadeh, B. Matthews, and T. Templin, *Multiclass anomaly detection in flight data using semi-supervised explainable deep learning model*, Journal of Aerospace Information Systems, vol. 19, no. 2, pp. 83-97, 2022.

[13] A. Sahu, Y. A. B. El-Ebiary, K. A. Saravanan, K. Thilagam, G. R. Devi, A. Gopi, and A. I. Taloba, *Federated LSTM model for enhanced anomaly detection in cybersecurity: A novel approach for distributed threat*, International Journal of Advanced Computer Science & Applications, vol. 15, no. 6, 2024.

[14] M. Ozkan-Ozay, E. Akin, Ö. Aslan, S. Kosunalp, T. Iliev, I. Stoyanov, and I. Beloev, *A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cybersecurity solutions*, IEEE Access, 2024.

[15] M. Basnet and M. H. Ali, *A deep learning perspective on connected automated vehicle (CAV) cybersecurity and threat intelligence*, in Deep Learning and Its Applications for Vehicle Networks, CRC Press, pp. 39-56, 2023.

[16] J. Axali, L. Devereaux, A. Spencer, and F. Vasilev, *A multicriteria decision-making approach for ransomware detection using MITRE ATT&CK mitigation strategy*, Authorea Preprints, 2024.

[17] S. Lin, C. Feng, T. Jiang, and H. Jing, *Evaluation of network security grade protection combined with deep learning for intrusion detection*, IEEE Access, vol. 11, pp. 130990-131000, 2023.

[18] D. Javaheri, S. Gorgin, J. A. Lee, and M. Masdari, *Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives*, Information Sciences, vol. 626, pp. 315-338, 2023.

[19] T. A. S. Srinivas, G. Mahalaxmi, A. D. Donald, and R. Varaprasad, *Traffic prediction using a wide range of techniques: A review*, IUP Journal of Information Technology, vol. 19, no. 1, pp. 19-47, 2023.

[20] Z. Zhao, A. Hussain, N. Zhang, K. Ullah, S. Yin, A. Awsar, and S. M. El-Bahy, *Decision support system based on bipolar complex fuzzy Hamy mean operators*, Heliyon, vol. 10, no. 17, 2024.

[21] T. Mahmood, U. U. Rehman, S. Shahab, Z. Ali, and M. Anjum, *Decision-making by using TOPSIS techniques in the framework of bipolar complex intuitionistic fuzzy N-soft sets*, IEEE Access, vol. 11, pp. 105677-105697, 2023.

[22] D. B. Chakraborty and J. Yao, *Event prediction with rough-fuzzy sets*, Pattern Analysis and Applications, vol. 26, no. 2, pp. 691-701, 2023.

[23] Z. Tan, *Cybersecurity threat and awareness program dataset [Data set]*, Kaggle, https://doi.org/10.34740/KAGGLE/DSV/9665651, 2024.

[24] V. Werner de Vargas, J. A. Schneider Aranda, R. dos Santos Costa, P. R. da Silva Pereira, and J. L. Victória Barbosa, *Imbalanced data preprocessing techniques for machine learning: A systematic mapping study*, Knowledge and Information Systems, vol. 65, no. 1, pp. 31-57, 2023.

[25] A. A. Almazroi and N. Ayub, *Enhancing smart IoT malware detection: A GhostNet-based hybrid approach*, Systems, vol. 11, no. 11, p. 547, 2023.

[26] T. Verdonck, B. Baesens, M. Óskarsdóttir, and S. vanden Broucke, *Special issue on feature engineering editorial*, Machine Learning, vol. 113, no. 7, pp. 3917-3928, 2024.

[27] N. Malik, M. Shabir, T. M. Al-shami, R. Gul, and M. Arar, *A novel decision-making technique based on T-rough bipolar fuzzy sets*, Journal of Mathematics and Computer Science, vol. 33, pp. 275-289, 2024.

[28] M. Z. Naser and A. H. Alavi, *Error metrics and performance fitness indicators for artificial intelligence and machine learning in engineering and sciences*, Architecture, Structures and Construction, vol. 3, no. 4, pp. 499-517, 2023.