Study on the Implementation of Multimodal Continuous Authentication in Smartphones: A Systematic Review

Rahmad Syalevi[1], Aji Prasetyo[2], Rizal Fathoni Aji[3]
Faculty of Computer Science, University of Indonesia, Jakarta, Indonesia[1, 3]
Database Center, Indonesian Agency for Meteorology, Climatology, and Geophysics, Jakarta, Indonesia[2]

***Abstract*—Profound societal shifts result from the inception of the 4.0 age of the Industrial Revolution and rapid technological advancements. The widespread adoption of e-services has resulted in substantial reliance on smartphones to access diverse offerings. Even so, account breaches and data leaks are risks that users take when they rely so heavily on their smartphones. Authentication is an essential method of safeguarding personal information. The purpose of this study is to undertake a thorough review of the literature on the deployment and trends of multimodal biometric authentication on smartphones. The studies will look at several biometric modalities, such as behavioral and physiological characteristics, and the algorithms for pattern recognition used in continuous authentication systems. The results show various biometric authenticators and emphasize the importance of behavioral features in smartphone authentication. In addition, the research underlines the significance of machine learning algorithms in pattern identification for rapid and accurate analysis. This study helps to understand the present authentication technique landscape and gives ideas for future advances in safe and user-friendly smartphone authentication systems.**

Keywords—Authentication; continuous multimodal; biometric authenticator; smartphone

I. Introduction

The Fourth Industrial Revolution gave birth to significant social disruption, characterized by rapid and highly advanced technological advancements with a particular emphasis on artificial intelligence, big data, and integration systems [1]. This trend encourages every element of society to use electronic service systems in every activity, ranging from the world of business, banking [2], transportation [3], and social organization [4].

In addition, many people use smartphones to access various electronic services via the internet, with 6.4 billion users or 79 percent of the world's total users. The utilization rate of intelligent mobile devices is significantly higher than other devices, such as portable computers and tablets [5].

Internet connection on intelligent mobile devices carries the risk of security vulnerabilities such as account theft and data leakage of its users [6]. Authentication is a meaningful way to keep personal information, such as personal data and more, from falling into the wrong hands [7]. Android devices have used authentication schemes, including pin codes or passwords, patterns, fingerprints, and biometrics [8], where patterns, pins, and alphanumeric passwords are still the preferred way to log into Android devices [9], computers, and web applications such as email, cloud storage, and online shopping services [10], [11].

A knowledge-based authentication, physiological biometrics authentication, behavioral biometrics authentication, and multi-factor authentication are the essential components that comprise the taxonomy of user authentication systems on mobile devices [12]. Regarding security, knowledge-based verification uses information that only people and systems know. The secret can be text, like PINs, codes of letters and numbers, or a picture, like a pattern [12].

Traditional or knowledge-based single-factor authentication has become a significant concern for security practitioners and researchers. While still a viable option due to its simplicity, using PINs, passwords, and patterns as authentication inputs comes with several vulnerabilities, such as surfing and smudge attacks and susceptibility to intercept [13]. Also, password vulnerability causes most users to use passwords that are easy to guess and do not change regularly [14]. The Cybersecurity and Infrastructure Security Agency (CISA) has also added single-factor authentication, such as password matching, to gain access to a system as a bad practice [15].

Other approaches initially anticipated that multi-factor authentication would enhance security [16] and ease ongoing protection for computing devices [17] and other critical services [18] from unauthorized access by using more than two types of credentials [19], such as biometrics and secret knowledge [12]. However, the enhanced security force is still limited. This limitation is supported by other studies that have understood the failure of multi-factor authentication on mobile devices [20]. One flaw in this scheme is that an attacker attempts to intervene in a communication between two interacting parties and modify the message or information transmitted so that the attacker can gain access to confidential data or perform unlawful acts. Furthermore, synchronization issues, hardware alterations, or faults in the implementation of authentication protocols might be used by attackers to gain sensitive information or carry out illicit acts.

Continuous user authentication approaches on smartphones through sensors, multimodal behavioral biometrics, and machine learning models have been introduced in recent research [21], [22], [23] to resolve the previously mentioned issue, improve accuracy, and reduce interference in authentication mechanisms. This method gives a higher level of protection while accessing electronic services via mobile devices, such as smartphones. Previous research in [24] has also conducted systematic reviews of continuous multimodal biometrics but has yet to focus on smartphone implementation. Therefore, this study investigates the possibility of implementing continuous multimodal authentication in mobile devices such as smartphones.

The structure of this paper is as follows. Section II presents the related works. Section III clarifies the concept of multimodal biometrics. Section IV describes the methods used in the study. Section V provide the study's findings and discuss its implications. In Section VI, we present the conclusion and outline future work.

II. Related Work

We discovered limited papers focusing on multimodal continuous authentication in smartphones. Researchers have examined authentication in various ways. For instance, [12] conducted surveys of existing authentication methods on mobile devices, while [13] suggested a behavioral biometric authentication scheme as secure and convenient. Moreover, [17] concluded that biometric authentication alone was insufficient and proposed multi-factor authentication mechanisms for more robust security. The study in [20] explored security vulnerabilities in multi-factor authentication schemes on mobile devices, while [21] identified continuous authentication with behavioral biometrics in smartphones as insightful and challenging for adoption. Furthermore, [23] found that continuous multimodal biometric authentication offers high accuracy and improved security, and [24] suggested implementing and evaluating such systems to demonstrate their feasibility. Based on these studies, we aim to investigate the implementation of multimodal continuous authentication in mobile devices, such as smartphones.

III. Multimodal Biometric

Biometric refers to recognizing patterns that establish a person's identity by comparing biological or behavioral features of biometric attributes. Biometric traits are a highly convenient means of verifying an individual's identity, as they offer high security (difficult to replicate) and cannot be stolen, forgotten, or misplaced [25].

Fingerprints, palm prints, hand geometry, faces, eyes, ears, electrocardiograms, and electroencephalograms are all physiological biometrics used in modern smartphones. Tapping behavior, hand motions, noises, gait, and daily activities are all examples of biometric behavior [12].

A biometric system is, in essence, a pattern recognition system that collects biometric data from a person, extracts a set of features from that data, and then compares the extracted features to a background of templates saved in a database. This process is known as "biometric matching." To put it another way, a pattern recognition system is what a biometric system is. Its performance is determined by the context in which it is used; for example, depending on the context, it may function in either a verification or identification mode [25].

Unimodal and multimodal represent two distinct categories within biometric systems, with their primary distinction lying in the number of modalities employed for authentication purposes. Unimodal biometric systems, exemplified by fingerprint and facial recognition technologies, are easier to create since they only require one identity. However, they are vulnerable to problems like spoofing and poor identification. On the other hand, multimodal systems, such as those combining facial and voice recognition or iris and fingerprint recognition, provide enhanced protection, durability, and adaptability to external influences by employing multiple characteristics. Their intricacy, however, resides in figuring out what, when, and how to combine data for authentication across several modalities [24].

IV. Methodology

The research strategy used for this project was called a Systematic Literature Review (SLR). The SLR technique is a tried-and-true research approach when gathering and analyzing data on a specific issue. We have used the PRISMA guidelines provided by Matthew J. [26]. This SLR consists of four main steps: primary study planning and search, study collection, data extraction, and data synthesis. Section IV(A) identifies research objectives and questions as the first step. In Section IV(B) and IV(C), search strategy steps involve study selection criteria, study selection procedures, keyword formulation for research, and search queries. In Section IV(D), the final step requires quality assessment.

A. Research Question and Objectives

The primary purpose of this SLR is to explore the implementation of continuous multimodal authentication in Smartphones. We create research questions to focus on the objectives of this research.

RQ1: What biometrics is used for authentication on smartphones?

RQ2: What technique is used for pattern recognition in continuous authentication on smartphones?

Based on this research question, the focus of this research objective is to review trends that have occurred in recent years, particularly the use of continuous multimodal authentication on smartphones, and explore biometric combinations used for authentication on smartphones.

B. Search Strategy

In this study, we searched using the electronic databases IEEE Xplore and Scopus. We prepared several lists of keywords to search for relevant literature on multimodal biometric authentication in smartphones from selected electronic databases. The search query utilized was:

“continuous” AND (*biometric* OR *multi*) AND (“authentication” OR “verification” OR “validation”) AND “smartphone” OR “mobile phone.”

Queries applied to article titles, abstracts, and keywords to get relevant articles from electronic databases.

C. Selection Criteria

We analyze the query results that have been obtained by removing duplicate articles. Filtering is also done based on the article’s title, abstract, and keywords. In addition, we also use inclusion and exclusion criteria. Fig. 1 shows the PRISMA diagram for this meta-analysis.

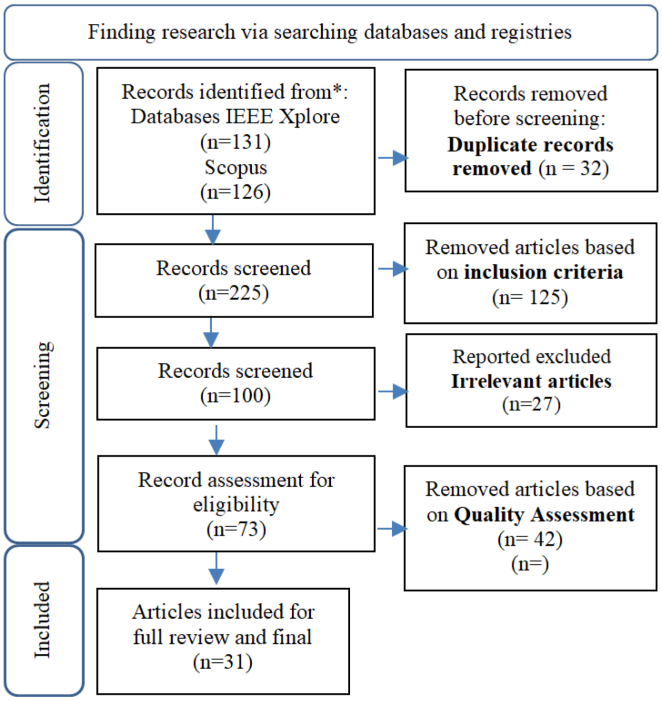
Finding research via searching databases and registries
Identification
Records identified from*: Databases IEEE Xplore (n=131) Scopus (n=126)
Records removed before screening: **Duplicate records removed** (n = 32)
Screening
Records screened (n=225)
Removed articles based on **inclusion criteria** (n= 125)
Records screened (n=100)
Reported excluded **Irrelevant articles** (n=27)
Record assessment for eligibility (n=73)
Removed articles based on **Quality Assessment** (n= 42) (n=)
Included
Articles included for full review and final (n=31)

Fig. 1. The PRISMA diagram for this meta-analysis.

We use the following inclusion criteria. The paper or article should talk about authentication in smartphones. In addition, papers or articles must be in English and published from 2018 – 2022 in journals or conference proceedings.

We used several article selection exclusion criteria in this study. Papers or articles discuss the continuous multimodal biometric authentication but not in smartphones. In addition, papers or articles in the title, abstract, or keyword section do not mention authentication; articles with survey methods or systematic reviews are not attached to the results of this study.

D. Quality Assessment

Quality assessment is used to assess the quality of the selected article. The quality assessment also evaluates whether the selected article is fully accessible and can answer our review. To determine consistency, we formulated some quality assessment questions.

QA1: Does the article mention the use of continuous multimodal biometric authentication, and is it clearly stated?

QA2: Does the article provide an answer to the formulated RQ?

QA3: Are the aims of the research clearly stated without ambiguity in the paper?

Yes or no can answer each question with weights of 1 and 0, respectively. The results are evaluated after an assessment of the quality of the entire article has been carried out. The quality assessment process is intended for all research articles according to quality assessment questions. Therefore, this review includes all 31 selected articles.

V. Result and Analysis

The study's conclusion will involve presenting research papers that investigate continuous authentication using multimodal methods. Additionally, the second step consists of conducting a mapping exercise to explore the application of biometrics based on specific biometric properties.

A. Significant Journal

In this literature review, 17 journal articles and 14 conference proceedings discuss continuous multimodal authentication. Here is a brief overview of the distribution of publications journals over the past five years. The result is shown in Table I.

Based on Table I, an in-depth analysis of the provided data reveals a diverse collection of journals across different quartiles. Within the esteemed Q1 quartile, we find a constellation of scholarly publications, including Computers & Security, Journal of Network and Computer Applications, IEEE Transactions on Industrial Informatics, IEEE Access, IEEE Internet of Things Journal, Human-centric Computing and Information Sciences, and IEEE Signal Processing Letters. Remarkably, these journals exhibit varying publication frequencies, ranging from 1 to 2, which discuss continuous authentication.

Transitioning to the intellectually stimulating Q2 quartile, we encounter an array of influential journals that contribute significantly to their respective fields. Noteworthy publications such as Electronics Microprocessors and Microsystems, IEEE Transactions on Information Forensics and Security, International Journal of Distributed Sensor Networks, and Sensors grace this quartile, each showcasing their research prowess with a single publication.

TABLE I. Distribution of Publications

Quartile	Journal Name	Quantity
Q3	International Journal of Advanced Computer Science and Applications	1
Q1	Computers & Security	1
Q1	Journal of Network and Computer Applications	2
Q1	IEEE Transactions on Industrial Informatics	1
Q1	IEEE Internet of Things Journal	1
Q2	Electronics	1
Q2	Microprocessors and Microsystems	1
Q1	IEEE Access	2
Q1	Human-centric Computing and Information Sciences	1
Q2	IEEE Transactions on Information Forensics and Security	1
Q2	International Journal of Distributed Sensor Networks	1
Q3	Wireless Communications and Mobile Computing	1
Q4	Indian Journal of Computer Science and Engineering	1
Q2	Sensors	1
Q1	IEEE Signal Processing Letters	1

Intriguingly, the scholarly landscape unveils the distinguished International Journal of Advanced Computer Science and Applications as the sole journal within the intellectually captivating Q3 quartile, signifying its profound impact with a singular publication.

B. Biometric Authenticators

A biometric is a pattern recognition system that establishes a person's identification by comparing biological or behavioral traits of biometric characteristics [26].

Table II presents a captivating exploration of the landscape surrounding biometric authentication within continuous multimodal biometric authentication systems on smartphones, offering a comprehensive overview of the diverse range of biometric authentication methods utilized in intelligent mobile authentication systems that seamlessly integrate multiple biometric modalities sustainably. From this table, we can identify and analyze various biometric authenticators employed in these systems, unveiling a rich tapestry of authentication techniques.

In addition, Fig. 2 illustrates the prevalence of different biometric modalities in authentication systems, revealing that 84% of behavioral characteristics are widely used for smartphone authentication, 13% choose to use physiological factors, and 3% combine behavioral and physiological characteristics. Notably, human gait, routine activities, and touch/swipe functions are emerging as highly preferred options for enhancing the security of continuous authentication processes.

TABLE II. A COMPILATION OF RESEARCH AND BIOMETRIC AUTHENTICATORS USED FOR CONTINUOUS MULTIMODAL AUTHENTICATION

Related Studies	Behavioral									Physiological			
	Gait	Gesture	Hand Movements	Handwriting	Keystroke	Routine Activities	Tapping	Touch/ Swipe	Mouth Movements	Ear	Face	Eye	Palmprint
[27]								√					
[28]	√												
[29]		√			√								
[30]	√												
[31]							√	√					
[32]													√
[33]	√					√							
[34]											√		
[35]									√				
[36]						√							
[37]	√					√							
[38]					√								
[39]											√		
[40]						√							
[41]									√		√	√	
[42]			√										
[43]			√				√						
[44]								√					
[45]		√											
[46]			√										
[47]	√			√									
[48]										√			
[49]								√					
[50]								√					
[51]			√										
[52]	√												
[53]						√							
[54]			√		√		√						
[55]						√							
[56]					√			√					
[57]								√					

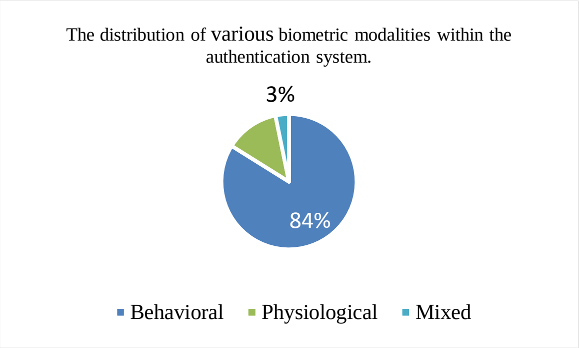

Fig. 2. The proportion of diverse biometric modalities utilized in the authentication system.

An innovative smartphone unlock scheme to improve user authentication through swipe behavior becomes a unique approach where the user selects a background image and performs a swipe action at a specified location on the smartphone screen. This combination ensures secure and reliable authentication, providing an additional layer of protection for smartphone users [27]. Other combinations, such as swipe and tap, result in increased security through continuous user authentication by paying attention to factors such as vibrations from walking, the effects of different positions, and trembling hands in cold temperatures [31] and the number of tap gestures implemented without any combination [49], [50], [57].

The continuous implementation of authentication and identification security is also demonstrated using behavioral characteristics in everyday life. Activities of daily living, such as walking, typing, and clapping, can be used for authentication and biometric identification. This demonstrates the feasibility of using natural activities for continuous biometrics with the help of smartphone motion sensors and inertial measurement datasets [53], [55]. Another approach through an innovative scheme also offers a dynamic and personalized user validation process by analyzing six everyday activities: walking, running, standing, sitting, walking up, and walking down. The variety of positions for smartphone placement on the user's body affects the user's recognition of each specific activity. This can optimize sensor placement and improve the overall performance of recognition systems [40].

The development of human gait recognition for smartphone access shows the advantages of biometric authentication methods to enhance security and prevent illegal user access [28]. The system's hidden nature, which does not require user interaction, further confirms its advantages as a convenient and user-friendly layer of security [30]. By utilizing smartphones' built-in inertial sensors, data collection can be done smoothly without burdening the user, making it a highly efficient, scalable, and robust modality for smartphone user authentication [33], [52].

Another approach in the realm of physiological characteristics, using the front-facing camera on devices, enables capturing the user's facial features and facial attributes (e.g., eyes) [39], [41]. Current face authentication approaches train the system using facial data from a single context or several contexts with no separation. However, camera exposure recognition is essential to improve facial recognition performance in different circumstances. The contingency for elevated accuracy thresholds arises when illumination conditions play a pivotal role in facial image recognition, owing to their substantial impact [39].

MetaEar is a cutting-edge method of modeling and authenticating Ear-Related Transfer Function (ERTF) biometrics from the human ear using Frequency-Modulated Continuous Wave (FMCW) ultrasonics. The system uses FMCW ultrasonic waves and twin microphones to record and analyze the feedback sound wave for extracting ERTF characteristics [48].

C. Pattern Recognition Techniques

Pattern recognition techniques play an essential role in smartphone continuous biometric authentication systems, enabling the automatic identification and classification of patterns in data for efficient and accurate analysis. Recent advances in machine learning algorithms have revolutionized pattern recognition, offering powerful tools for extracting meaningful information from complex data sets. Fig. 3 depicts utilization patterns of classification techniques in continuous multimodal biometric authentication systems based on an SLR.

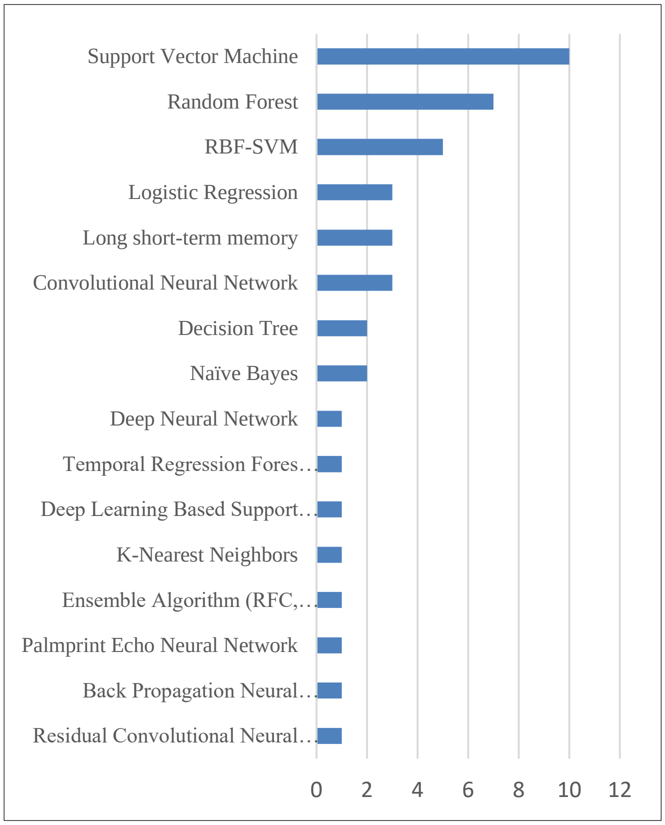

Fig. 3. The utilization patterns of classification techniques in continuous multimodal biometric authentication systems.

The study conducted by Benegui used four different Convolutional Neural Network (CNN) architectures with varying depths as embedding extractors [30]. These networks have a similar structure, using SoftMax activation at the classification layer and Rectified Linear Units (ReLU) at another layer. Experimental results demonstrate the outstanding suitability of the gait-based dataset for the task at hand, enabling the passive collection of gait data and continuous user identification, serving as a robust continuous authentication mechanism.

In addition, CNN shows superior performance compared to traditional machine learning classifiers such as Support Vector Machine (SVM), k-nearest Neighbors, Random Forest, and Linear Discriminant Analysis (LDA) when applied to behavioral characteristics based on routine activities [33]. The inherent time-invariant nature of CNN makes it particularly suitable for processing time series data in behavioral biometrics, such as the analysis of hand movements [42].

The Long Short-Term Memory (LSTM) model undergoes an optimization process to determine the optimal set of parameters for a particular task. Compared to CNN and ConvLSTM architectures, six-layer CNN outperforms ConvLSTM in terms of accuracy and generalization [30]. An LSTM-based architecture is used in the authentication model to capture user behavior patterns while holding their smartphone, regardless of activity. As shown through keystroke dynamics analysis, LSTM classifiers show promising potential in predicting user behavior, even with limited data availability [54].

Unsupervised user verification demonstrates remarkable performance with minimal training time. The authentication system effectively handles various activities and routines using a dedicated single-class SVM model, resulting in exceptional accuracy [37]. Moreover, SVM classifiers are trained on facial characteristics using advanced methods like face warping and textual feature extraction, ensuring precise face identification [41]. The authentication process further incorporates the analysis of touchscreen interactions and subtle micro-gestures, enhancing the overall accuracy and reliability of the system [31].

In other techniques, Random Forest (RF) is often used for prediction and classification because the computational complexity is relatively low, and the training is faster [50]. RF technique is also utilized to identify motion status, touch gesture characteristics, keyboard patterns, and short-term activities. [29], [45], [50]. The pattern recognition field also extensively uses another statistical method called logistic regression. On the other hand, the author favors this option due to its simplicity and dependability and the fact that it is included in the Weka library [29], [39].

D. Discussion

We discovered 13 biometric authenticators that use behavioral and physiological aspects for authentication. Behavioral factors are used most frequently for smartphone authentication, followed by physiological and mixed techniques. In addition, we identified 16 pattern recognition approaches critical for constructing a continuous multimodal biometric authentication system. Fig. 3 depicts the ranked pattern recognition techniques that were used.

Based on these findings, it can be concluded that behavioral traits have been widely implemented in smartphone authentication. The combination of biometric authentication ensures secure and reliable authentication, providing an additional layer of protection for smartphone users. Furthermore, selecting pattern recognition techniques is crucial in continuous biometric authentication systems on smartphones. This ensures the automatic identification and classification of data patterns for efficient and precise analysis.

VI. Conclusion and Future Works

A. Conclusion

The SLR method was employed in this study to investigate the implementation of continuous multimodal authentication in Smartphones. The study's findings revealed a diverse collection of journals across different quartiles, with notable publications discussing continuous authentication in Q1 and Q2 journals. The examination of biometric authenticators revealed a diverse set of methodologies, with behavioral traits being the most often utilized for smartphone authentication. Behavioral variables, such as human movement and customary activities, are used for smartphone authentication, followed by physiological characteristics and a mix of both.

Additionally, the research emphasized the popularity of pattern recognition algorithms, including neural networks based on convolution and long-term and short-term memory models. These showed more extraordinary performance when evaluating behavioral biometrics. Support Vector Machine, Random Forest, and Logistic Regression were also used for classification and prediction. Overall, the study provided insights into the landscape of biometric authentication and pattern recognition techniques in continuous multimodal biometric authentication systems on smartphones.

This research contributes to understanding the implementation of continuous multimodal authentication on smartphones. The findings highlight the importance of behavioral characteristics and the effectiveness of pattern recognition techniques in enhancing security and user authentication. The diverse range of journals and the prevalence of advanced machine-learning algorithms in the field demonstrate significant advancements in this area of research. Future studies can further explore the performance and usability of these authentication methods and investigate new approaches to enhance continuous authentication on smartphones.

B. Limitations and Future Works

The research had certain limitations. Initially, it concentrated primarily on multimodal continuous authentication in smartphones. Second, it only looked at multimodal biometrics, not unimodal biometrics. Future studies could investigate a broader range of devices that require authentication techniques. Furthermore, additional research might focus on unimodal biometrics or compare unimodal and multimodal biometrics across different devices.

References

[1] R. Sharma, C. J. C. Jabbour, and A. B. Lopes de Sousa Jabbour, “Sustainable manufacturing and industry 4.0: what we know and what we don’t,” Journal of Enterprise Information Management, vol. 34, no. 1, pp. 230–266, Jan. 2021, doi: 10.1108/JEIM-01-2020-0024.

[2] B. Machkour and A. Abriane, “Industry 4.0 and its Implications for the Financial Sector,” Procedia Comput Sci, vol. 177, pp. 496–502, 2020, doi: 10.1016/j.procs.2020.10.068.

[3] K. Mbowa, C. Aigbavboa, O. Akinshipe, and D. W. Thwala, “An overview of key emerging technologies transforming public transportation in the Fourth Industrial Revolution era,” IOP Conf Ser Mater Sci Eng, vol. 1107, no. 1, p. 012169, Apr. 2021, doi: 10.1088/1757-899X/1107/1/012169.

[4] OK. M. Fajar Ikhsan, R. Islam, K. Azman Khamis, and A. Sunjay, “Impact of digital economic liberalization and capitalization in the era of industrial revolution 4.0: case study in Indonesia,” Problems and Perspectives in Management, vol. 18, no. 2, pp. 290–301, Jun. 2020, doi: 10.21511/ppm.18(2).2020.24.

[5] Kompas.com, “Jumlah Pengguna Ponsel di Dunia Tembus 5 Miliar,” Kompas. Accessed: Apr. 26, 2023. [Online]. Available: https://tekno.kompas.com/read/2021/09/02/09144137/jumlah-pengguna-ponsel-di-dunia-tembus-5-miliar

[6] A. C. Cinar and T. B. Kara, “The current state and future of mobile security in the light of the recent mobile security threat reports,” Multimed Tools Appl, vol. 82, no. 13, pp. 20269–20281, May 2023, doi: 10.1007/s11042-023-14400-6.

[7] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,” in 2012 IEEE Symposium on Security and Privacy, IEEE, May 2012, pp. 553–567. doi: 10.1109/SP.2012.44.

[8] D. Kunda and M. Chishimba, “A Survey of Android Mobile Phone Authentication Schemes,” Mobile Networks and Applications, vol. 26, no. 6, pp. 2558–2566, Dec. 2021, doi: 10.1007/s11036-018-1099-7.

[9] N. Malkin, M. Harbach, A. De Luca, and S. Egelman, “The Anatomy of Smartphone Unlocking,” GetMobile: Mobile Computing and Communications, vol. 20, no. 3, pp. 42–46, Jan. 2017, doi: 10.1145/3036699.3036712.

[10] V. Zimmermann and N. Gerber, “The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes,” Int J Hum Comput Stud, vol. 133, pp. 26–44, Jan. 2020, doi: 10.1016/J.IJHCS.2019.08.006.

[11] S. Hadzidedic, S. Fajardo-Flores, and B. Ramic-Brkic, “User perceptions and use of authentication methods: insights from youth in Mexico and Bosnia and Herzegovina,” Information & Computer Security, vol. 30, no. 4, pp. 615–632, Oct. 2022, doi: 10.1108/ICS-07-2021-0105.

[12] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, “User authentication on mobile devices: Approaches, threats and trends,” Computer Networks, vol. 170, p. 107118, Apr. 2020, doi: 10.1016/j.comnet.2020.107118.

[13] C. Li, J. Jing, and Y. Liu, “Mobile user authentication-Turn it to unlock,” in 2021 6th International Conference on Mathematics and Artificial Intelligence, New York, NY, USA: ACM, Mar. 2021, pp. 101–107. doi: 10.1145/3460569.3460577.

[14] I. Mannuela, J. Putri, Michael, and M. S. Anggreainy, “Level of Password Vulnerability,” in 2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI), IEEE, Oct. 2021, pp. 351–354. doi: 10.1109/ICCSAI53272.2021.9609778.

[15] Cybersecurity and Infrastructure Security Agency, “CISA Adds Single-Factor Authentication to list of Bad Practices,” America’s Cyber Defense Agency. Accessed: Apr. 26, 2023. [Online]. Available: https://www.cisa.gov/news-events/alerts/2021/08/30/cisa-adds-single-factor-authentication-list-bad-practices

[16] E. M. Scheidt and E. Domangue, “Multiple factor-based user identification and authentication.” Google Patents, 2005.

[17] A. Bhargav-Spantzel, A. C. Squicciarini, S. Modi, M. Young, E. Bertino, and S. J. Elliott, “Privacy preserving multi-factor authentication with biometrics,” J Comput Secur, vol. 15, no. 5, pp. 529–560, Jul. 2007, doi: 10.3233/JCS-2007-15503.

[18] R. K. Banyal, P. Jain, and V. K. Jain, “Multi-factor Authentication Framework for Cloud Computing,” in 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation, IEEE, Sep. 2013, pp. 105–110. doi: 10.1109/CIMSim.2013.25.

[19] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-Factor Authentication: A Survey,” Cryptography, vol. 2, no. 1, p. 1, Jan. 2018, doi: 10.3390/cryptography2010001.

[20] Q. Wang and D. Wang, “Understanding Failures in Security Proofs of Multi-Factor Authentication for Mobile Devices,” IEEE Transactions on Information Forensics and Security, vol. 18, pp. 597–612, 2023, doi: 10.1109/TIFS.2022.3227753.

[21] P. K. Rayani and S. Changder, “Sensor-based continuous user authentication on smartphone through machine learning,” Microprocess Microsyst, vol. 96, p. 104750, Feb. 2023, doi: 10.1016/j.micpro.2022.104750.

[22] H. Purohit and P. K. Ajmera, “Multi-modal biometric fusion based continuous user authentication for E-proctoring using hybrid LCNN-Salp swarm optimization,” Cluster Comput, vol. 25, no. 2, pp. 827–846, 2022, doi: 10.1007/s10586-021-03450-w.

[23] D. B. Purba and B. N. Sari, “Implementasi Jaringan Hierarki Attention Untuk Klasifikasi Basis Data Multimodal Biometrik,” JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), vol. 7, no. 3, pp. 632–638, Aug. 2022, doi: 10.29100/jipi.v7i3.2879.

[24] R. Ryu, S. Yeom, S. H. Kim, and D. Herbert, “Continuous Multimodal Biometric Authentication Schemes: A Systematic Review,” IEEE Access, vol. 9, pp. 34541–34557, 2021, doi: 10.1109/ACCESS.2021.3061589.

[25] A. K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349.

[26] M. J. Page et al., “The PRISMA 2020 statement: an updated guideline for reporting systematic reviews,” Syst Rev, vol. 10, no. 1, pp. 1–11, 2021, doi: 10.1186/s13643-021-01626-4.

[27] W. Li, J. Tan, W. Meng, Y. Wang, and J. Li, “SwipeVLock: A Supervised Unlocking Mechanism Based on Swipe Behavior on Smartphones,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 11806 LNCS. School of Computer Science, Guangzhou University, Guangzhou, China, pp. 140–153, 2019. doi: 10.1007/978-3-030-30619-9_11.

[28] G. K. Chaitanya and K. R. Sekhar, “A human gait recognition against information theft in smartphone using residual convolutional neural network,” International Journal of Advanced Computer Science and Applications, vol. 11, no. 5, pp. 333–340, 2020, doi: 10.14569/IJACSA.2020.0110544.

[29] M. Smith-Creasey and M. Rajarajan, “A novel word-independent gesture-typing continuous authentication scheme for mobile devices,” Comput Secur, vol. 83, pp. 140–150, 2019, doi: 10.1016/j.cose.2019.02.001.

[30] C. Benegui, “A deep learning approach to subject identification based on walking patterns,” in Procedia Computer Science, Department of Computer Science, University of Bucharest, Romania, 2021, pp. 642–649. doi: 10.1016/j.procs.2021.08.066.

[31] A. Garbuz, A. Epishkina, and K. Kogos, “Continuous Authentication of Smartphone Users via Swipes and Taps Analysis,” in 2019 European Intelligence and Security Informatics Conference (EISIC), 2019, pp. 48–53. doi: 10.1109/EISIC49498.2019.9108780.

[32] L. Wang, W. Chen, N. Jing, Z. Chang, B. Li, and W. Liu, “AcoPalm: Acoustical Palmprint-Based Noncontact Identity Authentication,” IEEE Trans Industr Inform, vol. 18, no. 12, pp. 9122–9131, 2022, doi: 10.1109/TII.2022.3176627.

[33] B. Chakraborty, K. Nakano, Y. Tokoi, and T. Hashimoto, “An Approach for Designing Low Cost Deep Neural Network based Biometric Authentication Model for Smartphone User,” in TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), 2019, pp. 772–777. doi: 10.1109/TENCON.2019.8929241.

[34] L. Junfeng, “An Efficient Multibiometric-based Continuous Authentication Scheme,” in 2022 IEEE 10th International Conference on Computer Science and Network Technology (ICCSNT), 2022, pp. 118–121. doi: 10.1109/ICCSNT56096.2022.9972922.

[35] A. B. Wong, “Authentication through Sensing of Tongue and Lip Motion via Smartphone,” in 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), 2021, pp. 1–2. doi: 10.1109/SECON52354.2021.9491596.

[36] M. Abuhamad, T. Abuhmed, D. Mohaisen, and D. Nyang, “AUToSen: Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors,” IEEE Internet Things J, vol. 7, no. 6, pp. 5008–5020, 2020, doi: 10.1109/JIOT.2020.2975779.

[37] E. Klieme, C. Tietz, and C. Meinel, “Beware of SMOMBIES: Verification of Users Based on Activities While Walking,” in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, Aug. 2018, pp. 651–660. doi: 10.1109/TrustCom/BigDataSE.2018.00096.

[38] L. De-Marcos, J.-J. Martínez-Herráiz, J. Junquera-Sánchez, C. Cilleruelo, and C. Pages-Arévalo, “Comparing machine learning classifiers for continuous authentication on mobile devices by keystroke dynamics,” Electronics (Switzerland), vol. 10, no. 14, 2021, doi: 10.3390/electronics10141622.

[39] M. Smith-Creasey, F. A. Albalooshi, and M. Rajarajan, “Context Awareness for Improved Continuous Face Authentication on Mobile Devices,” in 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2018, pp. 644–652. doi: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00115.

[40] M. Ehatisham-ul-Haq, M. Awais Azam, U. Naeem, Y. Amin, and J. Loo, “Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing,” Journal of Network and Computer Applications, vol. 109, pp. 24–35, 2018, doi: 10.1016/j.jnca.2018.02.020.

[41] M. Smith-Creasey, F. A. Albalooshi, and M. Rajarajan, “Continuous face authentication scheme for mobile devices with tracking and liveness detection,” Microprocess Microsyst, vol. 63, pp. 147–157, 2018, doi: 10.1016/j.micpro.2018.07.008.

[42] J. Dybczak and P. Nawrocki, “Continuous authentication on mobile devices using behavioral biometrics,” in 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid), 2022, pp. 1028–1035. doi: 10.1109/CCGrid54584.2022.00125.

[43] Ö. D. Incel et al., “DAKOTA: Sensor and Touch Screen-Based Continuous Authentication on a Mobile Banking Application,” IEEE Access, vol. 9, pp. 38943–38960, 2021, doi: 10.1109/ACCESS.2021.3063424.

[44] J. Mallet, L. Pryor, R. Dave, N. Seliya, M. Vanamala, and E. Sowells-Boone, “Hold On and Swipe: A Touch-Movement Based Continuous Authentication Schema based on Machine Learning,” in 2022 Asia Conference on Algorithms, Computing and Machine Learning (CACML), 2022, pp. 442–447. doi: 10.1109/CACML55074.2022.00081.

[45] M. A. Alqarni, S. H. Chauhdary, M. N. Malik, M. Ehatisham-ul-Haq, and M. A. Azam, “Identifying smartphone users based on how they interact with their phones,” Human-centric Computing and Information Sciences, vol. 10, no. 1, 2020, doi: 10.1186/s13673-020-0212-7.

[46] A. Bhattarai and A. Siraj, “Increasing Accuracy of Hand-Motion Based Continuous Authentication Systems,” in 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2018, pp. 70–76. doi: 10.1109/UEMCON.2018.8796725.

[47] R. Matovu, A. Serwadda, D. Irakiza, and I. Griswold-Steiner, “Jekyll and Hyde: On The Double-Faced Nature of Smart-Phone Sensor Noise Injection,” in 2018 International Conference of the Biometrics Special Interest Group (BIOSIG), 2018, pp. 1–6. doi: 10.23919/BIOSIG.2018.8553043.

[48] Z. Chang, L. Wang, B. Li, and W. Liu, “MetaEar: Imperceptible Acoustic Side Channel Continuous Authentication Based on ERTF,” Electronics (Switzerland), vol. 11, no. 20, 2022, doi: 10.3390/electronics11203401.

[49] Z. Shen, S. Li, X. Zhao, and J. Zou, “MMAuth: A Continuous Authentication Framework on Smartphones Using Multiple Modalities,” IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1450–1465, 2022, doi: 10.1109/TIFS.2022.3160361.

[50] X. Liang, F. Zou, L. Li, and P. Yi, “Mobile terminal identity authentication system based on behavioral characteristics,” Int J Distrib Sens Netw, vol. 16, no. 1, 2020, doi: 10.1177/1550147719899371.

[51] X. Zhang, P. Zhang, and H. Hu, “Multimodal continuous user authentication on mobile devices via interaction patterns,” Wirel Commun Mob Comput, vol. 2021, 2021, doi: 10.1155/2021/5677978.

[52] K. Ambika and K. R. Radhika, “Multi-Modality Driven Sparse Inertial Feature Representation for Gait-Based Scalable Person Authentication System,” Indian Journal of Computer Science and Engineering, vol. 13, no. 4, pp. 1308–1330, 2022, doi: 10.21817/indjcse/2022/v13i4/221304045.

[53] M. Naseer, M. A. Azam, M. Ehatisham-Ul-Haq, W. Ejaz, and A. Khalid, “ADLAuth: Passive authentication based on activity of daily living using heterogeneous sensing in smart cities,” Sensors (Switzerland), vol. 19, no. 11, 2019, doi: 10.3390/s19112466.

[54] D. J. Gunn, K. Roy, and K. Bryant, “Simulated Cloud Authentication Based on Touch Dynamics with SVM,” in 2018 IEEE Symposium Series on Computational Intelligence (SSCI), 2018, pp. 639–644. doi: 10.1109/SSCI.2018.8628762.

[55] G. M. Weiss, K. Yoneda, and T. Hayajneh, “Smartphone and Smartwatch-Based Biometrics Using Activities of Daily Living,” IEEE Access, vol. 7, pp. 133190–133202, 2019, doi: 10.1109/ACCESS.2019.2940729.

[56] S. Y. Ooi and A. B.-J. Teoh, “Touch-Stroke Dynamics Authentication Using Temporal Regression Forest,” IEEE Signal Process Lett, vol. 26, no. 7, pp. 1001–1005, 2019, doi: 10.1109/LSP.2019.2916420.

[57] H. C. Volaka, G. Alptekin, O. E. Basar, M. Isbilen, and O. D. Incel, “Towards continuous authentication on mobile phones using deep learning models,” in Procedia Computer Science, Department of Computer Engineering, Galasaray University, Istanbul, 34349, Turkey, 2019, pp. 177–184. doi: 10.1016/j.procs.2019.08.027.