Parameter-Driven Evaluation of Zero Trust Security in Blockchain Networks Under Dynamic Threats

Samuthira Pandi V[1]*, T. Vijayanandh[2], A. Jeyamurugan[3], M.D. Boomija[4],
V. Parimala[5], S. Preena Jacinth Shalom[6], Lavanya. M[7], Veena. K[8]
Centre for Advanced Wireless Integrated Technology, Chennai Institute of Technology, Chennai, Tamil Nadu, India [1]
Dept. Electronics and Communication Engineering, Vel Tech Rangarajan Dr.Sagunthala
R&D Institute of Science and Technology, Chennai, Tamil Nadu, India [2]
Assistant Professor (Senior Grade)-Dept. of Artificial Intelligence and Data Science-Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, #42, Avadi – Vel Tech Road, Vel Nagar, Chennai, Tamil Nadu, India [3]
Dept. Computer Science and Engineering (Cyber Security), Prathyusha Engineering College, Chennai, Tamil Nadu, India [4]
Dept. Electronics and Communication Engineering, Chennai Institute of Technology, Chennai, Tamil Nadu, India [5]
Dept. Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamil Nadu, India [6]
Dept. Artificial Intelligence and Data Science, Adhiparasakthi College of Engineering, Kalavai, Tamil Nadu, India [7]
Dept. Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India [8]

***Abstract*—In this study, we investigate a parameterized method to evaluate the Zero Trust (ZT) security model integrated with blockchain networks under dynamic cyberattack conditions. Existing static trust-based security models fail to adapt to evolving adversarial behavior and dynamic attack conditions. To address these deficiencies, a discrete-time simulation model is constructed a discrete-time simulation model is developed to capture dynamic trust evolution, probabilistic attack patterns, and threshold-based access control within a financial network. In this regard, the proposed model considers significant parameters such as the probability of attack, trust decay rate, and access, isolation, and quarantine thresholds to evaluate their impact on network security performance. From the results, a significant correlation is noted between trust, mitigation, adversarial intensity, and policy parameter tuning. For instance, a strict threshold policy results in improved attack mitigation but compromises network participation, while a lenient approach results in improved network participation but compromises network security. The proposed framework is a more adaptive, scalable, and robust approach compared to conventional static approaches in addressing dynamic threats. From the results, optimal tuning of parameters is a fundamental aspect in achieving a balance in security enforcement in blockchain-based zero-trust networks.**

Keywords*—Zero trust; blockchain security; trust management; cyber-attack simulation; access control; financial networks

I. Introduction

The security of blockchain technology is ensured by its decentralized nature, cryptographic hashing, and consensus algorithms. However, there are still significant security risks in a distributed environment within financial institutions, and many attack vectors could create either financial/data-related issues, including 51% attacks, smart contract vulnerabilities, double-spending of digital assets, and breaches of privacy [1], [2]. With blockchain applications increasingly utilized beyond just cryptocurrency platforms to protect their integrity and security, there is an urgent need to implement security controls to mitigate risk to digital assets and to all blockchain-enabled applications. As highlighted in this report, proposed security solutions provide mechanisms to improve blockchain security through enhanced consensus mechanisms, multi-signature wallets, cold storage, zero-knowledge proofs, and periodic security audits [3], [4].

The Ethereum DAO hack, along with Walmart's use of blockchain technology, demonstrates how significantly safe coding, monitoring, and community involvement address exploits within blockchain security [5]. AI-powered threat analysis, quantum-resistant cryptography, and decentralized identity management are improving blockchain security at an accelerating rate. ZT principles introduce new requirements requiring continuous verification in order to provide continuous authentication for every user, device, and transaction, removing implicit trust as a factor for those entities [6]. The principle of least privilege restricts access on a need-to-know basis, limiting the attack surface and any potential consequences of a security incident on the system. Moreover, adaptive isolation or quarantine mechanisms make it possible for the network to react in real time to suspicious activity, thus minimizing the damage potential of compromised hosts [7]. The increased use of blockchain technology in financial and distributed systems has resulted in a significant increase in the attack surface. This makes the process of enforcing security more complex and challenging under adaptive and dynamic attack scenarios. In this regard, the existing perimeter and static trust models are not effective in addressing the challenges, especially in scenarios where attackers are highly adaptive and dynamic. Therefore, there is a critical need to develop adaptive and data-driven security models that can address the challenges while ensuring transparency [8].

When combined, the ZT principles provide a very robust base for a security framework, which can be implemented in a distributed, highly interconnected environment. Modern cyber threats have become more dynamic and sophisticated. Today, they employ random, adaptive, and targeted attack strategies [9]. Random attack strategies exploit vulnerabilities in users, devices, and transactions without targeting them; they do so by

*Corresponding author.

using automated scanning to determine potential targets [10]. Adaptive attack strategies adapt their approach based on the operational performance of existing defenses. Targeted attack strategies identify and exploit high-value resources by way of reconnaissance and tailored malware delivery [11]. The increasing complexity and coordination of these types of attacks have made traditional, static defense systems ineffective. Therefore, adaptive defense approaches such as moving target and mimic are employed to dynamically change system configurations and limit attack success [12], [13].

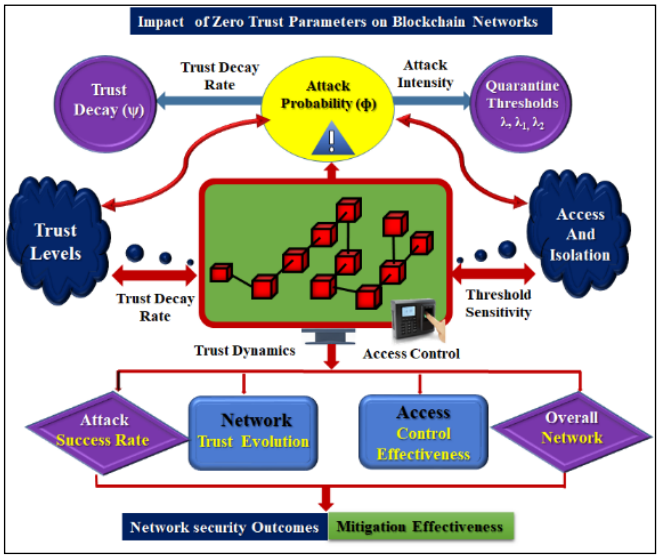

Fig. 1. Zero-trust blockchain framework illustrating trust decay (ψ), attack probability (φ), and attack intensity governing node trust and triggering quarantine thresholds (λ, λ1, λ2).

This research examines a financial network using a ZT Security Policy model for blockchain-enabled networks using a discrete-time simulation framework. Our model records trust evolution, probabilistic cyber-attacks, and threshold-based access control, which enables us to systematically vary our input parameters; i.e., attack probability (φ), trust decay rate (ψ), and access, isolation, and quarantine thresholds (λ, λ1, λ2). This analysis quantitatively evaluates how ZT policy tuning influences security effectiveness and resilience against evolving threats. The blockchain security framework using a ZT policy is shown in Fig. 1. A complete mathematical formulation of evaluation parameters has been shown in the system model section. This work has dynamically controlled access permissions based on user activity and device conditions, thereby enhancing security against various forms of insider threats and compromised credentials [17]. Various provisions have been made to quarantine or isolate devices to prevent lateral movement within networks. There have also been provisions for quarantining or isolating devices to prevent lateral movement within networks. Implementing ZTS in distributed, cloud, and hybrid environments has consistently yielded a higher security posture, a smaller attack surface area, and a reduction in risk from both internal and external threats [18]. Traditional centralized architectures are subject to single points of failure data is at risk of being tampered with or accessed by an unauthorized party. Blockchain is a shared and permanent ledger that offers a consolidated solution for the storage of all network and transaction data, including details of transactions, access logs, and events on the network [19].

Several studies have investigated the use of blockchain technology as a decentralized security layer for financial and distributed networks. This interest arises from its core characteristics, which include immutability, cryptographic security, decentralization, and consensus mechanisms. These features reinforce trust and improve the auditability of transactions [20], [21]. Access independence, decentralized identity management, and secure event logging are three examples of how blockchain technology improves accountability and resiliency against insider threats and data manipulation attacks. The majority of the work done in this area, however, is focused on static security policies and fixed trust assumptions (i.e., fixed levels of trust assigned to each user), with limited views into how dynamically changing levels of trust and changes in attack conditions affect the long-term operational behavior of a system [22].

Despite recent progress in zero-trust architectures and blockchain-based security systems, limited research builds on existing studies. Existing studies primarily rely on static trust assumptions and fail to capture the dynamic interplay among trust evolution, probabilistic cyberattacks, and adaptive countermeasure implementation. Most existing frameworks also fail to conduct a systematic analysis of how variations in trust decay, attack severity, and access control limits affect overall system performance. Furthermore, few efforts have explored how to combine blockchain-based auditability with dynamic ZT enforcement in one simulation model. These issues highlight the importance of developing a comprehensive, parameter-driven analysis to measure security-performance trade-offs under evolving threat conditions [23].

This study defines the key terms below to facilitate clarity and consistency throughout the entire study. The ZT Model defines a paradigm of security whereby no entity (e.g., user, device, or node) is by default trusted, and every access request must be continually verified. Evaluation parameters are those controllable variables used to perform the simulations, including the attack probability (φ), trust decay rate (ψ), and threshold values (λ, λ1, λ2). Security metrics are those quantitative measures used to evaluate the performance of a system (e.g., average network trust, number of attacks detected, and number of nodes quarantined). Policy enforcement mechanisms comprise rule-based actions initiated upon reaching predefined trust thresholds, including access authorization, isolation, and quarantine. The definitions provided above are uniformly applied throughout this study to ensure uniformity of interpretation. A list of key terms used in this study is provided in Table I to enhance clarity in the terminology used throughout this study.

TABLE I. KEY TERMINOLOGY AND DEFINITIONS USED IN THE ZT BLOCKCHAIN SECURITY MODEL

Term	Definition
ZT Model	Continuous verification, no implicit trust
Evaluation Parameters	φ, ψ, λ, λ1, λ2
Security Metrics	Trust, attacks, quarantines
Policy Enforcement	Access, isolation, quarantine

The major contribution of this study provides five outcomes:

- A simulation-based model of zero-trust security mechanisms in conjunction with an evaluation of a dynamic cyberattack environment and blockchain networks.
- A dynamic trust model that incorporates trust decay, the probabilistic nature of an attack, and threshold-based access controls.
- A systematic study of the sensitivity of overall performance to several factors or variables, including (but not limited to) the attack probability and trust decay rate; fixed thresholds for access control and quarantine; and the isolation thresholds.
- A blockchain-based mechanism for documenting security events, allowing for the processing of security event data into reports that are transparent, traceable, and auditable.
- Finally, this framework offers insight into the trade-off between security and performance so that tuning of parameters can enhance resilience and operational continuity.

The rest of this study has the following organization: Section II - Literature Review; Section III - System Modeling; Section IV - Simulation Design; Section V - Results & Analysis; and Section VI - Conclusion.

II. Literature Survey

ZT Security is emerging as a key term in the realm of network security. It solves many of the limitations of traditional perimeter-based security methods. Forrester Research first introduced the concept of ZT Security in 2010, positing that ZTS gives no inherent trust whatsoever to any user, and thus all access requests must be continually authenticated [14], [15]. Some research studies indicate that strict enforcement of policy-based access control without the use of identity management, multi-factor authentication, and the health of trusted devices cannot be carried out consistently. Users and services should also have access only to those resources necessary for them to conduct their business (i.e., as per the principles of attribute-based access control and least privilege) [16].

There have been many innovations regarding dynamic trust-update models, enabling real-time changes in user access permissions based on user activity and device context, enhancing protection from insider attacks and compromised credentials [17]. There have also been provisions for quarantining or isolating devices to prevent lateral movement within networks. Implementing ZTS in distributed, cloud, and hybrid environments has consistently yielded a higher security posture, a smaller attack surface area, and a reduction in risk from both internal and external threats [18]. Traditional centralized architectures are subject to single points of failure data is at risk of being tampered with or accessed by an unauthorized party. Blockchain is a shared and permanent ledger that offers a consolidated solution for the storage of all network and transaction data, including details of transactions, access logs, and events on the network [19].

Several studies have investigated the use of blockchain technology as a decentralized security layer for financial and distributed networks. This interest arises from its core characteristics, which include immutability, cryptographic security, decentralization, and consensus mechanisms. These features reinforce trust and improve the auditability of transactions [20], [21]. Access independence, decentralized identity management, and secure event logging are three examples of how blockchain technology improves accountability and resiliency against insider threats and data manipulation attacks. The majority of the work done in this area, however, is focused on static security policies and fixed trust assumptions (i.e., fixed levels of trust assigned to each user), with limited views into how dynamically changing levels of trust and changes in attack conditions affect the long-term operational behavior of a system [22], [23].

A. Limitations of Existing Approaches

Many existing evaluation methods have numerous limitations. The majority of ZT frameworks rely upon static or rule-based trust models and thus do not account for dynamic trust changes resulting from evolving attack behaviors. Blockchain methodologies focus primarily on audit capability but do not provide any means of quantitatively measuring the evolving nature of trust over time or adaptive evaluation capabilities of policy. Many studies do not take into account probabilistic modeling of attacks and offer only minor support for systematic evaluation based on security metrics or parameter sensitivity analysis. The framework proposed by this study aims to address these gaps by providing an integrated parameter-driven approach for modeling dynamic trust evolution (i.e., through probabilistic attacks) and enforcing policies based on thresholds. It operates within a single simulation environment to support full evaluation of the trade-offs between security and performance.

B. Comparative Analysis of Existing Frameworks

Currently, most ZT research is focused almost entirely on identity validation and a rules-based access control mechanism. There are little to no quantitative evaluations of presently available ZT mechanisms under dynamic condition variations. Some blockchain-based ZT applications (i.e., smart contracts) offer tangible auditability features. However, minor trust modeling is possible within these implementations. Machine learning-based ZT models currently provide anomaly detection capabilities but do not perform any type of sensitivity analysis on the identification parameters (i.e., φ, ψ, λ, $\lambda 1$, $\lambda 2$). The framework described within this document expands upon existing models by introducing both a parameter-driven evaluation methodology involving the evolution of dynamic trust and probabilistic attack modeling and policy enforcement based on threshold criteria. The new framework is able to systematically vary the values of evaluation parameters and provide an analysis resulting from these evaluation parameters used in three dimensions and in accordance with well-defined security metrics. A detailed overview of each evaluation category is provided in Table II, which compares the methodologies of existing models to the advantages and

methodologies of the framework contained within this document.

TABLE II. METHODOLOGICAL COMPARISON OF ZT SECURITY EVALUATION MODELS

Aspect	Existing Approaches	Proposed Framework
Trust Modeling	Static / discrete	Dynamic continuous
Attack Modeling	Limited / absent	Probabilistic (φ-based)
Evaluation	Qualitative / isolated	Parameter-driven simulation
Sensitivity Analysis	Not considered	Systematic
Security Metrics	Limited	Trust, attacks, quarantine
Policy Enforcement	Rule-based	Threshold-based (λ, λ_1, λ_2)

III. SYSTEM MODEL

The current study investigates a blockchain-aided, ZT-secured financial ecosystem through a discrete-time simulation model that accounts for trust development, cyber-attack behavior, and responsive adaptive security actions [24], [25]. The underlying representation of the ecosystem is depicted as a directed graph

$$G = (N, E),$$

where N = {1, 2,…,N} is an entity of the network (e.g., user, device, service, and blockchain node) and E represents logical communications/access relationships between nodes. The discrete time steps of the system are denoted by the numerical sequence:

$$t = 1, 2,\ldots, T.$$

At each discrete time interval t, node activity is monitored, trust scores for nodes are updated, node access decision records are maintained, and security incidents may occur within the system. Each node $i \in N$ has an associated dynamic trust score $T_i(t) \in [0,1]$ that represents, at time t, the level of authorization granted to the node under ZT security principles.

The main evaluation parameters for the ZT Model are defined precisely to describe the mathematical foundations of the model. The attack probability ($\varphi \in [0, 1]$) indicates the likelihood that a node will be subjected to a cyberattack during a time period. The trust decay rate ($\psi \in [0, 1]$) measures the level at which a node's trust declines because of behavioral deviations. The access threshold ($\lambda \in [0, 1]$) specifies the minimum amount of trust that must exist for a node to have the same access rights as usual. The two trust threshold values (λ_1 and λ_2) specify the thresholds for intermediate trust (λ_1) and critical trust (λ_2). These values can be defined in general terms as such: $0 \leq \lambda_2 < \lambda_1 < \lambda \leq 1$. All four parameters in total create trust growth, the impact of attacks on trust, and how policy will be enforced in the ZT Policy. Each nodal entity has a summation of baseline behavior patterns defined as Behavior Baseline (B_i). Deviations from how the node is expected to behave ($\Delta(t)$) at time t correspond to anomalous behaviors.

$$D_i(t) = |B_i(t) - B_{1i} \quad (1)$$

Trust degradation resulting from behavioral drift occurs as follows:

$$T_i(t+1) == T_i(t)e^{\psi \cdot \Delta_i(t)} \quad (2)$$

where $T_i(t)$ and $T_i(t+1)$ denote the trust score of node i at time steps t and $t+1$, respectively. Evaluation parameter interactions occur sequentially due to dependence on system dynamics. The probability of an attack φ determines whether a node is compromised at each time step and therefore introduces behavioral deviation Δ(t) that affects the trust update process. The trust degradation rate ψ affects the magnitude of the trust reduction. The trust score $T_i(t)$ after updating will be compared to predetermined threshold parameters (λ, λ_1, λ_2) to determine policy enforcement actions such as continuing access, isolating, or quarantining. Accordingly, φ impacts the evolution of trust through the indirect effect of Δ(t), and ψ influences how sensitive trust will be to degradation. Therefore, the thresholds of λ-based limits determine the response of adaptive systems to each situation. Trust-based access control decisions are made based on the three thresholds for trust (T) as follows:

- Access to the system is granted where $T_i(t) \geq \lambda$.
- The node will be isolated from the system where $\lambda_1 \leq T_i(t) < \lambda$.
- The node will be quarantined from the system where $T_i(t) < \lambda_2$.

Whereas, $0 \leq \lambda_2 < \lambda_1 < \lambda \leq 1$. Using a tiered response system, it allows for adaptive mitigation without being dependent on complex game theory models. Every security event that occurs will be documented in blockchain format. Blockchain provides an immutable trust log or audit trail for every event occurring and is therefore useful for increased trust, accountability, and analysis of incidents that have occurred in the past, and for increasing trust in the future; this is documented in blockchain technology through the use of consensus mechanisms and cryptography that is simulated.

IV. SIMULATION DESIGN

The simulation framework evaluates how ZT security mechanisms work with blockchain-based node management via the systematic variation of key security parameters and the recording of their impact on network behavior over discrete time steps. A fixed number of nodes compose the blockchain network, and over discrete time steps, all three factors are updated in response to the simulation. All simulations were implemented and executed using MATLAB to model trust evolution, probabilistic attacks, and threshold-based mitigation mechanisms.

1) Experimental setup: The simulations were run in MATLAB (R2023a) in a controlled computing environment (Intel i5/i7 processor & 8-16 GB of RAM, Windows/Linux operating system). The blockchain layer was modelled without actually deploying on an external platform to create N nodes (usually N = 50) initialized with trust values $T_i(0) \in [0.8, 1.0]$. The simulation runs through a discrete time series of t = 1 through T ≈ 100-200 in order to store the long-term behavior of events in the blockchain. At each time, attacks occur randomly with probability φ using Bernoulli trials, resulting in attack behavior changes and then driving trust decreases

through the decay model as they occur. There are multiple trials for each scenario (20-50 trials), and the averages are reported for statistical reliability. Parameters are selected as φ, $\psi \in [0,1]$ and $\lambda, \lambda_1, \lambda_2 \in [0,1]$, subject to $0 \leq \lambda_2 < \lambda_1 < \lambda \leq 1$. No external datasets are used, as the study relies on a synthetic simulation framework.

The complete evaluation methodology has been built around a structured pipeline. Initially, the various inputs are established ($\varphi, \psi, \lambda, \lambda_1, \lambda_2$) and represent both threat and policy conditions. Threat events, generated stochastically based on the φ value, may produce behavioral deviations for nodes. As part of the trust updating function, the value for ψ is used to manage the rate at which trust normally degrades. The resulting trust levels are then compared against pre-set thresholds by the policy enforcement module, which then activates appropriate action, for example, retaining access, isolating, and quarantining the node. The changes to trust levels and mitigation decisions will be recorded in the blockchain layer to ensure traceability and auditability. Lastly, the performance of the system will be measured using existing security metrics, which include average trust, average rate of detection of attacks, and average frequency of quarantine.

2) Parameter variation: The attack probability (φ) is selected over the range of [0,1] to designate varying degrees of adversarial activities. In this study, φ will remain constant through each simulation run, thus isolating the impact of the other parameters on the output(s). The rate at which trust disintegrates (ψ), is based on a normalized model for updating trust (via an ODE equation). Due to the need for a sensitivity analysis, the variable ψ is held constant through each experiment (but is varied in small increments when trying to determine the level of aggressiveness or gradualness in which trust deteriorates), while the access and mitigation thresholds (λ, λ_1, and λ_2) are varied independently on the range of [0,1] to assess the sensitivity of trust regarding the relative security of access controls. To isolate the effect of the strictness of access controls, only the access threshold (λ) is varied independently, while keeping ψ, λ_1, and λ_2 constant.

In this simulation loop, each time step produces a random attack, using φ to make nodes behave differently than normal. These behaviors then generate trust updates based on the decay rate (ψ), after which trust is the result of a threshold for determining access controls. Any nodes whose trust score is below the quarantine threshold (λ_2) will be isolated. One can rely on the blockchain record of Trust updates and attack mitigation actions for the validity and traceability of the system.

Several performance metrics are generated throughout the simulation, such as temporal changes in the average trust score, the number of detected attacks, and the total number of quarantined nodes. These metrics will help characterize the trust dynamics throughout the simulation as well as the activity related to attacks and mitigation efforts. The data will be used for conducting a sensitivity analysis on different parameter settings. To increase reproducibility, simulations are conducted in a manner where the initialization strategy is fixed, and the pseudo-random number generator is set to reproduce the patterns of attack. The simulation environment is flexible to enable the parameters to be varied independently for sensitivity analysis.

V. Results and Analysis

This section looks at how various aspects of ZT Security Parameters affect networks being attacked in the dynamic environment of cyberspace. The simulations are evaluated on trust evolution, the detection and mitigation of attacks, the sensitivity of the thresholds used to make those decisions, and how correlation between events is handled using a blockchain. The results presented in this section were produced by varying each parameter to isolate its individual impact. All multi-panel figures in this section are organized into sub-figures labeled (a), (b), and (c) to ensure clarity and consistency in the presentation and interpretation of simulation results.

A. Trust Evolution

As an example, by applying a fixed trust decay rate (ψ = 0.05) and assessing the effect on trust transitions across all three threshold values (λ =0.3, λ = 0.5, and λ =0.7) show that they progress in the same way. Thus, regardless of which of the above-mentioned thresholds was employed, the resulting trends of average trust decrease will be identical. This suggests that the dynamics of intrinsic trust are driven mainly by behavioral deviations and decay factors and not by policies relating to access control. Access threshold (λ) changes have an indirect effect on how many nodes are involved in the network. The average trust value for the network over time, based on different access limits, is depicted in Fig. 2. It has been observed that all the curves are declining, representing the decay of trust and attack effects. Higher levels of strictness (λ = 0.7) have a greater effect on the decline of the active node participation rate than lower levels of strictness (λ = 0.3).

Therefore, varying the value of λ changes the duration of time during which nodes can remain involved in the network while retaining an acceptable level of trust. When the access threshold is higher (i.e., higher λ), nodes will be more likely to become isolated or removed from the network as their trust scores change. These values also reduce the number of nodes participating in the network and accelerate the decline in the average trust of the network. Conversely, as the level of access/control decreases, there will be an increased ability of nodes to remain active and participate at a higher level of average trust. This demonstrates that the manner in which the access threshold is set impacts trust evolution indirectly through mitigation actions and not through a direct alteration of the trust update process.

The occurrence of attacks during simulation is driven entirely by the attack probability (φ = 0.01). As demonstrated in Fig. 3, there is a relationship between the occurrence of attacks and their quarantine actions. As can be clearly seen, the earlier we set a higher threshold to control entry, the quicker and more often we take action to quarantine an attack. However, the overall distribution of events remains statistically unchanged because the attack probability is fixed. So, the time of attack profile data is the same statistically regardless of the access threshold on the model. This suggests that differences in

the parameters of the security policy have no impact on the production of attacks but have an impact on the system's response to detected attacks.

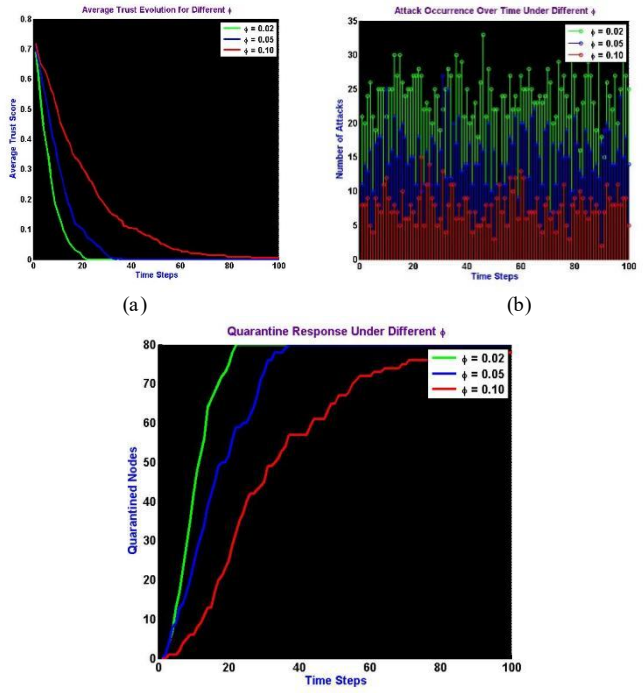

Fig. 2. (a) Temporal evolution of average network trust for different access thresholds (λ = 0.3, 0.5, 0.7), (b) corresponding variation in active node participation over time.

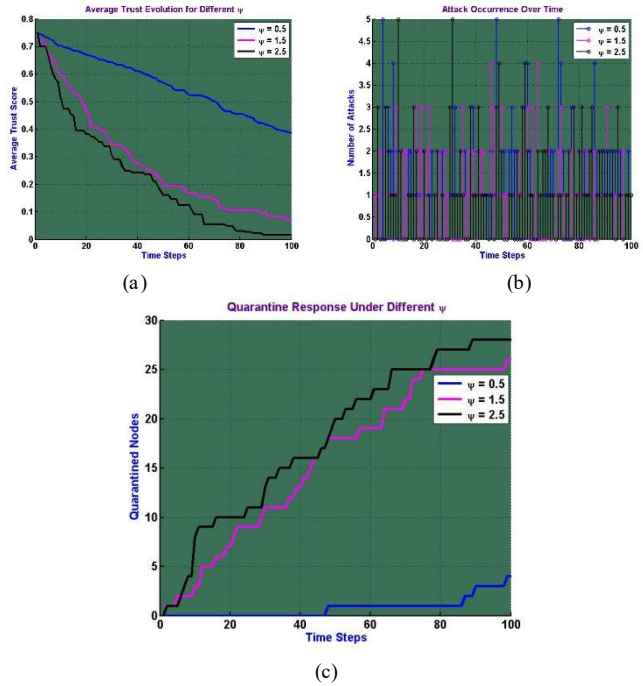

Fig. 3. (a) Attack occurrence over time, (b) corresponding quarantine response under different access threshold settings (λ), with fixed attack probability (φ = 0.01).

B. Attack Detection and Mitigation

The most frequent use of quarantine by an access threshold is to produce an early and frequent quarantine action after the trust level exceeds the defined isolation/quarantine limits. In fact, the average number of quarantined nodes will increase significantly faster under a stricter policy than under a relaxed policy.

On the other hand, when the access threshold is lower, the average time to make an isolation decision is extended, and the average number of quarantined nodes is reduced along with the average number of nodes participating in the network. The findings suggest that ZT enforcement regulates the strength of the system and its response to mitigation actions, whereas adversarial strength determines how often an attack is conducted.

C. Threshold Sensitivity

The access control policy can be shown as being sensitive to its access control policy strictness threshold, λ, through variations of λ while holding constant λ_1 (isolation threshold) and λ_2 (quarantine threshold).

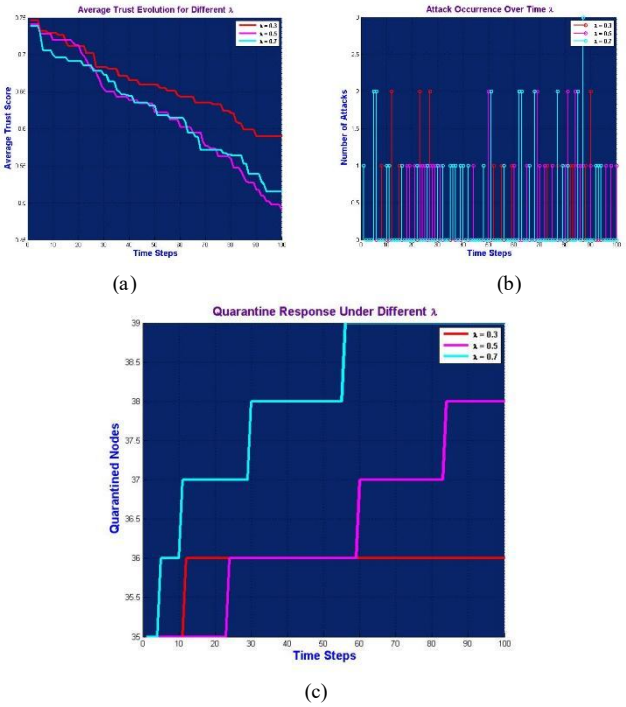

Fig. 4. (a) Sensitivity of attack occurrence to threshold variations, (b) corresponding isolation and quarantine response illustrating the impact of access threshold (λ).

The access threshold (λ) provides a measure of the sensitivity of the system, as shown in Fig. 4. The figure illustrates the system's response to varying threshold levels. While lower levels of the threshold prolong the node's active state, higher levels of the threshold lead to faster mitigation action. When λ is a low number, there will still be an increased number of trusted devices/nodes within the network that will be left connected to other users, resulting in fewer devices/nodes from prematurely entering isolation. Thus, although having high tolerance to device/node trust

degradation may additionally leave malicious/suspicious devices/nodes around longer, potentially allowing them to be subjected to additional future attacks, having λ as a high number results in higher levels of security responsiveness due to earlier initiation of isolation/quarantine actions, given the situation of trust degradation. This may limit the extent of damage from malicious or suspicious activities, but may result in increased levels of disruption to the network due to isolating nodes that have not yet been fully compromised.

Therefore, this data supports that the improper selection of one or more threshold values can either delay the mitigation of excessive amounts of network fragmentation. To balance between enforcing security measures and providing a workable operational environment, access to and isolation/quarantining. All require accurate calibration of their respective threshold values. Despite this, the attack and mitigation behavior is connected to Fig. 3 and 4. Fig. 3 specifically focuses on the temporal attack and response, whereas Fig. 4 focuses on the sensitivity of mitigation behavior to changes in the threshold parameters.

D. Network Size Scalability Analysis

To assess the scalability of the designed ZT blockchain security model, simulations were run to simulate three distinct network sizes (N = 20, 50, and 100). Attack probability (φ) and trust decay rate (ψ) were held constant throughout to evaluate if trust dynamic models and the response to mitigation performed consistently as additional nodes joined the network. Fig. 5a displays the average network trust over time for all network sizes evaluated.

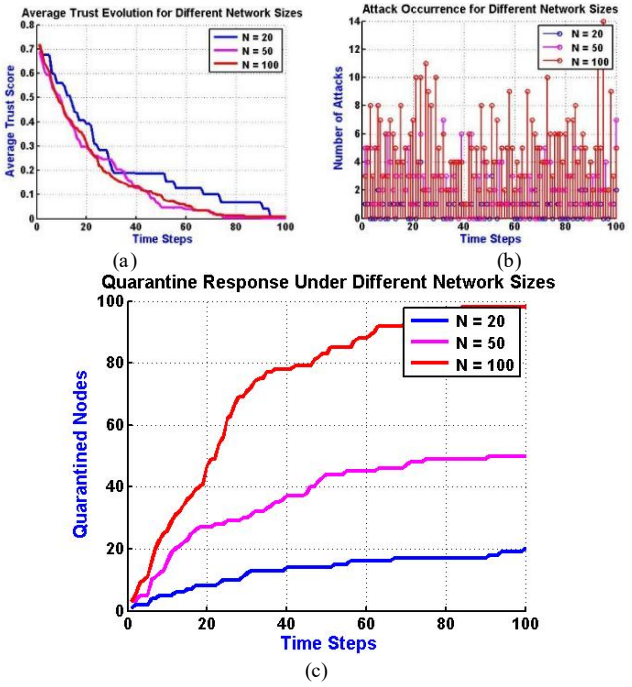

Fig. 5. (a) Average network trust over time for different network sizes (N = 20, 50, 100), (b) number of detected attacks, (c) quarantine response, illustrating scalability behavior under fixed attack probability (φ = 0.01).

Even though larger networks experienced more attacks than smaller ones, there were still consistent declines in trust across all configurations, indicating that trust dynamics remain stable as the number of nodes in a network scales. Fig. 5b and 5c illustrate the count of attack occurrences and quarantine response for all three network sizes evaluated within this experiment. As would be expected, larger networks produced higher counts of detected attacks and quarantined nodes. Though their proportional responses remained stable due to the implementations of threshold-based ZT policies within this framework. Thus, it can be concluded that the proposed framework scales effectively while maintaining both trust stability and mitigation efficiency.

E. Blockchain Event Logging and Correlation

During the simulation, all security events are temporally related and recorded on a conceptual blockchain logging layer. The analysis of the event streams has shown a strong correlation between the increase in attacks, the decrease in trust, and the initiation of quarantine actions due to threshold triggers. Therefore, these correlations demonstrate how blockchain logging can support post-incident audits by providing a transparent record of security-related decisions that cannot be altered. Moreover, these findings also show that blockchain log events provide a structured means for assessing the effectiveness of ZT policy implementation because these records provide the ability to correlate network behavior to specific parameter values. This traceability allows system administrators to perform adaptive security governance by using historical threat-pattern information and mitigation results information to adjust their trust decay rates and thresholds. These outcomes show that blockchain logging provides a reliable method for maintaining a trust ledger that is complementary to enforcing a ZT model through increased accountability, auditability, and the ability to make informed changes to policy.

VI. Discussion

The results of the simulation demonstrate that the overall effect of the intensity of attacks and the dynamic nature of trust determines the enforcement of security controls within the networks of blockchains with ZT Architectures. As the attack probability increases, behavioral deviations increase; also, as the rate at which trust decays increases, so too does the loss of credibility result in earlier threshold crossings and more isolated actions. These parameters are not simply independent of one another; they interact with one another to modify the structure of long-term trust stability and affect how fast parameters contribute to the transition of the system from a state of normal operations to a state of defensive enforcement. These results affirm that trust evolution in ZT Architecture is highly sensitive to both the pressures from adversaries and the tuning of policies. The relationship between parameter settings and their impact on trust dynamics and mitigation behavior is summarized in Table III.

The research provides insight into how an organization needs to manage its computer network by balancing secure access and the use of that network. A conservative approach will quickly identify questionable nodes and therefore prevent them from being able to execute further attacks on a computer network. This allows an organization to prevent a larger attack

from occurring while at the same time building greater resilience against attacker attempts.

TABLE III. EFFECT OF ZT PARAMETER SETTINGS ON TRUST DYNAMICS AND QUARANTINE BEHAVIOR IN BLOCKCHAIN NETWORKS

Parameter Setting	*Observed Trust Behavior*	*Quarantine Response*	*Security-Performance Trade-off*
High attack probability ($\varphi \uparrow$)	Rapid trust degradation; lower average trust	Frequent and early quarantines	Improved attack containment but reduced network stability
Aggressive trust decay ($\psi \uparrow$)	Accelerated trust loss under moderate attacks	Increased isolation of nodes	Fast anomaly response but higher false-positive risk
Strict access threshold ($\lambda \uparrow$)	Reduced effective trust participation	Sharp rise in quarantined nodes	Strong security enforcement with higher network disruption
Lenient access threshold ($\lambda \downarrow$)	Slower trust decline; higher participation	Fewer quarantines	Better usability but increased attack exposure
Low quarantine threshold ($\lambda_2 \downarrow$)	Early isolation of marginal nodes	Sustained quarantine growth	Maximized resilience with reduced adaptability
Balanced thresholds (λ, λ_1, λ_2 optimized)	Stable trust evolution	Controlled quarantine escalation	Optimal balance between security and continuity

However, implementing these stricter levels of enforcement creates the risk of legitimate users being denied access to the network, thus creating a disconnected computer network. Conversely, an organization that employs a lenient method for determining whether nodes may participate in the computer network will allow bad nodes to remain longer or execute additional attacks on other nodes. Organizations that operate in financial environments, where the continuity of service and the reliability of transaction processing are extremely critical, must balance these competing attributes when creating a trust-based policy. Unlike earlier studies, which have primarily focused on either interaction between ZT security mechanisms or blockchain technologies, this analysis presents a holistic framework for modeling these interactions in dynamic threat environments through the use of parameter-driven approaches. Specifically, it integrates continuous degradation of trust, probabilistic modeling of attacks, and threshold-based mechanisms for mitigating attacks into a blockchain-auditable context to generate a comprehensive understanding of how system-level dynamics related to adaptive mechanisms can influence long-term network resilience.

It is important to note some of the limitations of the proposed framework in relation to the strengths. The research applied a simulation-based model that may not fully represent the complexities of blockchain networks or the nature of dynamic cyberattacks. Fixed attack behavior (as measured with a single probabilistic parameter, φ) limits the consideration of many types of highly adaptive adversaries. Additionally, the trust evolution model is based on fixed (defined) decay rates and threshold values between two connected entities. The heterogeneity of the nodes' behavior is not taken into account while presenting the model. Also, the capabilities, latencies, or constraints of the nodes are not taken into consideration. Lastly, the blockchain layer is conceptually implemented without considering any computational overhead. Consequently, while the model offers insight into how decentralized models of trust evolve, there will need to be further validation of this model through real-world (or scalable) implementations. Future efforts will focus on validating the proposed model with adaptive attack models, heterogeneous networking environments, and considerations of practical implementations of blockchain technology.

The findings reveal that optimal deployments of blockchain employing ZT design principles should avoid extreme configurations of parameters. Appropriately tuning both trust decay and access thresholds will provide control over the escalation of quarantines while also maintaining a minimum threshold of participation from users. The summarized relationship of parameters to their expected behavior assists organizations in establishing configurations of ZT policies for financial networks that utilize blockchain technology. These results provided a framework for continued resilient operation in an ever-changing environment of adversarial activity.

VII. CONCLUSION

This study presented a simulated evaluation of ZT security policies in conjunction with blockchain technology for networks within the financial services sector in dynamic cyber-attacks that involve probabilistically modeled behavior of attacks, diminishing trust, and the employment of threshold-based access control. The framework established in this research models the relationships between the key parameters of attack probability (φ), trust decay rate (ψ), and access, isolate, and quarantine thresholds (λ, λ_1, λ_2) as they apply to the effects on trust evolution, mitigating factors, and network resilience. Additionally, the degree of sensitivity of these parameters has an important role in determining the level of security achieved through ZT-based blockchain solutions. When attack probabilities and the decay of trust are high, continued erosion of trust and a high frequency of quarantines occur. Lower participation in the network can be achieved by using higher levels of access and isolation. When a less strict threshold is used, connections are kept intact, but the attack impact is extended. This research demonstrates that trusting establishment and stability of operations in distributed financial networks depend on careful tuning of trust settings. The model proposed integrates dynamic trust assessments and blockchain-based auditability to enhance transparency and make it possible to analyze the enforcement of security by means of logging events that cannot be altered. The relationship between attack events, trust loss, and threshold-triggered actions to mitigate attacks is an example of how records on the blockchain may assist with post-incident analysis and evaluation of security policies. Future extensions of this work will examine the implementation of quantum-safe technologies, including quantum key distribution and quantum random number generators, as well as an improved adaptive attack model, to more thoroughly test the ZT blockchain environment against next-generation cyber threats. The framework identified is lightweight, extensible, and can be used to comprehensively benchmark ZT blockchain-enabled security policy.

ACKNOWLEDGMENT

S.P.V gratefully acknowledges the Centre for Advanced Wireless Integrated Technology, Chennai Institute of Technology, India, vide funding number CIT/CAWIT/2026/RP-011.

REFERENCES

[1] S. Joseph and N. Pandeeswari, "Secured IoT data transmission with enhanced integrated encryption techniques with blockchain technology," IETE Journal of Research, vol. 71, no. 4, pp. 1156–1175, 2025.

[2] P.-L. Pomerleau and D. L. Lowery, *Countering Cyber Threats to Financial Institutions*, 1st ed., Cham, Switzerland: Springer, 2020.

[3] P. K., S. Nayak, C. A. Chavadi, and Y. P. Pai, "Determinants of AI-enabled customer experience across healthcare sectors: A decade in review," Cogent Business & Management, vol. 12, no. 1, Article 2590241, 2025.

[4] B. B. Sezer, S. Akleylek, and U. Nuriyev, "PP-PQB: Privacy-preserving in post-quantum blockchain-based systems: A systematization of knowledge," IEEE Access, vol. 13, pp. 41382–41405, 2025.

[5] A. Punia, P. Gulia, and N. S. Gill, "The security and vulnerability issues of blockchain technology: A SWOC analysis," Peer-to-Peer Networking and Applications, vol. 18, Article 173, 2025.

[6] C. S. Kodete, B. Thuraka, and V. Pasupuleti, "A systematic review of AI-driven and quantum-resistant security solutions for cyber-physical systems," in *Proceedings of the International Conference on Computer Applications (ICCA)*, Cairo, Egypt, 2024, pp. 1–6.

[7] M. Plachkinova and K. Knapp, "Least privilege across people, process, and technology: Endpoint security framework," Journal of Computer Information Systems, vol. 63, no. 5, pp. 1153–1165, 2023.

[8] B. Todtmann, S. Riebach, and E. P. Rathgeb, "The honeynet quarantine: Reducing collateral damage caused by early intrusion response," in Proceedings of the 6th International Conference on Networking (ICN), Sainte Luce, Martinique, 2007, p. 96.

[9] K. Li et al., "Zero-trust foundation models: A new paradigm for secure and collaborative artificial intelligence for Internet of Things," IEEE Internet of Things Journal, vol. 12, no. 22, pp. 46269–46293, 2025.

[10] S. Rizvi, R. J. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, "Identifying the attack surface for IoT networks," Internet of Things, vol. 9, Article 100162, 2020.

[11] R. Sun, Y. Zhu, J. Fei, and X. Chen, "A survey on moving target defense: Intelligently affordable, optimized and self-adaptive," Applied Sciences, vol. 13, no. 9, Article 5367, 2023.

[12] M. I. Malik, A. Ibrahim, P. Hannay, and L. F. Sikos, "Developing resilient cyber-physical systems: A review of state-of-the-art malware detection approaches, gaps, and future directions," Computers, vol. 12, Article 79, 2023.

[13] Z. Zhang, M. Zargham, and V. M. Preciado, "On modeling blockchain-enabled economic networks as stochastic dynamical systems," Applied Network Science, vol. 5, Article 19, 2020.

[14] N. Okika et al., "Assessing the vulnerability of traditional and post-quantum cryptographic systems through penetration testing and strengthening cyber defenses with zero trust security," International Journal of Innovative Science and Research Technology, vol. 10, pp. 2456–2465, 2025.

[15] B. D. Lund, T.-H. Lee, Z. Wang, T. Wang, and N. R. Mannuru, "Zero trust cybersecurity: Procedures and considerations in context," Encyclopedia, vol. 4, pp. 1520–1533, 2024.

[16] T. J. Olorunlana, "Least privilege and access control principles in enterprise network security," International Journal of Science, Architecture, Technology and Environment, vol. 2, pp. 3048–3055, 2025.

[17] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, "A survey on trust models in heterogeneous networks," IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2127–2162, 2022.

[18] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of zero trust networks in cloud computing: A comparative review," Sustainability, vol. 14, Article 11213, 2022.

[19] C. Komalavalli, D. Saxena, and C. Laroiya, "Overview of blockchain technology concepts," in *Handbook of Research on Blockchain Technology*, Hershey, PA, USA: IGI Global, 2020, pp. 349–371.

[20] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey," IEEE Access, vol. 10, pp. 113436–113481, 2022.

[21] C. B. Haley, R. C. Laney, J. D. Moffett, and B. Nuseibeh, "Using trust assumptions with security requirements," Requirements Engineering, vol. 11, pp. 138–151, 2006.

[22] Y. Alghofaili and M. A. Rassam, "A dynamic trust-related attack detection model for IoT devices and services based on deep LSTM," Sensors, vol. 23, Article 3814, 2023.

[23] M. L. Gambo and A. Almulhem, "Zero trust architecture: A systematic literature review," Journal of Network and Systems Management, vol. 34, Article 25, 2026.

[24] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207, 2020.

[25] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.