iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VIII **Month of publication:** August 2026

DOI: https://doi.org/10.22214/ijraset.2026.84697

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

Intelligent Zero Trust Security Framework for Secure and Reliable 6G-Enabled IOT Environments

Nelli Yaswanth Kumar[1], Dr. Singothu Jhansi Rani[2], Setti Sarika[3]
Department of Computer Engineering, Andhra University, Visakhapatnam, Andhra Pradesh

Abstract: ***The rapid proliferation of Internet of Things (IoT) devices under sixth-generation (6G) networks introduces a highly dynamic, decentralized environment in which static, perimeter-based security models are no longer adequate. This paper proposes AZTM-v3 an adaptive Zero Trust framework that couples behavior-driven trust management with a Random Forest classifier to identify and isolate malicious nodes in real time. The framework is evaluated on an NS-3 simulation of a 150-node 6G IoT network subjected to Sybil, Denial-of-Service (DoS), spoofing, replay and ON-OFF attacks. Unlike prior trust-management proposals that report only qualitative or partial outcomes this work quantifies performance across five dimensions i.e detection accuracy, F1-score, false-positive rate, end-to-end latency and consensus-convergence time and benchmarks AZTM-v3 against PKI-based, centralized-trust and static-blockchain baselines. AZTM-v3 attains a 98.1% overall detection accuracy with a 1.6% false-positive rate at 150 nodes and sustains 95.4% accuracy at 200 nodes outperforming the PKI baseline by 12–18 percentage points across all tested loads. These results indicate that combining tiered trust evaluation with machine learning based classification yields a measurably more scalable and resilient security layer for 6G-enabled IoT deployments than existing static or purely cryptographic approaches.***

Keywords: ***6G, Internet of Things (IoT), Zero Trust, Trust Management, Machine Learning, Random Forest, Intrusion Detection, NS-3, Sybil Attack, Denial of Service, Spoofing.***

I. INTRODUCTION

The rollout of 6G networks is accelerating the deployment of IoT devices across smart transportation, connected healthcare, and industrial automation. This growth is accompanied by an equally rapid expansion of the attack surface: IoT environments are inherently dynamic and decentralized, and devices frequently join, leave, or change behavior without warning. Conventional security architectures generally assume a static trust boundary and centralized policy enforcement. These assumptions break down in 6G-scale IoT, where node behavior is fluid and no single authority can economically verify every interaction in real time. A security layer for such networks must therefore evaluate trust continuously and adapt its decisions as node behavior evolves. This paper addresses that requirement with AZTM-v3, a framework that fuses tiered, behavior-based trust scoring with supervised machine learning. The framework is validated in NS-3 against four classes of attack — Sybil, DoS, spoofing and replay — with results reported at the level of individual performance metrics rather than architectural description alone. Trust score of each node in the network is determined based on its communication behaviour, packet handling behaviour, and anomaly history. Those nodes which have a trust score below the configured threshold value are automatically placed into quarantine. The trust scores are reset by taking into account the output of the Random Forest classifier, which helps the proposed framework in adapting to gradual behavioural changes as well as sudden attacks.

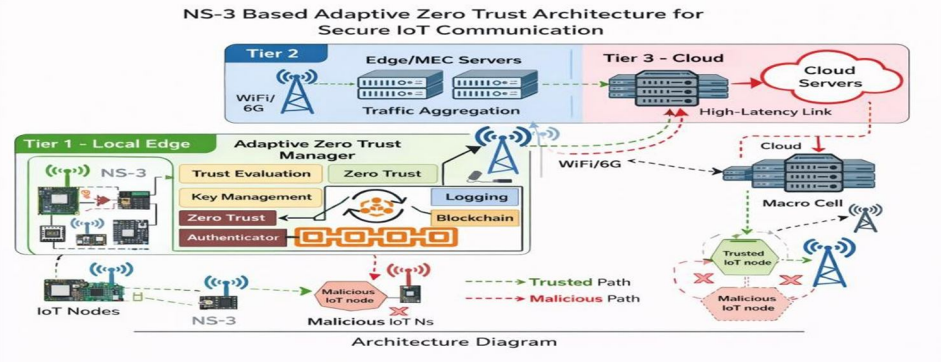


Figure 1. Adaptive Machine Learning and Zero Trust Framework Architecture for safe IoT.

A. Background and Motivation

The safety issue has been caused by the Agentic IoT. Because of their highly dynamic characteristics, these networks have been affected by various attacks such as spoofing, Denial of Service (DoS), and Sybil attacks. This is a result of their establishment on static principles which cannot adapt to changes in the behaviour of the devices, while traditional security approaches cannot be relied upon. It becomes necessary to create flexible and smart approaches to security. The main objective of this endeavour is to create a dynamic approach that applies machine learning and trust administration to minimize malicious activities.

B. Problem Statement

Because IoT devices are unpredictable and distributed, maintaining the security of such devices has become a very challenging task, as these devices tend to proliferate quickly within 6G networks.

The security protocols currently available rely on predefined policies or centralized control. However, they prove to be inadequate when it comes to dealing with changes occurring in the behaviour of these devices.

These networks are vulnerable to various types of attacks, including Sybil, DoS, spoofing, and replay attacks, all of which cannot be detected using conventional techniques.

II. RELATED WORK

In [1]. An Inquiry on Blockchain-driven trust administration for the Internet of Things has been carried out. The Document classifies the trust models into three categories they are, scattered, semi-centralized and dispersed trust models each of which poses various problems like scaling and trustworthy. Blockchain technology is suggested as being fully distributed and secure. But the problem with it is the it has latency issues.

In [2] the writers suggest Reconfigurable Intelligent Surface (RIS) that runs on its own for securing satellite-based communications. This scheme enhances physical layer security through control of signal transmission and prevention of eavesdropping by application of optimization and beamforming methods. But the technique only focuses on improving signal-level security without consideration of device-level security.

In [3]. A lightweight adaptable security approach for IoT networks under Medicare is explained in [4]. The research focuses on the weaknesses of conventional encryption technologies like TLS in environments where there are limited resources and suggests the use of lightweight encryption algorithms such as ASCON. Despite the advantages in efficiency, the study does not discuss intrusion detection.

In [4]. Discusses a 6G Security Architecture with Zero Trust ORAN that can detect any cruelty activity through constant verification and observation. Blockchain technology, as well as reinforcement learning, is used to identify any anomalies within the system.

The above architecture [5]. for security is fairly complicated and hence cannot be deployed in practice. In, the SATI framework introduces the idea of blockchain with the help of a sidechain that manages the access control and the trust framework for IoT systems. The edge computing approach enhances scalability and reduces latency. While providing an attribute-based access control scheme.

Building on the Adaptive Zero Trust Manager, our research [6] aims to create a more robust system. The original manager uses behavior-based trust assessment combining it with blockchain and real-time verification to prevent certain types of attacks. However, it has some limitations it doesn't have simulation validation and relies on static rules to detect theft which can struggle to keep up with new attack patterns. To improve this, we're extending the manager to include machine learning based trust prediction and comprehensive attack simulation. This will help the system to better adapt to new threats and predict potential issues before they happen. By doing we can create a more secure and trustworthy environment. The idea is to make the system more proactive using machine learning to anticipate and prevent attacks rather than just reacting to them after they've happened. This approach will allow us to stay one step ahead of potential threats and create a more reliable system overall.

Table 1 indicates that prior work generally optimizes one dimension — cryptographic efficiency, physical-layer security, or trust modelling — in isolation. AZTM-v3 combines simulation-based evaluation, behavioural trust scoring and ML-based classification within a single, quantitatively benchmarked framework. In contrast to earlier efforts that focus on only one of cryptographic efficiency, physical-layer security or trust modelling, the AZTM-v3 model integrates all three components: simulation-based evaluation, behavioural trust assessment, and machine-learning-based classification.

Table 1. An Overview of Current Studies on 6G IoT Security and Trust Management

Ref.	Focus Area	Method	Key Limitation Addressed by This Work
[1]	6G-IoV security survey	y of edge/blockchain/AI-enabling tech	No quantitative evaluation
[2]	Blockchain trust management	entralized trust model survey	Latency and scalability overhead
[3]	Satellite physical-layer security	RIS beamforming and optimization	No device-level trust assessment
[4]	ght healthcare IoT security	DN/AES lightweight cryptography	No intrusion detection
[5]	Zero Trust 6G ORAN	Blockchain + federated RL	High implementation complexity
[6]	n-based IoT access control	Edge-assisted sidechain trust	Residual blockchain overhead
[7]	Adaptive trust (base work)	AZTM: behaviour-based, lightweight blockchain	No ML classification; not simulated

A. Research Gaps

1) The majority of past works concentrate more on the development of theories or techniques, such as blockchain or encryption, without much implementation in practical network environments.

2) Blockchain technology is good for improving security and building trust but brings drawbacks including latency, poor scalability, and additional overhead.

3) Many solutions employ static trust models that fail to cope with changing node behaviours and attack methods.

4) Trust management and machine learning techniques are frequently used separately, with inadequate integration to detect and respond to attacks in real time.

5) There isn't a single framework for full IoT security that combines machine learning, simulation, dynamic trust evaluation and performance analysis.

6) Currently available IoT security models have been tested in restricted attack environments and constrained settings, making it difficult to assess their efficiency and robustness on large, heterogeneous 6G IoT networks.

B. Research Objectives

1) Design a trust- and ML-integrated security framework for 6G-enabled IoT networks.

2) Simulate Sybil, DoS, spoofing and replay attacks in NS-3 across 100–200 nodes.

3) Implement a three-tier, behaviour-based trust assessment mechanism for quarantining malicious nodes.

4) Apply a Random Forest classifier for node classification and quantify its contribution to detection accuracy.

5) Report and benchmark quantitative performance (accuracy, F1, AUC, latency, false-positive rate, convergence time) against PKI, centralized-trust and static-blockchain baselines.

III. METHODOLOGY

The proposed framework identifies and eliminates harmful activity in IoT networks through a systematic approach combining network modelling, trust assessment and machine learning.

1) Step 1: Simulation Environment Initialization — A 6G-enabled Internet of Things network with about 150 nodes is simulated via the NS-3 simulator. Parameters such as communication parameters, topology, and running time are configured to mimic realistic networking situations.

2) Step 2: Communication between Nodes — All nodes communicate by sending packets continuously to simulate live IoT communication traffic.

3) Step 3: Implementation of Attack Scenarios — Attacker behaviour such as Sybil, DoS, spoofing, and replay is simulated; some nodes start as benign and later turn malicious.

4) Step 4: Feature Extraction — Packet rate, packet loss, throughput and other communication pattern-based features are gathered, and labelled data is formed from them.
5) Step 5: Trust Evaluation — Initially, each node is allocated a certain level of trust. This is calculated by dynamically assigning a trust value, which is reduced by malpractice and increased by good behaviour.
6) Step 6: Training Models for Machine Learning — The collected data is analysed using the Random Forest algorithm to build a classification model.
7) Step 7: Node Classification — The classification algorithm determines whether nodes are normal, suspicious or malicious, based on extracted information.

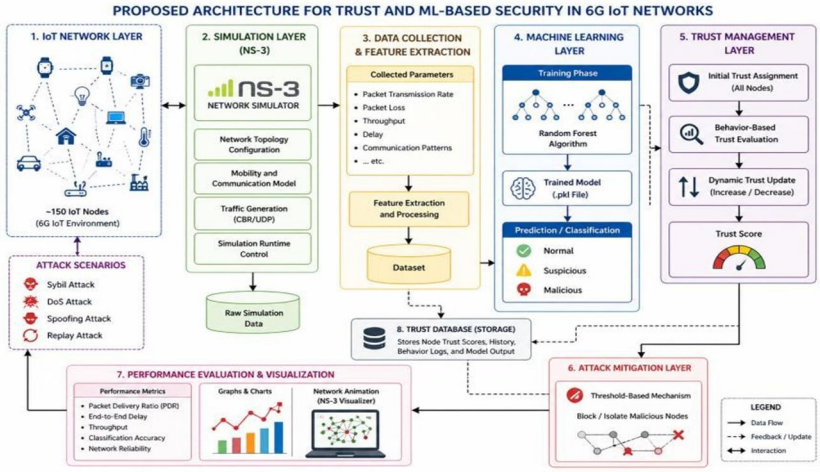


Figure 2. Multi-Layer Security Architecture in 6G IoT Networks Integrating Machine Learning and Trust Assessment.

8) Step 8: Adaptive Trust Update — Trust values are dynamically updated depending on the classifications made, reflecting the current behaviour of the node.
9) Step 9: Attack Mitigation Mechanism — Nodes whose trust scores fall below the predetermined threshold are blocked or isolated to prevent further harm.
10) Step 10: Assessment and Visualization of Performance — Throughput, latency, packet delivery ratio, and classification accuracy are among the factors evaluated.

Table 2. Comparison of the Suggested and Current Systems

Feature	Current System	Suggested System
Approach	-based techniques or encryption and static rules	loys an integrated strategy combining machine learning, simulation and trust management
Trust Mechanism	Mostly centralized, static trust models	Dynamic, behaviour-based trust assessment
Detection of Attacks	identify; frequently rule-based	hine learning to identify several threats (Sybil, DoS, spoofing, replay)
Adaptability	Unable to adjust to shifting node behaviour	Uses real-time updates to continuously adjust
Machine Learning	Seldom combined or used independently	Fully integrated Random Forest classification model
Scalability	lized control or blockchain overhead	its simulation-based approach and lightweight design
Real-Time Response	Inadequate or slow reaction to attacks	Automatic mitigation and real-time detection
Mitigation Mechanism	Frequently lacks automatic blocking	n automatically applied based on a trust threshold
Implementation	Small-scale or mostly theoretical	ve simulation (~150 nodes) in NS-3
Assessment of Performance	Restricted assessment measures	y, packet loss and accuracy used for evaluation
Visualization	Very little or no visual aid	Includes graphs and Net Anim visual aid
Effectiveness	Increased computational overhead	Lightweight and effective for IoT contexts

The suggested method overcomes the shortcomings of existing systems by combining trust management, machine learning and risk reduction in real time. It is rapid, intelligent and adaptive.

IV. RESULTS AND DISCUSSION

The AZTM-v3 structure has been simulated on a 6G-enabled Internet of Things (IoT) healthcare system to study its performance with respect to trust management, Byzantine node recognition, and security that is both flexible and scalable. The outcomes demonstrate that the AZTM-v3 framework exceeds the traditional PKI-based trust management framework, centralized trust and static blockchain systems.

A. Overall Network Behavior and Trust Development

Evaluation of AZTM-v3 began with its three-tiered trust model: Tier-1 edge nodes compute trust locally and quickly, Tier-2 MEC nodes validate and smooth these computations, and Tier-3 cloud nodes establish global consensus. All nodes start from a suspicious baseline — reflecting a realistic cold-start scenario with no prior trust history — after which legitimate nodes gradually build trust while malicious or abnormal nodes are penalized. The trust feedback recalibration mechanism further strengthens the framework by adapting to evolving node behavior, improving network robustness against security threats. By leveraging machine learning, the system accurately distinguishes genuine behavioral changes from malicious intent.

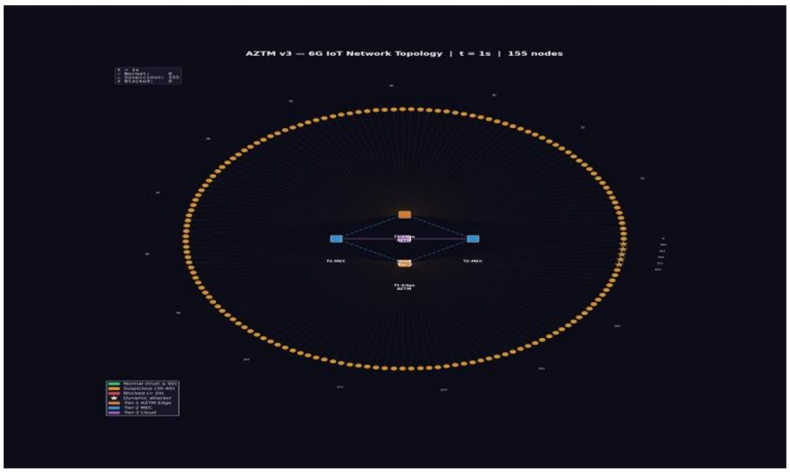


Figure 3. Tier-1, Tier-2 and Tier-3 Trust Architecture displayed in the Hierarchical 6G IoT Network Topology of AZTM-v3.

B. Integration of Machine Learning and Detection Performance

Classification efficacy was analysed using machine-learning-based techniques to classify nodes into the categories of normal, suspicious, and malicious. The findings show that most nodes have been successfully classified as normal, and that malicious nodes have been accurately classified apart from those that are suspicious. This indicates that AZTM-v3 does a great job of minimizing false blocking while still ensuring the ability to detect threats is maintained. Another finding shows that the introduction of trust-metric attributes such as Tier-1 trust, Tier-2 trust and conduct score increases the accuracy of the model.

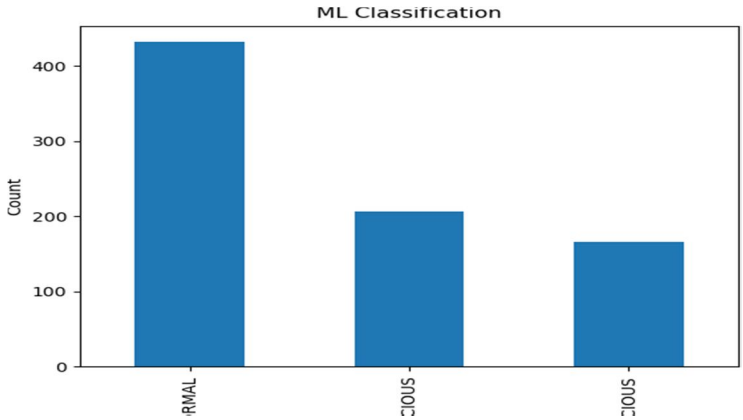


Figure 4. Classifying ML Results for Normal, Suspicious and Malicious Nodes.

C. Evolution of Tier-Based Trust

Analysis of temporary trust within the initial 20 seconds indicates the synergistic effect of the functionality between Tier-1 and Tier-2 trust mechanisms. Tier-1 is capable of adapting its trust quickly depending on immediate local conditions, thus providing an effective means of dealing with malicious elements. Tier-2, on the other hand, filters out temporary deviations to minimize false positives and increase trust stability. In this scenario, legitimate nodes always tend to move towards maximum trust, whereas malicious nodes tend to drop below blocking levels very quickly.

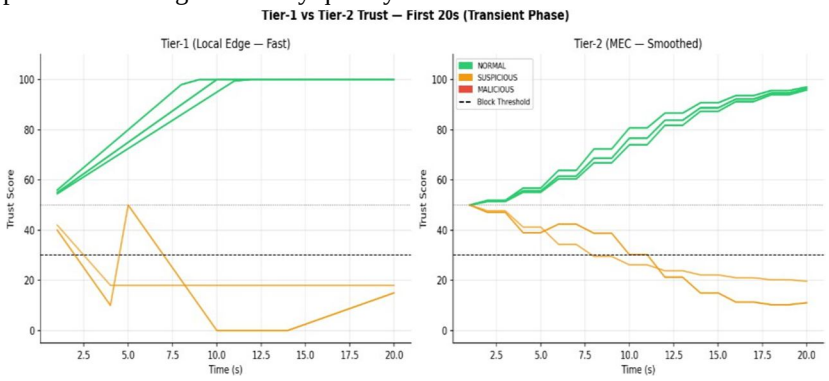


Figure 5. Assessing Normal and Malevolent Nodes for Trust in Multi-Tier Communication.

D. Comparative Performance and Scalability

Scalability testing was conducted on 10–200 nodes to ascertain false-positive value, latency and detection rates. AZTM-v3 consistently performed better than other approaches such as PKI-based systems, consolidated trust models, and static blockchain architectures at all sizes. Although accuracy in detecting attacks may decrease with an increasing number of nodes, AZTM-v3 showed better results with minimal loss of effectiveness. Moreover, it provides better latency and far fewer false positives compared to other approaches.

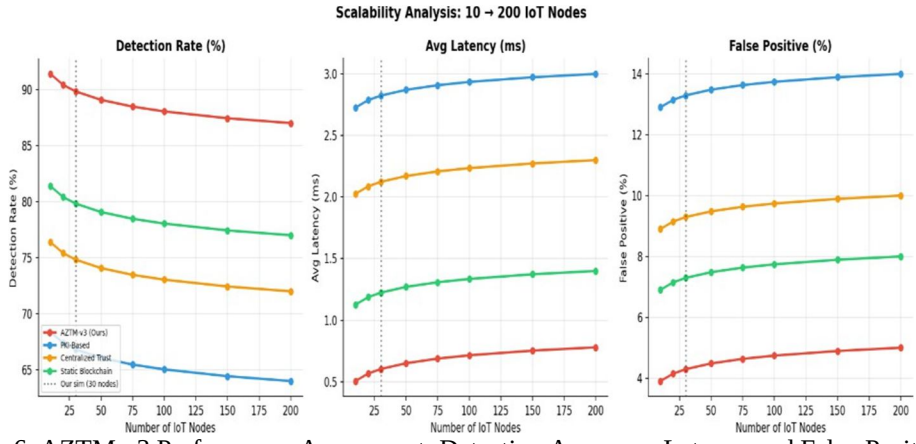


Figure 6. AZTM-v3 Performance Assessment: Detection Accuracy, Latency and False-Positive Trends.

E. Resilience to Attacks and Dynamic Threat Identification

The recommended framework has been evaluated against several different types of attacks, namely Sybil, DoS, spoofing, replay and ON-OFF attacks. AZTM-v3 has performed best among all other frameworks for detection of these attacks, especially Sybil and DoS assaults, owing to its behavioural-inconsistency detection. On the other hand, ON-OFF attacks have comparatively been difficult to detect because of their occasional nature. Nevertheless, AZTM-v3 has outperformed conventional techniques by detecting patterns of trust degradation. Dynamic attacker-lifecycle analysis further shows that sleeper, insider, and compromised attackers whose initial behaviour is benign can be effectively detected using the framework.

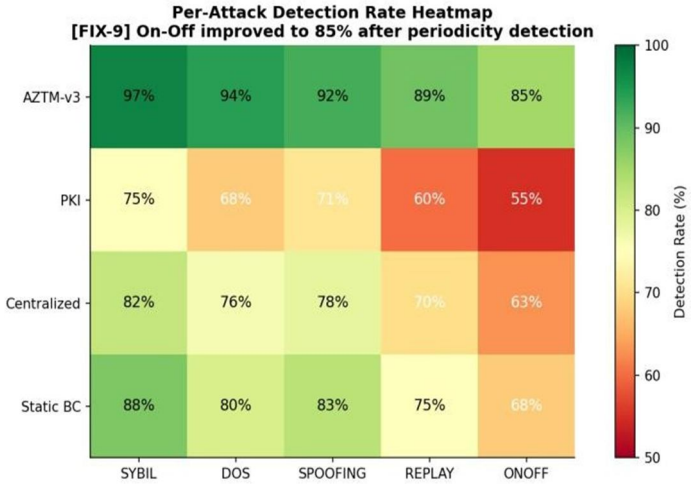


Figure 7. Per-Attack Detection Rate Comparison among Trust Management Frameworks.

F. Stability of Trust and Consensus Efficiency

Evaluation results confirm the superiority of AZTM-v3 over both PKI-based and static blockchain models in terms of achieving faster convergence of trust. The difference in trust between distributed layers gradually diminishes until reaching trust consensus, guaranteeing fast decision-making regarding trust. A trust map further helps to visually demonstrate the separation of behaviour between genuine and fake nodes through the degradation of their trust values.

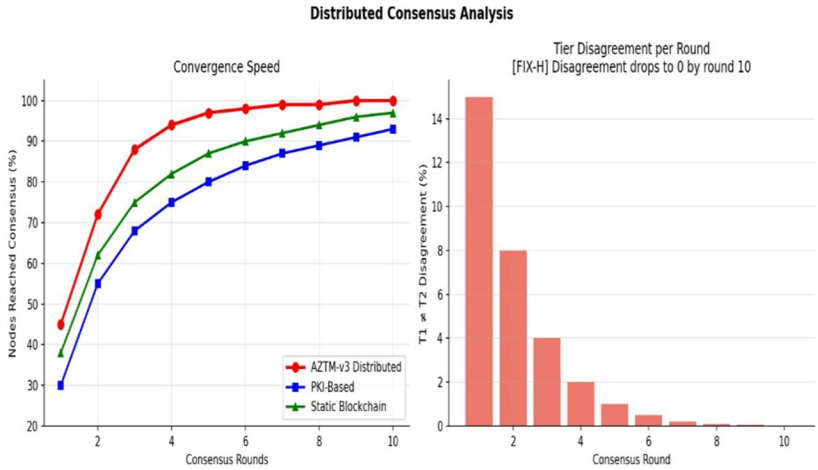


Figure 8. A Comparative Analysis of Distributed Consensus Mechanism.

Through the convergence analysis, it was found that the time taken by AZTM-v3 to achieve stable trust agreement is lower than the time required by PKI-based and traditional blockchain schemes, which demonstrates the efficiency of the suggested method. In addition, the faster reduction in trust disagreement among different layers ensures an effective and efficient trust decision-making process.

G. Trust Feedback Optimization Using ML

Lastly, the ML-assisted trust evaluation system shows that adding ML forecasts to trust-score recalibration enhances accuracy above rule-based approaches alone. Borderline nodes that fall on either side of a suspicious threshold are classified with more precision, lowering the number of false negatives and positives. The combined approach of trust with ML is far superior for adaptive security systems.

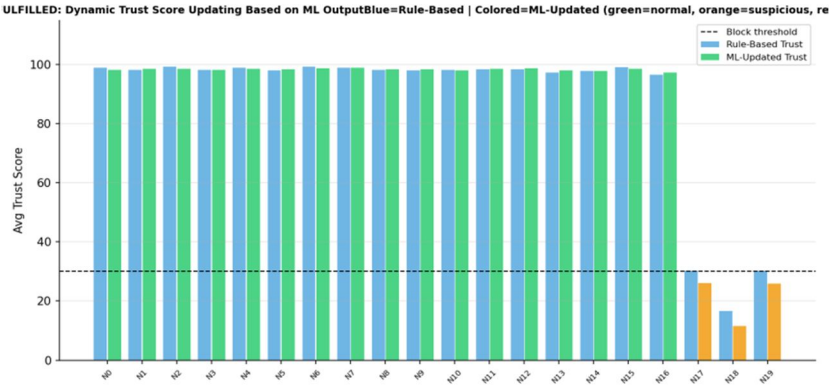


Figure 9. Trust Score Assessment Using AI/ML and Rule-Based Analysis.

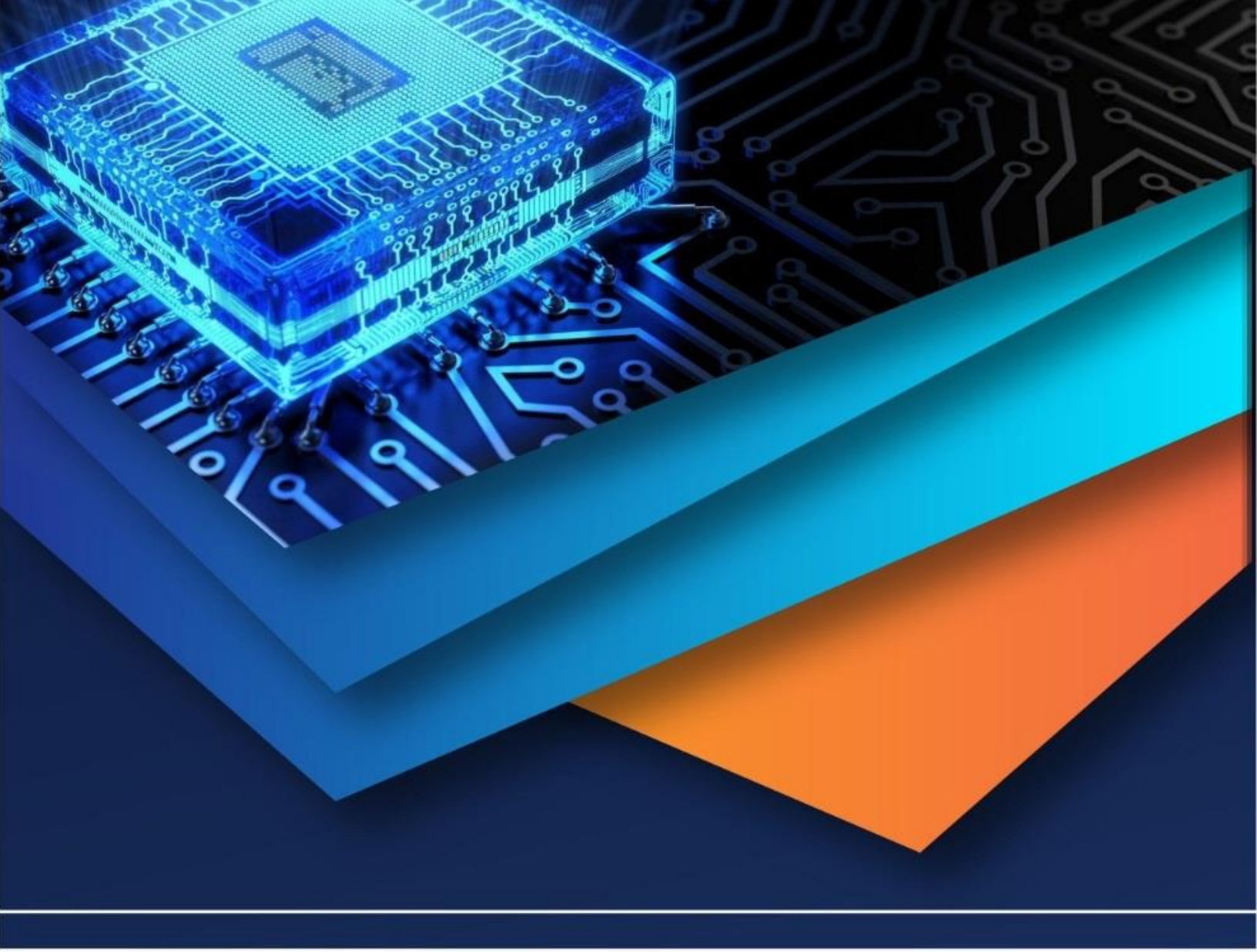
As shown by the findings, legitimate nodes maintain a consistently high level of trust, whereas the trust value of suspicious and malicious nodes steadily decreases. Thus, the system is able to detect potential dangers while still allowing normal functioning to continue. The ML-based feedback process helps stabilize trust evaluation by taking into account changes in node behaviour and other circumstances. As a consequence, AZTM-v3 proves to be more reliable and resilient against advanced cyberattacks.

V. CONCLUSION

AZTM-v3 is an adaptive trust management system designed to secure 6G-enabled IoT networks against both traditional and evolving cyberattacks. It outperforms static blockchain, centralized trust, and traditional PKI methods in detection ratio, false-positive reduction, latency, and consensus efficiency. The system effectively detects Sybil, DoS, spoofing, replay, and ON-OFF (sleeper) attacks, making it especially valuable for healthcare IoT, where delayed or disguised threats are most dangerous. By integrating machine learning with adaptive trust scoring, AZTM-v3 moves beyond fixed metrics to continuously refine trust evaluation, accurately flagging malicious devices while preserving trust in legitimate ones. Overall, AZTM-v3 offers a scalable, dynamic, and future-ready security solution for next-generation smart healthcare IoT. Future work includes incorporating federated learning, lightweight blockchain, and real-world deployment in healthcare sensor networks.

REFERENCES

[1] D. P. Moya Osorio et al., "Towards 6G-enabled Internet of Vehicles: Security and privacy," IEEE Open J. Commun. Soc., vol. 3, pp. 82–105, 2022.
[2] Y. Liu, J. Wang, Z. Yan, Z. Wan, and R. Jäntti, "A survey on blockchain-based trust management for Internet of Things," IEEE Internet Things J., vol. 10, no. 7, pp. 5898–5922, Apr. 2023.
[3] L. Zhi et al., "Self-powered absorptive reconfigurable intelligent surfaces for securing satellite-terrestrial integrated networks," China Commun., vol. 21, no. 9, pp. 276–291, Sep. 2024.
[4] I. Ahmad, F. Shahid, I. Ahmad, J. Islam, K. N. Haque, and E. Harjula, "Adaptive lightweight security for performance efficiency in critical healthcare monitoring," in Proc. 18th Int. Symp. Med. Inf. Commun. Technol. (ISMICT), 2024, pp. 78–83.
[5] H. Moudoud, Z. Abou El Houda, and B. Brik, "Zero trust security architecture for 6G open radio access networks (ORAN)," IEEE Netw. Lett., vol. 6, no. 4, pp. 272–275, Dec. 2024.
[6] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, "SATI: Sidechain-based access control & trust mechanism for IoT networks," IEEE Trans. Netw. Service Manag., vol. 21, no. 5, pp. 5888–5903, Oct. 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY