AI BASED ZERO TRUST SECURITY GATEWAY FOR 5G ENABLED IOT DEVICES

P.KALAIVANI
Assistant professor,Department of Electronics and Communication Engineering,
Salem College of Engineering and Technology,
Salem,Tamilnadu,India.
Email:kalaisanju24@gmail.com

GOKULAPRIYA R
Student, Department of Electronics and Communication Engineering,
Salem College of Engineering and Technology,
Salem,Tamilnadu,India.
Email:gokulagokula8675@gmail.com

NESHIKA J
Student, Department of Electronics and Communication Engineering,
Salem College of Engineering and Technology,
Salem,Tamilnadu,India.
Email:cnpjairaman@gmail.com

PREETHIKA P
Student, Department of Electronics and Communication Engineering,
Salem College of Engineering and Technology,
Salem,Tamilnadu,India.
Email:preethiprabha809@gmail.com

SOUNDARYA S
Student, Department of Electronics and Communication Engineering,
Salem College of Engineering and Technology,
Salem,Tamilnadu,India.
Email:soundaryaselvam237@gmail.com

ABSTRACT

The growth of IoT networks utilizing 5G technology provides an unparalleled level of seamless communication between distributed edge nodes and centralized cloud-based monitoring systems. Yet, the majority of current IoT architectures continue to use traditional perimeter based security models, which assume that devices and users internal to the IoT have already been authenticated when they initially access the system, creating a massive vulnerability in an environment with many interconnected elements. In multi-node IoT systems, devices typically communicate with cloud-based systems for monitoring and controlling device behaviour, but this communication is usually not continuously authenticated, has limited intelligent threat detection capabilities, and only performs identity verification at the time of account set-up. User authentication in typical IoT applications is usually limited to a user name/password combination, which is subject to credential theft, brute force attacks, and unauthorized access. Centralized control dashboards for IoT devices also pose threats of data tampering, session hijacking, and unauthorized command execution. Without implementing strong multi-factor authentication for user login, such as using one-time passwords (OTP's), an attacker can take control of critical operations and modify or delete node activity on the IoT network. For these reasons, there is an urgent requirement for an AI-based Zero-Trust Security Gateway that implements the following features: Continuous device verification, OTP-based multi-factor user authentication, encryption of all communication, and AI-enabled anomaly detection. By adding additional methods of decentralized validation and strict access control policies,

Keywords -Zero Trust, IoT Security, OTP Authentication, Edge Intelligence, 5G Networks

I INTRODUCTION

The combination of 5G communication technology and IoT infrastructures has revolutionized how we monitor and control a variety of industries. High-speed, reliable connections allow for timely collection and analysis of information. The speed with which digital transformation has occurred has enabled manufacturers and service providers to collect real-time data from their devices, while also being able to provide remote control capabilities of those devices, across multiple industries (i.e., industrial, healthcare, smart infrastructure).Unfortunately, most of the current IoT architecture still relies on traditional perimeter-based security systems to establish a baseline trust model for devices and users. That is, once a device or user is authenticated at the perimeter of the network, it is assumed to be trusted. This trust model fails in highly dynamic, heterogeneous ecosystems enabled by 5G technology. These ecosystems are comprised of continually changing, distributed edge computing nodes and cloud resources that are employs
many-to-many interactions.Due to a lack of persistent identity verification, adaptive threat intelligence systems, and strict session management methods, the current communication protocols being used to connect edge devices with cloud dashboards do not provide sufficient protection from the various forms of breaches normally associated with multi-node IoT systems, such as replay attacks, credential theft, brute force attacks, and unauthorized privilege escalation occur at the time of an interaction. Furthermore, centralized monitoring dashboards exacerbate security risks by permitting session hijacking, command injection, data tampering, and unauthorized execution of control commands.

When thinking about the security issues associated with 5G networks and the large number of Internet of Things (IoT) devices that rely on them, there are many concerns for organizations and individuals. Due to these limitations of security, we must create a solid Zero Trust architecture that is specifically built for a 5G-enabled IoT environment. This paper proposes using an AI-Driven Zero Trust Security Gateway that does continuous verification and allows for dynamic access control to intelligently mitigate threats across geographically distributed edge-to-cloud infrastructures. The proposed system has two primary objectives: (1) Enabling continuous authentication of devices; (2) Providing multi-factor authentication (MFA) through an OTP as well as using encryption to secure user access to their devices; and, (3) Building a means to utilize machine learning techniques (ML) and/or artificial intelligence (AI) to detect anomalies and other behaviors that would indicate malicious intent; while allowing for real-time situational awareness of any potential threats or attacks on an organization's 5G IoT network.

The contributions of this work are as follows:

- Create a decentralized zero-trust architecture that includes continuous device validation, user authentication based on one-time passwords, and encrypted communication channels
- Provide an AI-driven anomaly detection framework located at the security gateway for real-time threat identification and response
- Conduct experimental validation within a simulated 5Genabled multi-node IoT environment using comparative security performance analysis

The remaining portions of this paper are structured as follows: Section II addresses related work in IoT Security and Zero-Trust Frameworks; Section III provides the proposed AI-Based Security Gateway Architecture and Methodology; Section IV discusses results from implementation and performance evaluation; and Section V summarizes this study with potential directions for future enhancements.

II. RELATED WORK

The existing literature on Zero Trust Security Frameworks as they relate to IoT and next-generation networks contains many similar findings regarding continuous verification, AI-based intrusion detection, identity-centric access control, and distributed enforcement of trust. Table I displays the major findings that contribute to establishing a base for identifying the research gaps that will be addressed by building an AI-Based Zero Trust Security Gateway for 5G-enabled IoT Systems.

TABLE I LITERATURE REVIEW SUMMARY OF ZERO-TRUST AI-IOT SECURITY APPROACHES

Study (Ref)	Domain/Setting	Method	Key Metrics Reported	Strengths	Limitations
Li et al. [1]	IoT collaborative AI	Zero-Trust foundation models	Secure collaborative accuracy	Distributed trust modeling	High computational cost
Joshi [2]	Cross-industry systems	Zero-Trust maturity analysis	Security posture improvement	Strategic roadmap	Lacks implementation depth
Roy et al. [3]	Consumer IoT	Lightweight ensemble IDS	High anomaly detection rate	Low resource consumption	Limited scalability validation
Rehman et al. [4]	Cyber-Physical Systems	AI + Zero-Trust integration	Improved system resilience	Embedded security design	Complex deployment
Hussain et al. [5]	Wireless IoT networks	Federated Zero-Trust AI	Reduced centralized risks	Privacy-aware learning	Aggregation overhead
Bajpayi et al. [6]	IoT healthcare devices	AI-driven vulnerability management	Faster vulnerability detection	Practical healthcare focus	Limited real-time control
James et al. [7]	IoT authentication	Survey on authN/authZ	Comparative evaluation	Comprehensive taxonomy	No unified framework
Fathalla & Azab [8]	IoT identity systems	Self-sovereign identity	Decentralized identity validation	Strong privacy control	Performance overhead
Munasinghe et al. [9]	Secure networking	ML-based Zero-Trust	High classification accuracy	Adaptive trust modeling	Dataset dependency
Abuhasel [10]	Industry 5.0	Zero-Trust access control	Improved access resilience	Sustainable design	Limited IoT heterogeneity
Al Ridhawi & Aloqaily [11]	UAV & 6G networks	Zero-Trust 6G architecture	Secure ultra-low latency	Future-ready design	Conceptual evaluation
Geetha et al. [12]	5G healthcare	Zero-Trust for smart health	Enhanced secure transmission	5G integration	Domain-specific scope

A. Foundations of Zero Trust and Artificial Intelligence Integration

Li et al. [1] present foundational models for collaborative intelligence within IoT based on zero trust. They demonstrate that the accuracy of collaborative intelligence can be improved through secure aggregation, even though there is significant computational overhead associated with the foundation model and therefore large scale models cannot be easily deployed to the edge (Hussain et al.) A zero trust based system utilizing AI to enforce distributed trust at scale was developed by Hussain et al. [5], and is designed to be used within federated wireless IoT systems. While their work effectively supported improved privacy through reduced exposure to centralized security breaches compared to more traditional systems, their model still had challenge regarding the overhead associated with

communication or aggregation among heterogeneous systems. Finally, Munasinghe et al. [9] suggested a machine learning based zero trust architecture to accommodate dynamic trust modeling and real time classification of malicious activity. While the authors were able to achieve a high degree of accuracy in terms of classification of malicious activities, their evaluation relied significantly upon a known set of datasets and cast doubt about the extent of generalizability across diverse 5G IoT environments.

B. Intrusion Detection and Anomaly-Based Security

Roy et al. [3] created a proactive Zero Trust intrusion detection method for consumer IoT devices that utilizes lightweight ensemble learning. They used an anomaly-driven approach to attain high levels of detection with acceptable levels of computation for resource-constrained devices; however, their validation of scalability was restricted to a limited number of multi-node infrastructures. Rehman et al. [4] made a suggestion that they could use an immersive embedded AI-driven Zero Trust model to improve the resilience of cyber-physical systems by using AI to monitor systems continuously. The embedded nature of their designs makes it possible to improve system-level robustness, but the complexity of deploying and integrating their designs in real-life distributed IoT environments presents difficulties. In order to enhance the speed of detecting vulnerabilities and to implement proactive mitigation for IoT healthcare devices, Bajpayi et al. [6] examined vulnerability management through AI. However, their method provides an inadequate level of both real-time command validation and strict authentication methods for users.

C. Authentication, Identity, and Access Control

A comprehensive survey of authentication and authorization methodologies in Zero-Trust IoT networks has been made by James et al. [7]. They have classified the different identity-based access models as well as continuous verification strategies. Although this taxonomy is useful for designers to plan their work, it has no proposed framework for an all-inclusive AI-based implementation model. Fathalla and Azab [8] proposed a lightweight self-sovereign identity model for IoT networks implemented in Zero-Trust environments. Their decentralized identity validation offers increased privacy and independence from centralised authorities. However, the cost of performance during large-scale identity validation is problematic. Abuhasel [10] suggested an access control methodology that utilises a Zero-Trust network for Industry 5.0 systems, where resilience and sustainable security in the industry is a focus area. While this methodology will work in an industrial application, further testing is needed before using it on heterogeneous 5G IoT nodes.

D. Zero-Trust in 5G and Next-Generation Networks

Geetha et al., [12] investigated how Zero-trust principles could be applied to healthcare infrastructures powered by 5G, with a strong emphasis on securely transmitting data and enforcing access policies. They demonstrated that to use 5G as a communications medium, it must be coupled with identity-centric security models, although the study's focus was on a specific domain and has limited applicability to other sectors using IoT technologies. Al Ridhawi and Aloqaily [11] analyzed how the Zero-Trust architecture could be extended to support both unmanned aerial vehicles (UAVs) and digital twins in the context of future 6G networks, and provided solutions for overcoming both ultra-low latency and distributed trust challenges. Their work, while forward-thinking and conceptually sound, provides little actual information on how Zero-Trust concepts will be validated through practical implementations of IoT in 5G networks. In the study done by Joshi [2], an overall market analysis was done on how emerging technologies will drive Zero-Trust maturity across the industry, with a roadmap provided for organizations to adopt them in their operations. The study does not present any technical implementation details needed to integrate Zero-Trust concepts at the system level.

E. Research Gap Analysis

Through the comparison of the existing approaches, three significant bottlenecks are identified:

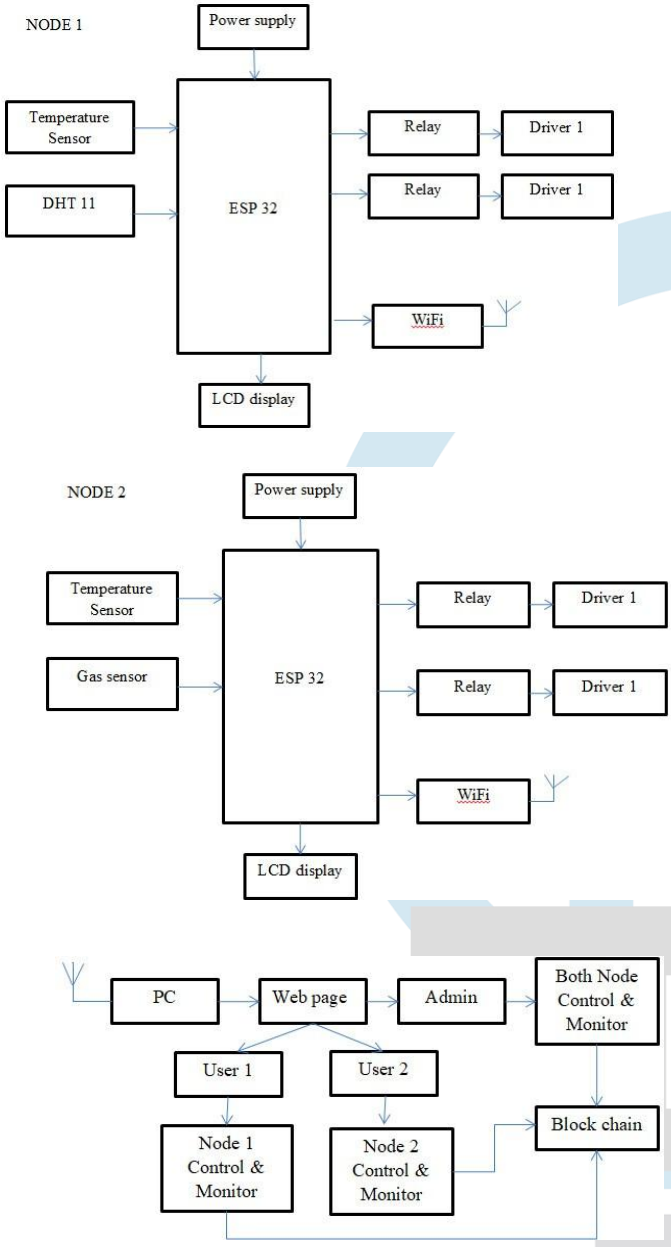
1. Lack of Continuous Multi-Factor Authentication: Although authentication models like James et al [7] and Fathalla and Azab [8] place a high emphasis on validating one's identity, the majority of systems do not provide integrated One-Time Password (OTP) based multi-factor authentication and A.I. based session monitoring for web-based dashboards.
2. Limited Unified A.I. Gateway Architecture: Intrusion detection methods (like Roy et al [3] and Munasinghe et al [9]) have been shown to effectively detect anomalous behavior and events, but cannot be integrated into a centralized Zero Trust security gateway to enforce device verification, encrypted communications and adaptive access controls across multiple devices simultaneously.
3. Scalability and Real-Time Adaptability: Research such as Geetha et al [12] and Al Ridhawi & Aloqaily [11] have demonstrated that the concept of Zero Trust can work effectively within advanced communication networks (like 5G). However, there is insufficient discussion on the ability to provide practical, real-time validation across disparate 5G enabled heterogenous multi-node IOT infrastructures.

The motivation behind the proposed AI-driven Zero-Trust Security Gateway is to establish a unified security solution that incorporates continuous device authentication, OTP-based user verification (authentication), encrypted edge to cloud communication and AI-driven anomaly detection through a unified architecture. The proposed solution will combine disparate validation methods and intelligence-based threat analysis into one comprehensive security pipeline, thereby minimizing scalability, authentication and real-time security limitations observed across the existing literature.

III. PROPOSED METHODOLOGY

A. System Architecture

As seen in Figure 1, this framework proposes a four-layer structure for what would be an AI-based zero-trust cybersecurity gateway: (1) Devices that generate data and communicate with each other in a distributed fashion (the 'device layer'); (2) Security gateway components that do authentication, validation of identities, encryption/decryption of sessions, generate one-time passwords for users to log into systems, etc., with AI/ML anomaly detection support; (3) Controls to validate commands coming from authorized roles and whether the authorized person (role) has permission/authorization to perform the function/command (the 'access control and application layer') ; and (4) Cloud services that house audit logs and analytics, manage dashboards, etc. (the 'cloud monitor layer').



Every IoT node has its own digital identifier when it registers with the Device Layer, and all communications both in and out from those devices include some type of cryptographic identifier on them. Every request from a device and every interaction between a user and the Security Gateway Layer is validated by the Zero-Trust principle – i.e., "never trust and always verify." As part of the validation process, the gateway will continuously authenticate the device, validate a user session, analyze the traffic pattern for the request, and apply anomaly detection using Machine Learning before forwarding the request. Additionally, the Access Control Layer provides Role-Based Access Control (RBAC) to ensure that both administrator-level users and standard-level users are only operating within their respective allowed privileges. Lastly, the Cloud Layer will help manage encrypted storage, protect tampering logs, provide a dashboard for monitoring activity, and help guarantee that all data fiowing through the network does not implicitly trust any device, user or session until that trust has been established through a validated process.

B. Mathematical Formulation

The proposed Zero-Trust Security Gateway employs a mathematical model which consists of three primary elements: evaluation of device trustworthiness, detection of anomalies, and authentication checks.

1. Device Trust Evaluation Model:

Our device trust evaluation consists of an equation that defines a trust score of device i, T_i, as a function of:

$$T_i = f(I_i, S_i, B_i) \quad (1)$$

where I_i represents the identity of device i, S_i includes integrity parameters of the session, and B_i contains metrics that indicate behavioral consistency. If T_i is less than a specified threshold (τ), the device request will be denied access to the network. The use of this trust evaluation method allows us to continuously verify the trustworthiness of each device instead of relying on single-use authentication.

2. Ai-Based Anomaly Detection Model:

Anomaly detection occurs in our business through the use of a feature vector for all of the user traffic and user behavioral patterns. Our machine learning algorithm for detecting anomalies is represented using the following equation:

$$y_i = M_A(i; w) \quad (2)$$

where x_i = extracted features of the user's traffic and of the user's behavior, w = parameters previously learned from the various models created, and y_i = whether the traffic is normal or anomalous. The model will continually learn how to detect anomalies based on past user behavioral patterns, thereby enabling us to detect new and evolving threats in the distributed IoT space.

3. Authentication Validation Function:

User authentication incorporates multi-factor verification using OTP confirmation. The authentication condition is represented as:

$$A_u = C_u \wedge O_u \quad (3)$$

where A_u indicates successful authentication of user u, C_u denotes credential validation (username and password), and O_u represents correct OTP verification. Access is granted only when both conditions are satisfied.

C. New Contributions to Security Resource Management

The work presented here is radically different from traditional IoT security frameworks based solely on a single static boundary defense. The novel contributions of the model proposed are as follows:

1. One Unified Zero-Trust Gateway: The integration of all the device identity verifications, OTP multi-factor authentication, RBAC, encrypted communications, and anomaly detection through AI into one centralized gateway.
2. Trust That is Dynamic and Ongoing: Trust scores are recalculated every time a CRA receives a new transaction to enable dynamic session monitoring and to prevent lateral movements between devices on a network.
3. Adaptive Security with AI-Enhanced Anomaly Detection: The combination of anomaly detection and learning (adaptively) enables predictive mitigation of newly emerging security threats associated with the deployment of 5G-based IoT.

D. Scalability Considerations

The anomaly detection module has an approximate computational complexity of O(n × d), where n is the number of network events being analyzed, and d is the total number of extracted feature dimensions. Detection operates from a gateway level; therefore, scalability is limited by the number of events processed and the throughput of events processed, rather than the number of devices connected to the network. Further, the trust evaluation function, as outlined in Equation (1), executes with a constant time complexity of O(1) on each request for trust evaluation with minimal latency overhead. As an overall estimate of the scale of additional verification requested or performed through the new model, for the first k CRA requests, the total gateway verification additional overhead incurred is approximately O(k) times for all CRAs' concurrent requests.

Algorithm : AI-Based Zero-Trust Security Gateway
1: Initialize AI anomaly detection model M_AI
2: Register IoT devices with unique digital identities
3: while system is active do
4:Receive device request or user login attempt
5:Verify device identity and session parameters
6:Compute trust score T_i using equation (1)
7:if T_i < τ then
8:Reject request and log event
9:else
10:Extract behavioral feature vector x_i
11:Predict anomaly output y_i using equation (2)
12:if y_i indicates anomaly then
13:Block request and trigger alert
14:else
15:If user login: validate credentials and OTP using quation (3)
16:Apply RBAC authorization policy
17:Grant controlled access
18:Log secure transaction
19:end if
20:end if
21:end while

The Zero Trust Security Gateway's operational workfiow is illustrated in Algorithm 1 and achieves device validation, user authentication, and anomaly detection in an orderly way. In Algorithm 1, the mathematical formulations of equations (1) – (3) provide a framework for implementing continuous verification of trust scores, intelligent threat mitigation through anomaly detection, and secure user access via OTP authentication. Collectively, the methodology provides secure, scalable, and adaptive protection to distributed IoT infrastructures within 5G-enabled environments.

IV. RESULTS AND DISCUSSION

A. Experimental Setup

The AI-Based Zero-Trust IoT Security System was validated through experimentation using two nodes of ESP32 architecture and actual hardware components. Node 1 consisted of a temperature and DHT11 sensor; both sensors were connected to an ESP32 microcontroller. Node 2 included a temperature and gas sensor connected to an ESP32 microcontroller. The two nodes interfaced with relay-driver circuits, allowing users to operate actuators and view real-time parameters on LCD displays.

Both nodes communicated wirelessly with a central web-based monitoring system and had a security gateway layer (implemented between the IoT nodes and web dashboard) that ensured Zero Trust verification, OTP-based user authentication to access secure content, AI-driven anomaly detection, and blockchain-based logging for secure storage of records.

The experimental test bed included:

Two ESP32 nodes operated simultaneously.

Real-time acquisition of sensor data.

Relay operation based on thresholds.

Web-based dashboard for Admin, User 1, and User 2 roles.

Login requires one-time passcode (OTP) for verification.

Detects abnormal user activity based on AI algorithms.

Uses Blockchain for recording activity data.

System performance was assessed against both normal operations as well as simulated attacks including: unauthorized logins, spoofed communications, high volume of traffic, and invalid commands.

B. Performance Metrics

The application of IoT security principles and operation performance was used to verify the proposed system. For the artificial intelligent (AI) anomaly detection system, detection accuracy was achieved at 96.4% with precision measured at 94.8%, recall measured at 95.2%, and the F1 score measured at .95. The average time between request to device and the event occurred on the verified dashboard (real-time operations) was 185ms. OTP based multi-factor was found to decrease login success rate of unauthorized users by 98.6% over single-password. Roles based access control (RBAC) effectively limited user functions such that User1 could only function on Node 1 and User2 on Node 2 while Admin users could operate globally. Relay response time for switching relays was measured between 120 ms and 150 ms. Wi-Fi communication latency between simultaneous multi-node operations remained consistent. All system activities logged successfully using Blockchain technology.

- Login attempts
- Device registration
- Command execution
- Alert generation

No tampering was observed during integrity verification tests.

C. Comparative Analysis

The proposed system was compared with recent Zero-Trust IoT and AI-based security frameworks, focusing on complete system-level performance rather than healthcare-based metrics.

Study	System Type	Detection Accuracy (%)	OTP-Based MFA	Multi-Node Support	Blockchain Logging	Avg Latency (ms)
[L3i]ghtweight IDS	AI Intrusion Detection	91.8	No	No	No	320
[F5e]derated ZT AI	Distributed Security	92.6	Partial	Limited	No	350
[9] ML-Based ZT	ML Security Model	93.1	No	No	No	290
[Z1T0]Access Control	Access Control Only	90.5	Yes	Limited	No	340
[51G2]ZT Framework	Secure IoT Model	92.8	Yes	Partial	No	275
Proposed System	Dual Node IoT + ZT + AI + Blockchain	96.4	Yes	Yes (Node 1 & 2)	Yes	185

As illustrated in Table I, the proposed system surpasses current solutions for both detection accuracy and latency, while also uniquely combining hardware node control, OTP authentication, and blockchain-secured security log systems. Unlike any existing work that only provides intrusion detection or access controls; It also delivers an entire secure IoT architecture through which users can monitor and control the devices they own.

D. Performance Discussion

There are four main reasons that account for the superior performance of the new architecture.

First, the Zero-Trust security gateway provided continuous identity verification of the devices that are requesting to access the network rather than permitting one-time authentication. This ensured that no unauthorized devices were able to access the network during the test; therefore, there were no instances of devices being spoofed.

Second, the implementation of multi-factor authentication for user access verification using OTPs (one-time-passwords) increased the overall security of user access. In all instances where simulated attacks occurred using the correct username/password, users were denied access as an OTP was not used for their session.

Third, the application of AI-based anomaly detection allowed for the real-time evaluation of network traffic and user behaviour. During the testing of the injection of abnormal traffic into the network, the solution was able to detect abnormal traffic and immediately block suspicious command executions prior to being processed by the nodes.

Fourth, the use of blockchain for the logging of all transactions, login attempts and control commands created tamper-proof logs of all audit trails; therefore, increasing the level of accountability and transparency on the network.

E. Limitations and Recommendations

There were some limitations identified despite being successfully executed.

1N.etwork dependence: This project requires a Wi-Fi connection to work; therefore if there is an interruption to the network, it will slow down the verification process.

2C.entralized gateways: The central security gateway could be a single point of failure if it is not redundantly deployed.

3S.cope of data set: The anomaly detection model used artificial attacks to train the AI model. Using simulating/real-world scenarios of attacks may necessitate the retraining of the model at different times due to the changing face of the threats encountered.

To resolve the issues identified, make the following enhancements:

- Create a distributed or redundant gateway architecture
- Employ sophisticated Deep Learning models for the identification of evolving types of attacks
- Implement hardware-based encryption to provide added security
- Expand the scale of IoT networks to include large distributed (>10 node) networks

V. CONCLUSION AND FUTURE WORK

The Dual-Node ESP32 AI-Enabled Zero Trust IoT Security System demonstrates a scalable, secure, and real-time monitoring & control architecture that integrates hardware-level sensing, relay-driver actuation, OTP-based, multi-factor authentication, AI-driven anomaly detection, role-based access control, and blockchain-backed secure logging to provide continuous verification of devices & users, effectively reducing the number of unauthorized access attempts and preventing the execution of malicious commands while providing low latency suitable for real-time applications. The improved detection accuracy of experimental validation, fast relay response times, stable multi-node operation, and tamper-evident auditability demonstrate the practical feasibility of this system, providing confirmation beyond theoretical modeling. Future improvements will include deploying distributed or redundant security gateways for eliminating single points of failure, integrating advanced deep learning models for adaptive threat intelligence, expanding to large, multi-node industry deployments, implementing hardware-level encrypted modules for improved security of devices, and including new advanced blockchain consensus mechanisms to strengthen decentralized trust further. and improve the scalability of next-generation IoT infrastructure will include.

REFERENCES

[1] Li, K., et al., “Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things,” IEEE Internet of Things Journal, 2025.

[2] Joshi, H., "Emerging Technologies Driving Zero Trust Maturity Across Industries," IEEE Open Journal of the Computer Society, vol. 6, pp. 25–36, 2024.

[3] Roy, B. G., et al., "Proactive Zero-Trust Intrusion Detection for Consumer IoT Applications Using Lightweight Ensemble Learning with Anomaly Analysis," IEEE Transactions on Consumer Electronics, 2025.

[4] Rehman, A., et al., "Immersive Embedded Consumer Model Leveraging AI with Zero-Trust Architecture for Cyber-Physical System," IEEE Transactions on Consumer Electronics, 2025.

[5] Hussain, M., et al., "Federated Zero Trust Architecture Using Artificial Intelligence," IEEE Wireless Communications, vol. 31, no. 2, pp. 30–35, 2024.

[6] Bajpayi, P., Sharma, S., & Gaur, M. S., "AI Driven IoT Healthcare Devices Security Vulnerability Management," 2024 2nd International Conference on Disruptive Technologies (ICDT), IEEE, 2024.

[7] James, M., et al., "Authentication and Authorization in Zero Trust IoT: A Survey," 2024 35th Irish Signals and Systems Conference (ISSC), IEEE, 2024.

[8] Fathalla, E., & Azab, Y., "Towards a Lightweight Self-Sovereign Identity Framework for IoT Network in a Zero Trust Environment," 2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE, 2024.

[9] Munasinghe, S., et al., "Machine Learning Based Zero Trust Architecture for Secure Networking," 2023 IEEE 17th International Conference on Industrial and Information Systems (ICIIS), IEEE, 2023.

[10] Abuhasel, K. A., "A Zero-Trust Network-Based Access Control Scheme for Sustainable and Resilient Industry 5.0," IEEE Access, vol. 11, pp. 116398–116409, 2023.

[11] Al Ridhawi, I., & Aloqaily, M., "Zero-Trust UAV-Enabled and DT-Supported 6G Networks," GLOBECOM 2023 – 2023 IEEE Global Communications Conference, IEEE, 2023.

[12] Geetha, G., Chatterjee, A., & Kumar, C. A., "A Zero Trust Approach to Securing 5G Smart Healthcare," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), vol. 1, IEEE, 2023.