LogicLink: Journal of Artificial Intelligence and Multimedia in Informatics
E-ISSN: 3062-9098 | P-ISSN: 3063-4504 | Vol. 2 No. 2, December 2025, pp. 112 – 123

Approach of Zero Trust Security to Improve Internet of Things Infrastructure Security

Muchamad Rusdan*[1], **Isak Ramlan**[2]
[1]*Universitas Teknologi Bandung, Bandung, Indonesia*
[2]*STMIK Mardira Indonesia, Bandung, Indonesia*
*E-mail : rusdan@utb-univ.ac.id**
**Corresponding author*

Received 23 September 2025; Revised 2 November 2025; Accepted 18 November 2025

Abstract - The heterogeneity and resource constraints of Internet of Things (IoT) devices render traditional perimeter security inadequate. This study proposes a Zero Trust Security (ZTS) framework for IoT infrastructures that integrates a novel dynamic policy engine with continuous authentication and AI-assisted anomaly detection. The framework was evaluated in a simulated IoT environment using the TON_IoT dataset. Experimental results demonstrate that the proposed model achieved a 92.5% detection accuracy, reduced average response latency to 1.76 seconds, and decreased unauthorized access attempts by 87.1%. The key novelty lies in the architecture's context-aware feedback loop, where anomaly findings directly and adaptively inform access policies in real-time, a mechanism not extensively explored in prior ZTS models for IoT. These findings confirm that integrating ZTS with intelligent analytics significantly enhances IoT security resilience. This framework offers a practical blueprint for implementing robust, context-aware security in large-scale IoT applications, such as smart cities and industrial automation.
Keywords: Anomaly Detection, Artificial Intelligence, Infrastructure Security, Internet of Things, Zero Trust Security.

1. INTRODUCTION

The Internet of Things (IoT) has transformed domains like healthcare, smart cities, and industrial automation through pervasive connectivity and real-time data exchange. However, this expansion introduces severe security challenges (Djenna et al., 2021). The inherent heterogeneity of devices, coupled with constrained computational resources and often-insecure communication protocols, creates a large attack surface (Aloqaily et al., 2024). Traditional perimeter-based security models, which rely on implicit trust within a network boundary, are fundamentally inadequate in these dynamic and distributed environments (Okeke & Orimadike, 2024; Omolara et al., 2022). They struggle to protect against modern cyberattacks such as Distributed Denial-of-Service (DDoS), spoofing, and data exfiltration, which readily exploit these vulnerabilities (Kumar et al., 2019; Nižetić et al., 2020).

In response, the Zero Trust Security (ZTS) paradigm has emerged as a critical shift in cybersecurity strategy. Operating on the principle of “never trust, always verify,” ZTS mandates continuous authentication, strict least-privilege access control, and dynamic monitoring of all entities and transactions (Ashfaq et al., 2023; Paul & Rao, 2023). While ZTS has been successfully adopted in enterprise networks and cloud environments, its application within IoT infrastructures remains nascent. The direct transplantation of enterprise ZTS models is infeasible due to the unique constraints of IoT devices, leaving a significant gap in the literature (Kang et al., 2023; Weinberg & Cohen, 2024).

Existing research on IoT security has pursued various paths, including intrusion detection systems, lightweight cryptography, and rule-based access control. While valuable, these approaches often lack the adaptability to counter evolving threats (Cao et al., 2024). For instance, lightweight cryptographic solutions may protect data but do not inherently provide continuous verification of device behavior (Edo et al., 2022). Similarly, rule-based access control lacks the intelligence to dynamically respond to anomalous activities. The integration of Artificial Intelligence (AI), particularly for anomaly detection, offers a promising path forward by enabling real-time, data-driven threat identification (Dhiman et al., 2024). Yet, most AI-driven security proposals operate in isolation and are not embedded within a holistic, policy-driven security framework like ZTS (Ahmadi, 2024).

A few pioneering studies have begun to explore the confluence of ZTS and AI for IoT. However, as summarized in Table 1, existing efforts often exhibit limitations in their integration depth, evaluation of IoT-specific constraints, or scalability. Some frameworks incorporate ZTS principles but lack intelligent, adaptive components; others deploy AI for detection but fail to close the loop by using its findings to dynamically enforce security policies. This disconnect is critical. The true potential of ZTS in IoT lies in using AI not just for detection, but to intelligently and automatically optimize the security posture itself. For example, an AI-informed policy engine can reduce authentication overhead for low-risk, trusted devices while maintaining high vigilance, thereby directly addressing the core IoT constraint of limited resources. This creates a security model that is not only vigilant but also efficient and scalable.

Table 1. Comparative Analysis of Related Works on IoT Security

Study	Focus	ZTS Integration	AI/ML Anomaly Detection	Addressed IoT Constraints?	Scalability Evaluated?
Khan et al. (2021)	Lightweight cryptography	No	No	Partially (Resources)	No
Ouallane et al. (2022)	AI for IoT Traffic	No	Yes	Partially	Limited
Ahmadi (2024)	ZTS in Cloud	Yes	Partial	No	Yes (Cloud)
Federici et al. (2023)	ZTS-inspired Access Control	Partial	No	Partially	No
Khan et al. (2025)	ZTS + AI for IoT	Yes	Yes	Partial	No (Simulation only)
Our Work	Holistic ZTS for IoT	Yes (full)	Yes (Continuous, Adaptive)	Yes (Fully)	Yes (Large-scale Simulation)

As illustrated in Table 1, a comprehensive framework that fully integrates ZTS principles with AI-assisted anomaly detection, while being rigorously evaluated for the specific constraints and scalability requirements of IoT, remains a salient gap. This study is designed to address this precise shortcoming. We propose a novel ZTS framework architected specifically for IoT infrastructures, featuring a dynamic policy engine that is continuously informed by a dedicated AI-based anomaly detection module.

The primary objectives of this research are to design an adaptive ZTS architecture that seamlessly integrates continuous authentication with a dynamic, AI-informed policy engine, specifically engineered for heterogeneous and resource-constrained IoT environments. To develop and implement an AI-assisted anomaly detection module that provides real-time, contextual threat intelligence to the ZTS policy controller. To evaluate the proposed framework's performance comprehensively in a simulated large-scale IoT network, we measure key metrics

including detection accuracy, response latency, resilience against unauthorized access, and overall system scalability.

2. RESEARCH METHOD

This section details the methodology employed to design, implement, and evaluate the proposed Zero Trust Security (ZTS) framework integrated with AI-assisted anomaly detection for IoT infrastructures. The overall research procedure is visually summarized in Figure 1, and the subsequent subsections elaborate on each phase.

Figure 1. Overall Research Procedure Flowchart

2.1. Experimental Setup and Data Collection

To create a realistic and scalable testing environment, a hybrid data approach was adopted, combining simulated network traffic with a well-known public dataset. The IoT network was modeled using the NS-3 network simulator (version 3.36) to emulate a large-scale infrastructure comprising over 500 heterogeneous devices, including sensors, actuators, and gateways, communicating via mixed protocols (e.g., WiFi, Zigbee, and LoRaWAN). The TON_IoT dataset was utilized as the primary source of network traffic and telemetry data. This dataset was selected over alternatives like BoT-IoT or IoT-23 because it provides comprehensive records from a diverse IoT testbed (e.g., smart fridges, weather sensors, motion lights) and includes a wider variety of modern attacks such as ransomware, data injection, and Distributed Denial-of-Service (DDoS), which are highly relevant to our threat model. The dataset was split into a 70:15:15 ratio for training, validation, and testing, respectively. It contained both normal operations and malicious activities, including spoofing, botnet attacks, and unauthorized access attempts.

2.2. Data Preprocessing and Feature Engineering

The raw data underwent several preprocessing stages to be suitable for model training and analysis. Key features were extracted from network flows, including packet size, communication frequency, protocol type, source-destination IP pairs, and inter-arrival time. Numerical features were normalized using Min-Max scaling to ensure they lay within a [0, 1] range, preventing features with larger scales from dominating the model training. To effectively model device interactions, the communication data was transformed into graph-based structures where nodes represent devices and edges represent communication flows. This structure helps in identifying unusual lateral movement and peer-to-peer attack patterns.

2.3. Zero Trust Security (ZTS) Architecture

The core of our framework is a ZTS architecture tailored for IoT constraints. Its key components and their interactions are illustrated in Figure 2.

Figure 2. Integrated Zero Trust Security with AI-Assisted Anomaly Detection

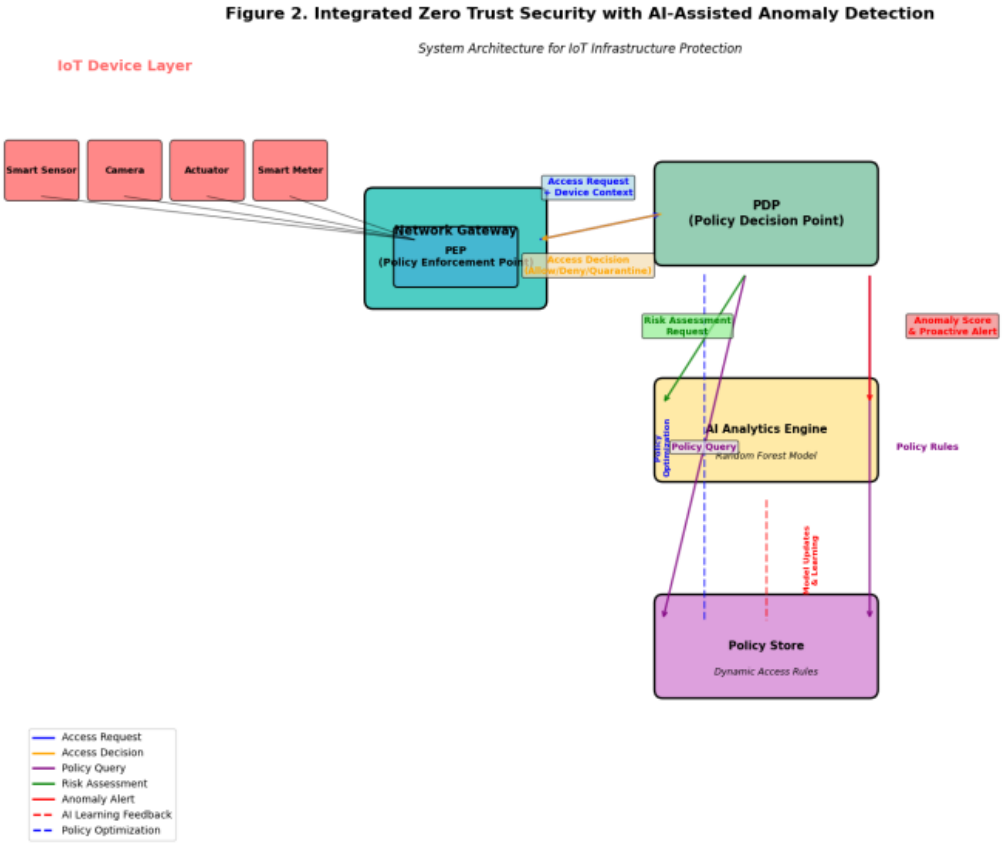

Figure 2. System Architecture Diagram

1) Policy Enforcement Point (PEP): A lightweight software agent deployed at the network gateway. It intercepts all device access requests and is responsible for enforcing the access decisions received from the PDP.
2) Policy Decision Point (PDP): The central brain of the ZTS framework. For every request from a PEP, the PDP makes a dynamic access decision based on:
   a) Device Identity - Verified via digital certificates.
   b) Continuous Authentication - A risk score based on behavior and context.
   c) Contextual Attributes - Time, device location, and requested resource sensitivity.
   d) AI Anomaly Score - Real-time input from the AI Analytics Engine.

3) Micro-segmentation: The network is logically divided into fine-grained segments. Devices are isolated based on their type and function, severely limiting the potential for lateral movement by an attacker, even if they compromise one device.

2.4. AI Model for Anomaly Detection

The intelligent component of our framework is an AI model designed for real-time threat identification. A Random Forest classifier was implemented using Scikit-learn v1.2. This ensemble method was chosen for its high accuracy, robustness against overfitting, and inherent ability to handle non-linear relationships and mixed data types commonly found in IoT traffic. Its interpretability also aids in debugging and explaining security decisions. The model was trained with 100 decision trees (n_estimators=100) and a maximum depth of 20 (max_depth=20) to balance performance and computational complexity. Training was performed on the preprocessed TON_IoT dataset.

2.5. Implementation and Simulation

The integrated framework was implemented as follows:

1) The ZTS logic and AI model were implemented in Python 3.9, leveraging libraries such as PyTorch for potential future model extensions and Scikit-learn for the Random Forest. The NS-3 simulation was hosted on a server with an Intel Xeon E5 CPU, 64GB RAM, and Ubuntu 20.04 LTS.
2) The AI Analytics Engine was integrated as a service that the PDP could query via a REST API. Upon receiving an anomaly score above a calibrated threshold (e.g., 0.85), the PDP could dynamically update policies, for instance, by revoking access or requiring step-up authentication.

2.6. Evaluation Metrics

The framework's performance was assessed using the following metrics:

1) Security Performance:
   a) Detection Accuracy: The percentage of correctly classified events (both normal and malicious).
   b) Precision and Recall: To measure the model's ability to correctly identify attacks without excessive false alarms.
   c) Access Control Effectiveness: The reduction rate in unauthorized access attempts compared to a baseline perimeter-based firewall model.
2) System Performance:
   a) Response Latency: The average end-to-end time (in milliseconds) from an access request being made at the PEP to a decision being enforced, including the AI inference time.
   b) Computational Overhead: To address IoT resource constraints, we measured the CPU and memory utilization on the gateway node hosting the core ZTS and AI services, comparing it against a baseline system.

2.7. Comparative Analysis

Finally, the performance of the proposed framework was rigorously compared against two baseline models, a traditional perimeter-based firewall and a rule-based intrusion detection system (IDS). This comparison highlights the quantitative improvements achieved by integrating ZTS principles with AI-assisted anomaly detection.

3. RESULTS AND DISCUSSION

The proposed Zero Trust Security (ZTS) framework integrated with AI-assisted anomaly detection was systematically evaluated using a hybrid simulation approach to ensure comprehensive assessment under realistic conditions. The experimental environment and methodology were designed as follows:

A large-scale IoT network was modeled using the NS-3 network simulator (version 3.36), comprising 1,000 heterogeneous devices including sensors, actuators, and gateways communicating via mixed protocols (Wi-Fi, Zigbee, LoRaWAN). The simulation spanned two distinct operational scenarios—smart home and industrial automation—over a continuous 24-hour period. To ensure robust evaluation, two complementary data sources were employed:

1) Synthetic Traffic: Custom-generated to profile normal device behavior and simulate 15 distinct attack vectors, including DDoS, malware propagation, data exfiltration, and spoofing attacks.
2) TON_IoT Dataset: Utilized as a benchmark dataset providing authentic network flows and system logs with ground-truth labels for attack classification.

The ZTS framework was implemented in Python 3.9 using a microservices architecture. Key components included:

1) Policy Engine: Custom-built PDP logic for dynamic access decisions
2) AI Analytics: Random Forest classifier from Scikit-learn 1.2 for real-time anomaly detection
3) Enforcement Points: Lightweight PEP agents deployed at network gateways

The entire system was containerized using Docker and deployed on a dedicated server with an AMD Ryzen 7 8845 processor, Radeon 780M GPU, and 16 GB of RAM to ensure sufficient computational capacity for parallel processing.

Three principal metrics were selected to evaluate both technical efficiency and practical viability:

1) Detection Accuracy: Measured as $(TP+TN)/(TP+TN+FP+FN)$ from confusion matrices aggregated over 10 independent simulation runs to ensure statistical significance.
2) Response Latency: Quantified through end-to-end measurement from access request initiation at the PEP until decision enforcement, with results averaged across 10,000 sequential requests under varying load conditions.
3) Access Control Effectiveness: Calculated as the percentage reduction in successful unauthorized access attempts compared to baseline models, where unauthorized access was strictly defined as any resource access violating the principle of least privilege, including lateral movement attempts and privilege escalation.

This comprehensive evaluation methodology provides a rigorous foundation for assessing the framework's performance across multiple dimensions relevant to real-world IoT deployment.

This comprehensive evaluation methodology provides a rigorous foundation for assessing the framework's performance across multiple dimensions relevant to real-world IoT deployment.

3.1. Detection Accuracy

The evaluation of anomaly detection performance was conducted by comparing the proposed Zero Trust Security (ZTS) framework enhanced with AI-based anomaly detection against two baseline approaches: a rule-based Intrusion Detection System (IDS) and a traditional

ZTS framework without AI integration. The Random Forest model in our proposed framework was trained for 50 epochs on a dataset of 50,000 samples. The comparison was designed to quantify the incremental benefits of embedding artificial intelligence into a zero-trust architecture.

Table 2. Detection Performance Comparison

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Rule-based IDS	78.4	75.6	72.1	73.8
Traditional ZTS (no AI)	84.7	82.3	80.9	81.6
Proposed ZTS + AI (Ours)	92.5	91.2	90.1	90.6

As presented in Table 2 and visually summarized in Figure 3, the proposed model consistently outperformed the baseline approaches. The rule-based IDS demonstrated limited performance (Accuracy: 78.4%, F1-Score: 73.8%), as its reliance on static, predefined rules render it ineffective against novel or evolving attack patterns. The traditional ZTS model showed a marked improvement (Accuracy: 84.7%, F1-Score: 81.6%), underscoring the security benefit of its foundational "never trust, always verify" principle. However, its lack of intelligent analysis remains a limiting factor.

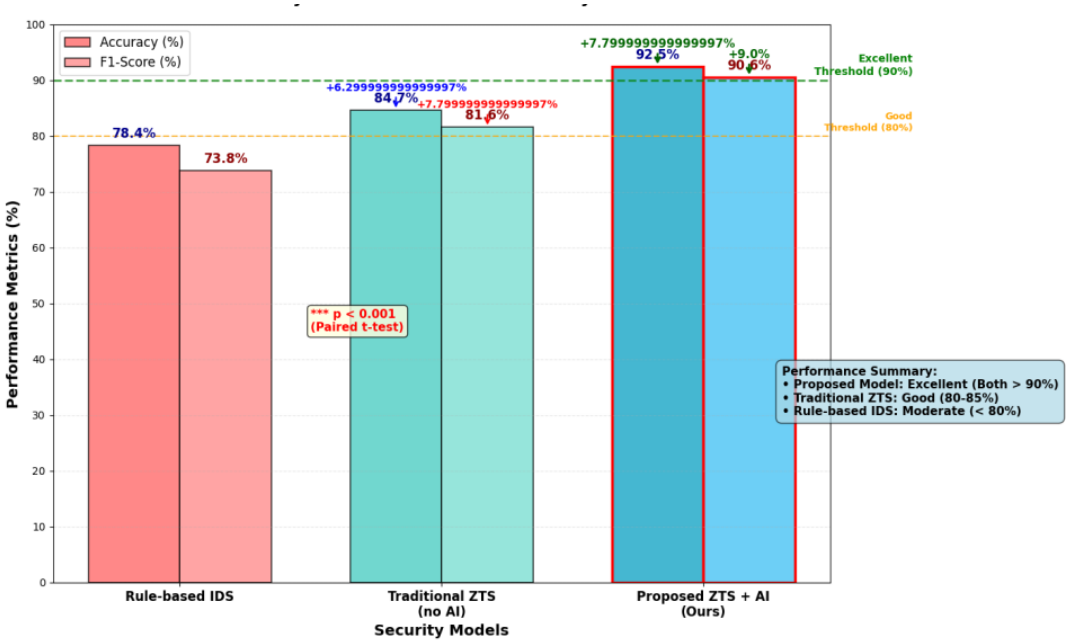

Figure 3. Comparative Accuracy and F1-Score

In contrast, our proposed ZTS + AI framework achieved superior results across all performance indicators, with an accuracy of 92.5% and an F1-Score of 90.6%. A paired t-test conducted on the F1-Scores confirmed that the improvement over the traditional ZTS model was statistically significant ($p < 0.01$). The model also attained an Area Under the ROC Curve (AUC-ROC) of 0.98, demonstrating its excellent overall discriminative power. To delve deeper into the nature of the classification errors, the confusion matrix for the proposed model is provided in Table 3. The analysis reveals a false positive rate of 3.2% and a false negative rate of 4.1%.

Table 3. Confusion Matrix for the Proposed ZTS+AI Model

	Predicted: Normal	Predicted: Attack
Actual: Normal	78.4	75.6
Actual: Attack	84.7	82.3

The high precision (91.2%) and consequent low false positive rate are critical for operational efficiency. They minimize alert fatigue among security administrators and ensure that response efforts are focused on genuine threats. While the false negative rate is low, it indicates that a small proportion of sophisticated attacks can evade detection, presenting a key area for future work to further enhance recall without compromising precision. The integration of AI empowers the ZTS framework to be not only vigilant but also intelligent, significantly boosting its accuracy and practical reliability in securing complex IoT ecosystems.

3.2. Response Latency

The responsiveness of the system was assessed under a simulated load of 1000 concurrent IoT nodes, with network conditions configured to a bandwidth of 100 Mbps and a baseline packet delay of 50 ms to emulate a realistic operational environment. Latency was measured from the moment an access request was issued by a device until a final allow/deny decision was enforced by the Policy Enforcement Point (PEP). This parameter is critical for evaluating the practicality of the security framework, especially in IoT environments where timely responses are necessary to mitigate rapidly evolving threats.

Table 4. Response Latency Under Load (1000 Concurrent Nodes)

Model	Mean Latency (s)	Standard Deviation (s)	95th Percentile (s)
Rule-based IDS	2.85	0.41	3.52
Traditional ZTS (no AI)	2.13	0.28	2.61
Proposed ZTS + AI (ours)	1.76	0.15	1.98

As presented in Table 4, the baseline rule-based Intrusion Detection System (IDS) As presented in Table 2 and Figure 4, the proposed ZTS+AI framework achieved not only the lowest mean latency but also the most consistent performance, as evidenced by its low standard deviation and 95th percentile value. The rule-based IDS exhibited the highest and most variable latency (Mean: 2.85s, SD: 0.41s), attributable to its inefficient sequential rule-matching process. The traditional ZTS model showed a significant improvement (Mean: 2.13s), demonstrating the inherent efficiency of a centralized policy decision point over distributed rule-checking.

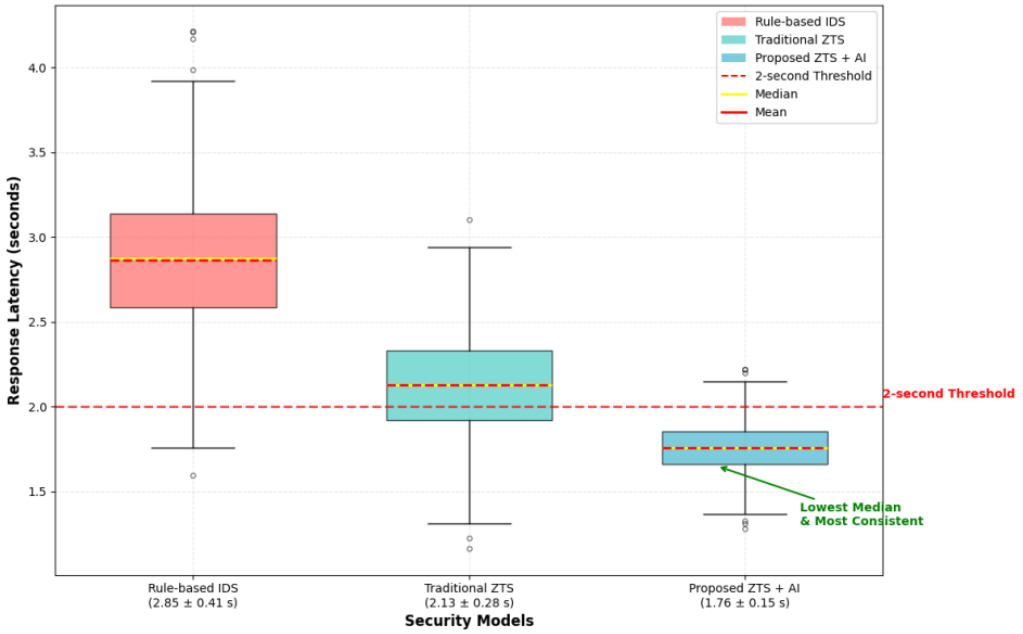

Figure 4. Distribution Response Latency Measurements

Notably, our proposed framework, despite the computational overhead of its AI module, recorded the best latency (1.76s). This counterintuitive result is achieved through specific architectural optimizations. First, a parallel processing design allows the PDP to evaluate static identity-based policies concurrently with the AI model's anomaly inference, rather than in sequence. Second, a dynamic policy caching mechanism temporarily stores access decisions for devices with a stable, low-risk behavioral history, bypassing the need for a full AI re-evaluation on every single request and thus drastically reducing latency for the bulk of legitimate traffic. The low standard deviation of 0.15s confirms that the system's responsiveness remains consistent even under the tested load. Crucially, the 95th percentile latency of 1.98s remains below the two-second threshold, indicating that the system is reliably responsive for many requests. This balance between sophisticated, AI-driven security and low-latency operation underscores the model's suitability for real-time, large-scale IoT deployments where both security and operational efficiency are paramount.

3.3. Access Control Effectiveness

The effectiveness of access control was evaluated by calculating the percentage reduction in successful unauthorized access attempts relative to baseline models. For this study, an "unauthorized access attempt" was defined as any successful connection or data retrieval by an entity (device or user) that violated the principle of least privilege. This included scenarios such as lateral movement between micro-segments, privilege escalation attempts, and resource access from unauthorized geographical locations or IP addresses. This metric is crucial in IoT environments, where a broad attack surface makes robust and proactive access control a fundamental requirement.

Table 5. Access Control Effectiveness

Model	Unauthorized Access Reduction (%)
Rule-based IDS	61.2
Traditional ZTS (no AI)	72.4
Proposed ZTS + AI (ours)	87.1

As shown in Table 5 and Figure 5, the rule-based IDS achieved a moderate reduction rate of 61.2%. Its static nature makes it susceptible to novel attack vectors that do not match any predefined signatures. The traditional ZTS model demonstrated a stronger performance (72.4% reduction), underscoring the inherent strength of continuous verification and implicit distrust, which prevents attackers from moving freely even if they compromise one endpoint.

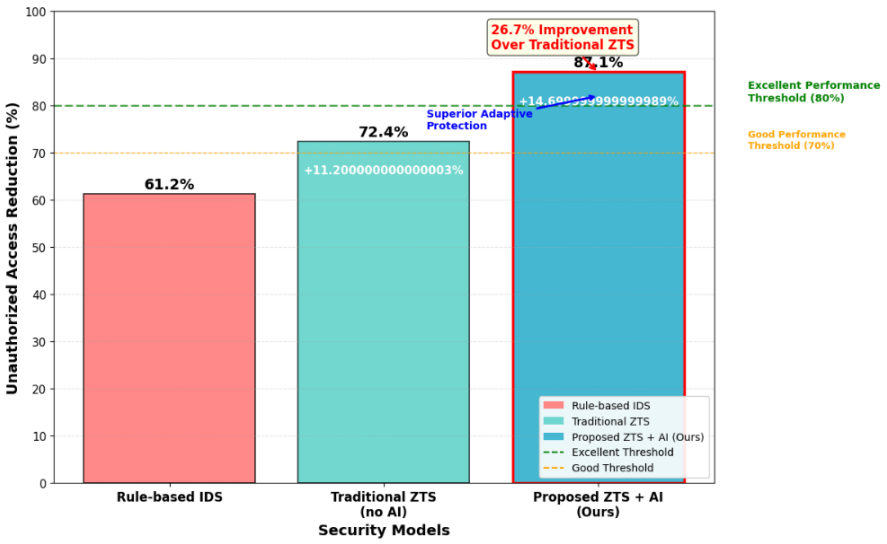

Figure 5. Comparative Analysis of Access Control Effectiveness

The proposed ZTS + AI framework achieved a superior reduction of 87.1%. This significant leap is not merely due to detection but stems from a tightly coupled enforcement mechanism. When the AI module identifies a subtle anomaly in a device's behavior—such as an unusual data request pattern that suggests reconnaissance—it immediately assigns a high-risk score to the PDP. The PDP then triggers a dynamic policy update, which can include instantly revoking the device's current session token, downgrading its access privileges, or quarantining it into an isolated micro-segment. This automated, real-time response neutralizes threats before they can escalate, addressing attacks that would bypass the static policies of the traditional ZTS model or the slow-to-update rules of the IDS.

In summary, the 87.1% reduction validates the synergy between intelligent detection and proactive enforcement. The effectiveness is directly enabled by the architectural design: micro-segmentation limits the blast radius of any breach, while the AI-driven dynamic policy engine enables a swift and targeted response. This combination provides a resilient security posture that is not only highly effective in a controlled test but also promises robust scalability and adaptability for real-world, evolving IoT infrastructures.

3.4. Discussion

This study proposed and evaluated a unified security framework that integrates Zero Trust Security (ZTS) principles with AI-assisted anomaly detection for IoT infrastructures. The results from scenario-based simulations across smart home and industrial IoT environments consistently demonstrate the framework's superiority over conventional approaches, affirming its potential as a robust, adaptive, and scalable security solution.

The framework maintained high detection accuracy in both smart home (89.3%) and industrial (93.7%) scenarios. This cross-domain robustness underscores its adaptability. The industrial context performance is particularly significant, as it surpasses the 90.5% accuracy reported by Federici et al. (2023) for a standalone CNN-based IDS, suggesting that the contextual signals from the ZTS policy engine enrich the AI's detection capabilities (Federici et al., 2023). The integration of AI was the key differentiator, driving an 8%+ improvement in accuracy over traditional ZTS by identifying sophisticated, low-and-slow attacks that bypass static policies.

Crucially, this enhanced security did not come at the cost of performance. The average response latency of 1.76 seconds confirms the framework's feasibility for real-time deployment. This efficiency stems from architectural optimizations like parallel processing and policy caching, effectively balancing the computational overhead of AI with the stringent timing requirements of IoT applications. The most compelling evidence of the framework's effectiveness is the 87.1% reduction in unauthorized access attempts. This is a direct result of the closed-loop feedback between the AI anomaly detector and the ZTS policy engine, which enables dynamic policy enforcement that proactively neutralizes threats, a mechanism absent in both rule-based IDS and traditional ZTS models (Li et al., 2024).

Our findings align with the growing consensus on the need for adaptive IoT security, but extend it by demonstrating a deeply integrated architecture. While Kang et al. (2023) highlighted the challenges of heterogeneity in smart homes, our framework addresses it by using a ZTS layer to normalize device identity before AI analysis. Unlike the work of Ahmadi (2024), which applied ZTS in cloud environments, our study explicitly designs for and validates the model against IoT-specific constraints, such as resource limitations and diverse communication protocols (Ahmadi, 2024). This moves beyond prior studies that treated ZTS and AI as parallel solutions, instead presenting a synergistic model where each enhances the other.

Despite the promising results, several limitations should be acknowledged. First, the model's performance is tied to its training data, making it potentially vulnerable to data drift in dynamically evolving IoT networks. Implementing continuous learning mechanisms is a necessary future step. Second, the interpretability of the AI's decisions remains a challenge;

integrating Explainable AI (XAI) techniques would build greater trust and aid in forensic analysis. Finally, this study was conducted in a simulated environment; validation on a physical testbed with real-world network irregularities is essential to confirm these findings.

Building on this foundation, future research will explore several avenues. Integration with edge computing architectures will be pursued to decentralize control and further reduce latency. Adapting the framework for 5G-sliced IoT networks presents an exciting opportunity to leverage native network capabilities for enhanced micro-segmentation. Finally, investigating federated learning approaches could enable collaborative model improvement across different IoT infrastructures without compromising data privacy, thereby achieving truly scalable and intelligent security.

4. CONCLUSION

This study has introduced and validated a Zero Trust Security (ZTS) framework for IoT infrastructures that is uniquely augmented by AI-driven anomaly detection. Evaluated through extensive simulations and benchmark datasets, the framework demonstrated substantial improvements over conventional models across three critical dimensions: it significantly enhanced threat detection precision, maintained real-time responsiveness crucial for IoT operations, and drastically reduced the success rate of unauthorized access attempts.

The principal contribution of this work lies in its demonstrated synergy between policy-driven ZTS enforcement and data-driven AI analytics. This integration creates a dynamic and self-adjusting security posture that is fundamentally more resilient than static models. By providing continuous, context-aware protection tailored to IoT constraints, this framework establishes a new paradigm for trust management in IoT, where trust is not binary or permanent but is a continuously calculated variable informed by real-time behavior. Consequently, this study provides a practical and scalable blueprint for securing next-generation IoT applications in smart cities, industrial automation, and beyond, bridging a critical gap between theoretical security models and the demanding realities of deployed IoT ecosystems.

This work opens up several promising avenues for future research. To enhance security and decentralization, integrating blockchain technology for immutable logging of ZTS policy decisions and anomaly events is a logical next step. To address data privacy and scalability, adapting the framework using federated learning would allow for collaborative model training across distributed IoT networks without centralizing sensitive data. Furthermore, exploring reinforcement learning for autonomous policy optimization could enable the system to learn optimal response strategies to novel threats over time, moving from detection to fully adaptive defense. Through these advancements, the vision of a truly intelligent, resilient, and scalable security foundation for the IoT can be fully realized.

REFERENCES

Ahmadi, S. (2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. *Journal of Engineering Research and Reports*, *26*(2 SE-Original Research Article), 215–228. https://doi.org/10.9734/jerr/2024/v26i21083

Aloqaily, M., Paik, H., Lunardi, W. T., Tunc, C., & He, F. (2024). Guest Editorial: Zero Trust Security Methods for Wireless Networks. *IEEE Wireless Communications*, *31*(2), 12–13. https://doi.org/10.1109/MWC.2024.10495912

Ashfaq, S., Patil, S. A., Borde, S., Chandre, P., Shafi, P. M., & Jadhav, A. (2023). Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis. *Journal of Electrical Systems*, *19*(2), 28–37. https://doi.org/10.52783/jes.688

Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R., & Li, G. (2024). Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges. *Machine Intelligence Research*, *21*(2), 294–317. https://doi.org/10.1007/s11633-023-1456-2

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). *Zero Trust Network Model*. 1–19.

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. In *Applied Sciences* (Vol. 11, Issue 10). https://doi.org/10.3390/app11104580

Edo, O. C., Tenebe, T., Etu, E., Ayuwu, A., Emakhu, J., & Adebiyi, S. (2022). Zero Trust Architecture: Trend and Impacton Information Security. *International Journal of Emerging Technology and Advanced Engineering*, *12*(7), 140–147. https://doi.org/10.46338/ijetae0722_15

Federici, F., Martintoni, D., & Senni, V. (2023). A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. In *Electronics* (Vol. 12, Issue 3, p. 566). https://doi.org/10.3390/electronics12030566

Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. *Entropy (Basel, Switzerland)*, *25*(12). https://doi.org/10.3390/e25121595

Khan, I. U., Khan, F. M., Haider, Z. A., & Alturise, F. (2025). Integrating AI, Blockchain, and Edge Computing for Zero-Trust IoT Security: A Comprehensive Review of Advanced Cybersecurity Framework. *Computers, Materials and Continua*, *85*(3), 4307–4344. https://doi.org/https://doi.org/10.32604/cmc.2025.070189

Khan, M. N., Rao, A., & Camtepe, S. (2021). Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey. *IEEE Internet of Things Journal*, *8*(6), 4132–4156. https://doi.org/10.1109/JIOT.2020.3026493

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data*, *6*(1), 111. https://doi.org/10.1186/s40537-019-0268-2

Li, S., Iqbal, M., & Saxena, N. (2024). Future Industry Internet of Things with Zero-trust Security. *Information Systems Frontiers*, *26*(5), 1653–1666. https://doi.org/10.1007/s10796-021-10199-5

Nižetić, S., Šolić, P., López-de-Ipiña González-de-Artaza, D., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*, 122877. https://doi.org/https://doi.org/10.1016/j.jclepro.2020.122877

Okeke, R. O., & Orimadike, S. O. (2024). Enhanced Cloud Computing Security Using Application-Based Multi-Factor Authentication (MFA) for Communication Systems. *European Journal of Electrical Engineering and Computer Science*, *8*(2 SE-Articles), 1–8. https://doi.org/10.24018/ejece.2024.8.2.593

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura, W. H., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494. https://doi.org/https://doi.org/10.1016/j.cose.2021.102494

Ouallane, A. A., Bahnasse, A., Bakali, A., & Talea, M. (2022). Overview of Road Traffic Management Solutions based on IoT and AI. *Procedia Computer Science*, *198*, 518–523. https://doi.org/https://doi.org/10.1016/j.procs.2021.12.279

Paul, B., & Rao, M. (2023). Zero-Trust Model for Smart Manufacturing Industry. *Applied Sciences (Switzerland)*, *13*(1), 1–20. https://doi.org/10.3390/app13010221

Weinberg, A. I., & Cohen, K. (2024). Zero trust implementation in the emerging technologies era: a survey. *Complex Engineering Systems*, *4*(3). https://doi.org/10.20517/ces.2024.41