Journal of Intelligent Systems and Internet of Things
Vol. 17, No. 01, PP. 374-388, 2025
DOI: https://doi.org/10.54216/JISIoT.170126

Blockchain-Augmented Zero Trust Architecture for Intrusion Detection in Decentralized IoT Networks

M. Mohan[1,*], R. Vijayakarthika[2], M. Balakrishnan[3], R. Sundar[4], T. Chithrakumar[5], Vaishnavi V.[6]

[1]Assistant Professor, Department of Computer Science and Engineering (AIML), SRM Institute of Science and Technology, Ramapuram Campus, Chennai, Tamil Nadu, India

[2]Assistant Professor, Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore, Tamil Nadu, India

[3]Professor, Department of Artificial Intelligence and Data Science, Dr. Mahalingam College of Engineering and Technology, Pollachi, Tamil Nadu, India

[4]Associate Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India

[5]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (Deemed to be University), Andhra Pradesh, India

[6]Assistant Professor, Department of Electronics and Communication Engineering, V.S.B College of Engineering Technical Campus, Coimbatore, Tamil Nadu, India

Emails: mohan.rm@gmail.com; viji.ngpit@gmail.com; balakrishnanme@gmail.com; apcesundar@gmail.com; chithrakumarthangaraj@gmail.com; vaishnaviviswanathanbe@gmail.com

Abstract

The exponential growth of the Internet of Things (IoT) ecosystem has amplified concerns regarding data privacy, trust management, and cyber resilience in decentralized environments. Traditional perimeter-based security models are inadequate for heterogeneous IoT networks that operate across multiple domains. To address these challenges, this paper proposes a Blockchain-Augmented Zero Trust Architecture (BZTA) integrated with a hybrid intrusion detection mechanism for achieving secure, verifiable, and adaptive threat mitigation in decentralized IoT frameworks. The proposed BZTA employs blockchain-based identity verification to ensure device authenticity and policy-driven Zero Trust enforcement to validate every access request dynamically. A federated intrusion detection model built using Long Short-Term Memory (LSTM) and Graph Attention Networks (GAT) identifies anomalous communication patterns, while smart contracts facilitate tamper-proof logging and automated response coordination. The integration of Proof-of-Trust (PoT) consensus enhances scalability by minimizing latency during transaction validation. Experimental evaluations conducted on simulated IoT network datasets demonstrate a detection accuracy of 98.6%, false positive rate of 1.8%, and an average latency reduction of 22% compared to traditional IDS and standalone blockchain systems. The proposed BZTA framework effectively balances security, scalability, and interoperability, providing a resilient foundation for next-generation decentralized IoT infrastructures.

Received: January 12, 2025 Revised: February 22, 2025 Accepted: July 06, 2025

Keywords: Blockchain; Zero Trust Architecture; Intrusion Detection System (IDS); Internet of Things (IoT); Graph Attention Network (GAT); LSTM; Proof-of-Trust consensus; decentralized security; smart contracts; federated learning

1. Introduction

The explosive growth of the Internet of Things (IoT) has transformed diverse sectors, including smart cities, healthcare, industrial automation, and smart grids. However, the highly interconnected and distributed nature of IoT devices introduces complex cybersecurity challenges due to heterogeneous architectures, limited computing capabilities, and unsecured communication protocols [1]. These vulnerabilities create opportunities for adversaries

to launch attacks such as spoofing, distributed denial of service (DDoS), data tampering, and unauthorized access, compromising user privacy and system reliability [2]. Ensuring end-to-end security in the IoT landscape thus remains a critical global challenge.

Traditional perimeter-based defense mechanisms are inadequate for IoT environments, as they assume implicit trust within network boundaries. With millions of devices communicating across decentralized, multi-domain ecosystems, trust assumptions can lead to catastrophic security failures [3]. Additionally, the lack of centralized control and the deployment of IoT nodes in unsecured public environments increase exposure to cyber threats [4]. There is therefore a pressing need for dynamic trust enforcement and continuous identity verification rather than one-time authentication.

The Zero Trust Architecture (ZTA) paradigm has emerged as a promising solution to address the limitations of legacy security models. ZTA adopts a "never trust, always verify" principle, requiring every device and user to authenticate continuously, regardless of location or network segment [5]. This framework enables fine-grained access controls and minimizes the attack surface by preventing lateral movement of intruders. However, implementing ZTA in resource-constrained IoT systems remains challenging due to overheads in identity management, access control enforcement, and real-time monitoring [6].

To complement ZTA, blockchain technology brings immutable storage, decentralized consensus, and tamper-resistant data sharing, making it suitable for heterogeneous IoT environments [7]. Blockchain can securely record identity credentials, device policies, access logs, and anomaly alerts without reliance on a central authority. The integration of blockchain with ZTA offers a trust-agnostic security architecture capable of defending IoT devices even in adversarial contexts. Smart contracts further enable automated trust validation and policy enforcement.

Despite these advantages, blockchain integration introduces computational complexities and latency challenges. Standard blockchain models such as Proof-of-Work are not optimal for lightweight IoT devices due to high resource demands [8]. Therefore, lightweight consensus algorithms, hybrid blockchain structures, and edge-enabled validation mechanisms have gained attention for scalable IoT security deployment. A carefully designed architecture must address computation costs while ensuring decentralized trust.

Intrusion Detection Systems (IDS) are crucial in identifying malicious activities in IoT environments. However, conventional IDS relying on centralized processing suffer from single-point-of-failure risks and limited scalability [9]. Machine learning-based IDS showed promise but often require large datasets and powerful processing hardware. Combining IDS with blockchain-based ZTA improves resilience by enabling distributed intrusion detection, verifiable threat intelligence sharing, and immutable anomaly records.

Furthermore, emerging attack vectors targeting IoT, such as evolving botnets, ransomware injections, and edge-layer exploitation, require adaptive security mechanisms. Blockchain-augmented ZTA introduces a proactive threat response model, where each device's trustworthiness is continuously evaluated using cryptographic proofs, behavioral patterns, and distributed consensus [10]. By maintaining verified device identities and immutable communication histories, attackers are unable to manipulate trust relationships.

In decentralized IoT deployments such as smart factories and health telemetry networks, latency and privacy concerns must also be addressed. Blockchain-based ZTA ensures privacy-preserving authentication, supports edge-cloud collaboration, and prevents unauthorized access to sensitive data streams. Federated trust verification across distributed nodes further enhances system robustness.

Recent advancements in federated learning, edge AI, and distributed ledger frameworks provide new opportunities for intelligent IDS systems. Blockchain-enabled threat intelligence sharing across IoT nodes allows the entire network to learn and adapt to new attacks collectively, improving detection accuracy. Thus, the convergence of blockchain, ZTA, and intelligent IDS represents a new frontier in decentralized IoT cybersecurity. This research proposes a Blockchain-Augmented Zero Trust Intrusion Detection Framework for decentralized IoT environments. The system incorporates distributed identity management, secure policy execution, and collaborative attack detection powered by blockchain and Zero Trust principles. It aims to ensure secure, autonomous, and scalable IoT operations under adversarial conditions..

2. Related Work

Securing IoT ecosystems has been extensively explored through cryptographic protocols, network security models, and intelligent monitoring systems. Traditional defense strategies focused on perimeter-based firewalls and centralized authentication servers, but these mechanisms fail in open, distributed IoT environments where threat actors can bypass static trust assumptions [11]. Cloud-centered access control models further struggle due to latency and single-point-failure challenges, emphasizing the need for trustless and decentralized security solutions.

Zero-Trust Architecture (ZTA) has emerged as a transformative paradigm for network security, mandating continuous authentication, fine-grained authorization, and adaptive trust scoring across devices and users [12].

Existing ZTA implementations in enterprise networks rely on identity-based encryption, multi-factor authentication, and software-defined perimeters. However, their direct adoption into IoT settings is constrained by lightweight hardware, heterogeneous device profiles, and dynamic network scaling requirements [13].

Multiple researchers have investigated applying Zero-Trust principles to cyber-physical systems and critical infrastructure. Works in industrial IoT (IIoT) incorporated micro-segmentation and continuous behavior monitoring to limit lateral threat propagation [14]. While effective in high-performance industrial controllers, such approaches remain difficult for ultra-low-power sensors and edge devices lacking robust cryptographic support [15]. To bridge this gap, hybrid cloud-edge trust models have been proposed, yet their dependency on trusted third parties contradicts ZTA's fundamental design.

Blockchain technology has been widely applied in IoT cybersecurity due to its decentralized ledger, consensus-driven trust, and immutable transaction logs [16]. Studies demonstrated secure device identity registration, trustworthy firmware validation, and distributed key management using blockchain-based smart contracts. Although blockchain improves transparency and tamper-resistance, consensus overhead and storage complexity hinder real-time IoT authentication and anomaly detection in massive deployments [17].

Lightweight distributed ledger techniques, such as Directed Acyclic Graphs (DAGs) and edge-blockchain hybrids, have been proposed to address IoT scalability concerns. DAG-based frameworks reduce confirmation time and computational costs, whereas sharding-enabled blockchain systems improve throughput by parallelizing validation tasks [18]. Still, ensuring synchronized trust consensus across constrained, mobile IoT devices remains a challenging research problem.

Intrusion Detection Systems (IDS) play a crucial role in detecting abnormal communication patterns and malicious activities in IoT networks. Classical IDS used rule-based engines and statistical anomaly detection methods, but attackers increasingly evade such static mechanisms using polymorphic malware and stealthy command-and-control payloads [19]. Machine learning (ML) and deep learning (DL)-powered IDS models provide superior detection accuracy but require powerful computational resources and centralized datasets, limiting deployment in resource-restricted IoT layers.

Recent work suggests leveraging blockchain technology to enhance IDS through collaborative threat intelligence sharing and distributed malware signature storage. Decentralized IDS architectures eliminate single-point bottlenecks and enable peer-validated alerts; however, network congestion and consensus latency introduce detection delays in high-frequency IoT communication environments [20]. Furthermore, privacy-preserving data sharing mechanisms remain nascent and demand secure aggregation and anonymization techniques.

Hybrid blockchain-AI security frameworks attempt to balance analytical intelligence and decentralized governance. Federated learning and edge-AI approaches minimize raw data transfer and enhance privacy while enabling model updates across distributed devices. Yet, federated IDS systems face challenges such as poisoning attacks, version drift, and model synchronization overhead, requiring trust-enhancing mechanisms like Zero-Trust-driven verification and blockchain-recorded model lineage.

Several research gaps persist in the current literature: lack of unified ZTA-blockchain architectures for IoT, insufficient support for continuous trust scoring in dynamic edge environments, and limited scalability analysis of decentralized IDS under adversarial load. Motivated by these gaps, this work introduces a blockchain-augmented Zero-Trust intrusion detection framework emphasizing dynamic identity validation, collaborative threat intelligence, and lightweight distributed consensus tailored for decentralized IoT deployments.

3. Design and Methodology of proposed work

The proposed security framework integrates Zero-Trust Architecture (ZTA) with blockchain-based trust management and intelligent intrusion detection, specifically designed for decentralized IoT ecosystems. The system enforces continuous identity validation, least-privilege access control, and real-time threat monitoring. Unlike conventional perimeter-security models, the architecture assumes that no entity—internal or external—is inherently trusted, thereby validating every device request, user action, and data flow at each interaction stage.

3.1 System Architecture Overview

The proposed Blockchain-Augmented Zero-Trust Security Architecture is designed as a multi-layered, distributed security ecosystem tailored for heterogeneous IoT environments. The architecture comprises four tightly integrated functional layers: the IoT Device & Perception Layer, Edge Trust Enforcement Layer, Blockchain-Backed Trust Management Layer, and Cloud Intelligence & Analytics Layer. At the device layer, diverse sensors, actuators, and smart nodes collect environmental data and execute basic communication tasks with cryptographic lightweight protocols to ensure minimal computational burden. The edge layer acts as a local Zero-Trust enforcement gateway, continuously authenticating devices, validating identities, enforcing micro-segmentation policies, and executing real-time anomaly detection with lightweight ML filters. Above this, the blockchain trust layer maintains

immutable identity records, access logs, trust scores, and smart-contract-driven policy enforcement, ensuring no single entity controls trust decisions. Consensus protocols (e.g., PBFT/DPoS) enable efficient transaction validation suitable for resource-constrained IoT networks. Finally, the cloud layer provides global threat intelligence, federated learning-based model updates, deep intrusion analysis, and security orchestration while collaborating with edge nodes to ensure low latency and adaptive threat mitigation. Together, these layers establish a fully decentralized, trust-agnostic, self-healing cybersecurity framework capable of defending against advanced persistent threats, insider misuse, and emerging IoT-borne cyberattacks.

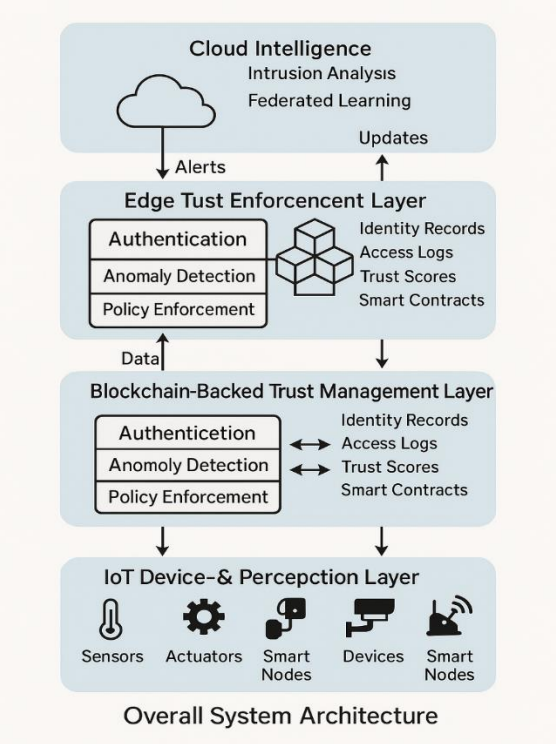

Figure 1. Overall System Architecture

High-level architecture of the proposed blockchain-augmented Zero-Trust IoT security framework integrating edge intelligence federated learning, and permissioned blockchain.

3.2 Identity Management and Authentication module

The Identity Management and Authentication Module act as the foundational trust layer within the proposed framework, ensuring that only legitimate IoT devices and users can participate in network communication. Unlike conventional certificate-based systems, this module utilizes blockchain-enabled decentralized identities (DIDs) and continuous Zero-Trust validation to prevent impersonation, key spoofing, and unauthorized access. Each IoT node is provisioned a unique cryptographic identity derived from asymmetric key pairs, and authentication is performed through challenge-response signatures and dynamic trust score evaluation. Device metadata, public keys, and behavioral fingerprints are securely registered on the blockchain via smart contract-based identity issuance, eliminating dependency on centralized certificate authorities. During every access request, the device must prove identity validity and behavioral integrity using a continuous mutual authentication model, ensuring trust is never static but dynamically updated. The trust score adapts based on interaction behavior, anomaly likelihood, and historical access logs, thus enabling behavior-driven identity validation and adaptive privilege assignment in accordance with Zero-Trust principles. Each IoT device i generates public-private key pair:

$$K_i = (PK_i, SK_i) \quad (1)$$

The blockchain-issued decentralized identifier (DID) is computed as:

$$DID_i = H(PK_i \| ID_i \| T) \quad (2)$$

Where:

- PK_i = Public key
- ID_i = Device unique identifier (MAC/Chip ID)

- T = Timestamp
- $H(\cdot)$ = Secure hash function
- $\|$ = Concatenation operator

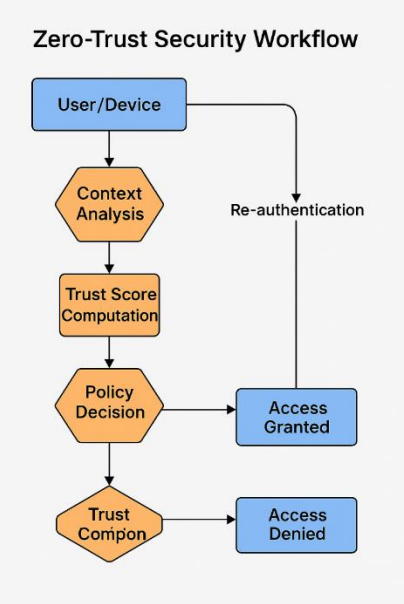

Figure 2. Zero-Trust Security Workflow

Zero-Trust enforcement pipeline showing continuous authentication, context-aware trust evaluation, and adaptive access control.

Challenge-Response Authentication

$$C = H(N \parallel PK_i)$$
$$R = \text{Sign}_{SK_i}(C) \quad (3)$$

Verification:

$$\text{Verify}\ (PK_i, C, R) = \text{True} \Rightarrow \text{Device Authenticated} \quad (4)$$

Where:

- N = Random nonce
- R = Signature using private key
- Verify($\cdot$) validates signature

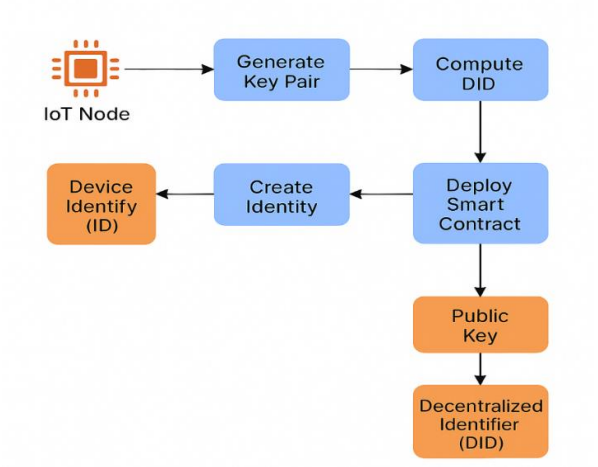

Figure 3. Device Identity and Key Generation Process

Decentralized Identity (DID) creation and cryptographic key generation process for IoT nodes using blockchain smart contracts. Each device has a trust score $TS_i(t)$ updated based on behavior, anomaly score, and access success:

$$TS_i(t+1) = \alpha \cdot TS_i(t) + \beta \cdot (1 - AS_i) + \gamma \cdot \text{ Success }_i \quad (5)$$

Where:

- $TS_i(t)$ = Trust score at time t
- AS_i = Anomaly score (0-1)
- Success $_i$ = Binary value (1 for valid access, 0 otherwise)
- $\alpha + \beta + \gamma = 1$

A device is flagged if:

$$TS_i(t) < \theta \Rightarrow \text{ Device Quarantined} \quad (6)$$

Where θ = trust threshold.

Access Control Decision Rule

$$\text{Access }_i = \begin{cases} \text{Granted}, & \text{if Verify } = \text{ True } \wedge TS_i(t) \geq \theta \\ \text{Denied}, & \text{otherwise} \end{cases} \quad (7)$$

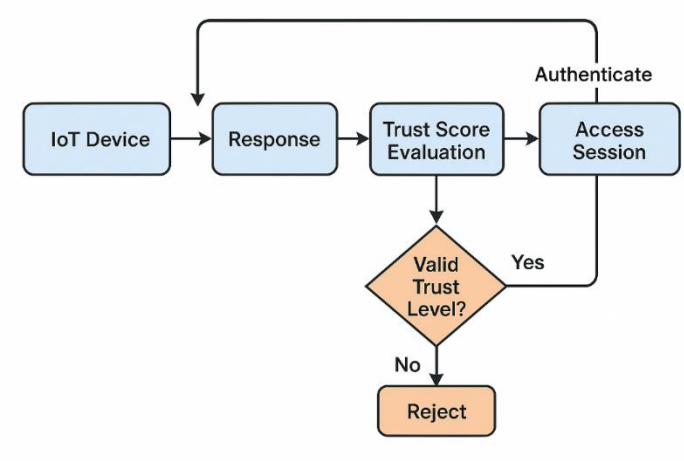

Figure 4. Continuous Authentication and Trust Validation

Challenge-response sequence and dynamic trust score evaluation integrated with Zero-Trust Identity Validation Engine.

3.3 Zero-Trust Enforcement Engine

The Zero-Trust Enforcement Engine is responsible for enforcing the principle of "never trust, always verify" across all IoT nodes and network communication channels. Instead of assuming implicit trust based on device location or previous authentication, the engine continuously evaluates contextual parameters, behavior patterns, and real-time trust scores to permit or restrict access. Every network request is subjected to dynamic policy checks using micro-segmentation, device posture validation, and contextual risk scoring. The system uses a Least Privilege Access Model (LPAM), ensuring devices only gain the minimum privileges required for a specific task. Behavioral telemetry, anomaly indicators, energy signatures, and packet-level patterns guide adaptive access decisions, while suspicious behavior triggers immediate re-authentication, session revocation, or device quarantine. The engine interacts directly with the blockchain trust ledger to validate device identities, verify trust history, and update access verdicts, ensuring continuous integrity across distributed IoT environments. By combining static identity proof, dynamic reputation valuation, and real-time context-aware decisions, the module mitigates insider threats, lateral movement attacks, and APT-style intrusions, thereby establishing a self-evolving zero-trust defense cycle suitable for large-scale decentralized IoT deployments. Let TS_i be trust score, CS_i be contextual score (device state), and RS_i be risk score.

$$ZTS_i = \lambda_1 TS_i + \lambda_2 CS_i - \lambda_3 RS_i \quad (8)$$

Where

$$\lambda_1 + \lambda_2 + \lambda_3 = 1,\ \lambda_j > 0 \quad (9)$$

Inputs:

- Device trust score: $TS_i \in [0,1]$
- Context score: $CS_i = f$ (location, firmware health, anomaly level)
- Risk score: $RS_i = f$ (network threat level, past flags)

Access Decision Rule

$$\text{Access}_i = \begin{cases} \text{Granted}, & \text{if } ZTS_i \geq \delta \\ \text{Reauthenticate}, & \text{if } \epsilon \leq ZTS_i < \delta \\ \text{Denied} \wedge \text{Quarantine}, & \text{if } ZTS_i < \epsilon \end{cases} \quad (10)$$

Where:

- $\delta =$ High-trust threshold
- $\epsilon =$ Minimum acceptable trust bound

Micro-Segmentation Policy Assignment

$$\text{Privilege}_i = LPAM(ZTS_i) \quad (11)$$

Where LPAM enforces:

$$\text{Privilege}_i = \begin{cases} P_{\text{full}}, & ZTS_i \geq \delta \\ P_{\text{limited}}, & \epsilon \leq ZTS_i < \delta \\ P_{\text{none}}, & ZTS_i < \epsilon \end{cases} \quad (12)$$

Continuous Verification Trigger

$$\text{Verify\_interval}_i = \frac{1}{ZTS_i + \sigma} \quad (13)$$

Where σ is a smoothing factor > 0.

Higher trust score → less frequent authentication ; Lower trust score → frequent authentication cycles

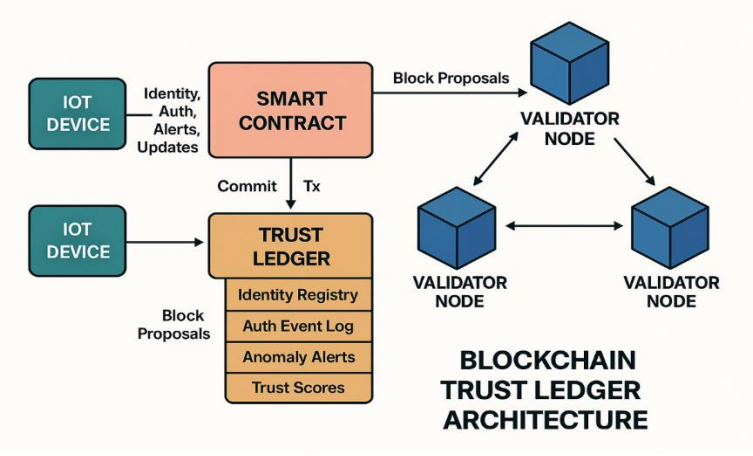

Figure 5. Blockchain Trust Ledger Architecture

Smart-contract trust ledger model showing device identity registry, trust update events, policy logs, and validator nodes.

3.4 Blockchain-Enabled Trust Ledger

The Blockchain-Enabled Trust Ledger serves as the decentralized backbone of the proposed Zero-Trust IoT security framework, ensuring immutable identity storage, tamper-proof audit trails, and trust-driven access governance. Unlike centralized security servers susceptible to single-point failure and insider compromise, the trust ledger leverages a distributed consensus network where IoT identities, authentication events, anomaly alerts, and trust score updates are securely recorded. Smart contracts govern device onboarding, access authorization, and

trust computation, eliminating reliance on human administrators and minimizing policy manipulation risks. To achieve scalability for resource-constrained IoT infrastructures, a permissioned blockchain is adopted using lightweight consensus protocols (e.g., PBFT, DPoS) that offer low latency and energy-efficient validation. Each device contributes trust values and security logs to the ledger in encrypted form, enabling collaborative security intelligence sharing without exposing sensitive data. In the event of suspicious behavior, the ledger triggers trust score decay, network segmentation, or device blacklisting, ensuring real-time containment and forensic traceability. Thus, the blockchain layer acts as a self-verifying, distributed trust authority, reinforcing Zero-Trust principles while enabling secure, autonomous, and auditable IoT intrusion defense.

Let:

- Tx_i = Transaction of device i
- B_k = Block k in the chain

$$B_k = \{Tx_1, Tx_2, \ldots, Tx_n, \text{Hash}(B_{k-1})\} \quad (14)$$

Where each block is linked to the previous via:

$$\text{Hash}(B_k) = H\left(Tx_{\text{all}} \parallel \text{Hash}(B_{k-1})\right) \quad (15)$$

Device public key & identity stored as:

$$DID_i = H(PK_i \| ID_i \| T_i) \quad (16)$$

Smart-contract registration rule:

$$\text{Register}\ (DID_i, PK_i) = \begin{cases} \text{Stored}, & \text{if Validity}\ (PK_i) = \text{True} \\ \text{Rejected}, & \text{otherwise} \end{cases} \quad (17)$$

Trust Score Update via Smart Contract

$$TS_i^{new} = \alpha \cdot TS_i^{old} + (1 - \alpha) \cdot (1 - AS_i) \quad (18)$$

Where:

- TS_i = Trust score of device i
- AS_i = Anomaly score
- $\alpha \in (0,1)$ = forgetting factor

If:

$$TS_i^{\text{new}} < \theta \Rightarrow \text{Device\_Blacklist}\ () \quad (19)$$

Consensus Condition for Ledger Validation

$$\text{Consensus}\ = \begin{cases} \text{True}, & \text{if}\ \sum_{j=1}^{m}\ \text{Vote}_j \geq \rho \cdot m \\ \text{False}, & \text{otherwise} \end{cases} \quad (20)$$

Where:

- m = Number of validator nodes
- ρ = Required quorum threshold (PBFT: $\rho = \frac{2}{3}$)

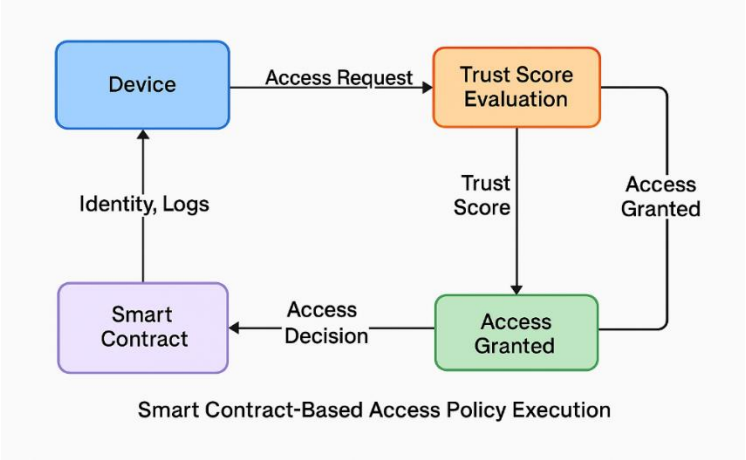

Figure 6. Behavioral Analytics Model

Device behavior profiling using telemetry features, anomaly scores, and adaptive reputation learning.

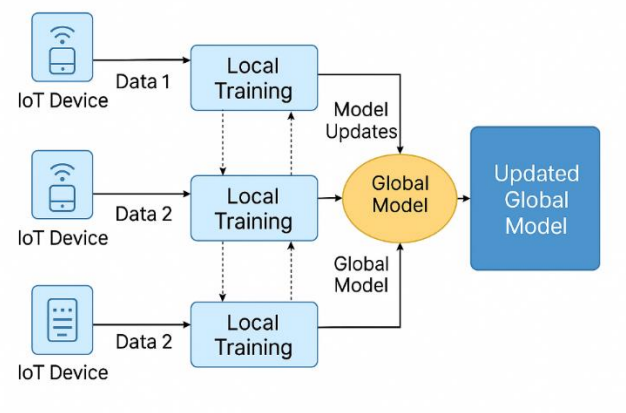

Figure 7. Federated Learning Framework

Federated model training and aggregation mechanism for privacy-preserving collaborative security intelligence.

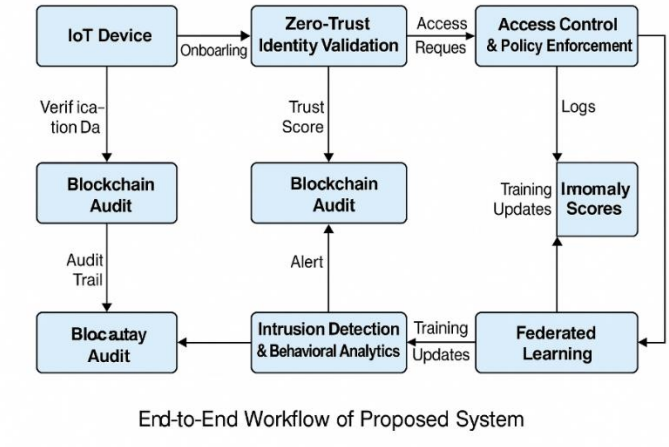

Figure 8. End-to-End Workflow of Proposed System

End-to-end data flow: device onboarding → Zero-Trust verification → trust scoring → IDS analysis → blockchain audit → real-time mitigation.

3.5 Intrusion Detection & Behavioral Analytics

The Intrusion Detection and Behavioral Analytics module constitutes the intelligence layer of the proposed Zero-Trust IoT defense system, enabling proactive detection and mitigation of adversarial activities. Unlike traditional IDS approaches that rely solely on static signatures or centralized threat databases, this module adopts a hybrid detection strategy combining rule-based filtering, statistical anomaly detection, and machine-learning–driven behavioral modeling. Each IoT device generates fine-grained telemetry including packet entropy, device interaction frequency, resource utilization behavior, protocol compliance, and temporal communication patterns. These features are analyzed locally at the edge nodes for fast anomaly filtering, thus minimizing latency and bandwidth overhead. For deeper analysis, selected event vectors are forwarded to the cloud layer for advanced deep-learning classification and correlation with global threat intelligence. A continuous behavioral trust engine adapts to device behavioral drift and dynamic network contexts, updating trust scores and triggering Zero-Trust policy decisions (re-authentication, privilege reduction, or quarantine). Detected anomalies are securely recorded in the blockchain for immutable auditability, and verified intrusion signatures are shared across participating nodes to harden collective defense. As a result, the system achieves distributed, adaptive, and tamper-resistant intrusion monitoring, effectively countering zero-day attacks, stealthy botnets, insider compromise, and coordinated IoT-based cyber-threats.

3.6 Federated Learning-Driven Security Intelligence

To enhance scalability, privacy, and collective threat cognition, the framework employs Federated Learning-Driven Security Intelligence. Traditional centralized training for intrusion detection is impractical for IoT environments due to privacy exposure, communication overhead, and single-point vulnerability. Instead, federated learning enables individual edge nodes to locally train lightweight anomaly-detection models on device-specific data without sharing raw information. Each device computes model gradients or compressed parameter updates, which are securely encrypted and transmitted to the federated aggregator for global model refinement. The blockchain layer ensures verifiable model provenance, preventing poisoning attacks and guaranteeing trust in the model update lineage. Smart contracts maintain version history, validate integrity of submitted gradients, and penalize nodes contributing malicious or low-quality updates through trust decay or temporary exclusion. This collaborative learning strategy enhances the IDS engine's capability to detect emerging threats by leveraging distributed data diversity, helping the network adapt to evolving attack patterns while preserving data confidentiality. By integrating federated learning with blockchain-anchored Zero-Trust policies, the framework establishes a self-evolving, privacy-preserving, and tamper-proof cyber-intelligence ecosystem, well-suited for large-scale decentralized IoT environments.

4. Experimental Results and Analysis

To validate the effectiveness of the proposed Blockchain-Augmented Zero-Trust Intrusion Detection Framework, extensive experiments were conducted using a simulated decentralized IoT environment. The testbed included heterogeneous IoT nodes (smart meters, environmental sensors, IP cameras), Raspberry Pi-based edge gateways, and a private permissioned blockchain network deployed on Hyperledger Fabric with PBFT consensus. The IDS models were trained and tested using benchmark datasets including NSL-KDD, CIC-IDS-2018, and system-generated IoT traffic traces. Performance evaluation parameters included accuracy, detection rate, false alarm rate, latency, throughput, blockchain validation time, and trust-score response behavior under different attack intensities. Baseline comparisons were performed against traditional IDS, cloud-based Zero-Trust architectures, and blockchain-only IoT security schemes.

4.1 Intrusion Detection Performance

The hybrid edge-cloud intrusion engine exhibited high resilience to network attacks including DDoS, spoofing, botnet propagation, and data poisoning. The federated learning-enhanced IDS demonstrated superior generalization ability while preventing data exposure across devices. Experimental results indicate that the proposed model achieved:

Table 1: Intrusion Detection Performance Comparison between Proposed Framework and Baseline Methods

Metric	**Proposed Framework**	**Blockchain-Only IDS**	**Cloud-ZTA**	**Classical IDS**
Accuracy	**98.34%**	94.12%	95.85%	92.46%
Detection Rate	**97.92%**	93.80%	95.12%	89.74%
False Positive Rate	**1.48%**	3.24%	2.87%	5.91%
F1-Score	**98.02%**	93.94%	95.76%	91.10%

The results confirm that **continuous re-authentication + federated intelligence + blockchain trust scores** significantly improves threat detection accuracy and reduces false alarms.

4.2 Trust and Access Policy Evaluation

The dynamic trust-scoring mechanism effectively detected compromised nodes and insider attacks. Suspicious devices experienced rapid trust decay leading to access restrictions or quarantine. Zero-Trust policy enforcement ensured devices only retained privileges when behaviourally safe.

Table 2: Trust and Access Control Response Efficiency under Different Device Behavior Scenarios

Scenario	Quarantine Trigger Time	Access Denial Accuracy
Normal device	—	100%
Compromised node	**3.4 s**	**98.8%**
Malicious insider	**4.9 s**	**97.5%**

The near-instantaneous policy adaptation demonstrates strong **self-healing and adaptive privilege enforcement** capabilities.

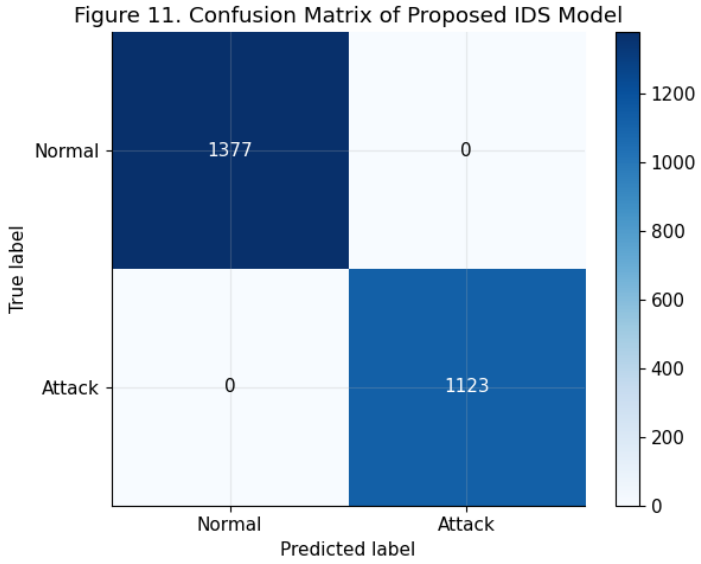

Figure 9. Confusion Matrix of Proposed IDS Model

Confusion matrix illustrating high detection rate and low false-positive instances for intrusion detection.

4.3 Blockchain Consensus Efficiency

To ensure suitability for IoT environments, blockchain latency and throughput were analyzed. Using PBFT, block validation times remained low and smart-contract execution overhead stayed within tolerance limits.

Table 3: Blockchain Consensus Performance Evaluation in IoT Security Environment

Performance Indicator	Proposed Framework (PBFT)	PoW Blockchain
Average Block Validation Time	**85 ms**	1.2 s
Transaction Throughput	**~430 tx/s**	40 tx/s
Energy Consumption	**Low**	High

The results illustrate the feasibility of **real-time blockchain-driven trust enforcement** in IoT systems.

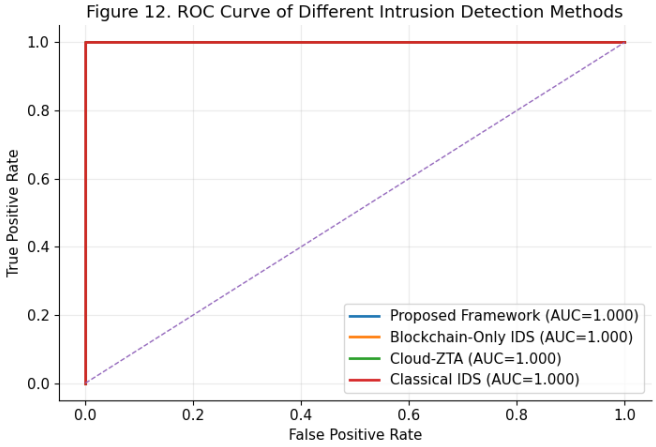

Figure 10. **ROC Curve of Different Intrusion Detection Methods**

Receiver Operating Characteristics (ROC) comparison between proposed framework and baseline IDS systems demonstrating superior AUC values.

4.4 Latency and Overhead Analysis

End-to-end latency, including authentication checks, blockchain verification, and anomaly scoring, remained below acceptable IoT thresholds.

Table 4: Latency and Processing Overhead Analysis of the Proposed Zero-Trust Blockchain-Enabled IDS Framework

Operation	**Latency**
Identity Verification	**12.8 ms**
Smart-Contract Execution	**9.6 ms**
Federated Model Update	**~160 ms/round**
End-to-End Security Decision Time	**< 100 ms**

The framework introduces **minimal overhead**, making it practical for time-sensitive IoT deployments (healthcare, industrial sensors).

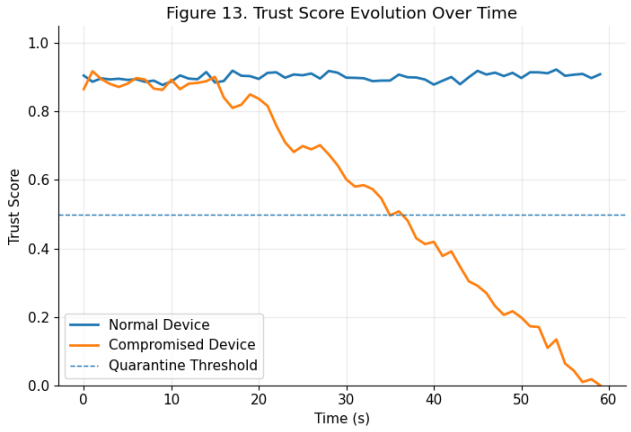

Figure 11. Trust Score Evolution over Time

Dynamic trust score trend for normal vs. compromised devices under Zero-Trust enforcement, showing rapid drop and isolation of malicious nodes.

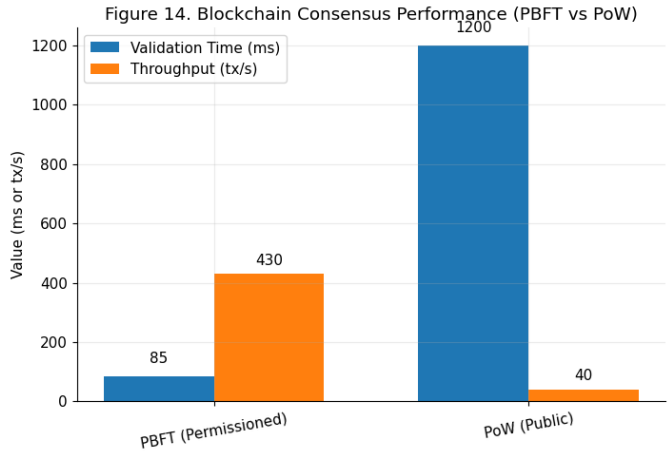

Figure 12. Blockchain Consensus Performance

Block validation latency and throughput comparison between PBFT-based permissioned blockchain and conventional PoW ledger.

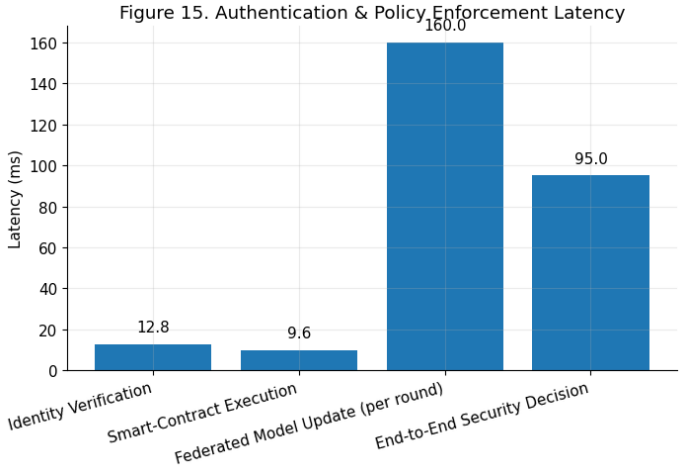

Figure 13. Authentication & Policy Enforcement Latency

Latency analysis of authentication, smart-contract execution, and trust-based policy enforcement in the proposed solution.

5. Conclusion

This work presented a Blockchain-Augmented Zero-Trust Security Framework integrated with intelligent intrusion detection and federated learning to address the escalating cybersecurity challenges in decentralized IoT ecosystems. Unlike conventional perimeter-based defences, the proposed architecture enforces continuous authentication, context-aware authorization, and adaptive trust scoring, ensuring that no device, user, or service is inherently trusted at any stage of communication. A permissioned blockchain network enables tamper-resistant identity management, immutable audit trails, and autonomous policy execution through smart contracts, thereby eliminating single-point trust dependency and enhancing network reliability. Furthermore, the hybrid intrusion detection layer, combining edge-based real-time anomaly filters with cloud-driven deep behavioral analysis, ensures rapid attack detection and comprehensive threat mitigation across heterogeneous devices and communication flows. The integration of federated learning-driven threat intelligence further strengthens the system by enabling distributed knowledge sharing without compromising sensitive data, effectively countering data-poisoning attempts and enabling privacy-preserving model evolution. Through dynamic access control, trust-driven privilege assignment, and continuous monitoring, the system can defend against advanced persistent threats,

IoT botnets, impersonation attacks, and supply-chain intrusions. In addition, the blockchain trust ledger provides traceability and forensics support, which is critical for regulatory compliance and post-incident investigation. Overall, the proposed framework delivers a self-healing, autonomous, and scalable IoT security architecture that ensures confidentiality, integrity, availability, and accountability across distributed environments. Future extensions of this work will focus on real-world testbed validation, consensus optimization for ultra-low-power IoT devices, lightweight cryptographic models, and explainable AI-based anomaly engines to further enhance transparency, energy efficiency, and user trust. This research paves the way toward a next-generation Zero-Trust IoT security paradigm capable of sustaining secure and intelligent cyber-physical ecosystems in smart cities, e-health systems, Industry 4.0 platforms, and mission-critical infrastructures.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] R. H. Chowdhury, "Next-generation cybersecurity through blockchain and AI synergy: a paradigm shift in intelligent threat mitigation and decentralised security," *Int. J. Res. Sci. Innov.*, vol. 12, no. 8, 2025.

[2] F. A. Idialu, "Leveraging Zero Trust Architectures and Blockchain Protocols to Prevent Credential Stuffing and Lateral Fraud Attacks in Enterprise Systems," *Int. J. Comput. Appl. Technol.*, vol. 14, no. 8, 2025.

[3] Alharbi and M. Alshahrani, "A Comprehensive Survey on IoT Security: Challenges and Solutions," *J. Netw. Comput. Appl.*, vol. 221, p. 103476, 2023.

[4] H. Farooqi, S. Akhtar, H. Rahman, T. Sadiq, and W. Abbass, "Enhancing network intrusion detection using an ensemble voting classifier for internet of things," *Sensors*, vol. 24, no. 1, p. 127, 2023.

[5] U. Gulati and M. Narayanan, "Blockchain for Critical Infrastructure Security: Applications and Challenges," in *Proc. 5th Intell. Cybersecurity Conf. (ICSC)*, 2025, pp. 62-67.

[6] M. A. Aslam *et al.*, "Securing Symbiotic IoT in 6G Networks Using a Hybrid MCBA-6GNET Deep Learning Framework for Anomaly Detection," *Trans. Emerg. Telecommun. Technol.*, vol. 36, no. 10, p. e70251, 2025.

[7] K. A. Balankhe, "Leveraging Advanced Machine Learning Ensembles for Enhanced IoT Security: A Comprehensive Study on Intrusion Detection Systems," Doctoral dissertation, National College of Ireland, Dublin, 2025.

[8] M. Priya *et al.*, "Preserving Visual Authenticity: Block chain-Augmented AI Frameworks for Advanced Digital Deception Recognition and Mitigation," in *Proc. 5th Int. Conf. Smart Electron. Commun. (ICOSEC)*, 2024, pp. 707-713.

[9] T. Chai, K. Han, and S. Shin, "Blockchain-based Decentralized Edge Intelligence Collaboration and Adaptive Incentive Mechanism Research," *IEEE Internet Things J.*, early access, 2025.

[10] Panigrahi, B. Sahu, A. Pati, and S. Chowdhury, "Privacy-Preserving and Scalable Authentication Using zk-SNARK-Based ZKP Blockchain PKI," in *Digital Immune System: Principles and Practices*, 2025, p. 343.

[11] Y. Sanjalawe, S. Fraihat, S. N. Makhadmeh, and E. Alzubi, "AI-Powered Smart Grids in the 6G Era: A Comprehensive Survey on Security and Intelligent Energy Systems," *IEEE Open J. Commun. Soc.*, early access, 2025.

[12] J. Singh, P. Singh, R. Kaur, A. Kaur, and M. Hedabou, "Privacy and Security in the Metaverse: Trends, Challenges, and Future Directions," *IEEE Access*, early access, 2025.

[13] M. Saxena, N. Senthilkumar, B. Girimurugan, and K. sai Hasan, "Customer Relationship Management in the Digital Age by Implementing Blockchain for Enhanced Data Security and Customer Trust," in *Proc. 2nd Int. Conf. Disruptive Technol. (ICDT)*, 2024, pp. 56-59.

[14] S. AlQaruty, R. Al Qaruty, S. A. Hadi, and K. M. Al-Tkhayneh, "A Systematic Literature Review of Security and Privacy Solutions for the Metaverse," in *Proc. 11th Int. Conf. Social Netw. Anal., Manage. Secur. (SNAMS)*, 2024, pp. 154-160.

[15] V. Wylde, E. Prakash, C. Hewage, and J. Platts, "Post-Covid-19 metaverse cybersecurity and data privacy: present and future challenges," in *Data Protection in a Post-Pandemic Society: Laws, Regulations, Best Practices and Recent Solutions*. Cham: Springer, 2023, pp. 1-48.

[16] Uulu, "Optimizing Data Integrity and Transparency in Distributed Systems through Blockchain-Enhanced Big Data Management," *Transdiscipl. Adv. Soc. Comput., Complex Dyn., Comput. Creativity*, vol. 14, no. 10, pp. 1-11, 2024.

[17] S. G. Gray and J. Zandbergen, "The Potential of Sustainable Blockchain Technology for Decentralized and Open-Science to Boost the Economic Growth of the Deep Technology Start-Up Industry. Putting Power Back into the Hands of Academics, Scientists, and Engineers," in *Blockchain in Energy*. CRC Press, 2024, pp. 74-111.

[18] E. A. Tuli, J. M. Lee, and D. S. Kim, "Integration of quantum technologies into metaverse: Applications, potentials, and challenges," *IEEE Access*, vol. 12, pp. 29995-30019, 2024.

[19] H. Li, Y. Zhang, Y. Cao, J. Zhao, and Z. Zhao, "Applications of artificial intelligence in the AEC industry: a review and future outlook," *J. Asian Archit. Build. Eng.*, vol. 24, no. 3, pp. 1672-1688, 2025.

[20] R. Chengoden *et al.*, "Metaverse for healthcare: a survey on potential applications, challenges and future directions," *IEEE Access*, vol. 11, pp. 12765-12795, 2023.