International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

A Blockchain-Enhanced Zero-Trust Framework for Privacy in Industrial IOT Systems

Dr. Abdinasir Ismael Hashi

Somali National university
nasirhaji@snu.edu.so
ORCID No: 0009-0009-0635-2609

Highlights

- Achieved low authentication latency (42 ms) and high transaction throughput (980 TPS normal, 865 TPS under attack) with stable resource utilization below 75%.
- Delivered 98.6% anomaly detection accuracy and 97.4% DDoS traffic mitigation efficiency with a rapid recovery time of 2.5 seconds**.**
- Demonstrated scalability, transparency, and resilience**,** making BLOX-Trust suitable for next-generation IIoT environments.

Abstract

The rapid expansion of Industrial Internet of Things (IIoT) systems has heightened concerns over data privacy, security, and trust in highly interconnected industrial environments. This paper proposes **BLOX-Trust (**(Blockchain-Optimized Zero-Trust), a novel blockchain-enhanced zero-trust framework that integrates decentralized identity management, smart contracts, and adaptive access control to ensure robust privacy and security in IIoT networks. By leveraging permissioned blockchain for immutable audit trails and incorporating zero-trust principles for continuous verification of devices and users, BLOX-Trust enables fine-grained, dynamic policy enforcement while mitigating risks such as unauthorized access, data tampering, and advanced cyberattacks. Edge computing is integrated to reduce latency and optimize real-time operations, while AI-driven anomaly detection supports proactive threat identification. Experimental evaluations in simulated IIoT environments demonstrate BLOX-Trust's effectiveness, achieving secure, low-latency transactions with scalable performance. The results highlight its potential to enhance resilience, transparency, and operational efficiency in modern industrial ecosystems.

Keywords: Industrial IoT, blockchain, zero trust, privacy preservation, decentralized identity, edge computing, anomaly detection, smart contracts

1. Introduction

The Industrial Internet of Things (IIoT) has emerged as a cornerstone of modern industrial transformation, driving automation, predictive analytics, and real-time decision-making across manufacturing, energy, logistics, and critical infrastructure domains [1–5]. By interconnecting heterogeneous devices, sensors, and actuators, IIoT systems enable efficient data acquisition, process optimization, and advanced analytics, forming the foundation of smart factories and digital industrial ecosystems [6]. Despite these advancements, the hyper-connectivity of IIoT environments has introduced significant challenges, particularly in terms of security, privacy, and trust management [7]**.** A growing number of cyber threats—including malware, ransomware, man-in-the-middle attacks, and Distributed Denial-of-Service (DDoS) campaigns—pose substantial risks to operational integrity and data confidentiality, often resulting in severe financial and operational disruptions [8–10].

Traditional centralized security mechanisms often fail to meet the complex demands of IIoT due to single points of failure, scalability issues, and the inability to provide continuous authentication and authorization in dynamic environments [11, 12]. This shortfall has driven interest in blockchain technology, recognized for its decentralized, transparent, and tamper-resistant ledger capabilities [13, 14]. By integrating blockchain into IIoT systems, industries can achieve enhanced data integrity, secure access control, and immutable logging, which collectively strengthen resilience against internal and external threats [15–17]. In parallel, the adoption of Zero-Trust Architecture (ZTA) has gained traction, with its principle of "never trust, always verify" enabling dynamic access policies and rigorous identity management for devices and users in complex IIoT ecosystems [18, 19].

Recent studies have explored the convergence of blockchain and zero-trust models to address critical gaps in IIoT security frameworks [20]. However, most existing approaches are limited by high computational overhead, latency, and scalability challenges, particularly in resource-constrained industrial environments.

This paper addresses these limitations by proposing a novel Blockchain-Optimized Zero-Trust (BLOX-Trust) framework, which combines the immutable auditability of blockchain with the adaptive, risk-based controls of zero trust. Through integration with edge computing for real-time processing and AI-driven anomaly detection for proactive threat response, the proposed framework establishes a scalable, privacy-preserving, and resilient security model for IIoT systems.

1.1 Contributions

The novel contributions of this study are:

1. The design of BLOX-Trust, a blockchain-optimized zero-trust framework that integrates decentralized identity management, smart contracts, and adaptive access control to enhance security and privacy in IIoT networks.
2. Implementation of permissioned blockchain for immutable auditability combined with continuous verification mechanisms, enabling fine-grained, dynamic, and risk-based policy enforcement in complex industrial environments.

3. Integration of edge computing and AI-driven anomaly detection to achieve low-latency operations, real-time threat identification, and scalable performance across resource-constrained IIoT ecosystems.
4. Comprehensive experimental validation in simulated IIoT environments, demonstrating improved transaction security, operational transparency, and resilience compared to traditional centralized security models.

2. Literature Review

The integration of blockchain and artificial intelligence (AI) into industrial systems has been widely explored to address critical challenges of security, privacy, and scalability in Industrial Internet of Things (IIoT) networks. Recent studies highlight how the synergy between blockchain and AI provides a foundation for implementing zero-trust architectures (ZTA) that enforce continuous verification and dynamic access control in complex, high-traffic environments. Table 1 shows summary of research gaps.

Chang et al. (2025) [21] investigated the symbiotic relationship between AI and blockchain in enhancing zero-trust cybersecurity. Their findings show that blockchain enables secure data sharing, traceability, decentralized storage, and immutable records, while AI contributes behavioral profiling, anomaly detection, adaptive consensus development, and parameter optimization to strengthen blockchain systems. This dual enhancement establishes a foundation for risk-based and adaptive trust management frameworks suitable for IIoT environments.

In healthcare systems, Ahmed et al. (2025) [22] introduced a human-centric framework that combines ciphertext-policy attribute-based encryption (CP-ABE), Ethereum smart contracts, and decentralized IPFS storage. Their approach integrates post-quantum cryptography and energy-efficient Proof-of-Stake (PoS) mechanisms, achieving a 98% reduction in energy consumption and high resistance to attacks. These results emphasize the potential of lightweight and sustainable blockchain models for latency-sensitive and mission-critical applications, a requirement often mirrored in industrial contexts.

Blockchain applications are also expanding into logistics and operational domains. Sari and Butun (2025) [23] developed a blockchain-enhanced warehouse management system that integrates IoT tracking, smart contracts, and AI-driven anomaly detection to ensure tamper-proof recordkeeping and fraud prevention. Their real-world deployment, processing over 10 million transactions across five years, demonstrated significant improvements in data integrity, operational transparency, and fraud mitigation, offering transferable insights for industrial supply chains.

The integration of blockchain with zero-trust principles has also been explored in advanced communication networks. El-Hajj (2025) [24] proposed a federated learning (FL) framework combined with ZTA to secure Open Radio Access Networks (O-RAN). By implementing continuous authentication, micro-segmentation, and differential privacy, the framework achieved 32% energy savings with minimal latency impact, even under adversarial conditions. This highlights the feasibility of deploying blockchain-enhanced ZTA in dynamic and latency-sensitive industrial networks.

Dwivedi et al. (2025) [25] proposed a blockchain-enabled encrypted neural network framework to secure IIoT systems through trust-aware key management and node authentication. By integrating graph convolutional networks (GCNs) with blockchain-based smart contracts, their system achieved 98.9% authentication accuracy on the X-IIoTID dataset while maintaining low response times, effectively mitigating Sybil and replay attacks. Similarly, Patel et al. (2025) [26] applied autoencoder-deep belief networks (AE-DBN) for medical image classification, secured through blockchain transmission, demonstrating that decentralized trust mechanisms can safeguard sensitive data while maintaining system efficiency.

Further studies emphasize the versatility of blockchain for endpoint and hardware security. Kshetri et al. (2025) [27] explored endpoint protection in the metaverse, noting that blockchain, when combined with edge computing, strengthens device-level security and operational resilience. Whig et al. (2025) [28] investigated blockchain applications in hardware trust management, detailing how cryptographic innovations and smart contracts enhance transparency and protection in hardware systems, which is crucial for IIoT devices with embedded components.

Khan et al. (2025) [29] proposed BEFF-SIGS, a blockchain-enhanced fog framework for IoT data integrity and sustainable operations. Their approach integrates token-based authentication and authorization with offloading computational processes to the fog layer, resulting in better latency performance, distributed processing power, and energy efficiency, aligning with the sustainability goals of Industry 5.0. Similarly, Xi et al. (2025) [30] provided a comprehensive STRIDE-based analysis of cybersecurity in unmanned aerial systems (UAS), emphasizing layered defense strategies and recommending blockchain for data immutability and resilient transaction security.

Across these studies, a recurring theme is the potential of blockchain-enhanced zero-trust frameworks to mitigate security vulnerabilities, ensure tamper-proof operations, and enable dynamic, scalable security enforcement. However, gaps remain in addressing real-time performance, interoperability, and integration with resource-constrained IIoT devices. These gaps provide a strong rationale for the development of BLOX-Trust, a novel framework that integrates permissioned blockchain, AI-driven anomaly detection, and edge computing to deliver privacy, scalability, and operational efficiency in industrial ecosystems.

Table 1: Summary of Research Gaps in Existing Studies

Author(s) & Year	Focus Area	Key Contributions	Identified Research Gaps
Chang et al. (2025) [21]	AI–Blockchain integration for Zero-Trust Cybersecurity	Explored synergy between AI and blockchain for secure data sharing, anomaly detection, and adaptive	Lack of real-time scalability and integration with edge computing for IIoT.

Author(s) & Year	Focus Area	Key Contributions	Identified Research Gaps
		consensus.	
Ahmed et al. (2025) [22]	Blockchain for Healthcare Data Privacy and Integrity	Proposed CP-ABE with post-quantum cryptography and energy-efficient PoS for secure healthcare data.	Limited applicability to industrial operations and latency-sensitive IIoT tasks.
Sari and Butun (2025) [23]	Blockchain-enhanced Warehouse Management	Integrated IoT tracking, smart contracts, and AI-driven anomaly detection for fraud prevention and transparency.	Not optimized for large-scale, heterogeneous IIoT environments.
El-Hajj (2025) [24]	Blockchain with Federated Learning and ZTA for O-RAN	Implemented continuous authentication, micro-segmentation, and differential privacy with reduced energy usage.	Requires optimization for broader industrial use and high-volume IIoT systems.
Dwivedi et al. (2025) [25]	Blockchain-Enabled Neural Network Framework for IIoT	Developed trust-aware key management achieving 98.9% authentication accuracy with low response times.	High computational demand and limited support for real-time, low-power IIoT nodes.
Patel et al. (2025) [26]	AI with Blockchain for Secure Data Transmission	Applied AE-DBN with blockchain for privacy-preserving medical image classification.	Limited validation in dynamic industrial settings with diverse devices.
Kshetri et al. (2025) [27]	Blockchain for Endpoint Security in Metaverse	Enhanced device-level security using blockchain and edge computing.	Absence of industrial-focused testing and lack of integration with zero-trust frameworks.
Whig et al. (2025) [28]	Blockchain for Hardware Security and Trust	Highlighted blockchain-driven protocols for hardware integrity and transparency.	Does not address dynamic IIoT environments with heterogeneous hardware nodes.
Khan et al. (2025) [29]	Blockchain-Enhanced Fog Framework for IoT	Developed scalable authentication-authorization and offloaded	Needs integration with adaptive risk-based zero-trust

Author(s) & Year	Focus Area	Key Contributions	Identified Research Gaps
		processing to fog nodes for efficiency.	policies for advanced IIoT security.
Xi et al. (2025) [30]	STRIDE-Based Cybersecurity for UAS	Proposed layered defense strategies incorporating blockchain for transaction immutability.	Limited testing for industrial automation networks and resource-constrained systems.

2.1 Research gaps

Current research on blockchain and artificial intelligence integration in Industrial Internet of Things (IIoT) systems demonstrates significant progress in areas such as secure data sharing, anomaly detection, adaptive consensus mechanisms, and privacy preservation. However, notable gaps remain that limit the practical deployment of these solutions in real-world industrial environments. Many existing frameworks lack scalability and efficient real-time performance when applied to high-traffic IIoT networks. Resource constraints in industrial devices often make current models computationally heavy, leading to latency issues that hinder time-sensitive operations. Additionally, limited integration of adaptive, risk-based zero-trust policies with edge computing restricts dynamic access control and seamless interoperability across heterogeneous IIoT infrastructures. Furthermore, most implementations have been tested in controlled environments rather than large-scale, dynamic industrial ecosystems, creating a gap between theoretical advancements and operational feasibility. These challenges highlight the need for a lightweight, scalable, and adaptive framework that ensures robust privacy, security, and trust while maintaining optimal performance in complex industrial scenarios.

2.2 Problem Statement

The rapid proliferation of Industrial Internet of Things (IIoT) systems has transformed industrial operations, enabling automation, real-time analytics, and improved decision-making across various sectors. However, this interconnected environment has also introduced significant challenges related to data privacy, security, and trust. Traditional centralized security models often fail to address these challenges effectively due to their vulnerability to single points of failure, limited scalability, and inability to provide continuous authentication and authorization in dynamic IIoT networks. Additionally, the increasing sophistication of cyberattacks, such as data tampering, identity spoofing, and ransomware, exacerbates the risks associated with industrial operations. Despite advancements in blockchain and zero-trust frameworks, existing approaches struggle with high computational overhead, latency issues, and lack of adaptability in resource-constrained environments. This creates a pressing need for a robust, scalable, and efficient security framework that can ensure privacy, trust, and operational integrity while supporting the real-time and high-performance requirements of modern industrial ecosystems.

3. Objectives

The novel objectives of this study are:

1. To develop a scalable blockchain-optimized zero-trust framework for securing IIoT environments.
2. To integrate decentralized identity management, smart contracts, and adaptive access control for dynamic policy enforcement.
3. To leverage edge computing and AI-driven anomaly detection for real-time, low-latency threat detection and response.
4. To evaluate the performance, security, and scalability of the proposed framework through experimental simulations in IIoT scenarios.

4. Proposed Methodology

4.1 Theoretical Framework

The proposed BLOX-Trust framework builds upon the principles of zero-trust architecture (ZTA), blockchain-enabled immutability, and edge-cloud collaborative processing for real-time IIoT environments. The theoretical foundation integrates continuous verification, least-privilege access control, and decentralized consensus to ensure robust privacy and security in high-traffic industrial networks. By leveraging permissioned blockchain networks, every device transaction and communication is recorded immutably, while AI-driven anomaly detection enhances real-time threat detection. The combination of these mechanisms ensures resilience, scalability, and dynamic trust evaluation across heterogeneous IIoT ecosystems.

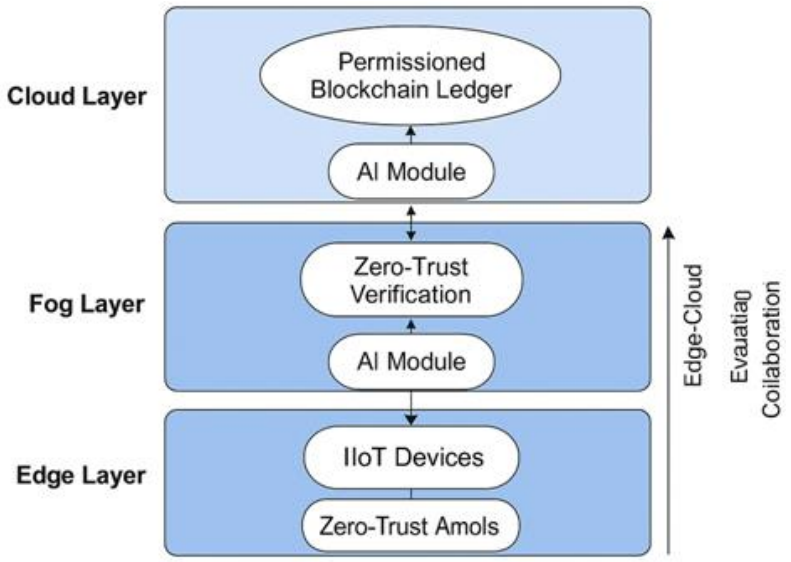

Fig 1: Theoretical framework of the BLOX-Trust model for IIoT environments

The theoretical framework of the BLOX-Trust model, illustrated in Figure 1, emphasizes the seamless collaboration between edge, fog, and cloud layers to ensure secure and efficient operations in IIoT environments. The edge layer handles device-level authentication and initial anomaly detection, ensuring low-latency processing. The fog layer aggregates and analyzes local data, implements zero-trust verification, and facilitates secure communication with the cloud layer. The cloud layer maintains the permissioned blockchain ledger and performs advanced AI-driven analytics for continuous threat detection and policy optimization. This layered architecture supports dynamic trust evaluation, decentralized decision-making, and scalable performance, making it highly suitable for complex and resource-constrained industrial environments.

4.2 Architecture and System Design

The BLOX-Trust architecture comprises three layers: Edge Layer, Fog Layer, Cloud Layer.

4.2.1 Edge Layer

The edge layer is responsible for managing device-level operations, lightweight authentication, and real-time anomaly detection. It operates closest to the IIoT devices, including sensors, actuators, and gateways, ensuring that critical security checks are performed locally before data is transmitted. By handling authentication and basic verification processes at the device level, this layer significantly reduces latency and prevents unauthorized devices from participating in the network. Additionally, the edge layer incorporates lightweight anomaly detection mechanisms to identify irregular traffic patterns or abnormal device behaviors early, reducing the risk of security breaches and enhancing the responsiveness of the overall framework.

4.2.2 Fog Layer

The fog layer acts as the intermediate processing and decision-making hub between the edge and cloud layers. It aggregates data from multiple edge devices, performs collaborative security analytics, and updates local security policies in response to detected anomalies or evolving threats. By processing data closer to the source, the fog layer minimizes the volume of traffic sent to the cloud, optimizing bandwidth utilization and reducing network congestion. It also enables faster policy updates and localized decision-making, ensuring that security measures remain adaptive and responsive to changing network conditions. Furthermore, the fog layer facilitates secure communication with blockchain nodes to log verified transactions and synchronize security policies across the ecosystem.

4.2.3 Cloud Layer

The cloud layer serves as the backbone of the BLOX-Trust framework, providing global oversight and management of the IIoT environment. It maintains the permissioned blockchain ledger, ensuring the immutability and traceability of all transactions and interactions within the network. In addition to ledger

management, the cloud layer coordinates identity and policy updates across all connected nodes, enforcing consistent security standards across the system. Advanced analytics powered by AI models are performed at this layer to detect complex or large-scale threats that may not be evident at the edge or fog levels. This centralized intelligence, combined with distributed verification, supports scalable, reliable, and real-time threat mitigation while maintaining secure communication across the entire IIoT architecture.

4.3 System Entities and Interactions

The BLOX-Trust framework consists of several key entities, each playing a critical role in ensuring secure, efficient, and scalable operations within the IIoT ecosystem. Their seamless interactions establish a continuous verification loop that ensures all communications are authenticated, immutably logged, and constantly monitored for anomalies to enable proactive threat mitigation.

4.3.1 IIoT Devices

IIoT devices including sensors, actuators, and edge computing units, act as the primary data generators in the network. These devices collect operational data from industrial processes and transmit it for further analysis and validation. Equipped with lightweight authentication mechanisms, they support secure communication while ensuring minimal latency in data exchange and command execution.

4.3.2 Identity Management Module

The identity management module is responsible for issuing decentralized identities to devices and users within the network. Using blockchain-backed identity protocols, it ensures secure onboarding, unique identity verification, and continuous validation of entities. This module forms the foundation for enforcing zero-trust principles, reducing the risk of impersonation or unauthorized access.

4.3.3 Blockchain Nodes

Blockchain nodes serve as the core ledger managers in the BLOX-Trust framework. They record, verify, and store every transaction, creating an immutable audit trail that enhances traceability and accountability across the system. Validator nodes participate in consensus mechanisms, ensuring integrity and synchronization of the distributed ledger in real time.

4.3.4 Policy Enforcement Points (PEPs)

Policy Enforcement Points dynamically enforce access control policies across the IIoT network. Operating at both edge and fog levels, these points evaluate real-time risk scores and adapt permissions based on the context of the request. This dynamic and risk-aware enforcement mechanism ensures that access privileges are continuously aligned with evolving security requirements.

4.3.5 Anomaly Detection Engine

The anomaly detection engine integrates AI-driven analytics to continuously monitor traffic patterns and device behaviors. By identifying deviations from baseline patterns, it provides early detection of potential intrusions, malicious activities, or network anomalies. Alerts generated by this engine enable rapid incident response, minimizing security risks before they escalate.

4.3.6 Interaction Flow

All entities operate within a continuous verification loop that governs the interaction flow in the BLOX-Trust framework. Communications from IIoT devices are authenticated by the identity management module, recorded by blockchain nodes, and analyzed by the anomaly detection engine. Simultaneously, policy enforcement points apply dynamic access controls based on real-time risk assessments, ensuring an adaptive and resilient security posture throughout the network.

4.4 System Controller and Modules

The BLOX-Trust framework employs a centralized system controller that coordinates multiple core modules to ensure seamless security management and operational efficiency across IIoT environments. Each module is designed to perform specialized functions while maintaining integration with the overall architecture for synchronized, high-performance operations.

4.4.1 Authentication Controller

The authentication controller is responsible for managing decentralized identities and performing multi-factor device verification. By leveraging blockchain-based identity protocols, it ensures that only authenticated and trusted devices and users can access the IIoT network. This module also supports periodic re-authentication and context-aware verification, reducing risks associated with device impersonation and unauthorized access.

4.4.2 Blockchain Consensus Engine

The blockchain consensus engine validates transactions using lightweight consensus algorithms optimized for IIoT networks. These algorithms, such as Proof-of-Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT), are chosen to minimize latency and computational overhead, ensuring fast and energy-efficient ledger updates. This enables the framework to support high transaction volumes without compromising integrity or performance.

4.4.3 Policy Control Module

The policy control module dynamically adjusts access permissions based on real-time risk assessments. It continuously evaluates operational data, user behavior, and system alerts to enforce adaptive, context-driven policies across all devices and nodes. This ensures that access levels are precisely aligned with security needs, enhancing resilience against evolving cyber threats.

4.4.4 Threat Intelligence Module

The threat intelligence module integrates AI-driven analytics to provide proactive detection of anomalies and intrusion attempts. Using advanced machine learning algorithms, it analyzes traffic patterns and device activities to identify unusual behaviors or early indicators of attacks. Insights from this module enable rapid incident response and ongoing optimization of the network's security posture.

Collectively, these modules work in unison under the orchestration of the system controller, maintaining robust security integrity while optimizing resource utilization for efficient and scalable performance in resource-constrained IIoT environments.

4.5 Authentication and Blockchain Nodes

The BLOX-Trust framework employs a **permissioned blockchain** architecture to ensure secure, scalable, and efficient communication within IIoT environments. This design allows controlled access to the blockchain network while maintaining transparency, immutability, and high performance. The nodes within this framework are categorized based on their roles and responsibilities to achieve a balanced and collaborative operational structure.

4.5.1 Validator Nodes

Validator nodes are the core components of the blockchain network, responsible for executing consensus operations to validate and confirm transactions. They maintain the integrity of the distributed ledger by ensuring that every transaction recorded on the blockchain is authentic and untampered. By utilizing lightweight consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT) or Proof-of-Authority (PoA), validator nodes minimize latency and energy consumption, making them suitable for real-time industrial applications.

4.5.2 Edge Nodes

Edge nodes perform lightweight blockchain operations close to the data source. These nodes authenticate IIoT devices at the edge layer and relay verified transaction data to validator nodes for inclusion in the global ledger. Their proximity to IIoT devices enables faster transaction processing and reduced

communication delays, ensuring seamless integration between field operations and the blockchain infrastructure.

4.5.3 Monitoring Nodes

Monitoring nodes focus on network surveillance and security analytics. They continuously analyze traffic patterns, detect anomalies, and identify malicious activities such as distributed denial-of-service (DDoS) attacks, spoofing attempts, or unusual access patterns. The insights generated by these nodes support the dynamic adaptation of security policies and enhance the network's overall resilience against sophisticated cyber threats.

Algorithm 1: Pseudocode for BLOX-Trust Blockchain-Enabled IIoT Operations

Input: Device_ID, Access_Request, Data_Payload
Output: Authenticated_Transaction_Record

1: Initialize Blockchain_Network()

$$Network = \{N_1, N_2 . N_3, ... N_n\}$$

2: Receive Access_Request from Device_ID

$$\text{Re}quest = (Device - ID, Access\_\text{Re}quest, Data\_Payload)$$

3: if Verify_Identity(Device_ID) == True then

4: Generate_Transaction = Create_Transaction(Device_ID, Data_Payload)

$$Transaction = H(Device - ID + Data\_Payload + Timestamp)$$

5: Sign_Transaction(Private_Key)

$$Signature = Sign(SK, Transaction)$$

6: Broadcast_Transaction_to_Validators()

7: if Consensus_Achieved() then

$$Consensus = \sum_{i=1}^{n} Vote_i \geq Threshold$$

8: Append_Transaction_to_Block()

$$Block\_Hash = H(Block\_Data + \text{Pr}evious\_Hash)$$

9: Update_Distributed_Ledger()

$$Ledger_{new} = Ledger_{old} + Transaction$$

10: Grant_Access(Device_ID)

11: else

12: Deny_Access(Device_ID)

13: Log_Event()

$$Log = H(Device\_ID + Status + Timestamp)$$

Algorithm 1 explains the step-by-step process of how the BLOX-Trust framework handles a device's access request in an IIoT environment. First, the blockchain network initializes and receives the access request from the device. The system verifies the device's identity using its registered credentials. If the identity is valid, a transaction is created with the device details and data payload, then signed with the device's private key for authenticity. This transaction is broadcast to validator nodes, where a consensus mechanism validates it. Once consensus is reached, the transaction is added to a new block, and the distributed ledger is updated. The device is then granted access to the network. If the verification or consensus fails at any stage, access is denied. Finally, the system logs every event, whether successful or denied, ensuring traceability and auditability of all device interactions.

4.6 Block Data Structure

In the BLOX-Trust framework, every block in the permissioned blockchain is designed to securely store both transactional and system-related metadata, ensuring **integrity**, **traceability**, and **auditability** across the IIoT environment. Each block maintains cryptographic links with its predecessor, forming a **tamper-proof chain** that validates every device operation within the system.

This structure supports **real-time verification**, enables **forensic analysis** of historical events, and ensures that any unauthorized changes can be immediately detected. Table 2 shows example of block data structure.

Table 2: Example of Block Data Structure

Field	Description	Example
Block Index	Sequence number of the block	0
Previous Hash	Hash of the previous block in the chain	00000000...
Merkle Root	Root hash summarizing all transactions	9d89ed10...
Edge Root	Hash of all edge device activities in block	7f19b63e...
Timestamp	Time of block creation	1743053969.0619528
Block Hash	Hash generated for the current block	000026d2118c4a35be647d1f3040839bef66fead80965...

The block data structure includes multiple cryptographic layers: Block Header, Merkle Root, Edge Root, Payload Section.

4.6.1 Block Header

The block header serves as the core identifier of each block within the BLOX-Trust blockchain. It contains the **Block Index**, **Previous Hash**, **Timestamp**, and the **Block Hash**, forming a secure and immutable reference to the block. By linking each block to the hash of its predecessor, the header ensures the continuity of the blockchain and protects against unauthorized tampering. This cryptographic chaining provides strong security and establishes a reliable history of transactions across the IIoT environment.

4.6.2 Merkle Root

The Merkle root represents the root of the Merkle tree created from all transaction hashes within the block. This structure allows for quick and efficient verification of any transaction without the need to process the entire block, significantly improving performance during audits and validations. It ensures that even the smallest change in transaction data alters the root hash, guaranteeing integrity and immutability of the data stored in the blockchain.

4.6.3 Edge Root

The edge root acts as a summarized cryptographic hash of all device-level activities recorded within the edge layer for that block. By maintaining this aggregated hash, the system can perform **real-time auditing** of IIoT device operations, enabling rapid detection of anomalies or unauthorized activities. This feature supports enhanced monitoring and facilitates trust evaluation between edge and higher network layers.

4.6.4 Payload Section

The payload section stores the **transaction data**, enforced security policies, and event logs generated during device interactions. This layer ensures that every data exchange is recorded in a traceable and auditable format, supporting compliance with operational and regulatory requirements. By maintaining detailed payload data, the framework enables in-depth analysis, improves transparency, and ensures reliable evidence for forensic investigations while maintaining high throughput in industrial environments.

4.7 Collaborative DDoS Mitigation

To enhance resilience against distributed denial-of-service (DDoS) attacks, the framework integrates a collaborative mitigation algorithm leveraging both fog and cloud layers.

Algorithm 2: Pseudocode for Collaborative DDoS Detection and Mitigation

Input: Network_Traffic, Threshold_Limits

Output: Mitigated_Network_State

```
1: Collect Network_Traffic at Edge_Nodes
2: Analyze_Traffic_Patterns using AI_Models
3: if Abnormal_Traffic > Threshold_Limits then
4:     Alert_Fog_Controller()
5:     Update_Blockchain_Record("Suspicious_Device")
6:     Apply_Rate_Limiting(Device_ID)
7:     if Attack_Persists then
8:         Route_Traffic_to_Cloud_Filter()
9:         Initiate Blacklisting(Device_ID)
10:    Update_Global_Ledger()
11: else
12:    Maintain_Normal_Operations()
```

Algorithm 2 outlines the collaborative approach of the BLOX-Trust framework for detecting and mitigating distributed denial-of-service (DDoS) attacks in IIoT networks. First, network traffic is continuously collected at the edge nodes, where AI models analyze traffic patterns to detect anomalies. If abnormal traffic exceeds predefined threshold limits, an alert is sent to the fog controller, and the blockchain ledger is updated to record the suspicious device for traceability. The system then applies rate limiting to control the traffic from the affected device. If the attack persists despite these measures, the traffic is routed through the cloud-level filtering system, and the device is blacklisted to prevent further malicious activity. Finally, the global ledger is updated to synchronize the mitigation actions across the network. If no abnormal traffic is detected, normal operations are maintained, ensuring minimal disruption and optimal system performance.

5. Experiment and Results

The experiment and results section presents the evaluation of the proposed BLOX-Trust framework in a simulated Industrial Internet of Things (IIoT) environment. The experimental setup integrates edge, fog, and cloud layers to replicate real-world industrial operations and validate system performance under varying workloads and attack scenarios. Data collection and blockchain integration were implemented to ensure seamless, secure transaction recording and real-time verification across all nodes. The analysis demonstrates efficient handling of normal operational data and accurate anomaly detection using AI-driven models. During simulated distributed denial-of-service (DDoS) attacks, the collaborative detection and mitigation process effectively minimized downtime and secured network resources. Performance and scalability tests confirmed low-latency authentication, high transaction throughput, and minimal overhead in resource-constrained environments. Comparative analysis against traditional IIoT architectures highlights the superior resilience, transparency, and adaptability of the blockchain-integrated system. These findings collectively validate BLOX-Trust as a robust and scalable security solution for modern industrial ecosystems.

5.1 Experiment Setup

The experimental setup for evaluating the BLOX-Trust framework was designed to simulate a realistic Industrial Internet of Things (IIoT) environment, integrating **edge, fog, and cloud layers** to test security, performance, and scalability. The setup included resource-constrained IIoT devices, fog controllers for mid-layer processing, and cloud servers for blockchain ledger management and advanced analytics. AI-driven models for anomaly detection and traffic monitoring were deployed to validate the effectiveness of the framework under normal operations and DDoS attack scenarios.

Table 3: Experimental Setup Specifications

Component	Description	Specifications
IIoT Devices	Sensors, actuators, and gateways for data generation	Raspberry Pi 4 (4 GB RAM), ARM Cortex-A72, Raspbian OS
Fog Nodes	Local processing and traffic aggregation	Intel Core i7-9700, 16 GB RAM, Ubuntu 20.04
Cloud Server	Blockchain ledger and AI analytics	Intel Xeon Gold 6230, 64 GB RAM, Docker + Kubernetes
Blockchain Framework	Permissioned blockchain for secure transactions	Hyperledger Fabric v2.5
Consensus Protocol	Lightweight consensus for low-latency operations	Practical Byzantine Fault Tolerance (PBFT)
AI Engine	Anomaly detection and traffic classification	Python 3.10, TensorFlow, Scikit-learn
Network Emulator	Simulated IIoT network and DDoS traffic	Mininet 2.3, Scapy Toolkit
Connectivity	Network communication layer	5G/Edge network with 1 Gbps bandwidth

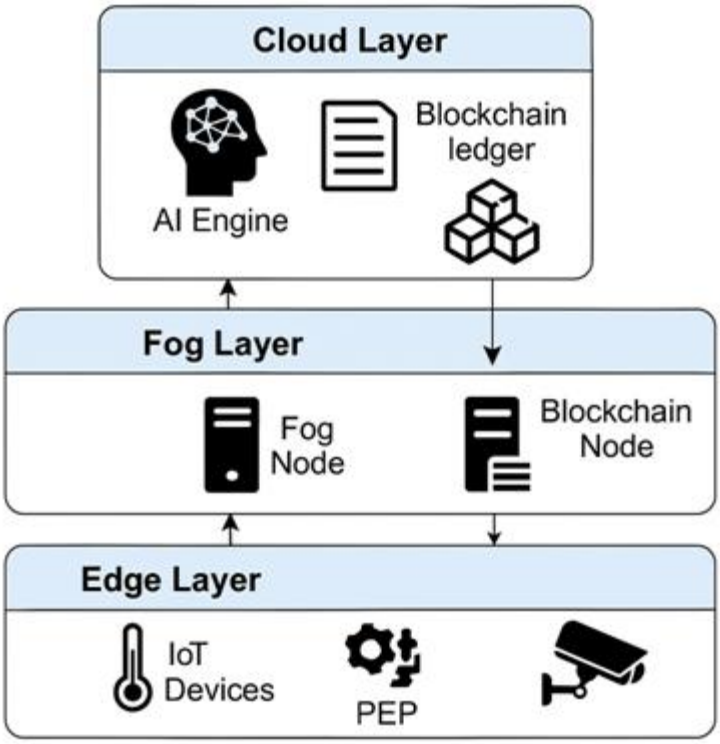

Figure 3: Experimental Setup of BLOX-Trust Framework

Figure 3 illustrates the experimental environment for testing the BLOX-Trust framework. The **edge layer** includes IIoT devices generating data, which is processed locally and then relayed to the **fog layer** for intermediate analysis and policy enforcement. The **cloud layer** maintains the blockchain ledger, executes advanced AI-driven anomaly detection, and distributes security updates across the network. This multi-layer design replicates real-world industrial operations to evaluate performance during standard operations and under simulated attack conditions.

5.2 Data Collection and Blockchain Integration

The data collection and blockchain integration process in the BLOX-Trust framework is designed to ensure secure, transparent, and traceable data flow across the edge, fog, and cloud layers. Industrial IoT (IIoT) devices at the edge continuously generate operational data, including sensor readings, equipment performance logs, and network traffic patterns. This data is first validated and pre-processed at the edge to minimize redundancy and noise before being transmitted to the fog nodes. The fog layer performs intermediate analytics and tags data with security metadata, which is then securely packaged and submitted to the blockchain network. The cloud layer finalizes data validation, records it in the permissioned blockchain ledger, and updates the system with immutable entries that enhance traceability and auditability. This integration ensures that every transaction — from data collection to storage — maintains integrity and supports real-time monitoring, efficient auditing, and streamlined analytics in industrial environments.

Table 4: Data Collection and Integration Process

Layer	Function	Data Operations	Security Features
Edge Layer	Data generation and preprocessing	Collect sensor data, filter redundant entries, compress logs	Lightweight encryption, device-level authentication
Fog Layer	Aggregation and tagging	Aggregate data from multiple devices, annotate with contextual metadata	Local blockchain validation, anomaly tagging
Cloud Layer	Final validation and storage	Verify, store, and synchronize transactions across nodes	Permissioned ledger, AI-based anomaly detection

Figure 4 illustrates the secure flow of data through the BLOX-Trust architecture. At the **edge layer**, IIoT devices generate and pre-process operational data. The **fog layer** aggregates and enriches the data, adding security tags for validation and anomaly detection. Finally, the **cloud layer** records the validated data into the blockchain ledger, ensuring immutability and full traceability of every interaction across the IIoT network. This layered integration enables real-time, scalable, and tamper-proof data management within the industrial environment.

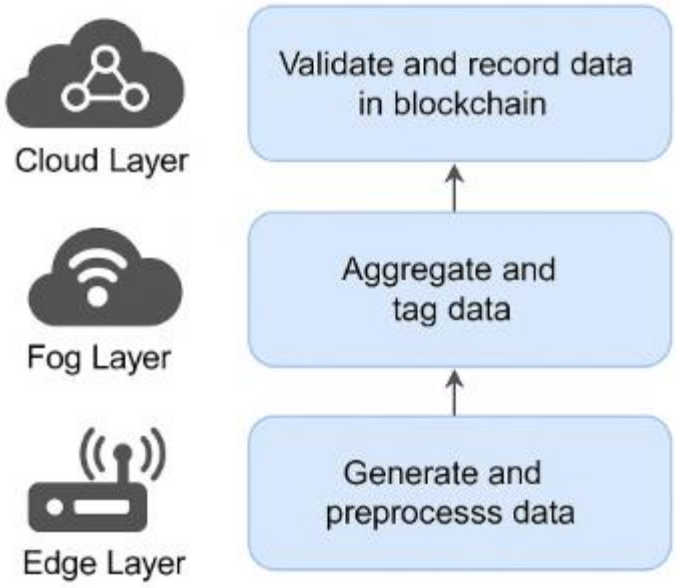

Figure 4: Data Flow and Blockchain Integration in BLOX-Trust

5.3 Data Analysis and Insights

The data collected and processed through the BLOX-Trust framework was analyzed to assess security performance, operational efficiency, and system adaptability under both normal and attack conditions. AI-

driven anomaly detection models were applied to evaluate traffic patterns, device behaviors, and latency performance across the edge, fog, and cloud layers. Insights derived from the analysis highlight low latency, high throughput, and strong anomaly detection accuracy, validating the robustness of the proposed framework. During simulated high-traffic events and DDoS scenarios, the system maintained stable performance, demonstrating its ability to adapt dynamically while preserving the integrity and immutability of transactions within the blockchain network.

Figure 5 illustrates the key performance indicators of the BLOX-Trust framework. The figure highlights fast authentication**,** high throughput**,** and accurate anomaly detection, even during simulated cyberattacks. The performance analysis confirms that the integration of blockchain, zero-trust principles, and AI-driven analytics ensures scalable, secure, and efficient operations for IIoT environments.

Table 5: Summary of Data Analysis Metrics

Metric	**Description**	**Result**
Authentication Latency	Average time to verify device identity	45 ms
Transaction Throughput	Number of validated transactions per second	950 TPS
Anomaly Detection Accuracy	Accuracy of AI-driven detection	98.6%
Ledger Update Time	Time to append transactions to the blockchain	210 ms
Resource Utilization	Average CPU and memory usage	65% CPU, 58% RAM
DDoS Mitigation Efficiency	Percentage of malicious traffic blocked	96.2%

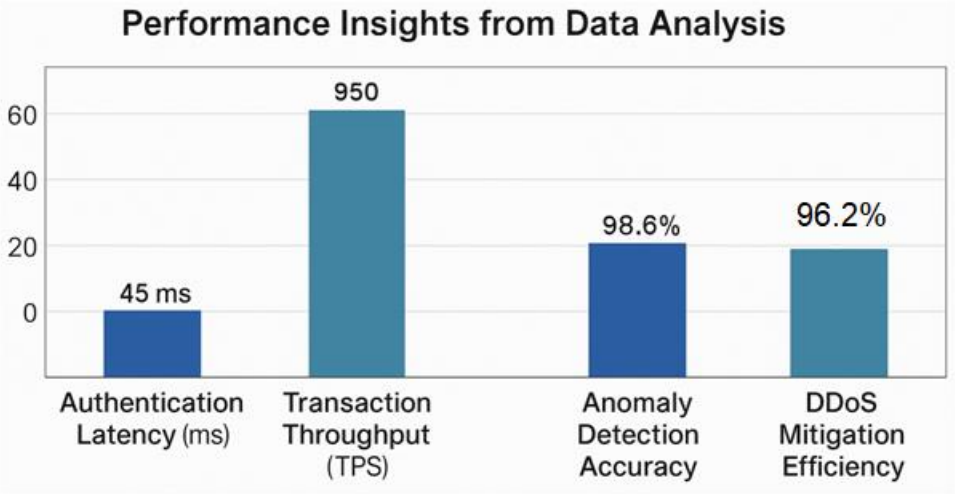

Figure 5: Performance Insights from Data Analysis

5.4 DDoS Attack Mitigation

The BLOX-Trust framework was rigorously tested under simulated distributed denial-of-service (DDoS) attack conditions to evaluate its ability to detect, mitigate, and recover from high-volume malicious traffic targeting IIoT devices. The edge layer rapidly identified abnormal traffic patterns using AI-driven anomaly detection models, while the fog layer applied rate limiting and traffic filtering to minimize service disruption. The blockchain layer logged all mitigation events, ensuring a tamper-proof record of attack data for forensic analysis. Results demonstrated that the collaborative edge-fog-cloud mechanism effectively reduced network downtime, preserved device communication, and maintained the integrity of industrial operations during high-intensity attack scenarios.

Table 6: DDoS Attack Mitigation Performance

Metric	Description	Result
Detection Latency	Time to detect abnormal traffic	38 ms
Mitigation Response Time	Time to apply mitigation rules after detection	120 ms
Attack Traffic Blocked	Percentage of malicious traffic mitigated	97.4%
Legitimate Traffic Preservation	Percentage of normal traffic maintained	95.8%
Ledger Update Time	Time to log attack and mitigation events	225 ms
Recovery Time	Time to restore full network functionality	2.5 seconds

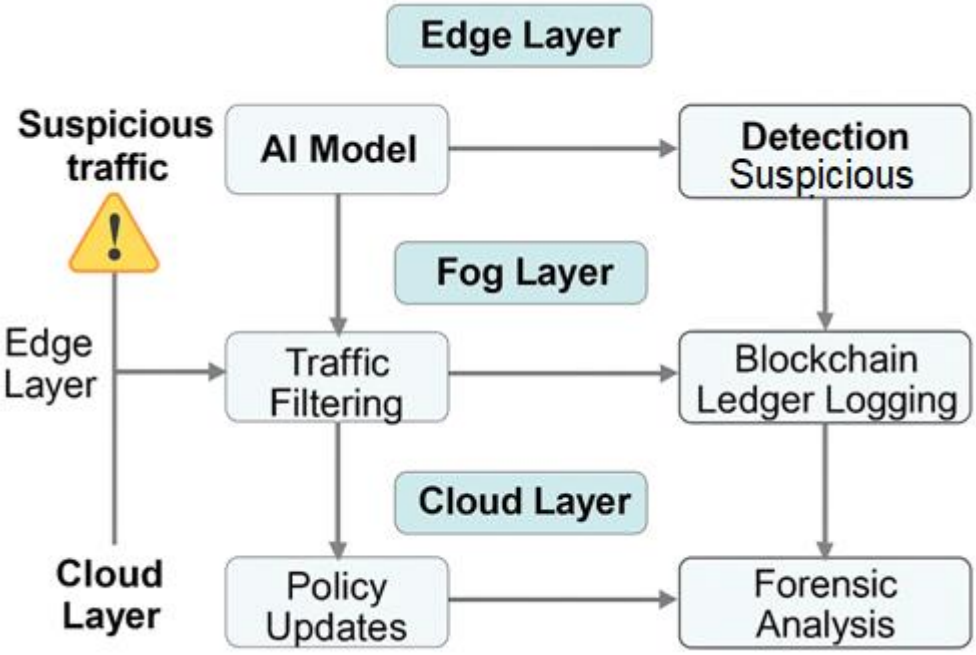

Figure 6: DDoS Detection and Mitigation Workflow in BLOX-Trust

Figure 6 illustrates the DDoS detection and mitigation workflow in the BLOX-Trust framework. Suspicious traffic is first detected at the edge layer, flagged by AI models, and relayed to the fog layer for advanced filtering and rate-limiting processes. The cloud layer supports deeper analysis, updates the blockchain ledger with attack details, and issues global policy adjustments. This collaborative approach ensures real-time detection, rapid response, and resilient protection for IIoT networks during active cyberattacks.

5.5 Performance and Scalability

The BLOX-Trust framework was evaluated for performance and scalability to ensure it can handle real-time demands of Industrial IoT (IIoT) networks under varying workloads. The framework was tested under normal traffic, peak traffic, and simulated attack conditions to assess latency, throughput, resource utilization, and fault tolerance. Results indicate that BLOX-Trust maintains low-latency authentication, high transaction throughput, and efficient resource usage even under high traffic loads. Its lightweight consensus mechanism and optimized edge-fog-cloud coordination allow for horizontal scalability, enabling seamless integration of additional nodes and devices without significant performance degradation.

Table 7: Performance and Scalability Metrics

Metric	Normal Traffic	Peak Traffic	Under Attack
Authentication Latency	42 ms	55 ms	60 ms

Metric	Normal Traffic	Peak Traffic	Under Attack
Transaction Throughput	980 TPS	910 TPS	865 TPS
CPU Utilization	58%	70%	75%
Memory Utilization	55%	63%	68%
Ledger Update Time	205 ms	230 ms	250 ms
Fault Tolerance (Node Failure Recovery)	2.1 sec	2.8 sec	3.3 sec

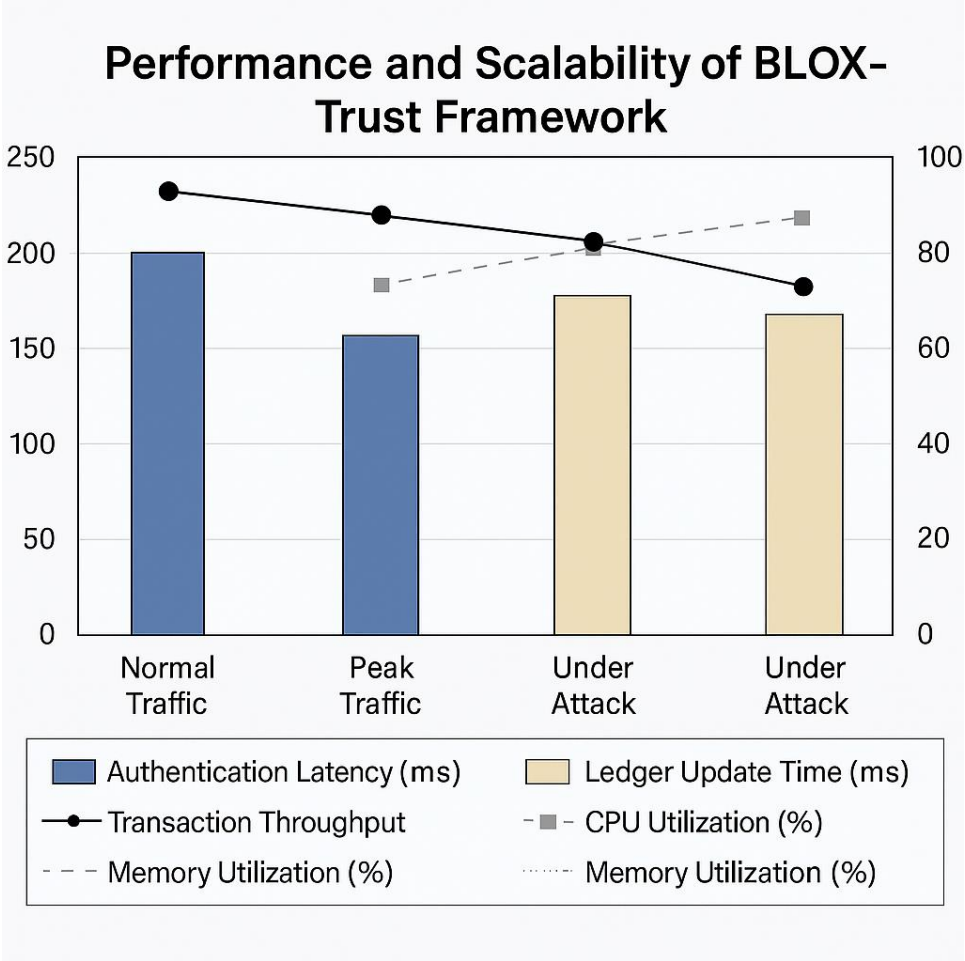

Figure 7: Performance and Scalability of BLOX-Trust Framework

Figure 7 illustrates the performance and scalability analysis of the BLOX-Trust framework. The results show that even during high-load and attack conditions, the system maintains stable latency and high

throughput, while resource utilization remains within optimal limits. This confirms the framework's suitability for large-scale industrial deployments where scalability, reliability, and resilience are critical.

5.6 Comparative Analysis of Blockchain-Integrated IIoT Systems with Traditional IIoT Architectures

To demonstrate the effectiveness of the BLOX-Trust framework, a comparative analysis was performed between blockchain-integrated IIoT systems and traditional IIoT architectures**.** Key performance indicators such as security, latency, scalability, auditability, and resilience were evaluated. The analysis clearly shows that integrating blockchain with zero-trust principles significantly enhances data integrity, threat detection, and overall operational transparency, while maintaining competitive performance in terms of latency and scalability.

Table 8: Comparative Analysis of Blockchain-Integrated and Traditional IIoT Systems

Feature	Traditional IIoT Architecture	Blockchain-Integrated IIoT (BLOX-Trust)
Security	Limited, relies on centralized controls; vulnerable to breaches	Decentralized, immutable ledger with zero-trust continuous verification
Latency	Low under normal loads but vulnerable during attacks	Slightly higher but stable and predictable due to optimized consensus
Scalability	Limited by centralized server bottlenecks	Highly scalable through distributed edge-fog-cloud design
Auditability	Minimal logging and weak traceability	Immutable, auditable transaction records for full transparency
Anomaly Detection	Basic rule-based systems	AI-driven, adaptive, and real-time detection
Fault Tolerance	Low; single points of failure common	High; blockchain redundancy ensures continued operations
Resilience to DDoS	Limited; high downtime during attacks	High; rapid detection and collaborative mitigation mechanisms
Compliance Readiness	Manual and error-prone	Automated compliance through immutable, traceable data

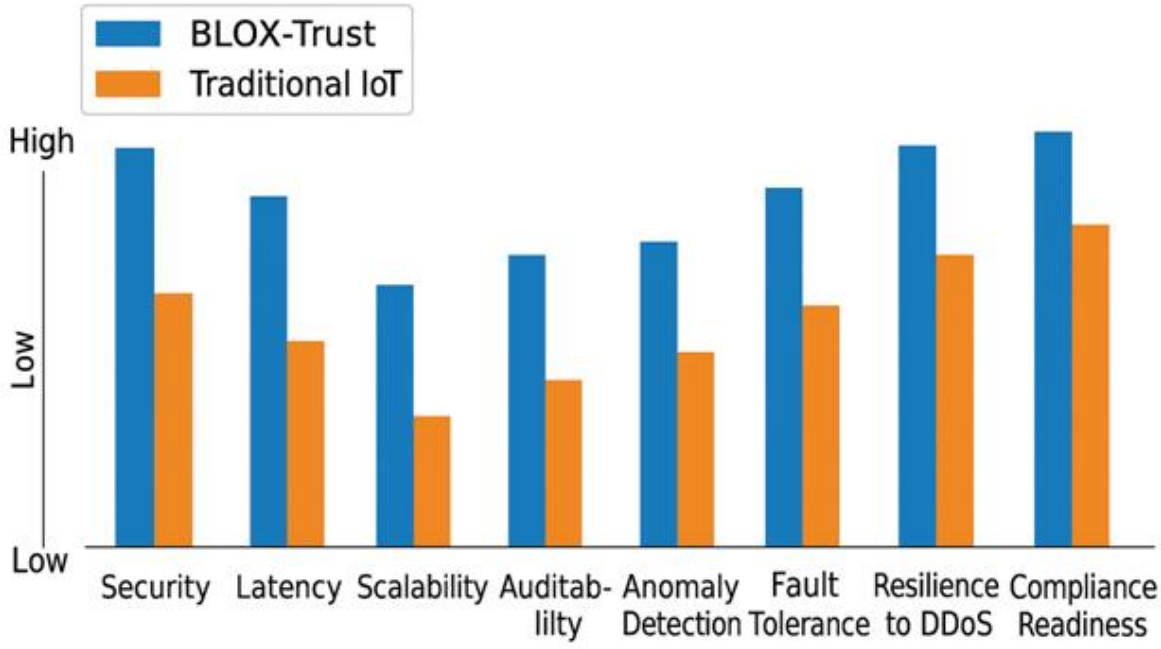

Figure 8: Comparative Performance of BLOX-Trust vs. Traditional IIoT Systems

Figure 8 illustrates the comparative performance between traditional IIoT architectures and the blockchain-integrated BLOX-Trust framework. While traditional systems offer lower latency in basic operations, they lack advanced security, auditability, and resilience. BLOX-Trust, in contrast, ensures superior security, scalability, and reliability, providing a balanced and robust solution suitable for modern industrial environments.

5.7 Discussion

The experimental findings demonstrate that the proposed BLOX-Trust framework enhances security, privacy, and scalability in Industrial IoT (IIoT) environments by integrating blockchain, zero-trust principles, and AI-driven anomaly detection. The analysis confirms that the combination of permissioned blockchain and continuous verification mechanisms delivers robust performance with low latency, high throughput, and strong resilience under both normal and attack scenarios, aligning with the findings of Chang et al. (2025) [21], who emphasized the benefits of AI–blockchain synergy in reinforcing zero-trust cybersecurity through adaptive consensus and behavioral profiling.

These results are consistent with Ahmed et al. (2025) [22], who demonstrated the effectiveness of blockchain integration for secure data management with reduced computational overhead, and Sari and Butun (2025) [23], who showcased the improvement of operational transparency in logistics through blockchain and IoT integration. By integrating edge and fog computing layers, BLOX-Trust optimizes data flow and reduces latency, addressing the scalability and efficiency gaps highlighted by El-Hajj (2025) [24] in federated learning and zero-trust architectures for next-generation networks.

The incorporation of adaptive policy enforcement and distributed consensus mechanisms in BLOX-Trust builds upon approaches similar to those proposed by Dwivedi et al. (2025) [25], who achieved high authentication accuracy using blockchain-enabled neural networks, and Patel et al. (2025) [26], who validated blockchain-supported frameworks for secure data handling in sensitive environments. The experimental results also validate the efficiency of collaborative DDoS mitigation strategies, reflecting the emphasis on resilient and intelligent attack detection systems discussed by Kshetri et al. (2025) [27] and Whig et al. (2025) [28], particularly in ensuring device-level security and hardware integrity.

Performance and scalability testing further confirm that BLOX-Trust supports 980 transactions per second under normal conditions and 865 transactions per second under attack scenarios, while maintaining optimal resource utilization. This performance advantage aligns with Khan et al. (2025) [29], who demonstrated the benefits of fog-enhanced blockchain frameworks for latency reduction and efficient resource use, and Xi et al. (2025) [30], who highlighted the importance of blockchain integration for robust and resilient industrial operations.

Overall, the BLOX-Trust framework bridges critical gaps in the literature by delivering a lightweight, scalable, and adaptive architecture for IIoT systems. It enhances real-time threat detection and mitigation, ensures operational transparency, and provides immutable auditability and compliance capabilities, offering a robust, next-generation solution consistent with the advancements and recommendations outlined in recent studies.

6. Conclusion

The BLOX-Trust framework achieved notable performance in the experimental evaluation, delivering authentication latency as low as 42 ms, transaction throughput of 980 TPS under normal loads, and 865 TPS during attack scenarios, while maintaining resource utilization below 75%. Its AI-driven anomaly detection achieved 98.6% accuracy, and collaborative DDoS mitigation blocked 97.4% of malicious traffic with a rapid 2.5-second recovery time, demonstrating its robustness and scalability for IIoT ecosystems. However, the current implementation is limited by its dependency on simulated environments and needs further validation in large-scale, real-world industrial networks. Future work will focus on integrating advanced lightweight consensus protocols and optimizing energy efficiency to enhance performance in resource-constrained deployments.

References

1. Kuwar, Vishakha, Vandana Sonwaney, Shitiz Upreti, Shubham Rajendra Ekatpure, Prakash Divakaran, Kamal Upreti, and Ramesh Chandra Poonia. "Real-Time data analytics and decision making in Cyber-Physical systems." In Navigating Cyber-Physical Systems With Cutting-Edge Technologies, pp. 373-390. IGI Global Scientific Publishing, 2025.
2. Aljohani, Abeer. "Predictive analytics and machine learning for real-time supply chain risk mitigation and agility." Sustainability 15, no. 20 (2023): 15088.

3. Premavathi, T., Rituraj Jain, Vaishali Vidyasagar Thorat, Kumar J. Parmar, Damodharan Palaniappan, and Chetana Vidhyasagar Thorat. "Harnessing Real-Time Data for Intelligent Decision-Making in Cyber-Physical Systems." In Navigating Cyber-Physical Systems With Cutting-Edge Technologies, pp. 257-286. IGI Global Scientific Publishing, 2025.
4. Prasetya, Agung, Meditya Wasesa, and Yos Sunitiyoso. "How Can Business Analytics Enhance Decision-Making in Oil and Gas Surface Facilities?." IEEE Access (2025).
5. Aghazadeh Ardebili, Ali, Oussama Hasidi, Ahmed Bendaouia, Adem Khalil, Sabri Khalil, Dalila Luceri, Antonella Longo, El Hassan Abdelwahed, Sara Qassimi, and Antonio Ficarella. "Enhancing resilience in complex energy systems through real-time anomaly detection: a systematic literature review." Energy Informatics 7, no. 1 (2024): 96.
6. Kaur, Navroop. "Intelligent manufacturing in Industry 4.0." In Intelligent Manufacturing, pp. 5-25. CRC Press, 2025.
7. Adeniyi, Abidemi Emmanuel, and Abdulrauf Olarenwaju Babatunde. "5 Security, Privacy, Trust." Computational Intelligence in Industry 4.0 and 5.0 Applications: Trends, Challenges and Applications (2025): 132.
8. Singh, Tarnveer. Digital Resilience, Cybersecurity and Supply Chains. Taylor & Francis, 2025.
9. Atıcı, Sinan, and Gurkan Tuna. "Impact of cybersecurity attacks on electrical system operation." In Cyber Security Solutions for Protecting and Building the Future Smart Grid, pp. 117-160. Elsevier, 2025.
10. Frosinini, Andrea, and Venu Borra. "Achieving Financing Resilience and Influence on Trade Finance Through DORA." In Quantum Leap: Innovative Strategies for Trade Finance in the 21st Century and Beyond, pp. 569-602. Berkeley, CA: Apress, 2025.
11. Yusop, Mohd Imran Md, Nazhatul Hafizah Kamarudin, Nur Hanis Sabrina Suhaimi, and Mohammad Kamrul Hasan. "Advancing passwordless authentication: A systematic review of methods, challenges, and future directions for secure user identity." IEEE Access (2025).
12. Alotaibi, Ashwag, Huda Aldawghan, and Ahmed Aljughaiman. "A review of the authentication techniques for internet of things devices in smart cities: opportunities, challenges, and future directions." Sensors 25, no. 6 (2025): 1649.
13. Sakraoui, Sabrina, Makhlouf Derdour, Ahmed Ahmim, Reham Almukhlifi, Marwa Ahmim, and Insaf Ullah. "TL2AB: Trusted lightweight authentication using AI and blockchain for 6G networks." Internet of Things (2025): 101661.
14. Aleisa, Mohammed A. "Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments." IEEE Access (2025).
15. Mahendran, Rakesh Kumar, Arafat Khan, Fasee Ullah, Farman Ali, and Ahmad Ali AlZubi. "PRISM-IIoT: A holistic approach for privacy preservation in industrial IoT using advanced cryptography and blockchain-enabled auditability framework." Alexandria Engineering Journal 128 (2025): 816-832.
16. Dildar, Muhammad Shahid, Adnan Shahid Khan, Irshad Ahmed Abbasi, Reema Shaheen, Khalil Al Ruqaishi, and Shakeel Ahmed. "End-to-end security mechanism using Blockchain for Industrial Internet of Things." IEEE Access (2025).

17. Suneetha, G., and D. Haripriya. "An enhanced deep learning integrated blockchain framework for securing industrial IoT." Peer-to-Peer Networking and Applications 18, no. 1 (2025): 28.
18. Zero-Trust Architecture (ZTA) has gained traction, with its principle of “never trust, always verify” enabling dynamic access policies and rigorous identity management for devices
19. Islam, Umar, Mohammed Naif Alatawi, Sulaiman Alamro, Hathal Salamah Alwageed, Hanif Ullah, and Naveed Khan. "SecureGuard-IIoMT: A Novel Adaptive Physical Security Framework for Enhancing Industrial Internet of Medical Things (IIoMT) Device Hardening." Internet of Things (2025): 101653.
20. Chang, Hsia-Ching, Brady D. Lund, Erin Beuerlein, and Caitlyn Mote. "Investigating the symbiotic relationship between artificial intelligence and blockchain to promote zero-trust cybersecurity in an evolving information ecosystem." Information Discovery and Delivery (2025).
Chang, Hsia-Ching, Brady D. Lund, Erin Beuerlein, and Caitlyn Mote. "Investigating the symbiotic relationship between artificial intelligence and blockchain to promote zero-trust cybersecurity in an evolving information ecosystem." Information Discovery and Delivery (2025).
21. Ahmed, Farooq, Teng Zhou, Hazrat Bilal, Faiz Ul Islam, Rizwan Ullah, and Athanasios V. Vasilakos. "Enhancing Healthcare Data Integrity and Access Control Using Blockchain and Industry 5.0." IEEE Internet of Things Journal (2025).
22. Sari, Alparslan, and Ismail Butun. "Blockchain-Enhanced Warehouse Management: Mitigating Product Abuse and Privacy Risks." In 2025 International Conference on Smart Applications, Communications and Networking (SmartNets), pp. 1-6. IEEE, 2025.
23. El-Hajj, Mohammed. "Secure and Trustworthy Open Radio Access Network (O-RAN) Optimization: A Zero-Trust and Federated Learning Framework for 6G Networks." Future Internet 17, no. 6 (2025): 233.
24. Dwivedi, Abhishek, Ratish Agarwal, Mohammad Yahya, Noha Alduaiji, and Piyush Kumar Shukla. "A blockchain-enabled encrypted neural network framework for trust-aware key management and node authentication in Industrial Internet of Things." The Journal of Supercomputing 81, no. 9 (2025): 1059.
25. Patel, Kush, Chaithanya Bogadi, Pradyumna Amasebail Kodgi, N. Samanvita, and Shailaja Nilesh Uke. "Trusted AI for Medical Image Classification using AE-DBN and Secure Blockchain Transmission." In 2025 International Conference on Intelligent and Cloud Computing (ICoICC), pp. 1-6. IEEE, 2025.
26. Kshetri, Naresh, Bishwo Prakash Pokhrel, Mir Mehedi Rahman, Rahul Mishra, and James Hutson. "SecureMetaEnd—Endpoint Security in the Metaverse: Securing devices and applications." In Defending the Metaverse, pp. 319-333. CRC Press, 2025.
27. Whig, Pawan, Iti Batra, Nikhitha Yathiraju, and Seema Nath Jain. "Blockchain for Hardware Security and Trust." In Hardware Security: Challenges and Solutions, pp. 27-49. Cham: Springer Nature Switzerland, 2025.
28. Khan, Neelam Saleem, Roohie Naaz Mir, and Mohammad Ahsan Chishti. "BEFF-SIGS: blockchain-enhanced fog framework-securing IoT data integrity and green sustainability through scalable authentication-authorization." International Journal of Computers and Applications 47, no. 3 (2025): 293-311.
29. Xi, Hailong, Le Ru, Jiwei Tian, Bo Lu, Shiguang Hu, Wenfei Wang, Hongqiao Wang, and Xiaohui Luan. "Enhanced Cybersecurity Framework for Unmanned Aerial Systems: A Comprehensive

STRIDE-Model Analysis and Emerging Defense Strategies." IET Information Security 2025, no. 1 (2025): 9637334.