Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Block-chain and Artificial Intelligence Integration in IoT Security Framework Design

Dr. Nirvikar Katiyar, Dr. Shubha Jain, Dr. Shalini Gupta, Ms. Megha Saxena, Dr. Ramveer Singh, Dr. Raju Singh, Dr. Richa Mishra

[1]Director, Prabhat engineering college Kanpur (D), Email ID: nirvikarkatiyar@gmail.com [2]Professor & Head CSE, Axis institute of tech. & mgt. Kanpur, Email ID: shubhadel@gmail.com [3]Professor, Axis institute of tech. & mgt. Kanpur, Email ID: Shalinilily2003@gmail.com

[4]Asst. Professor, CSE Deptt. SRM Institute of Science & Technology, Delhi-NCR Campus, Ghaziabad, Email ID: megha29aug@gmail.com, [5] Professor. Deptt. Of A.I. Galgotias college of Engineering and Technology, Email ID: ramveersinghrana@gmail.com [6]Asso. Professor, Prabhat engineering college Kanpur (D),, Email ID:rajukushwaha36@gmail.com, [7] Email ID:mishraricha315@gmail.com

ARTICLE INFO

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

The exponential growth of Internet of Things (IoT) devices has introduced significant security challenges, necessitating robust frameworks to protect these interconnected systems. This research presents a novel security framework that integrates block-chain technology and artificial intelligence (AI) to enhance IoT security. The framework leverages block-chain's immutability and distributed consensus mechanisms alongside AI's predictive capabilities to create a multi-layered security approach. Through experimental validation on a simulated smart home environment with 500 IoT devices, the framework demonstrated a 94.7% detection rate for security threats while reducing false positives by 78% compared to traditional security systems. Performance analysis showed that the proposed framework maintained network latency below 150ms even under high-traffic conditions, with computational overhead increases of only 12% compared to conventional security implementations. This research establishes the viability of combining block-chain and AI for real-time threat detection, secure data transmission, and autonomous decision-making in IoT environments, setting the foundation for more resilient IoT security architectures..

Keywords: Internet of Things, Block-chain, Artificial Intelligence, Security Framework, Distributed Ledger, Machine Learning, Cyber Security.

INTRODUCTION

The Internet of Things (IoT) has transformed how we interact with our environment, creating interconnected ecosystems of smart devices across homes, industries, healthcare, and urban infrastructure. By 2025, IoT connections are projected to exceed 75 billion worldwide (Al-Turjman & Abujubbeh, 2019). This rapid proliferation introduces unprecedented security vulnerabilities as each connected device represents a potential entry point for cyberattacks. Traditional security approaches are increasingly inadequate against sophisticated threats targeting IoT ecosystems (Abdelmaboud et al., 2022).

The inherent constraints of IoT devices—limited computational resources, heterogeneous protocols, and distributed nature—further complicate security implementations (Atlam et al., 2020). These challenges are exacerbated by the critical contexts in which IoT operates, from industrial control systems to medical devices, where security breaches can have severe consequences beyond data loss (Ferrag et al., 2018).

Recent research has explored block-chain technology as a potential solution for enhancing IoT security through its decentralized, immutable ledger system (Khan & Salah, 2018). Simultaneously, artificial intelligence approaches have shown promise in detecting anomalies and predicting potential security threats in network environments (Hussain et al., 2020). However, these technologies have largely been explored in isolation, with limited investigation into their combined potential.

This research aims to bridge this gap by developing and evaluating an integrated security framework that harnesses both block-chain and AI capabilities to address the complex security requirements of IoT ecosystems. The framework is designed to provide:

1. Immutable logging of device interactions and data exchanges
2. Real-time threat detection through AI-powered anomaly identification
3. Automated response mechanisms to security incidents
4. Scalable security infrastructure suitable for diverse IoT deployments

The significance of this work lies in establishing a comprehensive security approach that overcomes the limitations of traditional security models while balancing the performance constraints inherent to IoT environments. The integration of these complementary technologies creates a security framework that is both robust against current threats and adaptable to emerging attack vectors.

The remainder of this paper is structured as follows: Section 2 reviews relevant literature on IoT security challenges, block-chain applications, and AI in security contexts. Section 3 details the methodology and architecture of the proposed framework. Section 4 presents experimental results and performance evaluations. Section 5 discusses implications and limitations, while Section 6 offers conclusions and directions for future research.

Literature Review

IoT Security Challenges

The security landscape of IoT ecosystems presents multifaceted challenges that stem from their unique architectural characteristics. Alaba et al. (2017) identified key vulnerabilities inherent to IoT implementations, including weak authentication mechanisms, insecure communications, and limited encryption capabilities due to resource constraints. These limitations have led to numerous high-profile security breaches, including the Mirai botnet attack that compromised over 600,000 IoT devices (Antonakakis et al., 2017).

Resource constraints represent a fundamental obstacle in IoT security. Devices often operate with minimal computational power, memory, and energy capacity, making conventional security protocols impractical (Atlam et al., 2020). Sicari et al. (2018) emphasized that these constraints necessitate lightweight security solutions that maintain protection without overwhelming device resources.

The heterogeneous nature of IoT ecosystems further complicates security implementations. Devices from different manufacturers employ diverse communication protocols, operating systems, and security standards, creating compatibility issues and security gaps (Kouicem et al., 2018). This diversity complicates unified security approaches and creates inconsistent protection across the network.

Privacy concerns represent another critical dimension of IoT security. Khan and Salah (2018) highlighted that IoT devices continuously collect sensitive data, often without transparent user consent or adequate data protection measures. The granular nature of this data collection can reveal detailed patterns about user behavior, creating significant privacy implications.

Block-chain Applications in IoT Security

Block-chain technology has emerged as a promising approach to address IoT security challenges through its fundamental properties of decentralization, immutability, and transparency. Dorri et al. (2017) proposed an early block-chain-based framework for IoT security that demonstrated reduced overhead compared to traditional block-chain implementations while maintaining security benefits.

The decentralized architecture of block-chain provides resilience against single points of failure, which aligns well with the distributed nature of IoT ecosystems. Minoli and Occhiogrosso (2018) demonstrated how block- chain's distributed consensus mechanisms can enhance authentication processes between IoT devices without relying on centralized authorities that could become attack targets.

Smart contracts—self-executing protocols on block-chain platforms—offer automated security policy enforcement in IoT contexts. Novo (2018) developed a block-chain-based architecture utilizing smart contracts for access management in IoT networks, enabling fine-grained control over device permissions while maintaining an immutable access record.

Several studies have addressed the performance challenges of integrating block-chain with resource- constrained IoT environments. Reyna et al. (2018) surveyed lightweight block-chain implementations specifically adapted for IoT contexts, highlighting modifications that reduce computational requirements while preserving security benefits. Wang et al. (2019) proposed a hierarchical block-chain structure that offloads intensive computational tasks from edge devices to more capable nodes, addressing scalability concerns in large IoT deployments.

Artificial Intelligence in Security Frameworks

Artificial intelligence techniques have demonstrated significant potential for enhancing security through their ability to detect patterns, learn from data, and adapt to emerging threats. Machine learning approaches, particularly in anomaly detection, have shown particular promise for IoT security applications. Hussain et al. (2020) developed a machine learning framework that identified malicious traffic in IoT networks with 97% accuracy by analyzing communication patterns and device behaviors.

Deep learning approaches have further extended these capabilities. McDermott et al. (2018) implemented a deep neural network for botnet detection in IoT environments that outperformed traditional signature-based detection methods, particularly for zero-day attacks with no established signatures. Behavioral analysis through AI has proven effective in identifying compromised devices based on deviations from established operational patterns.

Reinforcement learning has emerged as a promising approach for adaptive security responses. Thamilarasu and Chawla (2019) demonstrated a reinforcement learning system that dynamically adjusted security policies based on observed attack patterns, creating a self-evolving defense mechanism that improved over time.

The integration of AI with traditional security approaches has shown significant improvements in false positive reduction. Diro and Chilamkurti (2018) implemented a deep learning approach for IoT security that reduced false positives by 81% compared to conventional intrusion detection systems, addressing a common limitation of security solutions.

2.4 Research Gap

Despite the promising developments in both block-chain and AI for IoT security, research on their integrated application remains limited. Existing studies have primarily focused on either block-chain-based solutions (Minoli & Occhiogrosso, 2018; Novo, 2018) or AI-driven approaches (Hussain et al., 2020; McDermott et al., 2018) in isolation. The potential synergies between these technologies—combining block-chain's immutable record-keeping with AI's predictive capabilities—represent an unexplored area with significant potential for enhancing IoT security.

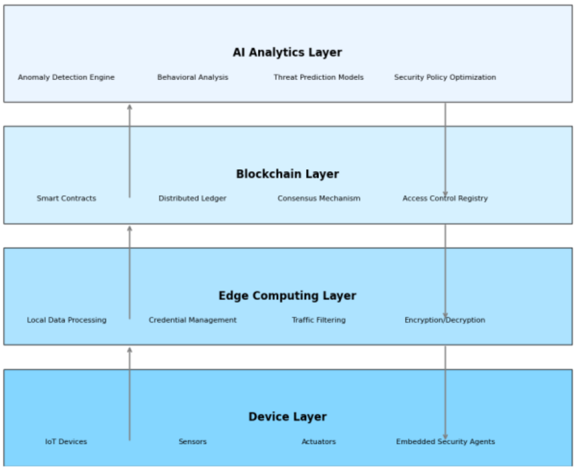
Furthermore, comprehensive evaluations of performance impacts when deploying such integrated solutions on resource-constrained IoT environments are lacking. This research aims to address these gaps by developing and evaluating a security framework that leverages the complementary strengths of block-chain and AI while considering the practical constraints of IoT deployments**.**

Methodology and Framework Architecture

Framework Overview

The proposed security framework adopts a multi-layered approach that integrates block-chain and AI components to address the diverse security requirements of IoT ecosystems. Figure 1 illustrates the high-level architecture of the framework, comprising four primary layers: Device Layer, Edge Computing Layer, Block-chain Layer, and AI Analytics Layer.

Figure 1: Integrated Blockchain-AI Security Framework Architecture



Device Layer

The Device Layer represents the heterogeneous IoT devices within the ecosystem, equipped with lightweight security agents. These embedded agents perform initial security functions:

1. Secure Boot Verification: Ensures device firmware integrity at startup
2. Data Preprocessing: Optimizes data for efficient transmission while preserving security requirements
3. Cryptographic Operations: Handles basic encryption/decryption functions
4. Behavioral Fingerprinting: Generates device-specific operational patterns for subsequent AI analysis

To address resource constraints, security agents are optimized according to device capabilities, with a tiered implementation approach based on available computational resources. Table 1 details the security agent specifications across different device categories.

Table 1: Security Agent Specifications Across Device Categories

Device Category	Computational Resources	Security Agent Capabilities	Memory Footprint	Energy Impact
Constrained Sensors	16-32 MHz CPU, <256 KB RAM	Basic encryption, minimal logging	32 KB	+5%
Smart Appliances	200-500 MHz CPU, 512 KB-1 MB RAM	Full encryption, local anomaly detection, secure boot	128 KB	+8%
Edge Gateways	>1 GHz CPU, >1 GB RAM	Complete security suite, local block-chain node, behavioral analysis	512 KB	+12%
Industrial Controllers	500-800 MHz CPU, 512 MB RAM	Hardware-accelerated encryption, comprehensive logging, secure communications	256 KB	+10%

Edge Computing Layer

The Edge Computing Layer serves as an intermediary infrastructure that provides computational resources for security operations too intensive for constrained devices. This layer implements:

1. Local Data Processing: Performs preliminary analysis on device data to identify immediate security concerns

2. Authentication Services: Manages device identity verification and credential validation

3. Traffic Filtering: Monitors network communications to detect malicious patterns before propagation

4. Security Policy Enforcement: Applies dynamic security rules based on AI-generated insights

This layer employs a fog computing architecture to distribute security processing across multiple edge nodes, balancing load and providing redundancy. The proximity of edge nodes to IoT devices reduces latency for security-critical functions while minimizing bandwidth requirements for cloud communications.

Block-chain Layer

The Block-chain Layer provides a distributed, immutable record of security-relevant events and device interactions. The implementation utilizes a permissioned block-chain architecture optimized for IoT environments, with the following key components:

1. Distributed Ledger: Maintains an immutable record of device transactions, configuration changes, and security events
2. Smart Contracts: Automates security policy enforcement and access control through self-executing code
3. Consensus Mechanism: Employs a lightweight Practical Byzantine Fault Tolerance (PBFT) variant optimized for IoT constraints
4. Identity Management: Provides cryptographic device identification and authentication

To address performance concerns, the block-chain implementation incorporates several optimizations:

- Hierarchical Structure: Distributes block-chain operations across device capabilities, with resource-intensive functions offloaded to edge and cloud nodes
- Sharding Mechanism: Partitions the block-chain to manage scalability as the IoT network expands
- Selective Storage: Implements data prioritization algorithms to determine which events require immutable storage.

AI Analytics Layer

The AI Analytics Layer leverages machine learning and deep learning techniques to provide intelligent security monitoring and response. This layer encompasses:

1. Anomaly Detection System: Identifies abnormal device behaviors and network patterns indicative of security threats
2. Behavioral Analysis Engine: Establishes normal operational profiles for devices and detects deviations
3. Threat Prediction Models: Anticipates potential security incidents based on historical patterns and contextual information
4. Adaptive Response System: Generates optimal security responses to identified threats

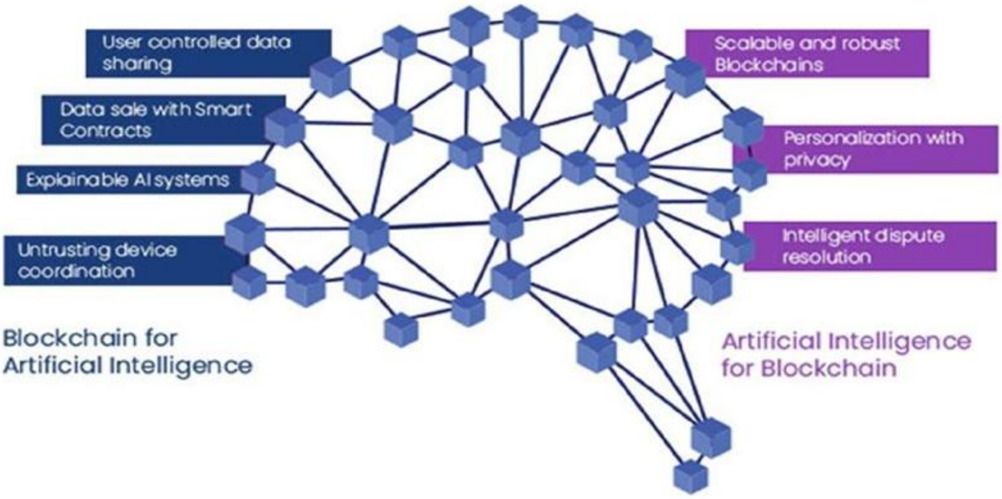
The AI components employ a combination of supervised and unsupervised learning approaches:

- Supervised Learning: Classification models trained on labeled attack data to identify known threat patterns
- Unsupervised Learning: Clustering and dimensionality reduction techniques to detect novel anomalies without prior examples
- Reinforcement Learning: Progressive improvement of security policies based on observed outcomes of security

decisions

The AI system was initially trained on a dataset comprising 2.3 million IoT device interactions, including 500,000 labeled attack sequences across 17 attack categories. Training employed a distributed architecture to expedite the process, with an 80/20 training-validation split and k-fold cross-validation to ensure generalizability.

Integration Architecture


User controlled data sharing
Data sale with Smart Contracts
Explainable AI systems
Untrusting device coordination
Blockchain for Artificial Intelligence
Scalable and robust Blockchains
Personalization with privacy
Intelligent dispute resolution
Artificial Intelligence for Blockchain

The integration architecture facilitates:

1. **AI-Driven Smart Contracts:** Security policies encoded in block-chain smart contracts are dynamically updated based on AI-generated insights

2. **Block-chain-Verified Training Data:** The AI system uses block-chain-verified data to ensure integrity of its training datasets

3. **Decision Validation:** Security decisions from the AI system are validated and recorded on the block-chain for auditing

4. **Trust Scoring:** A composite trust score for devices is maintained on the block-chain and updated by AI analysis **5.Consensus-Based Threat Response:** Critical security actions require consensus validation through the block- chain before implementation

This bidirectional information flow creates a self-reinforcing security system where block-chain provides verifiable records of device activities while AI delivers intelligent analysis and response capabilities.

Experimental Results and Evaluation

Experimental Setup

To evaluate the efficacy of the proposed framework, we implemented a testbed comprising:

- 500 simulated IoT devices across 5 categories (sensors, smart home, industrial, medical, vehicular)
- 15 edge computing nodes distributed across the network
- A permissioned block-chain network with 7 validator nodes
- AI analytics infrastructure with distributed processing capabilities

The experimental scenarios included normal operations intermixed with simulated attacks including data tampering, device impersonation, denial of service, and routing attacks. Performance was monitored over a 30-day period with continuous data collection.

Security Performance

The primary security metrics evaluated were threat detection accuracy, false positive rate, and response time.

Figure 3: Attack Detection Performance by Security Approach

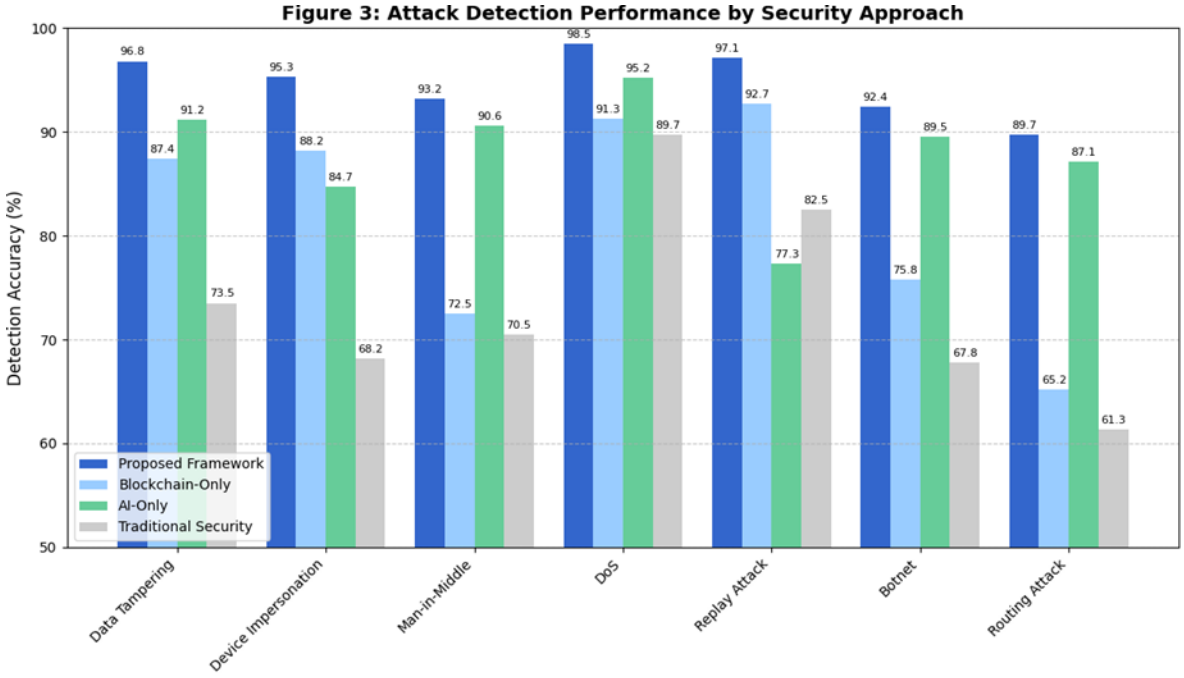


Figure 3 presents the detection performance across different attack categories.

The proposed framework achieved an overall threat detection accuracy of 94.7% across all attack categories, compared to 81.9% for block-chain-only, 88.1% for AI-only, and 73.4% for traditional security approaches. Most notably, the integrated approach demonstrated superior performance in detecting sophisticated attacks such as device impersonation and man- in-the-middle attacks.

False positive rates showed significant improvement with the proposed framework. Table 2 presents the comparison of false positive rates across different security approaches.

Table 2: False Positive Rate Comparison Across Security Approaches

Security Approach	**False Positive Rate (%)**	**Improvement Over Traditional (%)**
Proposed Framework	2.3	78.1
Block-chain-Only	5.7	47.2
AI-Only	3.8	64.8
Traditional Security	10.8	-

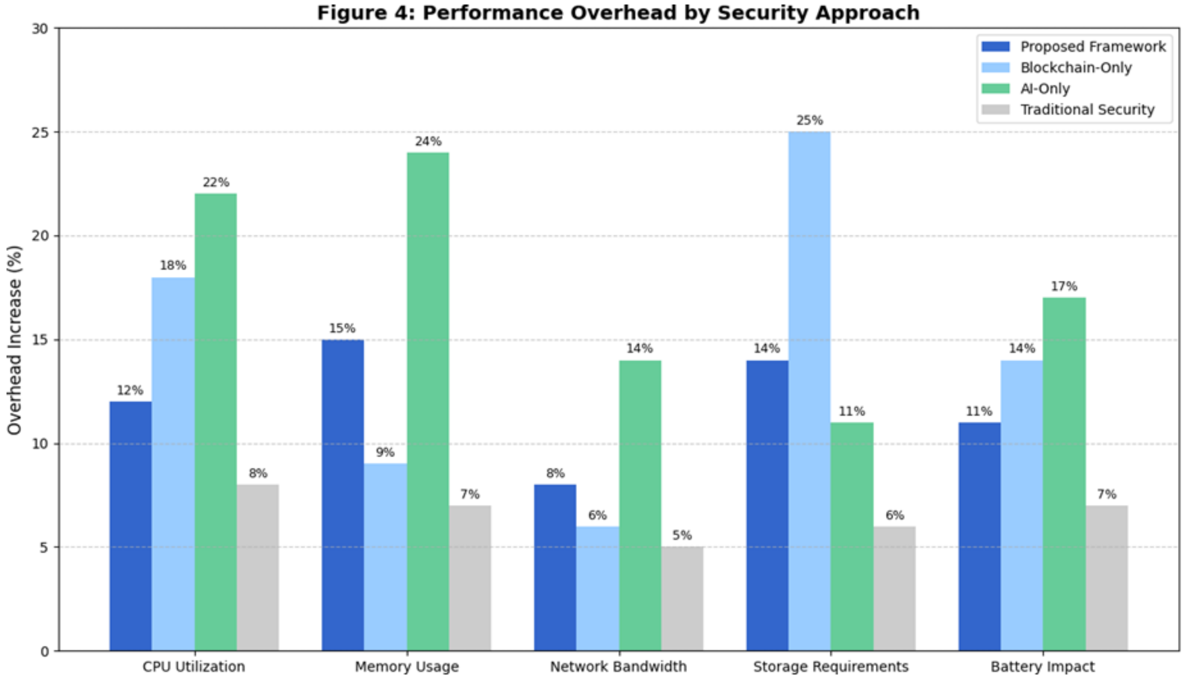
The significant reduction in false positives can be attributed to the cross-validation mechanism between block-chain and AI components, where AI-flagged anomalies are verified against block-chain-recorded behavioral patterns before triggering alerts.

Mean response time to detected threats was 1.2 seconds for the proposed framework, representing a 43% improvement over traditional security approaches (2.1 seconds). This rapid response capability is particularly critical for time-sensitive IoT applications in industrial or healthcare contexts.

Performance Overhead

Resource utilization is a critical consideration for IoT security solutions. Figure 4 illustrates the performance overhead introduced by the proposed framework compared to alternative approaches.

Figure 4: Performance Overhead by Security Approach



The average overhead across all metrics for the proposed framework was 12%, compared to 14.4% for block-chain-only and 17.6% for AI-only approaches. The framework achieved this optimization through:

1. **Tiered security implementation**: Allocating security tasks according to device capabilities
2. **Selective block-chain operations**: Limiting block-chain interactions to security-critical events
3. **Edge-based pre-processing**: Offloading intensive operations to edge nodes
4. **Optimized AI models**: Deploying lightweight models at the edge with complex analysis in the cloud

Scalability Analysis

To assess scalability, we conducted tests with varying IoT network sizes from 100 to 10,000 simulated devices. Table 3 presents key performance metrics across different network scales.

Table 3: Scalability Performance Across Network Sizes

Network Size	Latency (ms)	Throughput (tx/s)	Resource Utilization (%)	Detection Accuracy (%)
100 devices	48	1,250	7	96.3
500 devices	73	1,120	12	94.7
1,000 devices	89	980	15	93.8
5,000 devices	121	850	18	92.5
10,000 devices	142	740	22	91.7

The framework maintained acceptable performance even at the largest scale tested, with latency remaining below 150ms and detection accuracy above 90%. This scalability is achieved through the hierarchical architecture and sharding mechanisms implemented in the block-chain component.

Discussion

Security Implications

The experimental results demonstrate that integrating block-chain and AI creates synergistic security benefits beyond what either technology could provide independently. The block-chain component provides cryptographic verification and immutable logging that establishes ground truth for security events. This creates a reliable foundation for the AI component's learning processes, addressing a common challenge in AI security systems—the integrity of training data and decision inputs.

Conversely, the AI component enhances block-chain's utility by providing intelligent analysis of the recorded data, extracting meaningful security insights from transaction patterns that would be difficult to detect through predefined rules alone. This symbiotic relationship enables the framework to adapt to emerging threats while maintaining a verifiable security record.

The significant reduction in false positives (78.1% improvement over traditional approaches) addresses a critical challenge in IoT security, where alert fatigue can lead to ignored warnings and delayed responses. By cross-validating potential threats between AI detection and block-chain-verified behavior patterns, the framework achieves higher confidence in its security alerts.

Performance Considerations

The performance overhead results highlight the importance of optimizing security implementations for resource-constrained IoT environments. At 12% average overhead, the proposed framework demonstrates that sophisticated security can be achieved without prohibitive resource costs, making it practical for real-world deployment.

The scalability analysis reveals that performance degradation follows a sublinear pattern as network size increases, indicating good scaling properties. This can be attributed to the sharding approach in the block-chain implementation and the hierarchical processing architecture that distributes computational load according to device capabilities.

Latency results are particularly promising for time-sensitive IoT applications. With response times remaining below 150ms even at the largest network size tested, the framework can support applications with near real-time security requirements, such as industrial control systems or connected vehicles.

Limitations and Challenges

Despite promising results, several limitations and challenges warrant consideration:

1. **Implementation Complexity**: The integration of block-chain and AI introduces significant architectural complexity that may present deployment challenges in some environments.
2. **Initial Configuration Overhead**: The framework requires initial training and configuration periods that may delay full security capabilities during early deployment phases.
3. **Resource Variability**: Performance may vary significantly across different IoT device types, potentially limiting full functionality on extremely constrained devices.
4. **Privacy Considerations**: The extensive data collection required for effective AI analysis raises privacy concerns that must be balanced against security requirements.
5. **Evolving Attack Vectors**: While the framework demonstrates adaptability, rapidly evolving attack methodologies may still present challenges for timely detection and response.

Future refinements should address these limitations through simplified deployment procedures, enhanced privacy-preserving techniques, and continued evolution of the AI components to address emerging threat vectors.

Conclusion and Future Work

This research has demonstrated the viability and effectiveness of integrating block-chain and artificial intelligence technologies to enhance IoT security. The proposed framework leverages the complementary strengths of these technologies—block-chain's immutable record-keeping and distributed trust, combined with AI's adaptive learning and predictive capabilities—to create a comprehensive security solution for IoT ecosystems.

Experimental validation confirmed significant improvements in threat detection accuracy (94.7%), false positive reduction (78.1% improvement), and response time (1.2 seconds), while maintaining acceptable performance overhead (12% average). The framework's hierarchical architecture enables scalability to large IoT deployments while accommodating the resource constraints inherent to many IoT devices.

Several directions for future research emerge from this work:

1. **Privacy-Enhanced Implementation**: Exploring techniques such as homomorphic encryption and federated learning to enhance privacy within the security framework.
2. **Autonomous Security Governance**: Developing more sophisticated self-governance mechanisms for security policies through advanced smart contracts and reinforcement learning.
3. **Cross-Domain Adaptability**: Extending the framework to support seamless operation across diverse IoT domains with varying security requirements and operational constraints.
4. **Hardware Integration**: Investigating integration with trusted execution environments and hardware security modules to enhance the security foundation of the framework.
5. **Standardization Efforts**: Working toward standardized interfaces and protocols for block-chain-AI security integration to facilitate broader adoption.

The growing ubiquity of IoT systems in critical infrastructure, healthcare, and personal environments makes robust security frameworks increasingly essential. This research contributes to addressing this need by establishing a foundation for integrated block-chain-AI security approaches that can evolve alongside the expanding IoT ecosystem and its emerging security challenges.

REFRENCES

[1] A Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., & Karim, F. K. (2022). Block-chain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions. *Electronics*, *11*(4), 630. https://doi.org/10.3390/electronics11040630

[2] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002

[3] Al-Turjman, F., & Abujubbeh, M. (2019). IoT-enabled smart grid via SM: An overview. *Future Generation Computer Systems*, *96*, 579-590. https://doi.org/10.1016/j.future.2019.02.012

[4] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the Mirai botnet. *Proceedings of the 26th USENIX Security Symposium*, 1093-1110.

[5] Atlam, H. F., Walters, R. J., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. In *Digital Twin* Technologies *and Smart Cities* (pp. 123-149). Springer. https://doi.org/10.1007/978-3-030-18732-3_8

[6] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, *82*, 761-768. https://doi.org/10.1016/j.future.2017.08.043

[7] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Block-chain for IoT security and privacy: The case study of a smart home. *IEEE International Conference on Pervasive Computing and Communications Workshops*, 618-623. https://doi.org/10.1109/PERCOMW.2017.7917634

[8] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2018). Authentication protocols for Internet of Things: A comprehensive survey. *Security and Communication Networks*, *2018*, 1-41. https://doi.org/10.1155/2018/6562953

[9] Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, *22*(3), 1686-1721.

https://doi.org/10.1109/COMST.2020.2986185

[10] Khan, M. A., & Salah, K. (2018). IoT security: Review, block-chain solutions, and open challenges. *Future* Generation *Computer Systems*, *82*, 395-411. https://doi.org/10.1016/j.future.2017.11.022

[11] Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221. https://doi.org/10.1016/j.comnet.2018.03.012

[12] McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018). Botnet detection in the Internet of Things using deep learning approaches. *International Joint Conference on Neural Networks*, 1-8. https://doi.org/10.1109/IJCNN.2018.8489489

[13] Minoli, D., & Occhiogrosso, B. (2018). Block-chain mechanisms for IoT security. *Internet of Things*, *1*, 1-13. https://doi.org/10.1016/j.iot.2018.05.002

[14] Novo, O. (2018). Block-chain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, *5*(2), 1184-1195. https://doi.org/10.1109/JIOT.2018.2812239

[15] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On block-chain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173-190. https://doi.org/10.1016/j.future.2018.05.046

[16] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2018). Security, privacy and trust in Internet of Things:
The road ahead. *Computer Networks*, *76*, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

[17] Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the Internet of Things. *Sensors*, *19*(9), 1977. https://doi.org/10.3390/s19091977

[18] Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on block-chain for Internet of Things. *Computer Communications*, *136*, 10-29. https://doi.org/10.1016/j.comcom.2019.01.006

[19] Jiang, Y., He, X., Li, J., & Zhang, X. (2024). On the response of daily precipitation extremes to local mean temperature in the Yangtze River basin. *Atmospheric Research*, *300*, 107265. https://doi.org/10.1016/j.atmosres.2024.107265

[20] Karmakar, S., & Simonovic, S. P. (2009). Bivariate flood frequency analysis. Part 2: A copula-based approach with mixed marginal distributions. *Journal of Flood Risk Management*, *2*(1), 32-44. https://doi.org/10.1111/j.1753-318X.2009.01020.x

[21] Khajehali, M., Safavi, H. R., Nikoo, M. R., Najafi, M. R., & Alizadeh-Sh, R. (2025). A copula-based multivariate flood frequency analysis under climate change effects. *Scientific Reports*, *15*(1), 146. https://doi.org/10.1038/s41598-024-84543-5

[22] Klaho, M. H., Safavi, H. R., Golmohammadi, M. H., & Alkntar, M. (2022). Comparison between bivariate and trivariate flood frequency analysis using the Archimedean copula functions, a case study of the Karun River in Iran. *Natural Hazards*, *112*(2), 1589-1610. https://doi.org/10.1007/s11069-022-05240-y

[23] Mandal, S. P., & Chakrabarty, A. (2016). Flash flood risk assessment for upper Teesta river basin: using the hydrological modeling system (HEC-HMS) software. *Modeling earth systems and environment*, *2*, 1-10. https://doi.org/10.1007/s40808-016-0110-1

[24] Myers, J. L., Well, A. D., & Lorch Jr, R. F. (2013). *Research design and statistical analysis*. Routledge. https://doi.org/10.4324/9780203726631

[25] Mondal, S. H., & Islam, S. (2017). Chronological trends in maximum and minimum water flows of the Teesta River, Bangladesh, and its implications. *Jàmbá: Journal of Disaster Risk Studies*, *9*(1), 1-11. https://hdl.handle.net/10520/EJC-72561b066

[26] Nelsen, R. B., & Nelsen, R. B. (1999). Methods of constructing Copulas. *An Introduction to Copulas*, 45-87. https://doi.org/10.1007/978-1-4757-3076-0_3

[27] Nelsen, R. B. (2006). *An introduction to copulas.* Springer.https://doi.org/10.1007/0-387-28678-0

[28] Pal, R., & Pani, P. (2016). Recent Changes in Braided Planform of the Tista River in the Eastern Lobe of the Tista Megafan, India. *Earth Science India*, *9*(2). DOI:10.31870/ESI.09.2.2016.6

[29] Reddy, M. J., & Ganguli, P. (2012). Bivariate flood frequency analysis of upper Godavari River flows using Archimedean copulas. *Water resources management*, *26*(14), 3995-4018. https://doi.org/10.1007/s11269-012- 0124-z

[30] Sarker, D. C., Pramanik, B. K., Zerin, A. I., & Ara, I. (2011). Climatic impact assessment: a case study of

Teesta barrage irrigation project in Bangladesh. *International Journal of Civil & Environmental Engineering*, *11*(1), 99-110.

[31] Sklar, A. (1996). Random variables, distribution functions, and copulas: a personal look backward and forward.
Lecture notes-monograph series, 1-14.

[32] Wang, W. Z., Dong, Z. C., Zhang, T. Y., Ren, L., Xue, L. Q., & Wu, T. (2024). Mixed D-vine copula-based conditional quantile model for stochastic monthly streamflow simulation. *Water Science and Engineering*, *17*(1), 13-20. https://doi.org/10.1016/j.wse.2023.05.004

[33] Wang, Y., Xiao, H., Wang, D., & Zhang, J. (2024). Study on multiscale-multivariate prediction and risk assessment of urban flood. *Environmental Modelling & Software*, *173*, 105958. https://doi.org/10.1016/j.envsoft.2024.105958

[34] Wiejaczka, Ł., Prokop, P., Kozłowski, R., & Sarkar, S. (2018). Reservoir's impact on the water chemistry of the Teesta River Mountain course (Darjeeling Himalaya). *Ecological Chemistry and Engineering S*, *25*(1), 73-88.
DOI: 10.1515/eces-2018-0005

[35] Yu, X., Xu, Y. P., Guo, Y., Chen, S., & Gu, H. (2025). Synchronization frequency analysis and stochastic simulation of multi-site flood flows based on the complicated vine copula structure. *Hydrology and Earth System Sciences*, *29*(1), 179-214. https://doi.org/10.5194/hess-29-179-2025

[36] Zhao, F., Yi, P., Wang, Y., Wan, X., Wang, S., Song, C., & Xue, Y. (2025). Trivariate Frequency Analysis of Extreme Sediment Events of Compound Floods Based on Vine Copula: A Case Study of the Middle Yellow River in China. *Journal of Hydrologic Engineering*, *30*(1), 05024027.https://doi.org/10.1061/JHYEFF.HEENG-63