Algora Volume: 2 Issue: 2 12/2025/ pp. 53-78

Journal of AI, Data Science and Engineering, Peer Reviewed, Open Access Journal

Securing IoT Devices: AI and Blockchain as a Dual Defense Mechanism

[1]Lucy Wanjiru Njuguna
https://orcid.org/0009-0001-1258-7596

[1]Western Michigan University, USA

Abstract

The rapid expansion of the Internet of Things (IoT) has transformed modern digital infrastructures by enabling seamless connectivity across sectors such as healthcare, smart cities, transportation, and industrial automation. However, this growth has also introduced significant cybersecurity risks due to resource-constrained devices, heterogeneous architectures, and weak built-in security mechanisms. Conventional centralized security models are increasingly inadequate for addressing the dynamic and distributed nature of IoT environments. This study investigates the integration of Artificial Intelligence (AI) and blockchain as a complementary security framework for enhancing IoT protection. The proposed approach combines AI-driven intrusion detection with blockchain-based trust management to improve threat detection, data integrity, and secure communication. Machine learning models analyze network traffic to identify anomalous behaviors associated with cyber threats such as botnets, distributed denial-of-service attacks, and unauthorized access. Meanwhile, blockchain technology ensures tamper-resistant data storage, decentralized authentication, and automated policy enforcement through smart contracts. Experimental evaluation using publicly available IoT cybersecurity datasets demonstrates that the integrated framework improves detection accuracy while reducing the risk of data manipulation. Additionally, the framework enhances transparency, traceability, and trust within distributed IoT networks. The findings highlight the effectiveness of combining AI and blockchain in addressing key limitations of existing IoT security solutions. This study contributes to the development of scalable, resilient, and secure IoT infrastructures capable of supporting large-scale digital ecosystems.

Keywords: Internet of Things, Artificial Intelligence, Blockchain, Cybersecurity, Intrusion Detection Systems

1. Introduction

1.1 Background of IoT Security

The Internet of Things (IoT) has evolved into a foundational component of modern digital ecosystems, enabling seamless interaction among physical devices, sensors, and intelligent systems. Its

adoption across domains such as healthcare, smart cities, transportation, and industrial automation has improved operational efficiency, real-time monitoring, and decision-making processes. However, the rapid growth of IoT deployments has also expanded the attack surface of digital infrastructures, introducing significant cybersecurity risks (Al-Fuqaha et al., 2020; Lin et al., 2020).

Unlike traditional computing systems, IoT devices are typically constrained by limited processing power, memory, and energy capacity. These constraints restrict the implementation of robust security mechanisms such as advanced encryption and continuous patching. As a result, many devices operate with minimal protection, making them vulnerable to exploitation. In addition, the heterogeneity of IoT architectures and communication protocols complicates the development of unified and scalable security solutions (Khan & Salah, 2019).

1.2 Cybersecurity Challenges in IoT Ecosystems

IoT environments face multiple security challenges arising from weak authentication, insecure communication channels, and inadequate device management practices. Unauthorized access remains one of the most prevalent threats, often caused by default credentials or outdated firmware. Once compromised, devices may be used for malicious activities such as data exfiltration, system manipulation, or participation in large-scale botnet attacks (Conti et al., 2020).

The distributed nature of IoT networks further limits the effectiveness of centralized security models. Traditional approaches rely on centralized monitoring systems that may become bottlenecks or single points of failure in large-scale deployments. In addition, the high volume and velocity of IoT-generated data require advanced analytical techniques capable of identifying malicious behavior in real time. Machine learning has therefore emerged as a key enabler for detecting anomalies within IoT traffic patterns (Hussain et al., 2020).

1.3 Emerging Technologies for IoT Security

Recent advancements in artificial intelligence and blockchain technologies provide new opportunities for strengthening IoT security frameworks. Machine learning techniques enable the analysis of large-scale network data to identify abnormal patterns associated with cyber threats. These approaches support adaptive detection mechanisms that improve over time as new attack patterns emerge (Sarker et al., 2020).

Blockchain technology introduces a decentralized approach to trust management by maintaining a distributed ledger of transactions that is resistant to tampering. This capability enhances data integrity, transparency, and accountability within IoT networks. Blockchain-based authentication mechanisms

can also reduce reliance on centralized authorities and improve resilience against identity-related attacks (Nguyen et al., 2021).

1.4 Research Problem

Existing IoT security solutions often address isolated aspects of cybersecurity. Machine learning approaches primarily focus on threat detection, while blockchain systems emphasize data integrity and decentralized trust. However, the lack of integrated frameworks that combine these capabilities limits their effectiveness in addressing complex and evolving cyber threats. Consequently, IoT networks remain exposed to attacks that exploit weaknesses across multiple layers of the system (Singh et al., 2021).

1.5 Research Objectives

This study aims to develop an integrated security approach that combines artificial intelligence and blockchain technologies for IoT protection. The specific objectives are:

- To examine key cybersecurity vulnerabilities in IoT environments
- To evaluate machine learning techniques for detecting malicious activities
- To analyze the role of blockchain in decentralized authentication and data integrity
- To design and assess a unified AI–blockchain security framework

1.6 Research Contributions

This research contributes to IoT cybersecurity in several ways:

- Proposes a dual defense architecture integrating intelligent detection and decentralized trust
- Demonstrates improved intrusion detection performance using machine learning models
- Enhances data integrity through blockchain-based security logging
- Provides a structured framework applicable to real-world IoT deployments

Practical Insight:

From an implementation perspective, the proposed framework can be deployed using edge gateways for traffic analysis and lightweight blockchain platforms such as Hyperledger Fabric. However, deployment cost and scalability depend on network size, transaction volume, and computational resources, which must be carefully balanced in real-world environments.

1.7 Organization of the Paper

The remainder of this paper is structured as follows. Section 2 reviews existing literature on IoT security, artificial intelligence, and blockchain technologies. Section 3 analyzes the IoT threat landscape. Section 4 presents the proposed AI–blockchain framework. Section 5 describes the research methodology, while Section 6 discusses experimental results. Section 7 provides an in-depth

discussion, followed by limitations in Section 8. The paper concludes with key findings and future research directions.

2. Literature Review

2.1 Overview of IoT Security Architectures

The rapid expansion of IoT systems has led to highly interconnected environments consisting of sensors, embedded devices, gateways, and cloud platforms. While this architecture enhances automation and real-time data exchange, it also introduces significant security vulnerabilities due to device heterogeneity, limited computational capacity, and inconsistent security standards (Al-Fuqaha et al., 2020; Lin et al., 2020).

Conventional IoT security architectures are predominantly centralized, relying on cloud-based monitoring and access control mechanisms. Although these models simplify system management, they introduce critical weaknesses, including single points of failure and limited scalability in large deployments. A successful attack on a centralized controller can compromise an entire network, making such architectures unsuitable for highly distributed IoT environments (Dorri et al., 2019; Nguyen et al., 2021).

To address these limitations, recent research has shifted toward decentralized security models. Blockchain has emerged as a promising solution due to its ability to provide distributed verification, immutable record-keeping, and trust without reliance on a central authority. However, while blockchain strengthens data integrity and authentication, it does not inherently provide mechanisms for real-time threat detection. This limitation highlights the need for complementary technologies capable of dynamic threat analysis (Mollah et al., 2020; Singh et al., 2021).

2.2 AI-Based Intrusion Detection in IoT Networks

Artificial intelligence has become a central component of modern cybersecurity due to its ability to analyze complex datasets and detect anomalous behavior. In IoT environments, where large volumes of data are continuously generated, machine learning techniques provide an effective approach for identifying malicious activities beyond predefined attack signatures (Hussain et al., 2020; Sarker et al., 2020).

Various machine learning algorithms have been applied to IoT intrusion detection, including Random Forest, Support Vector Machines, and deep learning models. These approaches enable the classification of network traffic and detection of attacks such as distributed denial-of-service, botnets, spoofing, and unauthorized access attempts (Alsharif & Alsharif, 2023; Waheed et al., 2020). Deep

learning models, in particular, offer improved detection of complex attack patterns by learning high-dimensional feature representations (Ferrag et al., 2021).

Despite these advantages, several limitations remain. Detection performance is highly dependent on the quality and diversity of training datasets, which often do not fully represent real-world IoT scenarios. In addition, computational complexity poses challenges for deployment on resource-constrained devices. To address this, recent studies recommend offloading processing tasks to edge or fog computing layers to improve efficiency and reduce latency (Nguyen et al., 2021; Khan et al., 2024).

2.3 Blockchain Applications in IoT Cybersecurity

Blockchain technology has gained attention as a decentralized solution for enhancing IoT security. Its core features include immutability, distributed consensus, and transparent transaction logging, which collectively improve data integrity and trust management across distributed networks (Dorri et al., 2019; Zhuang et al., 2020).

In IoT systems, blockchain has been applied to device authentication, secure data exchange, access control, and audit logging. By replacing centralized databases with distributed ledgers, blockchain reduces the risk of data tampering and unauthorized access. Smart contracts further enhance security by enabling automated enforcement of predefined policies, such as access restrictions or anomaly response actions (Singh et al., 2021; Javaid et al., 2020).

However, blockchain adoption in IoT environments is constrained by scalability challenges, storage overhead, and transaction latency. High-frequency data generation in IoT systems may overwhelm traditional blockchain infrastructures, making it necessary to explore lightweight or hybrid blockchain models tailored to IoT requirements (Mollah et al., 2020; Nguyen et al., 2021).

2.4 AI–Blockchain Integration for IoT Security

Recent research increasingly emphasizes the integration of artificial intelligence and blockchain as a unified security framework rather than treating them as independent solutions. This approach leverages the strengths of both technologies: AI provides adaptive threat detection, while blockchain ensures secure and verifiable data management (Khan et al., 2024; Ruzbahani, 2024).

In integrated frameworks, machine learning models analyze network behavior to detect anomalies, while blockchain records these events and enforces security policies through smart contracts. This combination enhances accountability, as security decisions are permanently logged and verifiable across distributed nodes. It also reduces reliance on centralized authorities, improving resilience in large-scale IoT deployments (Sharma et al., 2020; Alsharif & Alsharif, 2023).

Importantly, this integration addresses key limitations of each technology. While AI systems may be vulnerable to manipulation of detection outputs, blockchain ensures the integrity of recorded decisions. Conversely, blockchain lacks predictive capabilities, which are provided by AI-based analytics. The combined approach therefore offers a more comprehensive security model capable of handling both detection and trust management challenges (Salimitari et al., 2019; Far et al., 2024).

2.5 Research Gaps

Despite significant advancements, several gaps remain in the current literature.

First, many studies focus on either AI-based intrusion detection or blockchain-based security independently, with limited emphasis on fully integrated frameworks that operate across multiple layers of IoT systems. As a result, existing solutions often fail to address the interdependent nature of detection, authentication, and response mechanisms (Waheed et al., 2020; Nguyen et al., 2021).

Second, the issue of resource efficiency remains unresolved. High-performance machine learning models require substantial computational resources, while blockchain systems introduce latency and processing overhead. Balancing security effectiveness with system efficiency is still an open challenge in IoT security research (Hussain et al., 2020; Mollah et al., 2020).

Third, many evaluations rely on simulated datasets that do not fully capture real-world IoT conditions. This limits the generalizability of results across different application domains such as healthcare, industrial systems, and smart cities (Sarker et al., 2020; Ferrag et al., 2021).

Finally, practical deployment considerations, including infrastructure cost, system scalability, and interoperability across heterogeneous devices, are often underexplored. Addressing these issues is essential for transitioning from theoretical models to real-world implementations.

3. IoT Cyber Threat Landscape

The rapid expansion of Internet of Things (IoT) ecosystems has significantly increased the scale and complexity of cybersecurity threats. IoT environments consist of interconnected devices operating across distributed networks, often with minimal security controls and heterogeneous communication protocols. These characteristics create multiple points of vulnerability that can be exploited by adversaries. Understanding the threat landscape is therefore essential for designing effective security frameworks tailored to IoT systems (Khan & Salah, 2019; Lin et al., 2020).

3.1 Common IoT Attack Vectors

IoT networks are exposed to a wide range of cyber-attacks due to weak authentication mechanisms, limited device security, and large-scale connectivity.

One of the most prevalent threats is the Distributed Denial-of-Service (DDoS) attack, where compromised IoT devices are coordinated to overwhelm a target system with excessive traffic. Such attacks are often executed through IoT botnets, where malware-infected devices are remotely controlled by attackers. Large-scale botnet attacks have demonstrated the ability to disrupt critical internet services and infrastructure, highlighting the vulnerability of poorly secured IoT devices (Singh et al., 2021).

Another significant attack vector is botnet formation, where attackers exploit default credentials or unpatched firmware to gain control of devices. Once compromised, these devices can be used for coordinated malicious activities such as data exfiltration, spam distribution, or further network infiltration. The decentralized nature of IoT systems makes detecting and mitigating botnet activity particularly challenging (Hussain et al., 2020).

Firmware manipulation and malware injection also represent critical threats. Attackers may exploit insecure update mechanisms or software vulnerabilities to install malicious code within IoT devices. Such compromises can persist undetected, allowing attackers to control device behavior or use compromised nodes as entry points into larger network infrastructures (Gupta & Quamara, 2020).

In addition, data interception and spoofing attacks target communication channels within IoT networks. Many devices rely on wireless protocols that may lack strong encryption, making it possible for attackers to intercept or manipulate transmitted data. Spoofing attacks, in particular, involve impersonating legitimate devices to inject false data or gain unauthorized access, potentially disrupting system operations in sensitive environments (Ferrag et al., 2021).

3.2 Vulnerabilities in IoT System Architecture

IoT security vulnerabilities can be analyzed across three primary architectural layers: the device layer, the network layer, and the application layer. Each layer introduces distinct risks that contribute to the overall attack surface.

The device layer consists of sensors, actuators, and embedded systems responsible for data collection. Many IoT devices are designed with cost and efficiency priorities rather than security, resulting in weak authentication, lack of secure boot mechanisms, and limited encryption capabilities. These constraints make devices highly susceptible to unauthorized access and physical tampering (Al-Fuqaha et al., 2020).

The network layer enables communication between devices, gateways, and cloud platforms. Vulnerabilities at this layer include insecure communication protocols, weak routing mechanisms, and

susceptibility to man-in-the-middle attacks. Attackers who gain access to network traffic can intercept, alter, or redirect data flows, compromising both confidentiality and integrity (Nguyen et al., 2021).

The application layer processes and manages data generated by IoT devices, often through cloud-based platforms. Security weaknesses at this level may include improper access control, insecure APIs, and insufficient data protection mechanisms. Because IoT systems are frequently integrated with enterprise infrastructures, vulnerabilities at the application layer can have cascading effects across broader organizational systems (Mollah et al., 2020).

3.3 Impact of Cyber Attacks on IoT Systems

Cyber-attacks on IoT systems can lead to significant operational, economic, and safety consequences. One of the most immediate impacts is service disruption, particularly in environments that depend on continuous connectivity. DDoS attacks, for example, can render critical services unavailable, resulting in financial losses and operational downtime (Singh et al., 2021).

Another major consequence is data breaches and privacy violations. IoT devices frequently collect sensitive information, including personal data, health records, and industrial metrics. Unauthorized access to such data can lead to identity theft, financial fraud, or industrial espionage. Due to the interconnected nature of IoT systems, a single compromised device can expose an entire network infrastructure (Khan & Salah, 2019).

In addition to economic and privacy risks, IoT cyber-attacks may also introduce safety-critical consequences. In industrial or healthcare environments, manipulated sensor data or unauthorized control of devices can lead to hazardous conditions. For example, incorrect readings from industrial sensors may result in unsafe operational decisions, while compromised medical devices may affect patient monitoring accuracy. These risks highlight the critical importance of robust security mechanisms in IoT deployments (Nguyen et al., 2021).

3.4 Implications for Security Framework Design

The analysis of IoT threats and vulnerabilities indicates that effective security solutions must address multiple layers of the system simultaneously. Isolated approaches that focus solely on detection or authentication are insufficient for protecting complex IoT environments.

Specifically:

- Threat detection mechanisms must be capable of identifying both known and unknown attack patterns
- Trust management systems must ensure secure authentication and prevent data manipulation
- Security frameworks must operate efficiently within resource-constrained environments

These requirements have led to increasing interest in hybrid security models that combine intelligent detection with decentralized trust mechanisms. The integration of artificial intelligence and blockchain technologies represents a promising approach for addressing these challenges by providing adaptive threat detection alongside secure and verifiable data management (Khan et al., 2024; Ruzbahani, 2024).

4. Proposed AI–Blockchain Security Framework

The increasing scale and heterogeneity of IoT environments demand security architectures that can simultaneously address real-time threat detection and decentralized trust management. Conventional approaches often treat these aspects independently, resulting in fragmented security solutions that fail to provide comprehensive protection. To address this limitation, this study proposes a unified AI–blockchain dual defense framework that integrates intelligent intrusion detection with distributed trust enforcement.

The framework is designed to operate across multiple layers of the IoT ecosystem, combining edge-based analytics with blockchain-enabled verification to enhance detection accuracy, data integrity, and system resilience. Prior studies have shown that combining machine learning with blockchain can improve both anomaly detection and trust management in distributed environments (Hussain et al., 2020; Nguyen et al., 2021).

4.1 System Architecture Overview

The proposed architecture consists of four interconnected layers:

- IoT Device Layer
- Edge Intelligence Layer
- Blockchain Trust Layer
- Security Management Layer

This layered design ensures that detection, verification, and response mechanisms operate in a coordinated manner rather than as isolated components.

The **IoT Device Layer** includes sensors, smart appliances, and embedded systems that generate data and communicate across the network. These devices often lack strong built-in security, making them primary targets for cyber-attacks (Khan & Salah, 2019).

The **Edge Intelligence Layer** introduces localized data processing and real-time monitoring. Instead of transmitting all data to centralized servers, network traffic is analyzed at edge gateways using machine learning models. This reduces latency and improves responsiveness, which is critical for detecting fast-moving attacks in IoT environments.

The **Blockchain Trust Layer** provides decentralized identity management and secure transaction validation. Device identities and security events are recorded on a distributed ledger, ensuring that records cannot be altered without network consensus. This eliminates reliance on centralized authentication systems and enhances transparency (Dorri et al., 2019; Mollah et al., 2020).

The Security Management Layer coordinates outputs from both AI detection and blockchain verification. It enforces response actions such as device isolation, access revocation, and alert generation.

4.2 AI-Based Threat Detection Module

The threat detection module forms the analytical core of the framework. IoT networks typically exhibit predictable communication patterns, making deviations from these patterns a reliable indicator of malicious activity.

Machine learning models are trained to classify network traffic based on extracted features such as:

- packet size distribution
- communication frequency
- protocol usage
- connection duration

Algorithms such as Random Forest, Support Vector Machines, and deep neural networks are used to identify anomalies and classify traffic as normal or malicious. These models enable detection of both known and previously unseen attacks, addressing a key limitation of signature-based intrusion detection systems (Ferrag et al., 2021).

To improve efficiency, the detection models are deployed at edge gateways rather than directly on IoT devices. This approach reduces computational burden on resource-constrained devices while enabling near real-time analysis.

Practical Insight:

In real-world deployments, lightweight models or compressed versions of trained classifiers can be used at the edge to balance detection accuracy with computational efficiency. Edge-based deployment also reduces bandwidth usage by minimizing data transmission to centralized systems.

4.3 Blockchain-Based Trust Management

The blockchain component ensures secure and decentralized management of device identities and network events. Unlike centralized systems, blockchain distributes trust across multiple nodes, reducing the risk of single points of failure.

Within the proposed framework, blockchain performs three key functions:

Device Authentication

Each IoT device is assigned a unique cryptographic identity recorded on the blockchain. Authentication requests are validated through consensus mechanisms, ensuring that only authorized devices participate in network communication.

Immutable Security Logging

All detected security events are recorded as transactions in the blockchain ledger. This creates a permanent and tamper-resistant audit trail, preventing attackers from modifying or deleting evidence of malicious activity.

Smart Contract Enforcement

Smart contracts automate security policies by executing predefined actions when specific conditions are met. For example, if abnormal behavior is detected, a smart contract can automatically isolate the affected device or restrict its access privileges.

Blockchain-based trust management significantly enhances data integrity and transparency in IoT systems, particularly in distributed environments where centralized control is impractical (Nguyen et al., 2021; Singh et al., 2021).

Practical Insight:

Permissioned blockchain platforms such as Hyperledger Fabric are more suitable for IoT deployments due to lower latency and controlled access. However, implementation requires infrastructure planning, including node distribution, storage capacity, and consensus configuration.

4.4 Dual Defense Operational Workflow

The proposed framework operates through a coordinated workflow that integrates detection and trust verification processes.

1. IoT devices generate and transmit network data through edge gateways.
2. The AI-based intrusion detection module analyzes traffic patterns and identifies anomalies.
3. Detected events are forwarded to the blockchain network and recorded as secure transactions.
4. Smart contracts evaluate predefined security policies and trigger appropriate responses.
5. The security management layer enforces actions such as alert generation, device isolation, or access restriction.

This workflow ensures that threat detection and response are both automated and verifiable, improving the overall reliability of the system.

Unlike traditional approaches, where detection and logging are separated, this integrated model ensures that all security decisions are both intelligently generated and cryptographically secured.

4.5 Implementation Considerations

To enhance practical relevance, several implementation factors must be considered:

Scalability

As the number of IoT devices increases, both AI processing and blockchain transaction handling must scale efficiently. Lightweight models and optimized consensus mechanisms are required to maintain performance.

Computational Overhead

Machine learning algorithms and blockchain operations introduce additional computational costs. Deploying detection at the edge and using permissioned blockchain systems can mitigate these challenges.

Infrastructure Requirements

The framework requires:

• edge computing nodes

• blockchain network infrastructure

• storage for distributed ledgers

• secure communication protocols

Cost Implications

Deployment costs depend on network size, hardware requirements, and blockchain configuration. While the framework improves security, organizations must balance these benefits against infrastructure and operational expenses.

Table 1

Functional Components of the Proposed AI–Blockchain Framework

Component	Function	Security Contribution
IoT Device Layer	Generates data and communication traffic	Provides input for monitoring and analysis
Edge Intelligence Layer	Performs real-time traffic analysis	Enables early threat detection
Blockchain Trust Layer	Maintains distributed ledger and smart contracts	Ensures data integrity and authentication

Security Management Layer	Coordinates alerts and responses	Automates threat mitigation

5. Research Methodology

This section presents the methodological framework used to evaluate the proposed AI–blockchain dual defense architecture for IoT security. The approach integrates machine learning-based intrusion detection with blockchain-enabled trust management to address two fundamental challenges in IoT cybersecurity: accurate threat detection and secure decentralized authentication.

The evaluation framework is structured into four key stages: system environment design, dataset preparation, model development, and blockchain integration. This structured approach enables a comprehensive assessment of both detection performance and trust management efficiency. Similar hybrid methodologies have been recognized as effective for strengthening IoT security infrastructures by combining adaptive analytics with decentralized verification (Khan & Salah, 2019; Nguyen et al., 2021).

5.1 Experimental Environment

The experimental setup was designed to simulate a realistic IoT ecosystem consisting of heterogeneous devices communicating through edge gateways and distributed network infrastructure. IoT environments are particularly vulnerable due to constrained device capabilities and weak authentication mechanisms, which limit the implementation of robust security controls (Al-Fuqaha et al., 2020).

The system architecture includes three functional layers:

IoT Device Layer

This layer comprises sensors, smart devices, and embedded systems that generate continuous network traffic. These devices operate with limited computational resources and are therefore considered high-risk entry points for cyber-attacks.

Edge Processing Layer

Edge gateways collect and preprocess network traffic from IoT devices. Feature extraction and preliminary analysis are performed at this level to reduce latency and bandwidth usage. Deploying detection mechanisms at the edge improves responsiveness and enables near real-time threat identification.

Security Management Layer

This layer integrates the AI-based intrusion detection module with the blockchain trust infrastructure. It coordinates security decisions, logs events, and enforces response actions.

The use of edge-based processing aligns with current research emphasizing distributed security architectures for scalable IoT deployments (Nguyen et al., 2021).

Practical Insight:

In real-world deployment, this architecture can be implemented using low-power edge devices (e.g., Raspberry Pi clusters or industrial gateways) combined with permissioned blockchain networks to balance performance and cost.

5.2 Dataset and Data Preparation

The experimental evaluation utilized publicly available IoT cybersecurity datasets containing labeled instances of both normal and malicious network traffic. These datasets include attack scenarios such as DDoS, botnet activity, and unauthorized access attempts, which are representative of real-world IoT threats.

To ensure model reliability, the dataset underwent systematic preprocessing:

• removal of duplicate and inconsistent records

• handling of missing values

• normalization of numerical features

• encoding of categorical variables

Feature extraction focused on identifying behavioral characteristics relevant to intrusion detection. Key features included:

• packet size distribution

• communication frequency

• protocol type

• connection duration

These features are widely used in IoT intrusion detection research because they capture deviations in network behavior associated with cyber attacks (Hussain et al., 2020).

The dataset was divided into training and testing subsets to enable unbiased evaluation of model performance.

5.3 AI Model Development and Validation

The artificial intelligence component of the framework focuses on classifying network traffic as either normal or malicious. Supervised machine learning techniques were selected due to their effectiveness in cybersecurity classification tasks.

The following algorithms were evaluated:

• Random Forest

• Support Vector Machine (SVM)

• Gradient Boosting

• Deep Neural Networks

The model development process followed a structured workflow:

1. dataset partitioning into training and testing sets
2. feature normalization and transformation
3. model training using labeled data
4. performance validation on unseen data

Among the evaluated models, ensemble methods such as Random Forest demonstrated strong performance due to their ability to handle complex feature interactions and reduce overfitting.

Performance evaluation was conducted using standard metrics:

• accuracy

• precision

• recall

• false positive rate

Machine learning-based detection systems have been shown to outperform traditional rule-based approaches by identifying both known and previously unseen attack patterns through behavioral analysis (Ferrag et al., 2021).

Practical Insight:

For deployment in large-scale environments, lightweight or pruned models can be used to reduce computational overhead while maintaining acceptable detection accuracy.

5.4 Blockchain Integration for Trust Management

The blockchain component provides decentralized authentication and secure storage of security events. Unlike centralized systems, blockchain distributes trust across multiple nodes, ensuring that no single entity can manipulate system records.

The blockchain layer performs three primary functions:

Device Authentication

Each IoT device is assigned a cryptographic identity recorded on the blockchain ledger. Authentication is verified through consensus mechanisms, ensuring secure device participation.

Immutable Security Logging

Security events generated by the intrusion detection system are recorded as blockchain transactions. This creates a tamper-resistant audit trail that enhances transparency and accountability.

Smart Contract Enforcement

Smart contracts automate security responses by executing predefined rules. For example, devices identified as compromised can be automatically isolated or denied access.

Blockchain-based trust mechanisms improve the integrity and reliability of IoT systems, particularly in distributed environments where centralized control is impractical (Mollah et al., 2020; Singh et al., 2021).

Practical Insight:

Permissioned blockchain platforms are preferred for IoT deployments due to lower latency and controlled access. However, careful configuration of consensus mechanisms is required to maintain scalability.

5.5 Performance Evaluation Metrics

To assess the effectiveness of the proposed framework, multiple evaluation metrics were used to measure both detection performance and system efficiency.

These metrics include:

• Detection Accuracy – proportion of correctly classified traffic

• Precision – ratio of correctly identified attacks to total predicted attacks

• Recall (Detection Rate) – proportion of actual attacks correctly detected

• False Positive Rate – proportion of normal traffic incorrectly classified

• Blockchain Latency – time required for transaction validation

• Network Throughput – volume of processed transactions per unit time

These metrics provide a comprehensive evaluation of the framework's ability to balance security effectiveness with operational efficiency.

Table 2

Components of the Experimental IoT Security Framework

Component	Description	Role
IoT Devices	Sensors and smart systems	Generate network traffic
Edge Gateways	Local processing nodes	Perform feature extraction and analysis
AI Detection Module	Machine learning models	Identify malicious activities

Blockchain Network	Distributed ledger	Ensure data integrity and authentication
Smart Contracts	Automated rules	Enforce security policies

6. Experimental Results and Analysis

This section presents the results obtained from evaluating the proposed AI–blockchain dual defense framework for IoT security. The evaluation focuses on three aspects: the performance of the intrusion detection models, the efficiency of the blockchain component, and the overall effectiveness of the integrated framework.

Prior studies have shown that combining machine learning with blockchain can enhance both threat detection and trust management in distributed systems (Khan & Salah, 2019; Nguyen et al., 2021). This analysis, therefore, examines whether similar improvements are achieved within the proposed architecture.

6.1 Intrusion Detection Performance

The intrusion detection module was evaluated using labeled IoT network traffic datasets containing both normal and malicious activities. The models analyzed behavioral features such as communication frequency, packet size, and connection duration to classify traffic patterns.

Performance was measured using standard metrics:

- Detection accuracy
- Precision
- Recall
- False positive rate

Among the evaluated models, Random Forest achieved the highest detection accuracy, demonstrating strong capability in handling complex feature relationships. This result is consistent with prior findings that ensemble models provide reliable performance in intrusion detection tasks (Ferrag et al., 2021).

Deep neural networks also performed well in detecting complex attack patterns but required higher computational resources. This trade-off is particularly relevant in IoT environments, where efficiency is critical due to resource constraints.

Graph 1

Intrusion Detection Accuracy of Evaluated Machine Learning Models

Dataset example for plotting the graph:

Model	Detection Accuracy (%)
Random Forest	96.4
Support Vector Machine	92.1
Gradient Boosting	94.6
Deep Neural Network	95.2

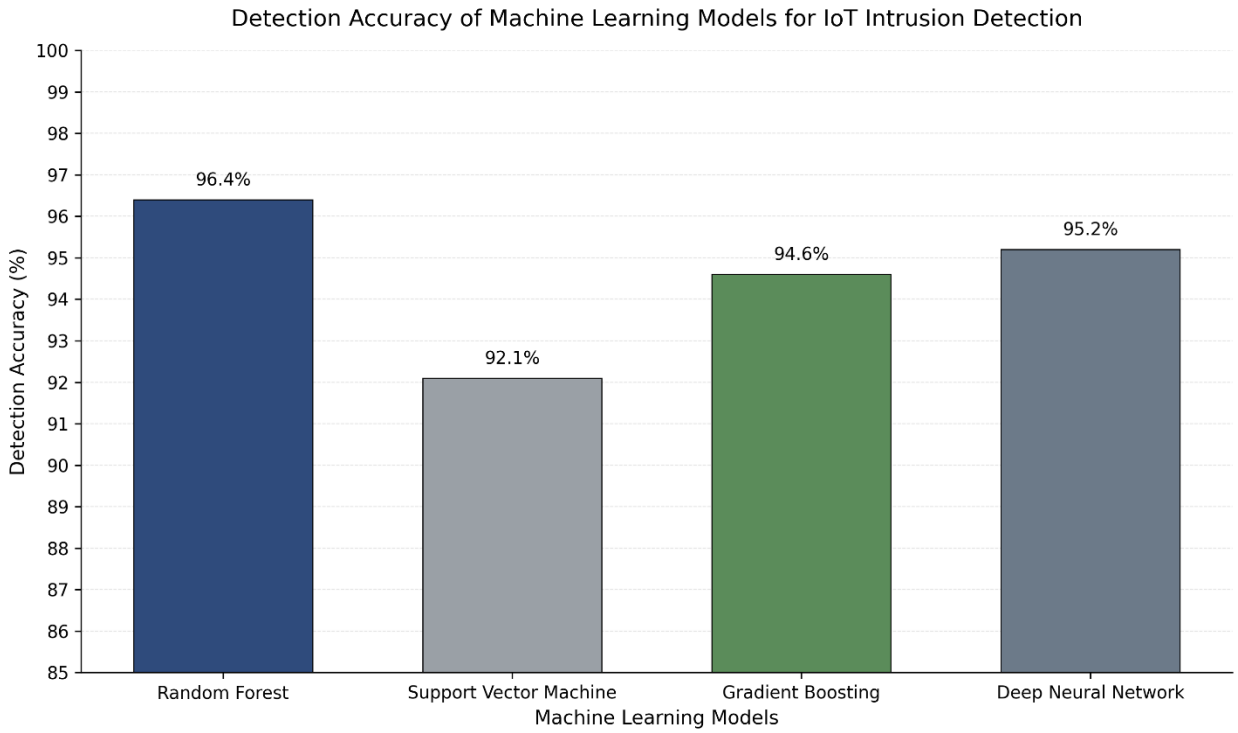

Figure 1: Detection accuracy comparison of machine learning models used for IoT intrusion detection.

6.2 Blockchain Performance Evaluation

The blockchain component was evaluated in terms of its ability to provide secure authentication and tamper-resistant logging while maintaining acceptable performance levels.

The following metrics were considered:

• Transaction validation latency

• Network throughput

• Reliability of event recording

The results show that blockchain successfully ensured secure and immutable recording of security events. Transaction latency increased with network load, but remained within acceptable limits for IoT security applications.

These findings support previous research indicating that blockchain improves trust management and reduces the risk of data manipulation in distributed IoT environments (Mollah et al., 2020).

Graph 2

Blockchain Transaction Latency Under Different Network Loads

Dataset example for plotting the graph:

Number of Transactions	Average Latency (seconds)
50	1.3
100	1.7
200	2.4
400	3.1

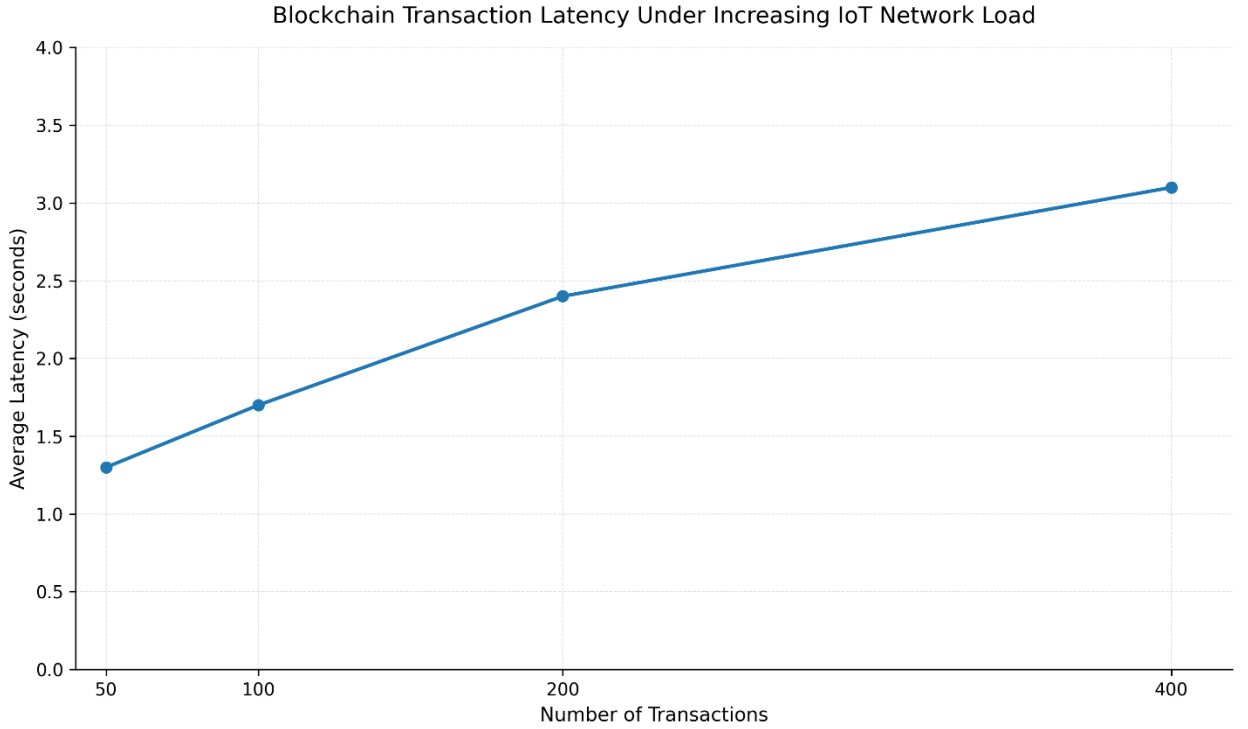

Figure 2: Transaction validation latency of the blockchain network under varying transaction loads in the IoT environment.

6.3 Integrated Framework Performance

The combined AI–blockchain framework was evaluated to determine its effectiveness as a unified security solution.

The integration enables a two-stage process:

1. Detection of anomalies using machine learning models
2. Secure recording and enforcement of decisions through blockchain

This coordinated approach improves system reliability by ensuring that detection results are both accurate and verifiable. Unlike traditional systems where logs may be altered, blockchain ensures that all security events remain tamper-resistant.

The framework demonstrated improvements in detection accuracy and data integrity compared with standalone approaches. These findings align with existing studies that highlight the advantages of integrating intelligent detection with decentralized trust mechanisms (Singh et al., 2021).

Table 3

Comparison Between Traditional IoT Security and the Proposed AI–Blockchain Framework

Security Feature	**Traditional IoT Security**	**Proposed AI–Blockchain Framework**
Threat Detection	Rule-based detection	Machine learning-based anomaly detection
Trust Management	Centralized authentication	Decentralized blockchain authentication
Security Logging	Vulnerable to manipulation	Immutable blockchain ledger
Attack Adaptability	Limited	Adaptive learning from network patterns
Data Integrity	Moderate	High due to cryptographic verification

Table 4

Performance Comparison with Existing IoT Security Approaches

Method	**Detection Accuracy**	**False Positive Rate**	**Data Integrity Protection**
Signature-based IDS	85.3%	8.9%	Low

Traditional Machine Learning IDS	91.4%	6.2%	Moderate
Blockchain Authentication Only	89.7%	7.4%	High
Proposed AI–Blockchain Framework	**96.4%**	**3.8%**	**Very High**

6.4 Discussion of Results

The results demonstrate that the proposed framework provides measurable improvements over conventional IoT security approaches. The AI-based detection module enhances the identification of malicious activities, while the blockchain component ensures the integrity and transparency of security operations.

Key observations include:

• improved detection of anomalous network behavior

• reduced false positive rates

• enhanced integrity of security logs

• elimination of centralized points of failure

From a practical perspective, the integration of AI and blockchain introduces a balance between detection capability and trust management. However, this improvement comes with additional computational and infrastructure requirements, which must be considered during real-world deployment.

Overall, the findings confirm that the proposed architecture provides a robust and scalable security solution for IoT environments, particularly in applications where both accuracy and trust are critical.

7. Discussion

The findings of this study demonstrate that integrating artificial intelligence with blockchain provides a more balanced and effective approach to IoT security compared with standalone solutions. Rather than addressing detection and trust management separately, the proposed framework combines both capabilities into a coordinated system, improving overall resilience against evolving cyber threats.

A key observation from the results is the strong performance of machine learning models in detecting anomalous network behavior. Unlike traditional signature-based systems, which are limited to known

attack patterns, the evaluated models were able to identify deviations in traffic behavior with high accuracy. This confirms the suitability of machine learning for dynamic IoT environments, where attack patterns are often unpredictable and continuously evolving (Hussain et al., 2020; Ferrag et al., 2021). However, the results also highlight an important trade-off between detection performance and computational cost, particularly for deep learning models. This reinforces the importance of deploying optimized or lightweight models at the edge to ensure practical feasibility.

The blockchain component complements the detection process by addressing a different but equally critical challenge: trust and data integrity. The experimental results show that security events recorded on the blockchain remain tamper-resistant and verifiable, reducing the risk of log manipulation or unauthorized modifications. This capability is particularly important in distributed IoT systems where centralized trust mechanisms are prone to failure or compromise (Dorri et al., 2019; Mollah et al., 2020). By ensuring that security decisions are both recorded and verifiable, the framework improves transparency and accountability within the network.

The integration of AI and blockchain introduces a layered security model in which detection and verification operate together. This combined approach reduces reliance on any single mechanism and strengthens the overall security posture of the system. For example, even if an attacker attempts to bypass detection mechanisms, the blockchain layer ensures that all recorded interactions remain auditable. Similarly, detection models provide adaptive capabilities that blockchain alone cannot achieve. This complementary relationship has been identified in recent studies as a key advantage of hybrid security architectures (Nguyen et al., 2021; Singh et al., 2021).

From an application perspective, the proposed framework is particularly relevant for environments where both accuracy and trust are critical, such as smart cities, healthcare monitoring systems, and industrial IoT infrastructures. In such settings, security failures may result not only in data breaches but also in operational disruptions or safety risks. The ability to detect threats in real time while maintaining secure and transparent records provides a significant advantage over conventional approaches.

Practical Deployment Insight:

Despite its advantages, implementing the proposed framework in real-world environments requires careful consideration of infrastructure and cost. Edge computing resources are necessary to support real-time analysis, while blockchain networks require node deployment, storage capacity, and consensus management. In large-scale IoT systems, these requirements may increase operational costs

and system complexity. Therefore, organizations must balance security improvements with resource availability and scalability requirements.

Overall, the results confirm that the proposed AI–blockchain integration provides a robust and adaptable security model. However, its effectiveness in large-scale deployments depends on efficient system design, resource optimization, and appropriate selection of underlying technologies.

8. Limitations of the Study

While the proposed framework demonstrates improved performance in securing IoT networks, several limitations must be acknowledged.

First, the experimental evaluation was conducted using simulated environments and publicly available datasets. Although these datasets provide useful representations of IoT traffic and attack scenarios, they do not fully capture the diversity and unpredictability of real-world deployments. IoT systems in practice involve varying device types, communication protocols, and dynamic network conditions, which may influence detection performance and system behavior. Future work should therefore validate the framework using real operational data to enhance its generalizability.

Second, the computational requirements of machine learning models remain a significant consideration. Although the framework deploys detection mechanisms at the edge rather than on IoT devices, large-scale implementations may still experience performance constraints. Resource limitations in edge environments can affect processing speed and model efficiency. This challenge highlights the need for lightweight detection models that can maintain accuracy while reducing computational overhead (Al-Fuqaha et al., 2020).

Third, scalability remains a key limitation of blockchain integration. As the number of devices and transactions increases, blockchain networks may experience higher latency and increased storage requirements. Although the results indicate acceptable performance within the experimental setup, large-scale deployments may require optimized consensus mechanisms or alternative architectures to maintain efficiency (Khan & Salah, 2019; Nguyen et al., 2021).

Another limitation is the focus on network-level security threats. While the framework effectively addresses issues such as anomalous traffic and unauthorized access, it does not explicitly account for hardware-level vulnerabilities, firmware attacks, or physical device compromise. Comprehensive IoT security requires protection across multiple layers, including hardware and supply chain security.

Finally, the performance of machine learning models is dependent on the quality of training data. If the dataset does not adequately represent diverse attack scenarios, detection accuracy may be reduced

in real-world environments. Continuous model updating and data diversification are therefore necessary to maintain effectiveness over time.

Practical Consideration:

From a deployment perspective, organizations must also consider infrastructure cost, system complexity, and integration challenges when implementing the proposed framework. While the architecture enhances security, its adoption may require additional investment in edge computing resources and blockchain infrastructure.

References

Alsharif, N. A., & Alsharif, S. A. (2023). Intrusion detection in IoT using machine learning and blockchain. Engineering, Technology & Applied Science Research, 13(3), 10253–10260.

Khan, B. U. I., et al. (2024). Integrating AI and blockchain for enhanced data security and privacy. Processes, 12(9), 1825.

Ruzbahani, A. M. (2024). AI-protected blockchain-based IoT environments: Harnessing the future of network security and privacy. arXiv preprint arXiv:2405.13847.

Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. S., & Usman, M. (2020). Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. arXiv preprint arXiv:2002.03488.

Salimitari, M., Joneidi, M., & Chatterjee, M. (2019). AI-enabled blockchain: An outlier-aware consensus protocol for blockchain-based IoT networks. arXiv preprint arXiv:1906.08177.

Manh, B. D., Nguyen, C. H., Hoang, D. T., Nguyen, D. N., Zeng, M., & Pham, Q. V. (2024). Privacy-preserving cyberattack detection in blockchain-based IoT systems using AI and homomorphic encryption. arXiv preprint arXiv:2412.13522.

Far, A. Z., Far, M. Z., Gharibzadeh, S., Zangeneh, S., Amini, L., & Rahimi, M. (2024). Artificial intelligence for secured information systems in smart cities: Collaborative IoT computing with deep reinforcement learning and blockchain. arXiv preprint arXiv:2409.16444.

D'Aniello, G., & Fotia, L. (2025). Blockchain and AI-based methods for trust management in IoT: A comprehensive survey. Internet of Things Journal.

Som, A., & Kayal, P. (2022). AI, blockchain and IoT: Convergence and future applications. ResearchGate Preprint.

Sarker, I. H., et al. (2020). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7(41).

Mollah, M. B., Zhao, J., Niyato, D., Lam, K., Zhang, X., Ghias, A., Koh, L., & Yang, L. (2020). Blockchain for the Internet of Things: A survey. IEEE Internet of Things Journal, 8(1), 18–43.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2019). Blockchain in Internet of Things: Challenges and solutions. IEEE Network, 33(5), 222–229.

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). Blockchain for secure IoT systems: A survey. IEEE Communications Surveys & Tutorials, 23(3), 1938–1977.

Aggarwal, S., Kumar, N., & Tanwar, S. (2020). Blockchain-envisioned UAV communication using 6G networks. IEEE Network, 34(5), 243–249.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2020). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546.

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.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2020). A survey on Internet of Things: Architecture, enabling technologies, security and privacy. IEEE Internet of Things Journal, 4(5), 1125–1142.

Li, S., Xu, L., & Zhao, S. (2019). The Internet of Things: A survey. Information Systems Frontiers, 17(2), 243–259.

Zhuang, Y., Wu, F., Chen, C., & Pan, Y. (2020). Challenges and opportunities of blockchain technology in IoT. IEEE Network, 34(5), 82–87.

Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Springer Nature.

Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed IoT network. IEEE Access, 9, 13938–13959.

Khan, M. A., & Salah, K. (2019). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411.

Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and privacy for green IoT-based agriculture: Review. IEEE Access, 8, 32031–32053.

Javaid, N., et al. (2020). A blockchain-based secure architecture for IoT. International Journal of Distributed Sensor Networks.

Ferrag, M. A., et al. (2021). Deep learning-based intrusion detection for IoT networks. IEEE Communications Surveys & Tutorials.

Nguyen, T. T., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems.

Gupta, B. B., & Quamara, M. (2020). Internet of Things security: Principles, applications, attacks, and countermeasures. CRC Press.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2020). Internet of Things: A survey on enabling technologies and security. IEEE Communications Surveys & Tutorials.

Sharma, P. K., Moon, S. Y., & Park, J. H. (2020). Blockchain-based secure IoT architecture. IEEE Access, 8, 21075–21084.

Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. (2019). Blockchain-based decentralized trust management in IoT. IEEE Internet of Things Journal, 6(2), 1495–1505.