ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN FOR TRUSTWORTHY INTERNET OF THINGS SECURITY: A COMPREHENSIVE FRAMEWORK

Abstract

The Internet of Things (IoT) has transformed conventional computing environments by connecting physical devices, sensors, machines, and intelligent applications through communication networks. The rapid expansion of IoT has created significant opportunities in healthcare, smart cities, industrial automation, transportation, agriculture, and home automation. However, the distributed and heterogeneous nature of IoT introduces substantial security, privacy, and data-management challenges. Artificial Intelligence (AI) can provide intelligent mechanisms for detecting abnormal behavior, identifying cyber threats, and automating security decisions, while blockchain can provide decentralized trust, data integrity, and transparent transaction management. This paper investigates the integration of AI and blockchain technologies for developing trustworthy IoT security systems. A conceptual framework is proposed in which IoT devices generate data, AI models analyze device and network behavior, and blockchain provides a distributed trust layer for recording important security events and verifying data integrity. The paper examines machine learning-based anomaly detection, decentralized authentication, secure data management, privacy preservation, smart contracts, and intelligent threat response. Major challenges involving computational overhead, scalability, energy consumption, interoperability, model reliability, and blockchain storage requirements are also discussed. The study further identifies future research directions involving federated learning, edge intelligence, explainable AI, lightweight blockchain protocols, and privacy-preserving security mechanisms. The proposed integration demonstrates the potential to create more resilient and trustworthy IoT ecosystems while highlighting the need for efficient architectures suitable for resource-constrained environments.

Keywords: Artificial Intelligence, Blockchain, Internet of Things, Cybersecurity, Machine Learning, Data Integrity, Smart Contracts, Anomaly Detection, Privacy

1. Introduction

The Internet of Things has become an important component of modern digital infrastructure. IoT enables physical objects to collect information through sensors and exchange that information with other devices, edge nodes, servers, and cloud platforms. The technology is now used in many environments, including smart homes, healthcare systems, industrial facilities, transportation networks, agriculture, and environmental monitoring.

The increasing number of connected devices has created significant advantages but has simultaneously expanded the potential attack surface. IoT devices can contain vulnerabilities caused by weak authentication, outdated software, insecure communication protocols, inadequate access control, and limited computational resources. A compromised device can potentially become an entry point into a larger network.

Traditional security mechanisms generally rely on predefined rules and centralized management. Such approaches may have difficulty responding to rapidly changing attack patterns. Artificial Intelligence provides an opportunity to improve IoT security by analyzing large volumes of data and identifying patterns associated with abnormal behavior.

Blockchain provides another important technology for IoT security. Its decentralized architecture can support tamper-resistant records, distributed trust, and verification of transactions. Recent research has specifically examined the combination of blockchain and AI to strengthen IoT security against threats such as unauthorized access, distributed denial-of-service attacks, and data manipulation.

The combination of AI and blockchain therefore provides an interesting research direction. AI can provide intelligence, while blockchain can provide trust and integrity. A recent 2026 systematic survey also examined blockchain-enabled AI for industrial IoT and highlighted applications involving smart industries, security, data management, and Industry 4.0.

This paper presents a conceptual framework for integrating AI and blockchain into IoT security systems. It examines the role of each technology, discusses system architecture, evaluates major security challenges, and presents future research opportunities.

2. Background

2.1 Internet of Things

IoT is a distributed computing environment consisting of interconnected physical objects. These objects normally contain sensors, communication modules, processors, and software.

An IoT environment can include:

- Sensors
- Smart appliances
- Wearable devices
- Industrial machines
- Vehicles

- Cameras
- Environmental monitoring systems
- Smart energy meters
- Edge gateways

These devices continuously generate information. Depending on the application, the information may include temperature, location, network activity, machine conditions, images, environmental measurements, or device status.

The diversity of devices creates challenges for centralized security management. Different devices may use different hardware architectures, operating systems, communication protocols, and security capabilities.

2.2 Artificial Intelligence

Artificial Intelligence enables computer systems to perform tasks that traditionally require human intelligence. Machine learning is particularly useful for IoT security because it can learn patterns from historical data.

AI can be applied to:

- Intrusion detection
- Malware classification
- Anomaly detection
- User behavior analysis
- Device authentication
- Network traffic analysis
- Security-event classification
- Predictive maintenance

Machine learning models can examine device behavior and identify deviations from normal patterns.

2.3 Blockchain Technology

Blockchain is a distributed ledger technology that records transactions across a network of participating nodes. Cryptographic mechanisms help protect the integrity of recorded information.

Important blockchain characteristics include:

1. Decentralization
2. Transparency
3. Tamper resistance
4. Distributed verification
5. Cryptographic security

These properties make blockchain potentially useful for IoT environments in which multiple devices and organizations need to establish trust without depending entirely on one centralized authority.

3. Related Work

The integration of AI, blockchain, and IoT has become an active research area. Recent research has explored the use of blockchain and AI together for industrial IoT, where AI provides analytical capabilities and blockchain can support trusted data management.

Research published in 2026 has also investigated blockchain combined with federated learning in edge environments to improve IoT data reliability. Such approaches are particularly relevant because IoT data can be distributed across many devices and organizations.

Another recent systematic review examined the intersection of AI, IoT, blockchain, and quantum cryptography, emphasizing the importance of secure digital systems and identifying research opportunities involving privacy and future cryptographic technologies.

The convergence of AI, edge computing, and blockchain has also emerged as a major research theme in recent Computer Science conferences and research publications.

These studies indicate that individual technologies can address different aspects of IoT security. However, combining them requires careful architectural design because AI and blockchain have different computational and operational requirements.

4. Proposed AI-Blockchain-IoT Framework

This paper proposes a conceptual architecture consisting of five major layers.

4.1 IoT Device Layer

The first layer consists of physical devices and sensors. These devices collect information from their environments and transmit selected information to gateways or edge nodes.

Because many IoT devices have limited processing and battery capacity, security mechanisms should be lightweight.

4.2 Communication Layer

The communication layer connects IoT devices with gateways, edge nodes, and cloud systems.

Secure communication is essential because data transmitted over networks can potentially be intercepted or modified.

Encryption and authentication mechanisms should therefore be applied to protect communication.

4.3 AI Analytics Layer

The AI layer analyzes IoT data and network behavior.

A machine learning model can establish a baseline of normal device behavior. When new observations significantly differ from this baseline, the system can classify them as potential anomalies.

For example, if a normally inactive sensor suddenly generates an unusually high number of network requests, an AI-based monitoring system could identify the behavior as suspicious.

4.4 Blockchain Trust Layer

The blockchain layer provides a decentralized mechanism for recording important events.

Instead of storing all raw IoT data on a blockchain, the proposed architecture can store selected metadata, security events, hashes, and verification records.

This approach can reduce blockchain storage requirements while maintaining evidence of data integrity.

4.5 Management Layer

The management layer provides administrators with information about devices, security events, model performance, and blockchain records.

Administrators can use the information to investigate security events and update system policies.

5. AI-Based Threat Detection

5.1 Anomaly Detection

Anomaly detection is one of the most important applications of AI in IoT security.

A system can learn normal patterns from historical device activity. Abnormal behavior can then be identified by comparing new observations with learned patterns.

Potential features may include:

- Number of network connections
- Packet frequency
- Data transmission volume
- Device activity time
- Authentication frequency
- Resource utilization
- Communication destinations

The effectiveness of anomaly detection depends on the quality of training data.

5.2 Classification-Based Security

Supervised machine learning can classify network activity into predefined categories.

For example, a model can potentially distinguish between:

- Normal traffic
- Suspicious traffic
- Unauthorized activity
- Denial-of-service patterns
- Scanning behavior

Classification models require representative training datasets and appropriate evaluation methods.

5.3 Deep Learning

Deep learning can identify complex patterns in high-dimensional datasets. Neural networks can be used to analyze network traffic, device behavior, or security logs.

However, large models may not be suitable for small IoT devices. Edge computing and model optimization can help address this limitation.

5.4 Explainable AI

Security administrators may need to understand why an AI model classified an event as suspicious.

Explainable AI can provide information about important features or patterns that contributed to a prediction.

This can improve transparency and assist security analysts in validating automated decisions.

6. Blockchain-Based IoT Security

6.1 Decentralized Authentication

Traditional IoT authentication may depend on centralized servers. Blockchain can support decentralized identity and authentication mechanisms.

A device can be associated with a cryptographically protected identity. Authorized participants can verify device information before allowing network access.

6.2 Data Integrity

IoT systems frequently rely on sensor data for decision-making. If data are modified, subsequent analysis may become unreliable.

Blockchain can maintain records or cryptographic hashes that help verify whether important information has been altered.

6.3 Smart Contracts

Smart contracts are programmable rules executed within blockchain environments.
In an IoT security system, smart contracts could potentially enforce predefined policies.
For example, a smart contract might record device-registration events or manage permissions between participating entities.

6.4 Decentralized Security Logs

Security logs are important for investigating incidents.
A blockchain-based logging mechanism can create a tamper-resistant record of selected security events.
Rather than placing complete logs on-chain, systems can store large datasets separately while keeping hashes or references on the blockchain.

7. Integration of AI and Blockchain

AI and blockchain provide complementary capabilities.

Technology	Primary Contribution
IoT	Data generation and physical interaction
AI	Analysis and intelligent decision-making
Blockchain	Trust and data integrity
Edge Computing	Low-latency local processing
Cloud Computing	Large-scale storage and computation

The proposed integration can operate as follows:

IoT Devices → Edge Processing → AI Analysis → Blockchain Verification → Cloud/Management Platform

IoT devices first generate information. Edge nodes preprocess the information and perform initial AI inference. Important events can then be recorded through blockchain mechanisms. The cloud platform can provide long-term storage and more computationally intensive analytics.
This architecture can reduce unnecessary data transmission while providing additional security and trust mechanisms.

8. Privacy Preservation

Privacy is a major concern in IoT systems because connected devices may collect sensitive information.
Examples include:

- Location information
- Personal activity patterns
- Health-related measurements
- Household information
- Industrial data

Sending all raw data to centralized platforms may increase privacy risks.

8.1 Local Processing

Processing information locally can reduce the need to transmit raw information.

8.2 Federated Learning

Federated learning enables multiple devices to contribute to machine learning without directly transferring their local training datasets.
Each participating device trains a model locally and sends model updates to a coordinating system.
Blockchain can potentially be used to maintain records of participation and model-update transactions.
Recent research has specifically explored blockchain and federated learning together in edge environments for improving IoT data reliability.

8.3 Data Minimization

Systems should collect only information necessary for their intended purpose. Data minimization can reduce both privacy exposure and storage requirements.

9. Security Threats

Despite the advantages of the proposed framework, several threats remain.

9.1 False AI Predictions

AI models can produce false positives and false negatives. Excessive false alarms can overwhelm security administrators, while missed threats can create security vulnerabilities.

9.2 Poisoned Training Data

If malicious information enters the training dataset, an AI model may learn incorrect patterns.
Therefore, training data should be validated and protected.

9.3 Blockchain Attacks

Blockchain systems are not automatically secure against every possible attack. Poorly designed consensus mechanisms, vulnerable smart contracts, compromised credentials, or implementation errors can create security risks.

9.4 Device Compromise

Even if blockchain records are secure, a compromised IoT device can generate false information.

Blockchain can help preserve records, but it cannot guarantee that the original sensor measurement is truthful.

9.5 Privacy Leakage

Blockchain's transparency can create privacy concerns if sensitive information is stored directly on the ledger.

Consequently, sensitive raw data should generally be handled separately, with blockchain used selectively for verification and integrity mechanisms.

10. Performance and Scalability

10.1 Computational Overhead

AI algorithms and blockchain operations can consume significant computational resources.

This is particularly challenging for small IoT devices.

Lightweight AI models and efficient blockchain protocols are therefore important.

10.2 Energy Consumption

Many IoT devices operate under strict energy constraints. Continuous AI inference or blockchain participation can increase energy consumption.

Edge servers and gateways can perform more computationally demanding tasks on behalf of constrained devices.

10.3 Blockchain Scalability

Large IoT networks can generate enormous numbers of events. Recording every event directly on a blockchain may create scalability problems.

A more practical architecture can store only important security metadata or cryptographic proofs on-chain.

10.4 Network Traffic

AI and blockchain systems can generate additional communication requirements.

Efficient message aggregation and selective synchronization can help reduce network overhead.

11. Applications

11.1 Smart Homes

Smart homes contain connected cameras, sensors, appliances, and access systems.

AI can monitor device behavior and detect unusual activity, while blockchain can support trusted device identities and security records.

11.2 Healthcare IoT

Healthcare IoT systems can use connected sensors and wearable devices to collect information.

AI can identify relevant patterns, while blockchain can support integrity and controlled sharing of selected records.

Because healthcare information can be sensitive, privacy-preserving mechanisms are particularly important.

11.3 Industrial IoT

Industrial systems contain machines, sensors, controllers, and production platforms.

AI can detect unusual machine behavior and network anomalies. Blockchain can provide trusted records between multiple organizations and industrial components.

Recent research specifically identifies blockchain-enabled AI for industrial IoT as an important research direction involving security and data management.

11.4 Smart Cities

Smart cities contain many connected systems, including transportation, energy, environmental monitoring, and public infrastructure.

The proposed architecture can support trusted data exchange between different city services.

11.5 Smart Agriculture

IoT sensors can monitor agricultural conditions while AI models analyze environmental information.

Blockchain can provide records of selected agricultural data and transactions between participating organizations.

12. Challenges

Several challenges must be addressed before large-scale deployment.

12.1 Interoperability

IoT ecosystems contain devices from different manufacturers and use different protocols. Developing common interfaces remains an important requirement.

12.2 Resource Constraints

Many devices cannot execute complex AI algorithms or blockchain protocols efficiently.

12.3 Model Management

AI models require monitoring, updating, validation, and retraining.

Managing models across thousands of distributed devices can be complex.

12.4 Regulatory Requirements

Different applications may be subject to privacy and data-management regulations.

Security architectures should therefore consider regulatory requirements from the beginning of system design.

12.5 Cost

Deploying edge servers, specialized AI hardware, blockchain infrastructure, and secure IoT devices can increase implementation costs.

Organizations must balance security improvements with operational requirements.

13. Future Research Directions

Future research can investigate several important directions.

First, lightweight blockchain mechanisms should be developed specifically for resource-constrained IoT environments.

Second, researchers should investigate federated learning and privacy-preserving AI for distributed IoT networks.

Third, explainable AI can make automated security decisions more understandable.

Fourth, edge computing can be integrated more deeply into the proposed architecture to reduce latency and communication overhead.

Fifth, researchers should investigate AI models capable of adapting to changing attack patterns without requiring complete retraining.

Sixth, quantum-resistant cryptographic mechanisms may become increasingly relevant as computing technologies evolve. Recent reviews have already examined the relationship between AI, IoT, blockchain, and quantum cryptography.

Finally, standardized evaluation benchmarks are needed so that researchers can compare AI-blockchain IoT security solutions using consistent datasets, metrics, and experimental conditions.

14. Conclusion

The rapid expansion of the Internet of Things has created significant opportunities for intelligent computing while simultaneously increasing cybersecurity challenges. Conventional centralized security approaches may not provide sufficient flexibility for highly distributed IoT environments.

This paper examined a conceptual framework combining Artificial Intelligence and blockchain for trustworthy IoT security. AI provides intelligent capabilities for anomaly detection, classification, behavioral analysis, and automated threat identification. Blockchain provides decentralized trust, data integrity, authentication support, and tamper-resistant records.

The combination of these technologies can potentially strengthen IoT security, but it also introduces computational, scalability, energy, privacy, and interoperability challenges. Therefore, successful deployment requires carefully designed architectures that consider the limitations of IoT devices.

Future research should focus on lightweight AI, efficient blockchain protocols, federated learning, edge intelligence, explainable security models, privacy preservation, and standardized evaluation. The convergence of these technologies has the potential to establish more secure, intelligent, and trustworthy IoT ecosystems across healthcare, industry, smart cities, agriculture, and other application domains.

References

1. Rahman, A., Kundu, D., Debnath, T., et al. (2026). A systematic survey of blockchain-enabled artificial intelligence for industrial IoT: recent advances, integration challenges, and future prospects. Artificial Intelligence Review.
2. Kaushik, D., Gulia, P., Gill, N. S., Yahya, M., Shukla, P. K., et al. (2026). Synergizing blockchain and AI to fortify IoT security: a comprehensive review. Artificial Intelligence Review.
3. Silva, E. N., Pinto, G. P., Silva, C. J. N., et al. (2026). Enhancing IoT data reliability with blockchain and federated learning in edge environments. Discover Internet of Things.
4. Adere, K., Hailu, S., Abebe, M., et al. (2026). A systematic review of artificial intelligence applications in Internet of Things, blockchain, and quantum cryptography. Discover Artificial Intelligence.
5. Zhu, J., Li, F., & Chen, J. (2024). A survey of blockchain, artificial intelligence, and edge computing for Web 3.0. Computer Science Review, 54, 100667.
6. Privacy and security for 6G networks via Fog/Edge Computing, Blockchain, and Federated Learning: A survey and taxonomy. Journal of Network and Computer Applications, 252, 104510, 2026.
7. Energy efficient cyber-physical control of renewable microgrids using edge-AI enabled IoT and secure blockchain coordination. Scientific Reports, 16, 20194, 2026.