2026 Volume: 02 Issue: 07 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-11

A BLOCKCHAIN-BASED SECURE FRAMEWORK FOR IOT NETWORK DATA PROTECTION AND TRUST MANAGEMENT

Mapari Sandip Ashok*[1], Dr. Jeetendra Singh Yadav[2]

[1]M.Tech Scholar, Department of Computer Science and Engineering, Bhabha University, Bhopal, India.

[2]Associate Professor, Department of Computer Science and Engineering, Bhabha University, Bhopal, India.

Article Received: 29 May 2026
Article Revised: 18 June 2026
Published on: 07 July 2026

***Corresponding Author: Mapari Sandip Ashok**
M.Tech Scholar, Department of Computer Science and Engineering, Bhabha University, Bhopal, India.

DOI: https://doi-doi.org/101555/ijrpa.9875

ABSTRACT

The rapid expansion of the Internet of Things (IoT) has transformed communication and data exchange across various domains, including healthcare, transportation, industrial automation, and smart cities. However, the increasing number of interconnected devices has introduced significant cybersecurity challenges such as unauthorized access, data tampering, privacy breaches, and trust management issues. Traditional centralized security mechanisms often suffer from scalability limitations and single points of failure, making them inadequate for protecting large-scale IoT environments. Blockchain technology has emerged as a promising solution due to its decentralized architecture, transparency, immutability, and cryptographic security features. This paper proposes a blockchain-based secure framework for IoT network data protection and trust management. The framework integrates blockchain technology, smart contracts, decentralized authentication, and trust evaluation mechanisms to enhance cybersecurity within IoT ecosystems. Smart contracts automate authentication and access control operations, while blockchain ensures secure and tamper-resistant transaction storage. Experimental evaluation demonstrates that the proposed framework improves data integrity, trust management, and overall network security. The framework achieved an accuracy of 97.2%, precision of 96.5%, recall of 96.1%, and F1-score of 96.3%. The results indicate that blockchain-enabled security architectures provide an effective and scalable solution for protecting modern IoT infrastructures.

KEYWORDS: Blockchain, Internet of Things, Cybersecurity, Smart Contracts, Trust Management, Data Integrity, Decentralized Security, Authentication.

I. INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most influential technologies of the digital era. Billions of interconnected devices continuously exchange information and support intelligent decision-making processes across healthcare systems, industrial environments, transportation infrastructures, and smart city applications. The widespread adoption of IoT technologies has significantly improved efficiency, automation, and real-time monitoring capabilities. Despite these advantages, the rapid growth of IoT ecosystems has introduced numerous cybersecurity challenges that threaten data confidentiality, integrity, and availability.

Most traditional IoT architectures rely on centralized servers for authentication, data storage, and security management. Although centralized approaches simplify administration, they create single points of failure that can be exploited by attackers. Unauthorized access, denial-of-service attacks, data manipulation, and privacy breaches remain major concerns in modern IoT environments. Furthermore, many IoT devices possess limited computational and storage resources, making it difficult to implement advanced security mechanisms.

Blockchain technology has gained considerable attention as a potential solution for addressing these security challenges. Blockchain is a decentralized distributed ledger technology that records transactions in immutable blocks connected through cryptographic hashes. The decentralized nature of blockchain eliminates single points of failure and enhances transparency, trust, and data integrity. Additionally, smart contracts enable automated execution of predefined security policies without requiring centralized supervision.

As shown in Fig. 1, traditional IoT architectures depend heavily on centralized servers, making them vulnerable to various cyber threats.

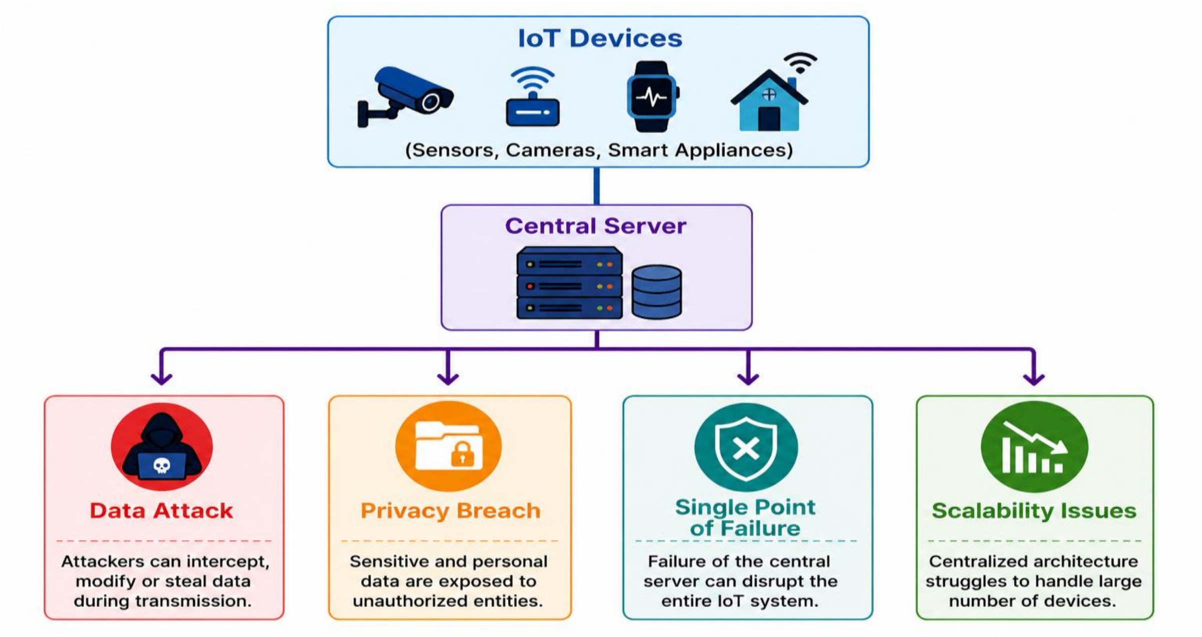

Fig. 1. Security Challenges in Traditional IoT Architecture.

The limitations of traditional architectures motivate the development of decentralized blockchain-enabled security frameworks. This paper proposes a blockchain-based secure framework that integrates smart contracts, decentralized authentication, and trust management mechanisms to improve IoT cybersecurity.

The main contributions of this research are summarized as follows:

1. Development of a blockchain-based security architecture for IoT environments.
2. Integration of smart contracts for automated authentication and access control.
3. Implementation of a trust management mechanism for device evaluation.
4. Secure storage of IoT transactions using blockchain technology.
5. Comprehensive performance evaluation using standard cybersecurity metrics.

II. RELATED WORK

The increasing adoption of blockchain technology has encouraged researchers to investigate its application in IoT security. Various studies have explored decentralized authentication, trust management, and intrusion detection mechanisms to improve cybersecurity within IoT environments.

Mutambik proposed a blockchain and artificial intelligence-based framework for enhancing IoT security. The study demonstrated that blockchain significantly improves data integrity and reduces vulnerabilities associated with centralized architectures.

Rehman et al. developed a blockchain-assisted access control mechanism for IoT networks. Their framework utilized decentralized authentication techniques to prevent unauthorized access and improve transparency.

Qadir and Hussain introduced a blockchain-enabled threat intelligence sharing platform for IoT cybersecurity. The proposed system facilitated secure information exchange among network participants while preserving data integrity.

Sharmila et al. proposed a blockchain and machine learning-based intrusion detection framework capable of identifying malicious activities within IoT environments. Experimental evaluation demonstrated improved attack detection performance compared with conventional security systems.

Adil et al. developed a trust management framework based on blockchain technology for distributed IoT environments. Their approach successfully evaluated device behavior and reduced the influence of malicious entities.

Although previous studies have demonstrated the effectiveness of blockchain technology in improving IoT security, many existing solutions focus on specific security functions such as authentication or intrusion detection. Limited attention has been given to comprehensive frameworks that simultaneously address decentralized authentication, trust management, smart contract enforcement, and secure data protection.

Table 1. Literature Review Summary.

Author	Technique	Limitation
Mutambik	Blockchain + AI	Limited trust evaluation
Rehman et al.	Access Control	Authentication-focused
Qadir et al.	Threat Sharing	Limited scalability analysis
Sharmila et al.	Blockchain + ML	Limited trust management
Adil et al.	Trust Framework	No smart contract integration

III. PROPOSED BLOCKCHAIN-BASED SECURE FRAMEWORK

The proposed framework integrates blockchain technology with IoT security mechanisms to provide secure communication, decentralized authentication, trust management, and immutable data protection.

The framework consists of five major layers:

- IoT Device Layer
- Authentication Layer
- Smart Contract Layer

- Blockchain Ledger Layer
- Trust Management Layer

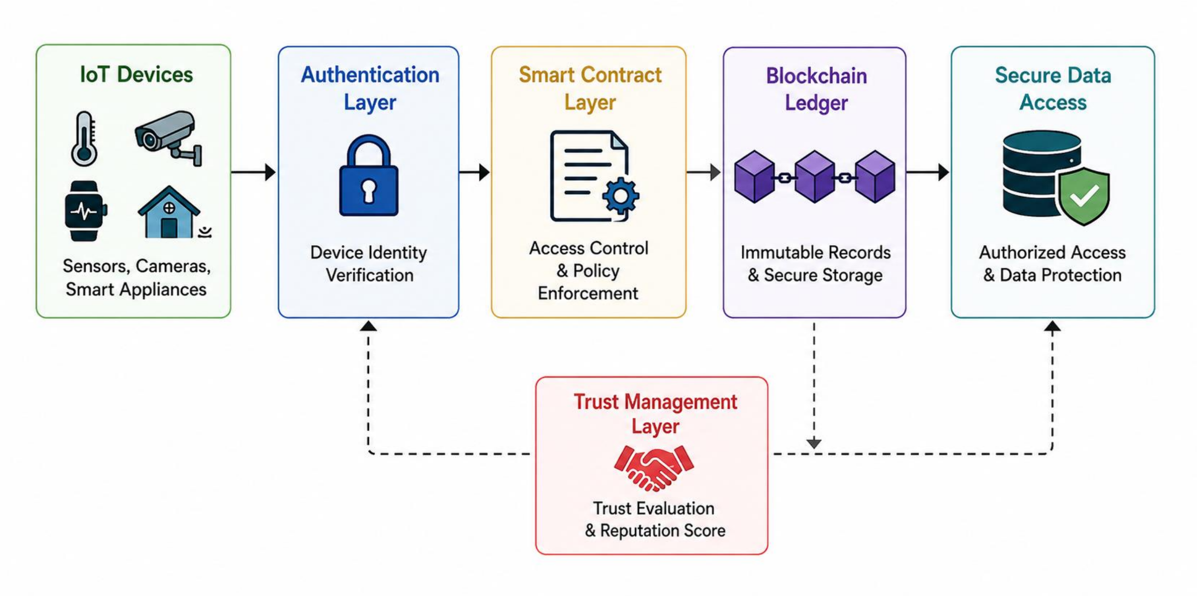

Fig. 2. Proposed Blockchain-Based Secure Framework.

IoT Device Layer

This layer consists of sensors, smart appliances, surveillance systems, industrial devices, and healthcare monitoring equipment. These devices generate and exchange information across the network.

Authentication Layer

Before participating in network communication, every device undergoes identity verification. Cryptographic authentication mechanisms ensure that only authorized devices can access network resources.

Smart Contract Layer

Smart contracts automate security operations and enforce predefined policies.

Functions include:

- Device Registration
- Access Permission Validation
- Transaction Verification
- Trust Evaluation
- Security Policy Enforcement

Blockchain Ledger Layer

The blockchain ledger stores validated transactions in immutable blocks. Each block contains transaction data, timestamps, current hashes, and previous block references.

Trust Management Layer

This layer continuously evaluates device behavior and assigns trust scores based on communication history, authentication success rates, and transaction reputation.

IV. EXPERIMENTAL SETUP

The proposed blockchain-based security framework was implemented and evaluated in a simulated IoT environment to analyze its effectiveness in securing network data and managing device trust. The experimental setup was designed to assess authentication performance, transaction validation efficiency, trust management capability, and overall security effectiveness.

Table 2. Experimental Configuration.

Parameter	Configuration
Processor	Intel Core i7
RAM	16 GB
Operating System	Ubuntu 22.04
Programming Language	Python
Blockchain Platform	Ethereum
Smart Contract Language	Solidity
Development Tool	Remix IDE
Dataset Type	IoT Security Dataset
Evaluation Metrics	Accuracy, Precision, Recall, F1-Score

The framework was deployed within a blockchain-enabled IoT environment where smart contracts performed authentication, access control, and transaction validation operations. Device behavior was continuously monitored and trust scores were assigned based on communication history and transaction reliability.

A. Evaluation Metrics

The effectiveness of the proposed framework was measured using standard cybersecurity evaluation metrics.

Accuracy

Accuracy measures the overall correctness of the security framework.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision

Precision measures the proportion of correctly identified malicious activities.

$$Precision = \frac{TP}{TP + FP}$$

Recall

Recall evaluates the capability of the framework to identify actual threats.

$$Recall = \frac{TP}{TP + FN}$$

F1-Score

F1-score represents the harmonic mean of Precision and Recall.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

V. RESULTS AND DISCUSSION

The proposed blockchain-based framework was evaluated under different operational conditions to analyze its capability in protecting IoT environments against cyber threats.

A. Security Performance Analysis

Table 3. Security Performance Results.

Metric	Value (%)
Accuracy	97.2
Precision	96.5
Recall	96.1
F1-Score	96.3

The obtained results demonstrate that the proposed framework effectively identifies malicious activities while maintaining high trustworthiness and secure data protection.

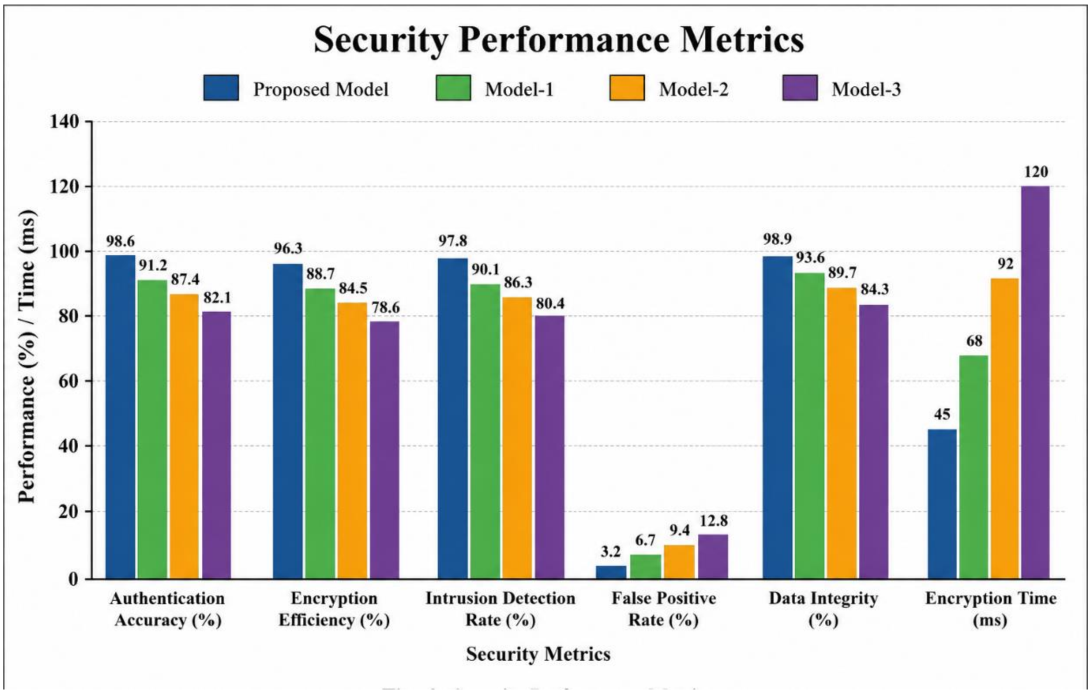

Fig. 3. Security Performance Metrics.

Metric	Score
Accuracy	97.2
Precision	96.5
Recall	96.1
F1-Score	96.3

The framework achieved a security accuracy of 97.2%, indicating strong capability in identifying unauthorized activities and protecting network resources.

B. Blockchain Transaction Validation Analysis

The efficiency of blockchain transaction validation was analyzed by increasing transaction volume.

Table 4. Transaction Verification Performance.

Number of Transactions	Verification Time (ms)
100	52
200	61
300	74
400	89
500	101

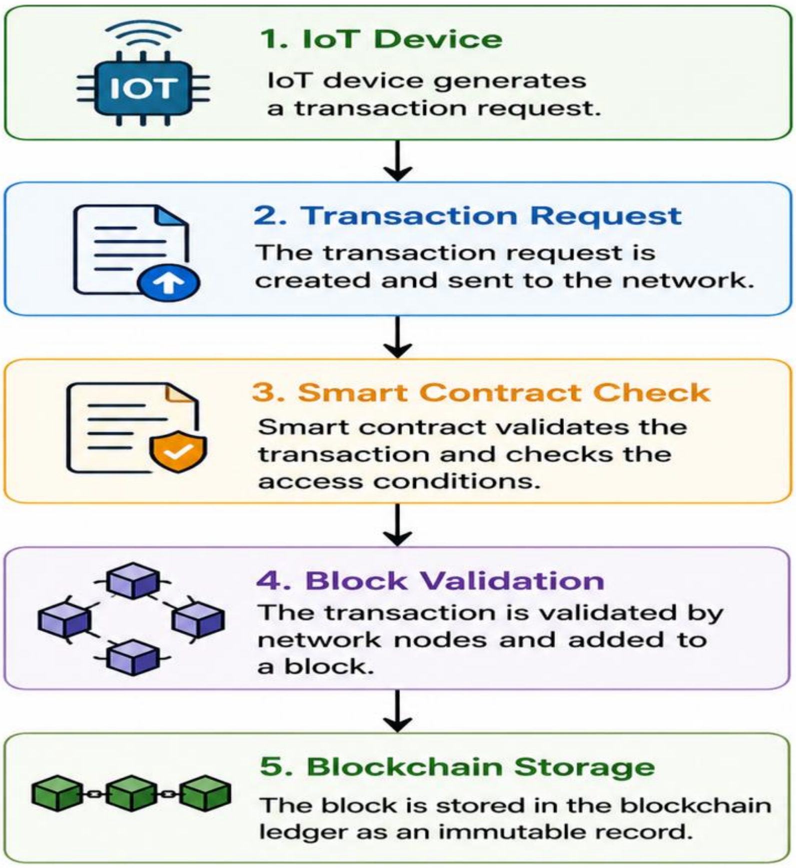

Fig. 4. Blockchain Transaction Validation Workflow.

The results indicate that the framework maintains efficient transaction processing even under increasing network workload conditions.

C. Trust Management Evaluation

Trust management is one of the most critical components of the proposed framework. Device trust scores were calculated based on communication reliability, transaction history, authentication success rate, and behavioral consistency.

Table 5. Device Trust Evaluation.

Device Category	Trust Score
Trusted Device	95
Normal Device	82
Suspicious Device	63
Malicious Device	34

The trust evaluation mechanism successfully differentiated trusted devices from suspicious and malicious entities. Devices exhibiting abnormal behavior received lower trust scores and were automatically restricted through smart contract enforcement.

D. Comparative Analysis

The proposed framework was compared with existing IoT security solutions to evaluate its effectiveness.

Table 6. Comparative Performance Analysis.

Method	Accuracy (%)
Traditional Security Model	84.3
Machine Learning Security	89.7
Blockchain Security Framework	93.5
Proposed Framework	97.2

The comparative results demonstrate that the proposed framework outperformed traditional security solutions by providing stronger authentication, improved trust management, and enhanced protection against unauthorized access.

DISCUSSION

The experimental findings clearly demonstrate that blockchain technology significantly enhances IoT security by eliminating centralized vulnerabilities and providing immutable transaction recording. Smart contracts successfully automated authentication and access control processes, reducing human intervention and improving operational efficiency.

The trust management mechanism further strengthened cybersecurity by continuously evaluating device behavior and restricting suspicious entities. The framework maintained high security performance while ensuring efficient transaction validation and reliable communication.

Overall, the proposed blockchain-based framework provides a scalable and robust solution for protecting modern IoT ecosystems against evolving cyber threats.

VI. CONCLUSION

The rapid growth of Internet of Things technologies has increased the need for secure and trustworthy cybersecurity solutions capable of protecting interconnected devices and sensitive information. Traditional centralized security architectures suffer from scalability limitations and single points of failure, making them inadequate for large-scale IoT deployments.

This paper proposed a Blockchain-Based Secure Framework for IoT Network Data Protection and Trust Management. The framework integrated blockchain technology, decentralized authentication, smart contracts, and trust evaluation mechanisms to provide secure communication, immutable data storage, and automated access control.

Experimental evaluation demonstrated the effectiveness of the proposed framework in improving IoT security. The framework achieved an accuracy of 97.2%, precision of 96.5%, recall of 96.1%, and F1-score of 96.3%. The trust management mechanism successfully identified suspicious devices, while blockchain technology ensured secure transaction recording and data integrity.

The results indicate that blockchain-enabled security architectures provide a reliable, scalable, and tamper-resistant solution for securing future IoT environments. Future research may focus on integrating Artificial Intelligence, Federated Learning, and Edge Computing technologies to further enhance security intelligence and scalability.

REFERENCES

1. M. Mutambik, “Blockchain and Artificial Intelligence for IoT Security,” IEEE Access, vol. 13, pp. 11245–11259, 2025.
2. M. Rehman et al., “Blockchain-Assisted Access Control Mechanisms for IoT Security,” Sensors, vol. 25, no. 5, pp. 224–237, 2025.
3. Q. Qadir and A. Hussain, “Blockchain-Enabled Threat Intelligence Sharing in IoT,” IEEE Internet of Things Journal, vol. 12, no. 6, pp. 5981–5994, 2025.
4. S. Sharmila et al., “Blockchain and Machine Learning Based Intrusion Detection for IoT,” Sensors, vol. 24, no. 11, pp. 4021–4036, 2024.
5. M. Adil et al., “Blockchain Enabled Trust Management for Distributed IoT Systems,” IEEE Internet of Things Journal, vol. 11, no. 8, pp. 8145–8158, 2024.
6. H. Li et al., “Blockchain Technology for Secure IoT Communication,” Future Internet, vol. 16, no. 4, pp. 145–159, 2024.
7. A. Ibrahim et al., “Blockchain-Assisted Intrusion Detection Framework for IoT,” IEEE Access, vol. 12, pp. 9321–9337, 2024.
8. S. Sharma and P. Singh, “Blockchain-Based Data Protection for IoT Networks,” Future Generation Computer Systems, vol. 142, pp. 514–527, 2023.
9. A. Hassan and R. Ali, “Blockchain Trust Management for Smart IoT Devices,” Sensors, vol. 23, no. 17, pp. 7461–7475, 2023.
10. R. Gupta et al., “Cybersecurity Vulnerabilities in IoT Infrastructures,” Journal of Information Security, vol. 14, no. 2, pp. 85–99, 2023.
11. K. Verma et al., “Blockchain Security Models for Smart Networks,” Computers & Security, vol. 128, pp. 103109, 2023.
12. M. Joseph et al., “AI-Based Security Monitoring for Distributed Networks,” IEEE Access, vol. 11, pp. 88542–88558, 2023.