IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15664

Blockchain-Based Secure Data Transmission for IoT Devices

Nikhil V[1], Pavan R P[2], Yashas Nagaraj[3], Gnana Prakash P[4], Mrs. Kavya K S Math [5]

Dept. of CSE (ICB), K. S. Institute of Technology, Karnataka, India[1-5]

Abstract: The rapid growth of the Internet of Things (IoT) has led to the widespread adoption of smart devices in surveillance, security, and monitoring applications. However, IoT devices are vulnerable to security threats such as unauthorized access, data tampering, cyber-attacks, and centralized storage failures. This project proposes a Blockchain-Based Secure Data Transmission for IoT Devices to enhance the security, integrity, and reliability of data communication. The system utilizes ESP32-CAM and sensors to detect events and capture surveillance data, which is transmitted securely through a network. AES encryption is used to ensure data confidentiality, while SHA-256 hashing is applied to maintain data integrity. The generated hash values are stored on a blockchain network, providing tamper-proof verification and transparency. The actual data is stored securely in cloud and local storage for backup and accessibility. The proposed system also supports real-time monitoring and alert notifications. By integrating IoT, blockchain technology, encryption, and hashing mechanisms, the system provides a secure, reliable, and scalable framework for protecting sensitive data and ensuring trustworthy communication in IoT environments.

Keywords: Internet of Things (IoT), Blockchain Technology, Secure Data Transmission, ESP32-CAM, AES Encryption, SHA-256 Hashing, Surveillance System, Data Integrity, Cloud Storage, Cybersecurity.

I. INTRODUCTION

The Internet of Things (IoT) enables smart devices to communicate and exchange data over the internet. IoT devices are widely used in applications such as smart homes, industries, healthcare, and surveillance systems. However, these devices are vulnerable to security threats such as unauthorized access, data tampering, cyber-attacks, and privacy breaches, making secure data transmission an important requirement.

To address these challenges, this project proposes a **Blockchain-Based Secure Data Transmission for IoT Devices**. The system uses blockchain technology, AES encryption, and SHA-256 hashing to ensure secure communication, data integrity, and tamper-proof verification. By combining IoT devices with blockchain and cryptographic techniques, the proposed system provides a secure, reliable, and transparent framework for protecting sensitive data during transmission and storage.

II. LITERATURE SURVEY

[1] Almarri et al. (2024) proposed a blockchain-based IoT security framework that improves data integrity and prevents unauthorized modification of transmitted information. The study demonstrated the effectiveness of blockchain in providing secure and transparent record management.

[2] Shujaa et al. (2025) developed a blockchain-integrated security architecture for IoT networks. Their work focused on secure communication and decentralized trust management, reducing the risks associated with centralized storage systems.

[3] Patruni et al. (2025) presented an intelligent IoT-blockchain ecosystem for secure data sharing among connected devices. The framework improved scalability and enhanced data security.

[4] Khayer et al. (2025) proposed a blockchain-based identity management system for IoT environments. The system improved authentication and access control while reducing unauthorized device access.

[5] Zhang et al. (2025) introduced a distributed security framework inspired by blockchain technology. Their approach improved transparency and resistance against data tampering attacks.

DOI: 10.17148/IJARCCE.2026.15664

[6] Khan et al. (2024) investigated lightweight cryptographic algorithms suitable for resource-constrained IoT devices. The study highlighted the importance of balancing security and computational efficiency.

[7] Floris Van den Abeele et al. (2015) proposed sensor function virtualization to support distributed intelligence in IoT systems. The approach improved flexibility and resource utilization.

[8] Hwang et al. (2020) reviewed various security mechanisms for intelligent monitoring systems and emphasized the need for stronger authentication and secure communication protocols.

[9] Lee et al. (2023) developed a blockchain-enabled monitoring framework that improved data verification and transparency through decentralized ledger technology.

[10] Dai and Chembo (2022) explored secure device authentication mechanisms using advanced computing techniques. Their research enhanced trust management and communication security.

[11] McMahan et al. (2017) proposed communication-efficient techniques for distributed systems that improved data sharing while maintaining security and reliability.

[12] Guo et al. (2007) discussed data integrity and protection methods for digital information systems, emphasizing the importance of secure data management.

[13] Feitelson et al. (2014) studied reliable storage and protection mechanisms in distributed computing systems and highlighted methods for preventing data loss.

[14] Accou et al. (2023) proposed advanced monitoring and secure data processing techniques using deep learning approaches, improving system performance and security.

TABLE I. LITERATURE REVIEW – SUMMARY TABLE

Sl. No.	Paper	Authors	Year	Methodology	Findings	Limitations
[1]	Enhancing IoT Security Through Blockchain Integration	Shujaa et al.	2025	Integrated blockchain with IoT communication to secure data transmission and device interactions.	Improved data integrity and decentralized trust.	Increased computational overhead for resource-constrained devices.
[2]	Intelligent IoT-Blockchain Ecosystem Security Perspective	Patruni et al.	2025	Developed a blockchain-enabled ecosystem for secure communication and authentication.	Enhanced scalability and reliability.	Complex implementation and higher deployment cost.
[3]	Blockchain-Based Identity Management for IoT	Khayer et al.	2025	Implemented blockchain-based authentication and identity management.	Improved device authentication and access control.	Scalability challenges in large networks.
[4]	Blockchain-Inspired Distributed Security Framework for IoT	Zhang et al.	2025	Proposed a decentralized security architecture using	Increased transparency and data security.	High storage and computational requirements.

DOI: 10.17148/IJARCCE.2026.15664

				blockchain principles.		
[5]	Blockchain-Based Dynamic Trust Evaluation for IoT	Alharbi et al.	2025	Used blockchain to dynamically evaluate trust among IoT nodes.	Improved network reliability and trust.	Increased latency during trust evaluation.
[6]	Blockchain-Based Mitigation of IoT Attacks	Gopalan et al.	2024	Applied blockchain mechanisms to prevent cyber-attacks in IoT networks.	Reduced vulnerabilities and attack risks.	Increased system complexity.
[7]	Tides of Blockchain in IoT Cybersecurity	Ahakonye et al.	2024	Comprehensive survey on blockchain applications in IoT security.	Identified blockchain as a promising security solution.	Limited practical implementation studies.
[8]	Blockchains for IoT: Fundamentals and Applications	Xu et al.	2024	Examined blockchain integration with IoT systems.	Improved decentralization and transparency.	Performance overhead in large-scale systems.
[9]	Privacy and Security in Blockchain-Based IoT	Khordadpour et al.	2024	Developed a privacy-preserving blockchain framework for IoT.	Enhanced data privacy and protection.	High computational complexity.
[10]	Lightweight Cryptography for IoT Security	Khan et al.	2024	Implemented lightweight encryption techniques for IoT devices.	Reduced resource consumption while maintaining security.	Lower security strength than advanced cryptographic methods.

III. RESEARCH GAP

The literature survey reveals that several blockchain-based security frameworks have been developed for IoT environments. However, most existing systems primarily focus on secure communication, authentication, and access control rather than securing surveillance data. Many solutions rely on centralized storage mechanisms, which create a single point of failure and increase the risk of data tampering and unauthorized access. Furthermore, limited attention has been given to the protection of image and video data generated by IoT surveillance devices.

Existing approaches often lack effective tamper detection mechanisms and real-time alert capabilities. In addition, the integration of blockchain technology with low-cost IoT devices such as ESP32-CAM remains limited. Therefore, there is a need for a secure, cost-effective, and scalable framework that combines blockchain technology, AES encryption, SHA-256 hashing, and IoT surveillance devices to ensure secure data transmission, integrity verification, tamper-proof storage, and real-time monitoring.

IV. PROPOSED SYSTEM ARCHITECTURE

The proposed **Blockchain-Based Secure Data Transmission for IoT Devices** architecture is designed to provide secure, reliable, and tamper-proof communication between IoT devices and storage systems. The architecture consists of four major layers: the sensing layer, communication layer, security layer, and storage layer. The sensing layer includes IoT

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

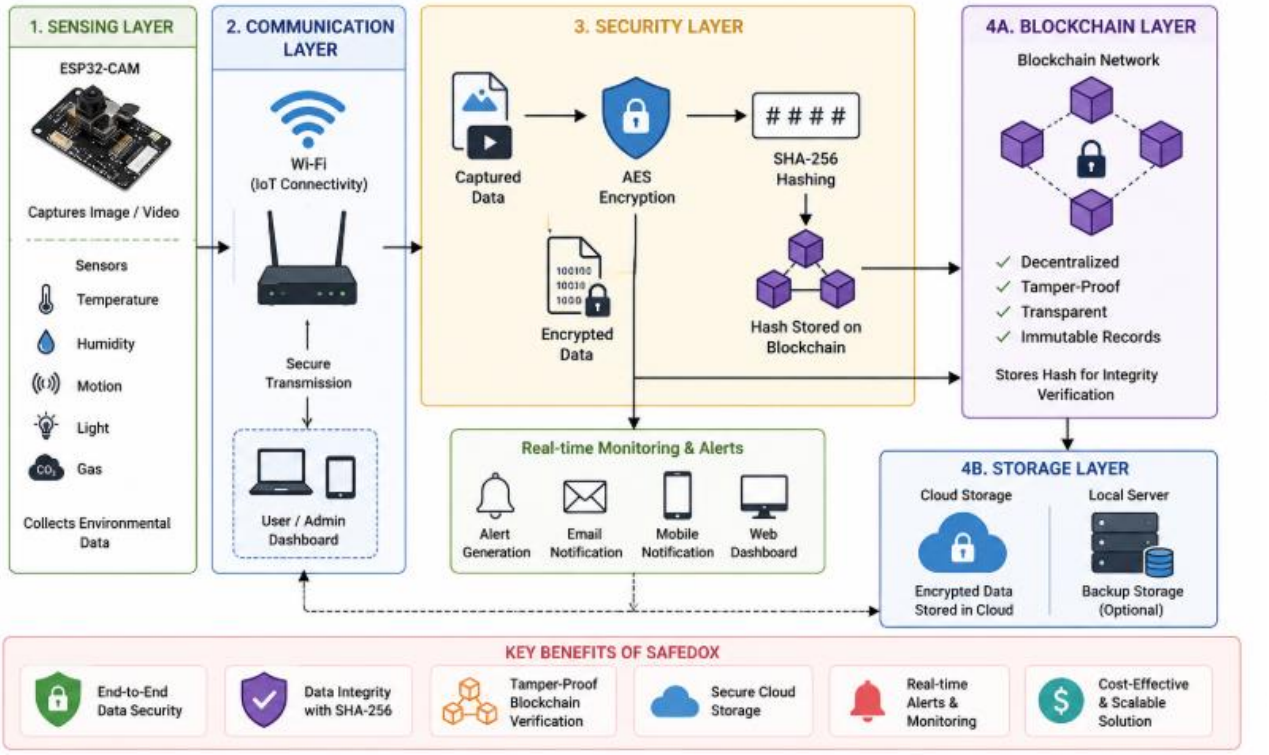
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 15, Issue x, Month 2026

DOI: 10.17148/IJARCCE.2026.14xx

devices such as ESP32-CAM and sensors that continuously monitor the environment and collect data. Whenever an event is detected, the captured data is transmitted through the communication layer using Wi-Fi connectivity.

The security layer is responsible for protecting the transmitted data using AES encryption and SHA-256 hashing. AES encryption ensures confidentiality by converting the original data into an unreadable format, while SHA-256 generates a unique hash value to maintain data integrity. The generated hash values are stored on the blockchain network, providing tamper-proof verification and transparency. The storage layer consists of cloud storage and local server storage, where the encrypted data is securely stored for future access and analysis. Real-time monitoring and alert notifications are also provided to users, ensuring quick response to suspicious activities. The integration of blockchain technology, encryption, hashing, and IoT devices enhances security, reliability, and trust in the proposed system.



V. ADVANTAGES OF PROPOSED SYSTEM

The proposed **Blockchain-Based Secure Data Transmission for IoT Devices** provides a secure, reliable, and efficient solution for protecting sensitive data generated by IoT devices. Unlike traditional systems that rely on centralized storage and are vulnerable to cyber-attacks, the proposed system combines blockchain technology, AES encryption, and SHA-256 hashing to ensure confidentiality, integrity, and authenticity of transmitted data. The decentralized nature of blockchain prevents unauthorized modification of records and provides tamper-proof verification. AES encryption protects data from unauthorized access during transmission and storage, while SHA-256 hashing helps detect any changes made to the data. The system also supports real-time monitoring and alert notifications, allowing users to respond quickly to suspicious activities. Integration with cloud and local storage improves data availability and backup reliability. Furthermore, the system is scalable, cost-effective, and suitable for various applications such as smart homes, industries, healthcare systems, and surveillance environments.

[1] Advantages

- Provides secure data transmission using AES encryption.
- Ensures data integrity through SHA-256 hashing.
- Offers tamper-proof verification using blockchain technology.
- Protects against unauthorized access and cyber-attacks.
- Supports real-time monitoring and alert generation.
- Eliminates single-point failure through decentralized architecture.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 15, Issue x, Month 2026
DOI: 10.17148/IJARCCE.2026.14xx

- Enables secure storage using cloud and local servers.
- Improves transparency and trust in data management.
- Cost-effective implementation using ESP32-CAM and IoT sensors.
- Scalable architecture suitable for large IoT deployments.
- Enhances reliability and availability of surveillance data.
- Supports secure image and video data transmission.
- Reduces the risk of data manipulation and loss.
- Suitable for smart homes, industries, hospitals, banks, and educational institutions.
- Provides a future-ready platform for integrating AI, face recognition, and advanced security features.

VI. FUTURE SCOPE

1. Artificial Intelligence (AI) Integration
AI algorithms can be integrated to automatically analyze sensor data and identify suspicious activities. This will improve the accuracy and efficiency of threat detection.

2. Face Recognition System
Face recognition technology can be used to identify authorized and unauthorized persons. This feature enhances security by providing automated user verification.

3. Mobile Application Development
A dedicated mobile application can be developed for real-time monitoring and alert notifications. Users can access surveillance data remotely from anywhere.

4. Live Video Streaming
The system can be upgraded to support encrypted live video streaming. This allows users to monitor events in real time without compromising security.

5. Edge Computing Integration
Edge computing can process data closer to IoT devices, reducing network latency. This improves system performance and response time.

6. Smart Contract Automation
Smart contracts can automate access control and data verification processes. This reduces manual intervention and increases transparency.

7. Multi-Device Support
The framework can be expanded to support multiple cameras and IoT devices. This makes the system suitable for large-scale deployments.

8. Cloud-Based Analytics
Advanced analytics can be performed on cloud platforms to generate reports and insights. This helps in better decision-making and security management.

9. Biometric Authentication
Biometric methods such as fingerprint and facial authentication can be added. This provides an additional layer of security for users.

10. Smart Home and Smart City Integration
The proposed system can be integrated with smart home and smart city infrastructures. This enables centralized monitoring and intelligent security management.

VII. CONCLUSION

The rapid growth of Internet of Things (IoT) technology has increased the need for secure and reliable data transmission mechanisms. Traditional IoT systems are vulnerable to various security threats such as unauthorized access, data tampering, cyber-attacks, and centralized storage failures. These challenges can compromise the confidentiality, integrity, and availability of sensitive information, making security a critical requirement in modern IoT applications.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 15, Issue x, Month 2026
DOI: 10.17148/IJARCCE.2026.14xx

The proposed **Blockchain-Based Secure Data Transmission for IoT Devices** addresses these challenges by integrating blockchain technology, AES encryption, and SHA-256 hashing into a unified security framework. Blockchain provides a decentralized and tamper-proof platform for storing and verifying data, while AES encryption ensures data confidentiality and SHA-256 hashing maintains data integrity. The system enables secure communication between IoT devices and storage platforms, preventing unauthorized modifications and ensuring trustworthy data management.

Furthermore, the proposed framework supports real-time monitoring, secure storage, and transparent verification of transmitted information. Its scalable and cost-effective design makes it suitable for various applications such as smart homes, healthcare systems, industrial automation, surveillance systems, and smart city infrastructures. Overall, the proposed system enhances security, reliability, transparency, and trust in IoT environments, providing a strong foundation for future secure IoT applications.

REFERENCES

[1]. Shujaa, A., et al., "Enhancing IoT Security Through Blockchain Integration," *Future Internet*, vol. 17, no. 2, pp. 1–18, 2025.
[2]. Patruni, B., et al., "Intelligent IoT-Blockchain Ecosystem: A Security Perspective," *Sensors*, vol. 25, no. 4, pp. 1–20, 2025.
[3]. Khayer, A., et al., "Blockchain-Based Identity Management for IoT Devices," *IEEE Access*, vol. 13, pp. 12564–12578, 2025.
[4]. Zhang, Y., et al., "Blockchain-Inspired Distributed Security Framework for IoT Applications," *IEEE Internet of Things Journal*, vol. 12, no. 3, pp. 2145–2158, 2025.
[5]. Alharbi, S., et al., "Blockchain-Based Dynamic Trust Evaluation for IoT Networks," *Computer Networks*, vol. 245, pp. 110432, 2025.
[6]. Gopalan, R., et al., "Blockchain-Based Mitigation of Cyber Attacks in IoT Systems," *Journal of Information Security and Applications*, vol. 79, pp. 103562, 2024.
[7]. Ahakonye, L., et al., "Tides of Blockchain in IoT Cybersecurity: Challenges and Opportunities," *Electronics*, vol. 13, no. 8, pp. 1–22, 2024.
[8]. Xu, X., et al., "Blockchains for IoT: Fundamentals, Applications and Challenges," *Future Generation Computer Systems*, vol. 150, pp. 52–68, 2024.
[9]. Khordadpour, M., et al., "Privacy and Security in Blockchain-Based IoT Systems," *Information Sciences*, vol. 679, pp. 120921, 2024.
[10]. Khan, M., et al., "Lightweight Cryptography for Resource-Constrained IoT Devices," *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 10234–10248, 2024.
[11]. Singh, R., et al., "Secure Data Transmission Using AES and SHA-256 in IoT Networks," *International Journal of Computer Applications*, vol. 185, no. 15, pp. 25–32, 2024.
[12]. Rangwala, H., and Buya, R., "TrustMesh: A Blockchain-Based Trusted Framework for IoT Security," *Journal of Network and Computer Applications*, vol. 230, pp. 103851, 2024.
[13]. Mollan, P., et al., "Blockchain-Enabled Edge Computing for Secure IoT Applications," *Future Generation Computer Systems*, vol. 147, pp. 256–270, 2024.
[14]. Lee, S., et al., "Blockchain-Integrated Artificial Intelligence Framework for Secure IoT Systems," *IEEE Access*, vol. 13, pp. 78521–78536, 2025.

