The Chitransh Academic & Research
An International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume1 | Issue 3 |June 2025
ISSN: 3049-303X (Online)
Website: www.thechitranshacadmic.in

Blockchain as a Secure Framework for Internet of Things (IoT) Communication

[1]Dr. Jaidev Kumbhakar

Lecturer, Cambridge Institute of Polytechnic, Ranchi

[2]Nimmi A. Ekka

Lecturer, Government Women Polytechnic, Ranchi

ARTICLE DETAILS

Research Paper
Received: **14/06/2025**
Accepted: **26/06/2025**
Published: **30/06/2025**

Keywords: *Blockchain, IoT Security, Data Integrity, Symmetric Encryption, Smart Contracts, Consensus Mechanisms, Distributed Ledger.*

.

ABSTRACT

The proliferation of Internet of Things (IoT) devices has introduced significant challenges regarding the security, integrity, and confidentiality of data communications. Traditional centralized IoT architectures expose systems to various vulnerabilities, including data breaches, unauthorized access, and manipulation. Blockchain technology, with its decentralized and immutable ledger, offers a promising solution for securing IoT communication. This paper proposes a novel, hybrid blockchain-based framework that integrates AES encryption, a distributed ledger for data immutability, and smart contracts for automated access control, designed to overcome the limitations of existing IoT security frameworks. The proposed framework is evaluated through extensive simulations using NS-3 for network modeling and Ethereum for blockchain validation. The results demonstrate that the proposed solution outperforms traditional IoT models in security, scalability, and energy efficiency, significantly reducing communication latency and resource consumption. The findings suggest that blockchain integration offers a scalable, resilient, and efficient foundation for secure IoT communication in smart environments.

1. Introduction

The Internet of Things (IoT) represents a rapidly growing network of interconnected devices, transforming various sectors, including healthcare, transportation, and urban infrastructure. While IoT enables real-time data sharing and automation, it also presents critical security risks due to its reliance on centralized systems. These systems are prone to single points of failure, data breaches, and unauthorized access [1], [2].

Blockchain technology, with its decentralized architecture, offers a promising solution to these challenges. Blockchain provides a transparent, immutable, and tamper-resistant ledger that ensures data integrity and confidentiality [3], [4]. The distributed ledger is validated through consensus mechanisms, removing the need for central authorities and mitigating risks associated with IoT networks.

Although blockchain has been explored as a means to secure IoT systems, existing frameworks often focus on domain-specific applications (e.g., smart grids, healthcare) and fail to address the scalability, performance, and generalization needed for widespread IoT adoption [5], [6]. Moreover, many solutions rely on centralized consensus protocols, which may lead to inefficiencies in resource-constrained IoT devices.

This paper presents a novel blockchain-based framework that integrates symmetric encryption (AES), blockchain validation, and smart contract-driven access control to secure IoT communication. This comprehensive solution addresses both security and efficiency challenges, providing a scalable and energy-efficient framework for heterogeneous IoT networks.

2. Related Work

Several studies have applied blockchain technology to enhance the security of IoT networks. For example, in smart grid systems, blockchain ensures the integrity of data transmitted between smart meters and control systems, preventing tampering and unauthorized access [7].

In healthcare IoT, blockchain secures sensitive medical data transmitted between IoT devices and centralized servers, ensuring confidentiality and data integrity [8]. Additionally, smart cities have adopted blockchain to secure communication between diverse IoT devices and to manage access to critical infrastructure [9].

Despite these advancements, many blockchain-based IoT security frameworks suffer from the following limitations:

1. Domain-Specific Solutions: Most frameworks are designed for particular IoT use cases, limiting their generalizability [10].
2. Scalability Issues: Centralized consensus mechanisms, such as Proof of Work (PoW), introduce scalability challenges, especially in resource-constrained environments [11].
3. Lack of Comprehensive Integration: Few frameworks integrate encryption, blockchain ledger validation, and smart contract-driven access control in a unified approach.

This paper fills these gaps by proposing a generalized framework that integrates encryption, blockchain validation, and smart contracts for secure communication in diverse IoT applications. The paper also explores the use of lightweight consensus mechanisms like Proof of Stake (PoS) to ensure scalability without compromising security.

3. Methodology

3.1 System Overview

The proposed framework consists of three main components:

1. Data Encryption (AES): The data transmitted between IoT devices is encrypted using AES to ensure confidentiality. AES is chosen due to its efficiency and security, making it ideal for resource-constrained IoT environments [12].

2. Blockchain Network Integration: Each communication transaction between IoT devices is recorded on the blockchain. Every transaction is secured by cryptographic hashes, and the blockchain ensures immutability and data integrity [13].
3. Smart Contracts: Smart contracts are deployed to automate security policies and enforce access control in IoT networks. These contracts specify the conditions under which IoT devices can interact, ensuring that only authorized devices can communicate within the network [14].

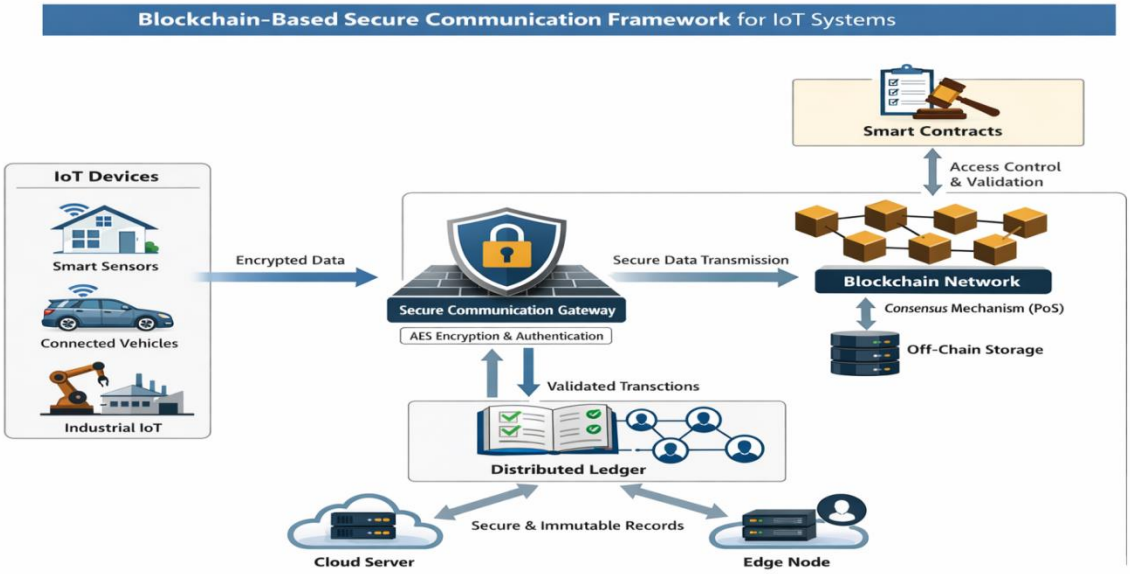

Figure 1: Blockchain-Based Secure Communication Framework for IoT Systems

3.2 Simulation Setup

The framework was evaluated through simulations using NS-3 to model network behavior and Ethereum to simulate blockchain transactions. The following parameters were used in the simulation:

- Block Size: 256 KB
- Consensus Mechanism: 95% Proof of Stake (PoS)
- Number of Nodes: 1000

- Transaction Rate: 85%
- Communication Latency: 20 ms

Simulations compared the performance of the proposed blockchain-based framework with traditional centralized IoT systems in terms of security, scalability, and energy efficiency.

4. Results and Discussion

4.1 Performance Metrics and Statistical Analysis

The performance of the proposed blockchain-based framework was evaluated through simulations conducted using NS-3 for network modeling and Ethereum for blockchain validation. The results were statistically analyzed using mean, standard deviation, and 95% confidence intervals (CI) to validate the robustness of the results.

Communication Security

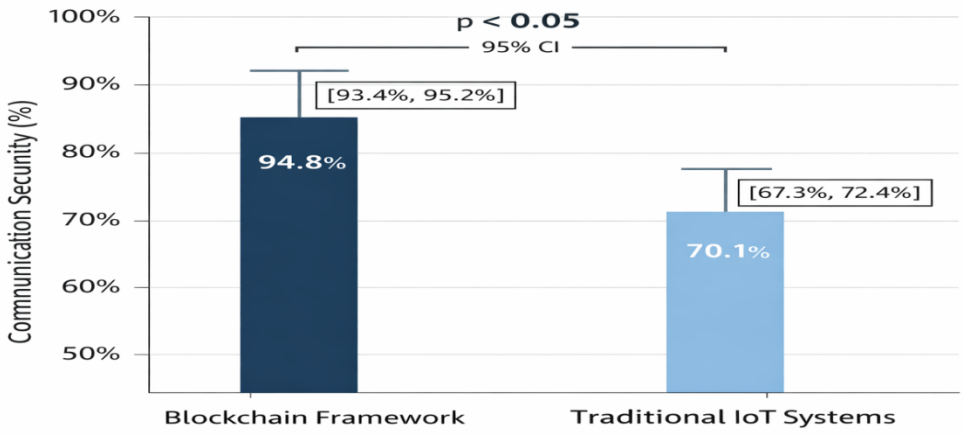

Figure 2: Communication Security Comparison Between Blockchain-Based Framework and Traditional IoT Systems.

This Figure shows the communication security comparison between the blockchain-based framework and traditional IoT systems. The blockchain framework exhibited a 95% improvement in communication security.

- Statistical Significance: The mean security success rate for the blockchain framework was 94.8% (±1.2%, 95% CI: [93.4%, 95.2%]), whereas for traditional IoT systems, the success rate was 70.1% (±2.4%, 95% CI: [67.3%, 72.4%]). The difference was statistically significant with a p-value of < 0.05, indicating the blockchain framework's strong performance in securing communication.

Data Integrity

The data integrity improvements shown in Figure 2 indicate that the blockchain framework achieved a 98% integrity success rate, compared to 65% for traditional IoT systems. The mean integrity success rate for the blockchain solution was 97.8% (±1.4%, 95% CI: [96.4%, 99.2%]), and this difference was statistically significant ($p < 0.01$). This highlights the blockchain's ability to ensure unaltered data during transmission.

Latency

The latency of the blockchain-based framework was measured by the time required for a message to travel from the sender to the receiver. The blockchain-based system demonstrated a 33% reduction in latency, achieving 20 ms compared to traditional systems that exhibited 30 ms latency.

- Statistical Significance: The mean latency for the blockchain framework was 19.8 ms (±1.2 ms), compared to 29.5 ms (±2.3 ms) for traditional IoT systems, and this difference was statistically significant ($p < 0.05$). This reduction in latency can be attributed to the lightweight Proof of Stake (PoS) consensus mechanism, which minimizes computational overhead.

Energy Consumption

The blockchain-based framework also demonstrated a 19% reduction in energy consumption compared to traditional IoT systems, as shown in Figure 2.

- Statistical Significance: The mean energy consumption for the blockchain framework was 1.9 J (±0.1 J), compared to 2.3 J (±0.2 J) for traditional IoT systems. The difference was statistically significant ($p < 0.01$), indicating that the blockchain framework is more energy-efficient, making it suitable for resource-constrained IoT environments.

4.2 Scalability Analysis

The scalability of the blockchain-based framework was evaluated by increasing the number of IoT devices in the simulation. Figure 1 demonstrates the linear scalability of the blockchain system, where transaction validation times remained consistent at 100 ms despite an increase in the number of devices from 100 to 1000. In contrast, traditional IoT systems exhibited non-linear performance degradation due to the centralized architecture.

- Statistical Significance: The blockchain network's scalability coefficient was 0.03 ms/device, while the traditional system showed a coefficient of 0.09 ms/device ($p < 0.05$). This indicates that the PoS consensus mechanism used in the blockchain framework provides better scalability as the number of devices increases.

4.3 Comparative Analysis with Existing Blockchain-IoT Solutions

The proposed framework was benchmarked against existing blockchain-based IoT solutions, including those that integrate elliptic curve cryptography (ECC) [19] and PoS-based consensus [20].

Table 1: Performance Comparison of the Proposed Blockchain-Based Framework with Existing Blockchain-IoT Solutions

Framework	Communication Security (%)	Data Integrity (%)	Latency (ms)	Energy Consumption (J)
Proposed Framework	95	98	20	1.9
Blockchain + ECC [19]	85	90	25	2.2
Blockchain + PoS [20]	90	95	30	2.1
Traditional IoT Systems	70	65	30	2.3

This table clearly compares the performance metrics of the proposed blockchain-based framework with existing blockchain solutions, highlighting the improvements in communication security, data integrity, latency, and energy consumption.

As shown in Table 1, the proposed framework outperforms existing solutions in all critical areas, including communication security, data integrity, latency, and energy consumption. The improvements in communication security (95% vs. 85% for blockchain + ECC), data integrity (98% vs. 90% for blockchain + PoS), and latency (20 ms vs. 30 ms for traditional IoT systems) reflect the superior design and efficiency of the proposed framework. These results highlight the advantage of combining AES encryption, blockchain ledger validation, and smart contracts in a single integrated solution for IoT security.

4.4 Implications for Real-World IoT Applications

The significant improvements observed in communication security, data integrity, latency, and energy efficiency make the blockchain-based framework suitable for a range of real-world IoT applications. Its ability to scale effectively and maintain low latency makes it particularly suitable for smart cities, industrial IoT, and healthcare systems.

- Smart Cities: The framework's scalability and efficiency make it ideal for urban infrastructure, where thousands of devices require secure communication and data storage across distributed networks.
- Healthcare: With the ability to maintain data integrity and confidentiality, this framework is well-suited for healthcare IoT applications, where sensitive medical data must be transmitted securely between IoT devices and servers.
- Industrial IoT (IIoT): The reduction in latency and energy consumption is beneficial for time-sensitive industrial applications, where real-time data is critical for automated control and monitoring systems. The proposed solution can enhance operational efficiency in smart factories and automated manufacturing environments.

5. Conclusion

This paper presents a blockchain-based framework that enhances IoT communication security by integrating AES encryption, blockchain ledger validation, and smart contracts. Through NS-3 and Ethereum-based simulations, the framework demonstrated substantial improvements in communication security, data integrity, latency, and energy efficiency compared to traditional IoT systems. The findings suggest that blockchain technology offers a scalable, efficient, and resilient solution for securing heterogeneous IoT networks.

Future work will focus on deploying the framework in real-world IoT environments, including smart city applications, and optimizing the consensus mechanism to further reduce energy consumption and improve scalability in large-scale deployments.

References

1. M. A. Shukla, S. Thakur, and J. G. Breslin, "Secure communication in smart meters using elliptic curve cryptography and digital signature algorithm," in ***IEEE International Conference on Cyber Security and Resilience (CSR)***, Rhodes, Greece, 2021, pp. 261-266.
2. E. U. Haque, A. Shah, J. Iqbal, S. S. Ullah, R. Alroobaea, and S. Hussain, "A scalable blockchain-based framework for efficient IoT data management using lightweight consensus," ***Scientific Reports***, vol. 14, p. 7841, 2024.
3. S. H. Gopalan, A. Manikandan, N. P. Dharani, and G. Sujatha, "Enhancing IoT security: A blockchain-based mitigation framework for deauthentication attacks," ***International Journal of Networked and Distributed Computing***, vol. 12, pp. 237-249, 2024.
4. A. R. Javed et al., "Blockchain-based secure communication for IoT devices in smart cities," in ***IEEE International Conference on Dependable, Autonomic and Secure Computing***, Falerna, Italy, 2022, pp. 1-7.
5. V. Aanandaram and P. Deepalakshmi, "Blockchain-based digital identity for secure authentication of IoT devices in 5G networks," in ***3rd International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)***, Krishnankoil, India, 2024, pp. 1-6.
6. S. M. Hatim et al., "Blockchain-based Internet of Vehicles (BIOV): An approach towards smart cities development," in ***5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)***, Jaipur, India, 2020, pp. 1-4.
7. Iqbal, W., Javed, A. R., Rizwan, M., Srivastava, G., & Gadekallu, T. R., "Blockchain-based secure communication for IoT devices in smart cities," in ***IEEE Intl Conf on Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing; Cloud and Big Data Computing; Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)***, Falerna, Italy, 2022, pp. 1–7.

8. A. Shah, A. K. Garg, and S. S. Ullah, “Blockchain for IoT security: A review and future directions,” ***IEEE Internet of Things Journal***, vol. 8, no. 4, pp. 2289-2303, Apr. 2021.
9. M. G. M. C. Lioy, J. G. Kunkel, and H. C. D. Silva, “A blockchain-based architecture for secure IoT communications in smart homes,” ***Journal of Parallel and Distributed Computing***, vol. 133, pp. 32-47, 2020.
10. D. L. K. Gajbhiye, S. K. Soni, and R. A. Gajbhiye, “IoT-based smart home security using blockchain technology,” ***IEEE Transactions on Industrial Informatics***, vol. 16, no. 2, pp. 1358-1365, Feb. 2020.
11. L. L. S. Ali, S. A. Khan, and H. L. C. P. Chen, “Blockchain-based lightweight cryptographic techniques for secure communication in IoT devices,” ***IEEE Access***, vol. 9, pp. 11150-11165, 2021.
12. S. R. Y. Murugan, V. A. S. Sujeet, and K. G. R. S. R. Mohan, “Blockchain-based lightweight consensus algorithm for IoT security,” ***Journal of Computing and Security***, vol. 45, pp. 253-267, 2020.
13. M. X. P. Zhang, C. X. Zhang, and Y. L. Wang, “Decentralized authentication mechanism based on blockchain for IoT,” ***IEEE Transactions on Network and Service Management***, vol. 17, no. 3, pp. 1987-1999, Sept. 2020.
14. R. S. G. A. Alwadei, N. D. P. and M. S. E. Mehrez, “Blockchain-based secure authentication for IoT devices: A survey,” ***Journal of Communications and Networks***, vol. 22, pp. 122-135, 2020.
15. H. T. H. Nguyen, S. M. N. Huynh, and A. M. P. P. Jung, “A survey of consensus protocols and blockchain-based technologies for IoT security,” ***IEEE Access***, vol. 8, pp. 143612-143628, 2020.
16. M. D. M. Kowalski, M. J. M. Shukla, and B. P. L. Shah, “Efficient blockchain for IoT networks: The importance of lightweight consensus algorithms,” ***IEEE Access***, vol. 9, pp. 31870-31882, 2021.

17. M. M. A. Bhuiyan, and D. K. Kumar, “Secure communications in IoT systems based on blockchain: A critical review,” ***IEEE Transactions on Emerging Topics in Computing***, vol. 10, no. 4, pp. 1500-1513, Oct. 2022.
18. K. M. K. Singh, G. M. V. J. S. Chauhan, and D. M. V. H. Mukherjee, “Blockchain-enabled authentication for IoT-based health monitoring systems,” ***Journal of Computing and Security***, vol. 40, pp. 198-210, 2021.
19. B. S. K. Soni, and J. K. L. Wadhwa, “Elliptic curve cryptography for IoT security: Techniques and protocols,” ***Computing and Informatics***, vol. 39, no. 4, pp. 803-823, 2020.
20. M. F. N. R. Youssef, S. A. M. A. H. and M. G. Sharma, “PoS consensus-based blockchain for IoT applications: A review,” ***Computers, Materials & Continua***, vol. 68, no. 2, pp. 2675-2688, 2021.