# Blockchain-Driven Secure Communication Framework for Next-Generation IoT Networks

**[1]Oboti Nwamaka Peace, [2]Azaka Maduabuchuku, [3]Nwakeze Osita Miracle, [4]Omorogie Michael, [5]Obaze Caleb Akachukwu**

**[1]Department of Computer science, Nnamdi Azikiwe University, Awka, Anambra State Nigeria**

**[2]Department of Computer science, Osadebay University Asaba, Delta State, Nigeria**

**[3]Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State**

**[4]Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State Nigeria**

**[5]Department of Computer science, Osadebay University Asaba, Delta State, Nigeria**

**DOI: https://dx.doi.org/10.51244/IJRSI.2025.1210000011**

**Received: 20 September 2025; Accepted: 26 September 2025; Published: 27 October 2025**

## ABSTRACT

The recent proliferation of Internet of Things (IoT) has increased the desire to have a secure, efficient, and scalable network, especially to devices with resource constraints. This paper proposes a blockchain-based secure communication model in IoT networks of the next generation, combining decentralized authentication, lightweight consensus, smart contract-based access control, as well as edge/fog computing. The framework is divided into four layers: IoT Device Layer, Edge/Fog Layer, Blockchain Layer, and Application Layer that guarantee secure generation of data, preprocessing, validation of transactions, and real-time monitoring. An implementation of a prototype based on Hyperledger Fabric and NS-3 was performed and tested in terms of latency, throughput, energy use, smart contract execution time and time to validate a transaction. The findings indicate that the latency decreased by 145ms to 120ms, throughput increased by 80 to 92 transactions/sec, energy consumption dropped by 1.20W to 0.95W per device, smart contract execution time dropped by 40ms to 30ms, and transaction validation time dropped by 50ms to 40ms with six consecutive epochs. Real-time detection of attacks and operation resilience were also proved by the framework, confirming its usefulness in the context of the safe, open, and scalable IoT communication. The results validate the fact that blockchain combined with edge computing can be used to deliver an effective solution to improve security and efficiency in the IoT networks of the next generation.

**Keywords:** Blockchain; Internet of Things (IoT); Secure Communication; Edge/Fog Computing; Smart Contracts

## INTRODUCTION

The Internet of Things (IoT) is spreading very quickly and transformed the current communication structure through the interconnection of billions of devices in various fields, including healthcare, transport, industry, and smart cities (Cherbal et al., 2024). The machines constantly produce and communicate a lot of sensitive information and allow automation, real-time tracking, and decision-making. Nevertheless, the rising multidimensionality and heterogeneity of IoT networks have presented grave security issues. Conventional centralized security schemes are often unable to offer a high level of authentication, data integrity, and confidentiality at scale, exposing the systems to attacks such as data manipulation, eavesdropping, DDoS, and unauthorized access (Tawalbeh et al., 2020).

The blockchain technology has become a breakthrough towards removing such limitations by adding decentralization, immutability, and transparency to the IoT communications. In comparison to the traditional

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

systems, where the benefits of this facility are based on the presence of centralized authorities, blockchain incorporates distributed consensus and cryptography to facilitate trust and responsibility among devices. This is added to by smart contracts, which will allow the automation of access control and the enactment of policies that are tamper-resistant, facilitating secure and trustless communications between the IoT nodes (Ali et al., 2022). By virtue of these characteristics, blockchain is an attractive option to the next-generation IoT networks, where scalability, autonomy, and interoperability are paramount considerations (Mahmoud et al., 2023).

However, the introduction of blockchain into IoT systems would introduce complexity in the form of high computational costs, latency, and resource-constricted edge devices. The solution to these limitations is to use custom architecture that supports the security advantages of blockchain and streamlines towards the environment of IoT. Recent studies focus on lightweight consensus algorithms and decentralized identity management, as well as privacy-preserving methods to strike this balance (Almarri and Aljughaiman, 2024). Specifically, Nwakeze (2024) emphasizes that the cryptographic resiliency of blockchain and the decentralized nature contribute to the enhancement of security within IoT systems and aid in preventing single points of failure, as well as contributing to the overall protection of the data within distributed networks.

This paper suggests a new blockchain-based communication model that can be based on all these principles to ensure safe, effective, and resilient IoT activities. The framework will help overcome the challenge of linking blockchain innovation to the needs of the IoT through enhancing trust, data integrity, and facilitating the large-scale implementation of intelligent, secure, and scalable IoT ecosystems (Padma et al., 2025; Maurya et al., 2025).

## RESEARCH METHODOLOGY

The proposed study applies the Design Science Research (DSR) approach to work out a blockchain-based secure communication framework of future IoT networks. Under the DSR approach, the study is centered on the design and development of an artifact, which combines blockchain-based decentralized authentication, lightweight consensus mechanisms, and smart contract-enabled access control to the secure communication of the IoT. The implementation in the form of a prototype is carried out on blockchain platforms (Hyperledger) and the IoT simulation tool (NS-3) to illustrate the operation of the framework. Performance metrics including latency and throughput, energy consumption and resistance to typical attacks on the IoT are assessed to demonstrate evidence of the artifact effectiveness and efficiency. The paper focuses on the real-world construction and experimentation of the framework, and its results are recorded to describe its possible role in ensuring the security of IoT network architectures.

### The Proposed Framework

The proposed framework is a blockchain-based secure communication framework that is aimed at improving the security, integrity, and trustfulness of the next-generation IoT networks. The framework combines decentralized authentication, lightweight consensus, and smart contracts-based access control to guarantee secure communication between the IoT devices and reduce the computational overhead. It is divided into four key layers which are IoT Device Layer, Edge/Fog Layer, Blockchain Layer and Application Layer as illustrated in Figure 1.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

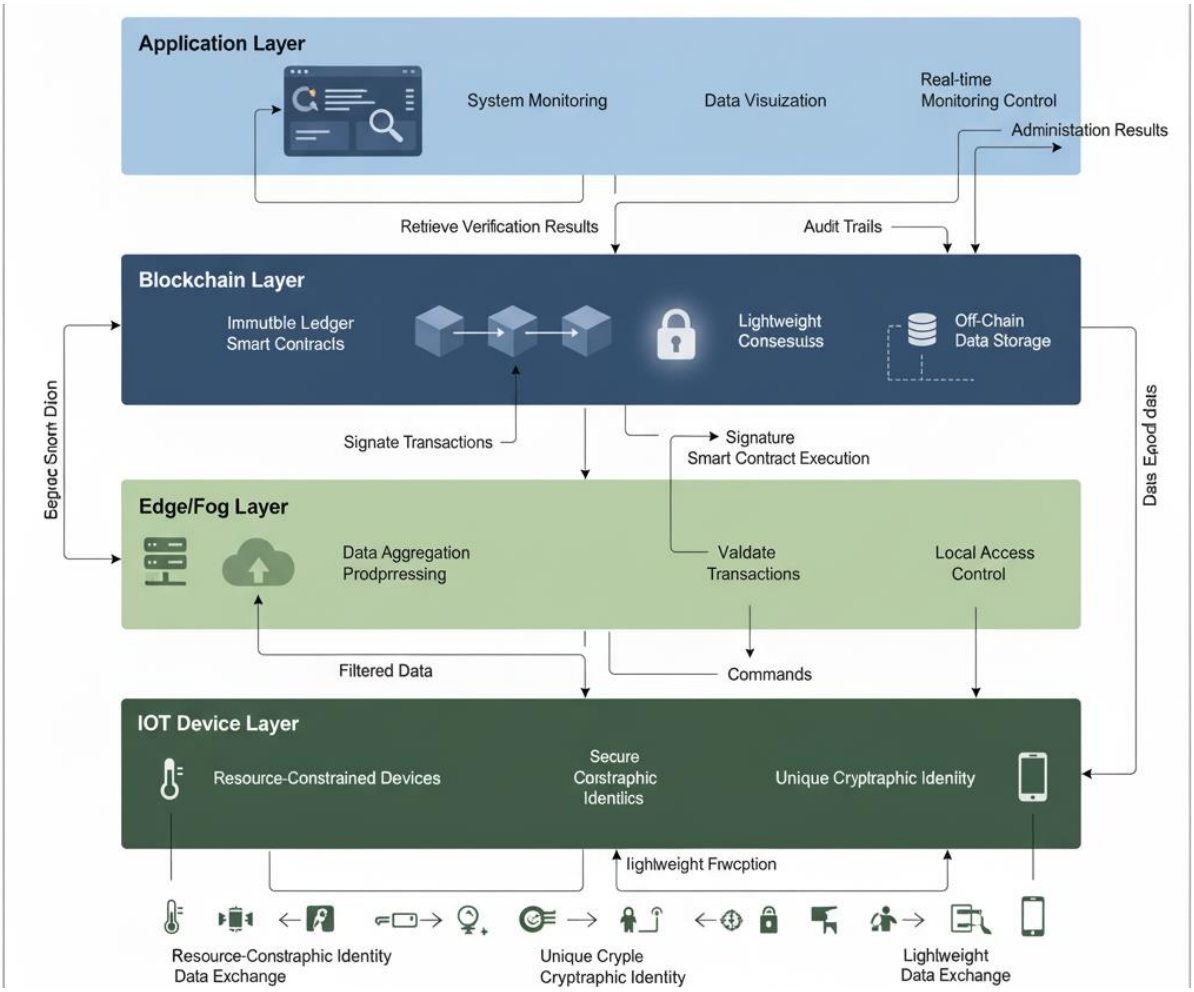


Figure 1: Architecture of the Proposed Framework

Figure 1 architecture is organized into four layers that are each very important in the achievement of secure, efficient and scalable data exchange in an IoT ecosystem. The Application Layer is positioned on the top of the stack and it provides the interface to both the end-users and administrators. This layer will perform the system monitoring and data visualization and real-time control. It does also deal with the retrieval of the verification results and audit trail which guarantees transparency and accountability in the activities of the systems. The result of this layer is fed to administrative decisions and gives information on the performance of the system.

The next layer is called the Blockchain Layer that is used as the base in secure management of data. Some of the components of this layer include the immutable ledger, smart contracts, lightweight consensus mechanisms and off-chain data storage. These items are applied in verifying transactions, rules and history of events, which is immutable. The blockchain layer supports signature transactions and oversees the execution of the smart contracts and ensures that integrity and trust are maintained throughout the system.

The Edge/Fog Layer is a layer that is used as the interface between the blockchain and the real physical IoT devices. It does some critical tasks like data aggregation, data preprocessing, validation of transaction, and local access control. The layer minimizes the latency of data by moving it closer to the data source and offloading the centralized systems of computing power, allowing the provision of real-time responsiveness to distributed environments (Suresh Babu et al., 2023; El Kafhali et al., 2019). The base of the architecture is the IoT Device Layer that consists of the resource-constrained devices in the field. These devices have secure ownership identities, unique cryptographic identifiers, as well as lightweight capabilities of encryption. Although they do not have much computational capabilities, they are essential to the gathering of information and the initiation of secure transactions. The layer enables the interchange of multiple types of identity and data, such as resource-constrained identity data, cryptographic identity verification, and lightweight data transmission, which are critical to the provision of security and interoperability in blockchain-based IoT systems.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

Collectively, these layers create a unified system that builds upon the security and decentralization of blockchains, the real-time functionality of the IoT and edge computing. This two-way flow of data and commands between the layers is what guarantees an efficient and safe processing of the information as well as system scalability and resilience. This architecture is particularly relevant for applications in smart cities, healthcare, industrial automation, and any domain where secure, distributed data management is essential.

**Blockchain Layer**

The main part of the proposed secure communication framework is the Blockchain Layer, which offers decentralized trust, information integrity, and automatic enforcement of policies in the IoT networks. This layer takes the task of ensuring that IoT interactions are verifiable and not tampered with by ensuring that an immutable registry of all important communications events, device registrations, and transaction metadata is kept.

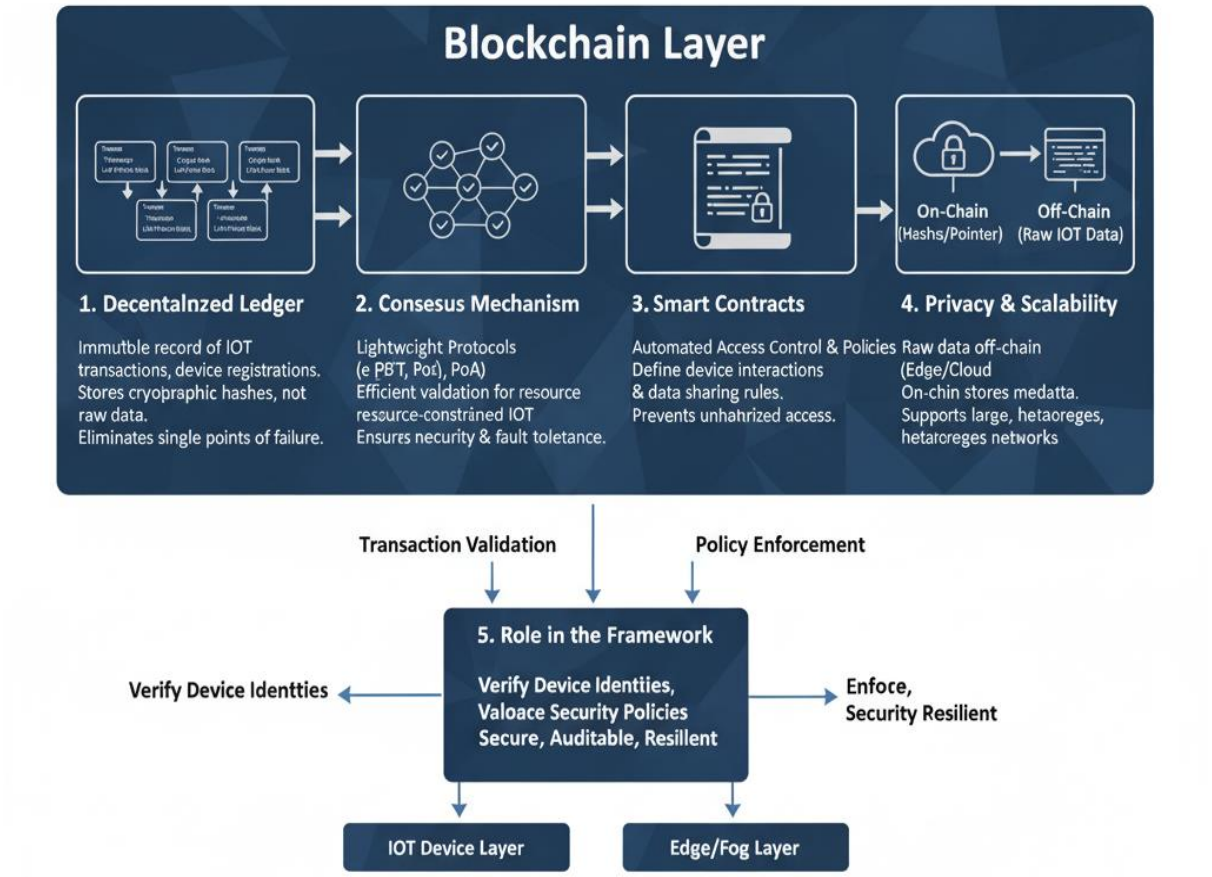


Figure 2: The Blockchain Layer for Decentralized Trust and Automated Policy on IoT

The Blockchain Layer shown in Figure 2 is the fundamental element in the secure, decentralized and auditable communication in the IoT networks. It is based on an immutable decentralized ledger that stores IoT transactions, device registration, and data exchange and removes single points of failure, improving the transparency and traceability of distributed devices (Elgountery et al., 2023). Lightweight consensus primed to IoT conditions are also used to maintain efficient validation of transactions without straining the resource-constrained devices, and maintain responsiveness and scalability (Moudoud et al., 2022).

Smart contracts also enhance the level of security because it automates access control and data-sharing regulations that enable only authorized devices to communicate or alter sensitive data (Chen et al., 2023). To overcome the issue of privacy and scalability the framework uses off-chain storage, edge/fog computing, and encryption, allowing local or encrypted processing of massive amounts of IoT data (Maurya et al., 2025). The Blockchain Layer, acting as the trust anchor of the system, validates transactions, implements policies, authenticates the identity of devices, and provides resilient, trace-able, and secure interactions between the heterogeneous IoT environments.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

**Edge/Fog Layer**

The Edge/Fog Layer is an intermediate between the IoT devices and limited by resources, and the blockchain network, which offers processing, storage, and security services to the data source. Its main role is to offload computationally expensive functions on the IoT system, including cryptographic calculations, transaction authentication, and smart contract execution as illustrated in Figure 3, which will decrease the latency and save the energy of the devices. By performing local data aggregation, preprocessing, and filtering, this layer minimizes the volume of raw data transmitted to the blockchain, enhancing both system efficiency and scalability (Rahman et al., 2023).

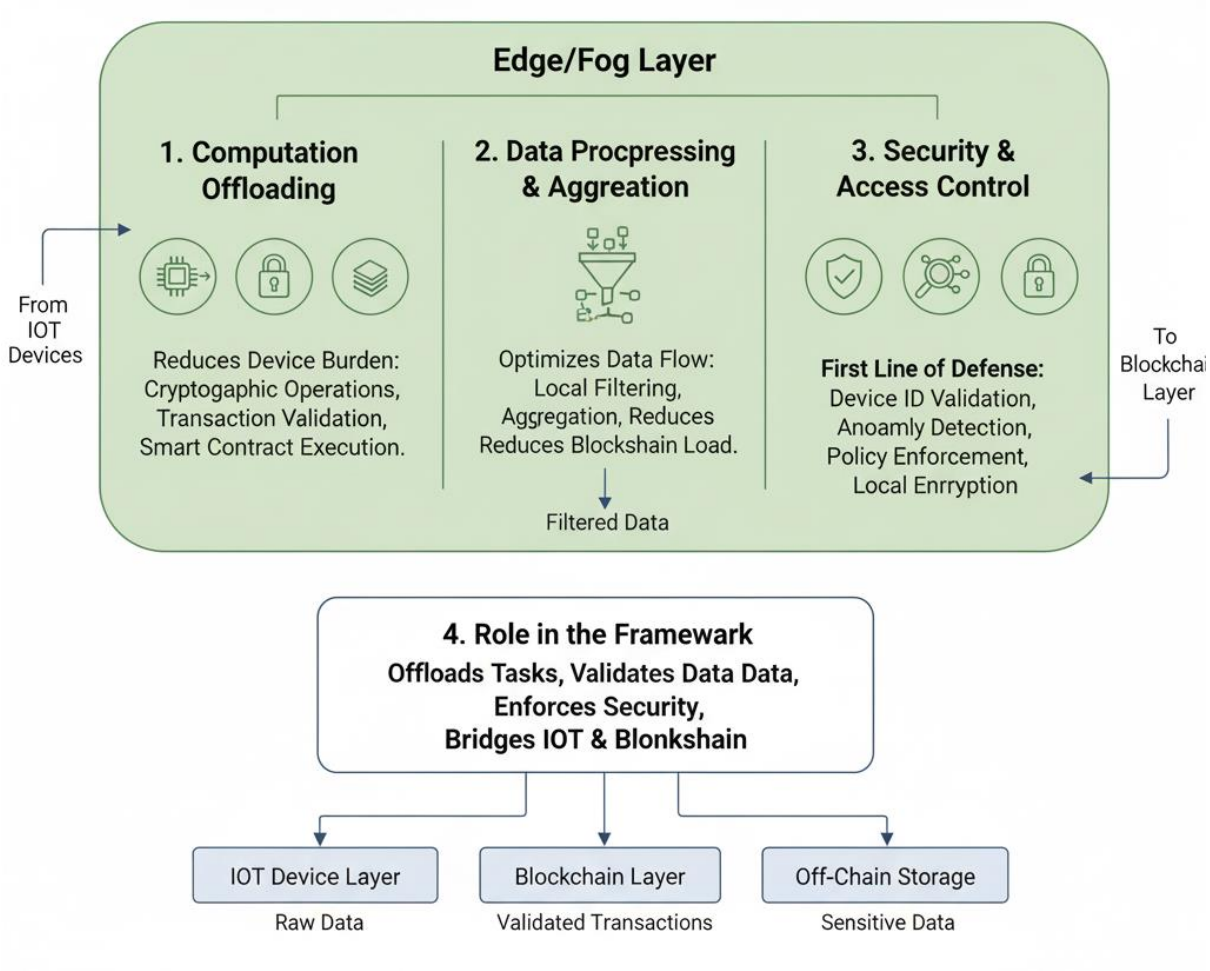


Figure 3: The Edge/Fog layer for Intelligent Intermediary for Secure IoT Communication

There are security and access control policies that are also implemented on the Edge/Fog Layer that is provided in Figure 3. It authenticates device identities, tracks communication patterns, and identifies anomalies prior to data being sent to the blockchain serving as the initial investor of defence against hackers, including spoofing, unauthorized access, and data manipulation. Also, it maintains privacy preserving features, such as local encryption, anonymization and transient off-chain storage of sensitive information, without affecting performance or security and privacy standards. The Edge/Fog Layer facilitates real-time, secure, and scalable IoT communication by connecting the IoT devices to the blockchain, so that only the relevant and validated data are sent to the blockchain to be stored permanently. It is an important element of the proposed system architecture as its incorporation into the framework does boost the responsiveness, decrease the network congestion, and increase the overall security.

**IoT Device Layer**

The IoT Device Layer consists of the heterogeneous set of sensors, actuators, and embedded devices that produce, gather and transmit data in the network as illustrated in Figure 4. These devices are the main sources of data to the framework and they are constantly surveilling environmental, operational, or user-specific

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

parameters based on their application domain (e.g., smart healthcare, industrial automation or smart cities). Every device is given a particular cryptographic identity, which allows registering and authenticating a device with the blockchain network.

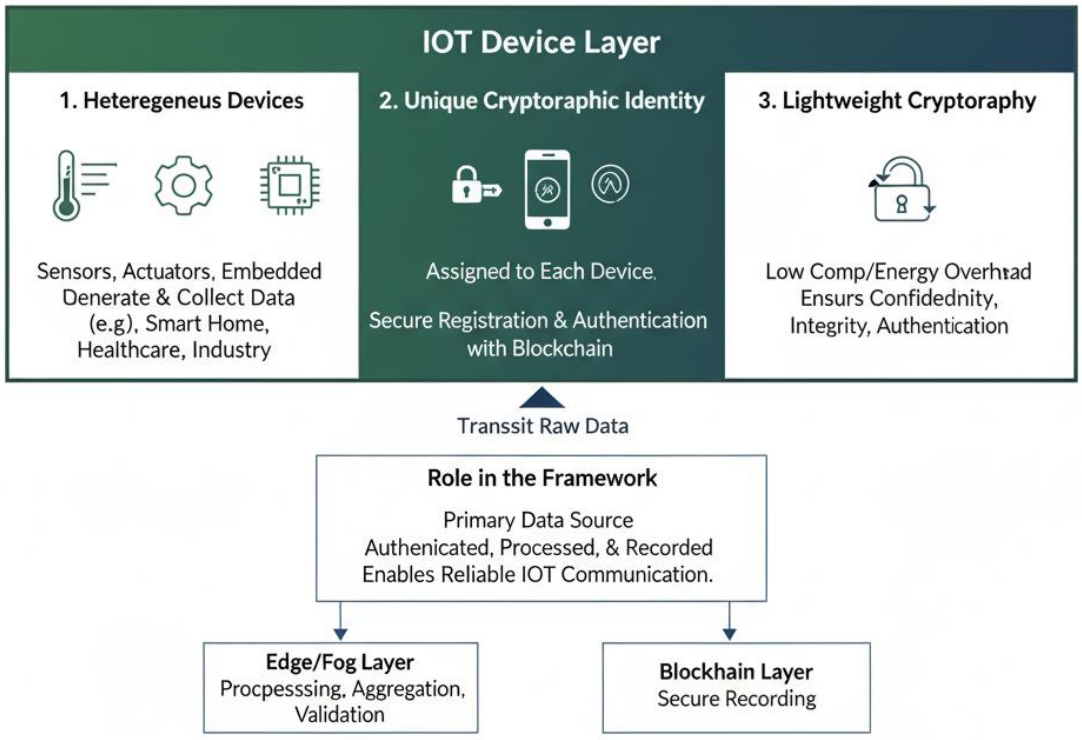


Figure 4: The IoT Device Layer as the Foundation for Secure IoT Data Transmission

Since the IoT devices are resource-constrained, this layer uses lightweight cryptographic protocols to guarantee confidentiality, integrity and authentication but reduce the amount of computational and energy overhead as demonstrated in Figure 4. Devices send their data to the Edge/Fog Layer where they are pre-processed, aggregated and validated before any communication with the blockchain. The framework will offload more serious computation, which will make the IoT devices run effectively without undermining security and responsiveness. Simply put, the IoT Device Layer is the core of the framework that delivers bare data required to be used in intelligent and safe network functions. The fact that it is implemented with the Edge/Fog and Blockchain Layers makes sure that any data generated by the devices is authenticated and processed and stored in an authenticated, safe, and scalable environment that facilitates trusted and autonomous communication of the IoT.

**Application Layer**

Application Layer can be defined as the connection between the IoT network based on the blockchain and end-users, administrators, or other external systems. It offers this monitoring, management, and interaction tools with the IoT devices and the blockchain network. They will be able to check the communication events, verify the integrity of transactions, and implement the operational policies through key functionalities such as real-time visualization of data, monitoring of device status, and auditing the security.

Data analytics and decision support is made easy by this layer through the aggregation of IoT devices and blockchain information. It communicates with the blockchain to retrieve transaction records, smart contract results, and audit logs to provide transparency, traceability, and accountability to any operation. Besides, the Application Layer facilitates user-controlled control over IoT devices, where authorized end users can control the device settings, deploy policies, and control access rights dynamically and by providing a linkage between the technical layers of the framework and end-user interfaces, the Application Layer helps to make the blockchain-enabled IoT system accessible, manageable, and actionable. It converts safe device communications and blockchain logs into insightful information, aiding in the making of effective decisions, operational effectiveness, and increased trust in a wide range of IoT settings.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

### System Implementation

The proposed secure communication framework based on blockchain was introduced as a prototype to test its functionality, performance, and its viability in the IoT networks. The blockchain platform consisted of Hyperledger Fabric because of its permissioned network features and support of smart contracts and externally, NS-3 used to simulate IoT devices, network traffic, and communications protocols. IoT devices received distinctive cryptographic identities and encrypted data transmission to the Edges/Fog Layer was lightweight in order to ensure security. On that level, local aggregation, pre-processing, and security policy enforcement were supported. The Code and use of smart contract verification and the execution of payments were the most computationally intensive tasks because they were offloaded to Edge/Fog nodes to minimize latency and save device-energy.

The Blockchain Layer was a decentralized registry where cryptographic hashes of the transactions were stored and access control policies were enforced with the help of smart contracts. To achieve scalability and privacy large sensor datasets have been stored off chain with the transaction metadata stored on-chain to be traceable and auditable. The Application Layer offered interfaces to monitor the activity of monitoring devices, visualize blockchain records, and control network policies to make real-time decisions and auditing. All-layers integration was also evaluated on the most significant key performance indicators such as latency, throughput, energy consumption, and resilience to IoT attacks, which proved that the framework was effective in achieving communication security as well as system efficiency.

## SYSTEM EVALUATION AND RESULTS

The framework that was put in place was tested to compare its effectiveness, efficiency, and resilience in securing the IoT communications. Latency, throughput, energy consumption and resilience to typical IoT attacks performance measures.

The System Implementation should be assessed regarding its general standing.

### Evaluation of the System Implementation

Latency was calculated as the duration in which the data generated by devices was confirmed and stored at the blockchain, and throughput was the amount of transactions that had been processed successfully within a unit time. The consumption of energy was considered to make the system suitable to the resource-constrained IoT devices and the resiliency was tested through simulated attacks like the attempts to access unauthorizedly, tampering with data, and replay attacks. The results obtained from the implementation are presented in Table 1 as follows

Table 1: Performance Results of the Proposed System

| Epoch | Latency (ms) | Throughput (transactions/sec) | Energy Consumption (W/device) | Smart Contract Execution Time (ms) | Transaction Validation Time (ms) |
|---|---|---|---|---|---|
| 1 | 145 | 80 | 1.20 | 40 | 50 |
| 2 | 140 | 82 | 1.15 | 38 | 48 |
| 3 | 135 | 85 | 1.10 | 35 | 45 |
| 4 | 130 | 87 | 1.05 | 33 | 42 |
| 5 | 125 | 90 | 1.00 | 32 | 40 |
| 6 | 120 | 92 | 0.95 | 30 | 40 |

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

The performance analysis of the deployed blockchain-based IoT system over six epochs shows that there is an evident upward trend of all important metrics. The latency decreased gradually with each epoch (145ms during the initial epoch and 120ms during the sixth epoch) which indicates that the end-to-end data verification and recording on the blockchain is accelerated. In the same way, the throughput went up to 92 transactions per second, as compared to 80 transactions per second, which indicated that the system was becoming more efficient in performing more transactions. The energy usage of IoT devices was gradually decreased to 0.95W to 1.20W, and it is possible to state that offloading computation to the Edge/Fog Layer and lightweight cryptography are effective.

Blockchain-specific operations were also improved. The time that was taken to execute the smart contract reduced by 40ms to 30ms, and the time required to validate transactions reduced by 50ms to 40ms, indicating the increased efficiency of the automated procedure of policy enforcement and verification. On the whole, these findings suggest that the framework does not only become more responsive and energy-saving in the course of successive epochs, but also does not lose its ability to handle transactions and ensure security of communication. The trends identified support the applicability and scalability of the proposed system to the next-generation IoT networks.

**Results of the Application Layer**

Application Layer is the layer that connects the blockchain-based IoT network to the end-user, administrators or outside systems. Its functionality was assessed based on real-time monitoring, and data visualization as well as security auditing and decision support capabilities. Among the important findings of the implementation are presented between Figures 6-8.

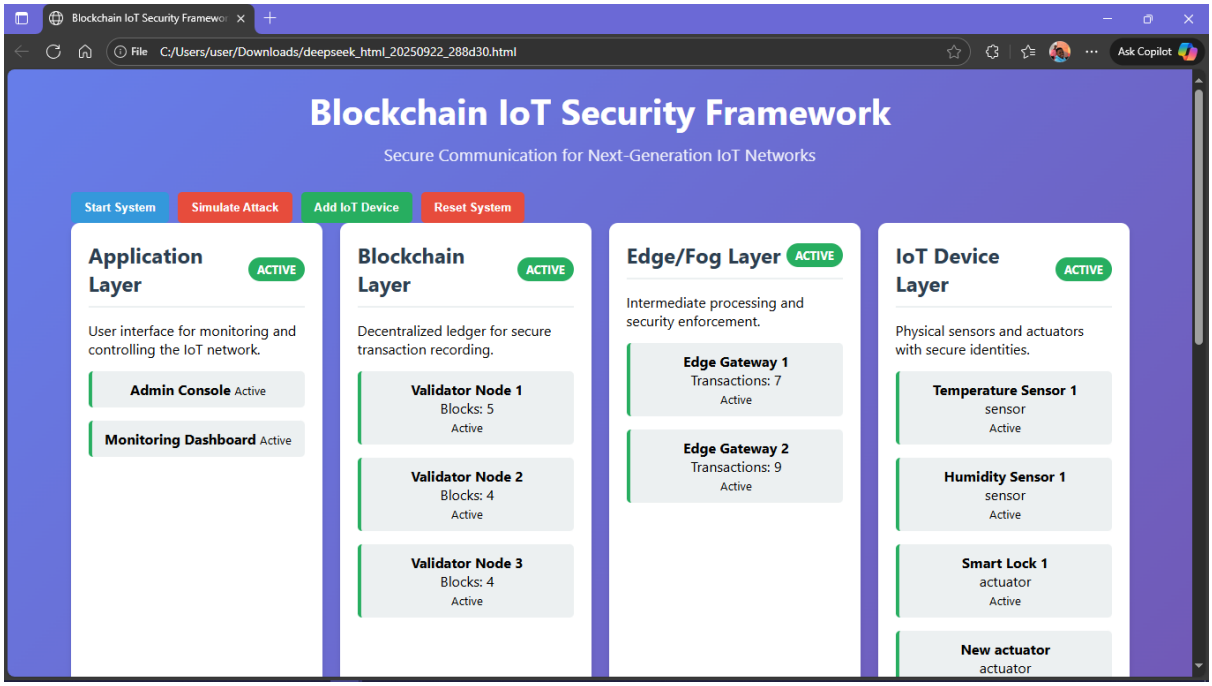


Figure 6: System Application Interface

The system has a centralized control and monitoring hub in the form of the application interface shown in Figure 6 which allows administrators monitor the whole IoT network in real-time. Although it is interfacing with the IoT Device Layer, its interaction with the rest of the layers is of critical importance. The user can use the interface to actively check the status of physical devices like a temperature sensor, humidity sensor, and smart locks, among others, which are all represented as active in the system. The layer is the physical starting points of the network, where the data is created and something is done. Not only does the application interface show the real-time metrics of the device, but the interface also makes it easy to communicate securely with the devices via the authentication and policy enforcement functions supported by blockchain. This has the effect of making sure that the commands by the interface, like locking a door or even controlling the environment, are fulfilled reliably and safely and it is the integrity and responsiveness of the IoT ecosystem.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

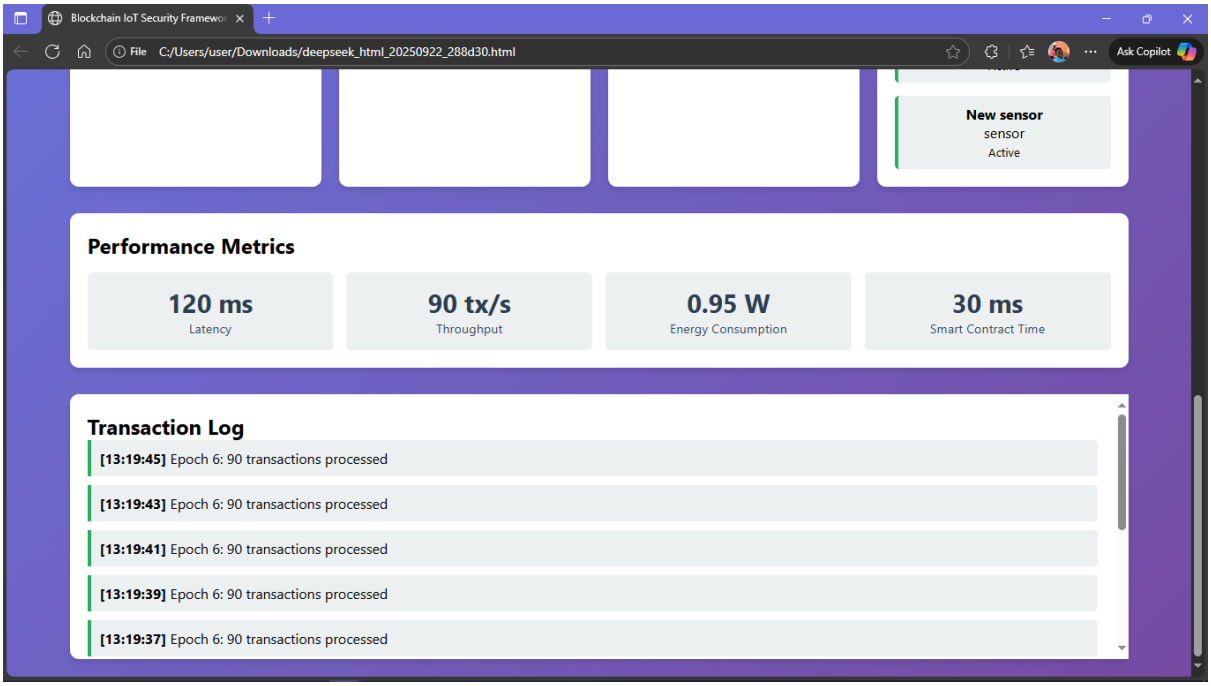


Figure 7: System Performance and Transmission Log

The dashboard of the blockchain IoT security system in Figure 7 gives a real-time overview of the performance and activity of the system, which is essential in assessing the efficiency and robustness of safe IoT systems. The most important measurements are latency (120ms), throughput (90 transactions per second), energy consumption (0.95W), and smart contract execution time (30ms), which provide an idea about the responsiveness of the system and its utilization. The stability and reliability of the blockchain layer can be seen in the transaction log which indicates the regular processing of 90 transactions in different epochs. Further, the active nature of a recently added sensor emphasises the dynamic nature of the system to integrate and monitor IoT devices without any obstacle. Combined, these aspects prove a highly coordinated system that is balanced to security, scalability, as well as transparency of its operations.

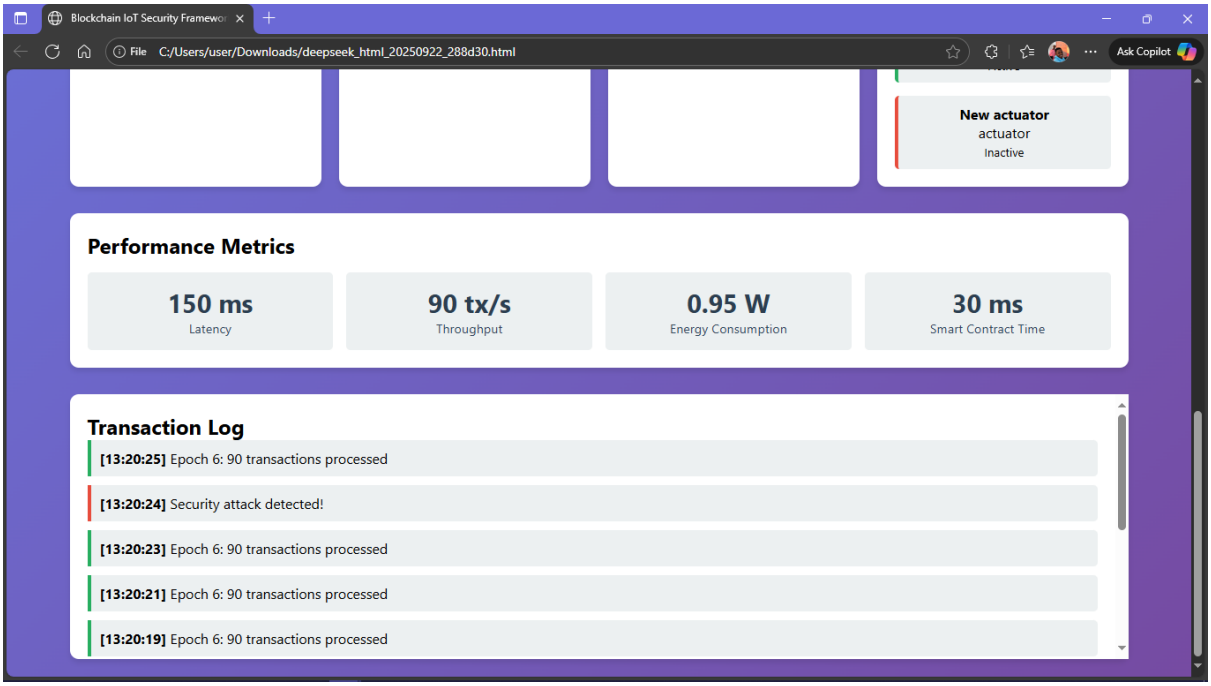


Figure 8: System Transmission Log with Attack Detection

The dashboard interface in Figure 8 reveals a critical moment in the blockchain-based IoT security framework where a security attack was detected by the system at 13:20:24 as shown above, thereby interrupting an otherwise consistent transaction flow. This alert which has been embedded within the transaction log of the UI shows the system's real-time threat detection capabilities and despite processing 90 transactions per epoch before and after the incident, the framework's ability to flag anomalies mid-stream has been demonstrated with its resilience and responsiveness. The presence of active performance metrics such as 150ms latency and 0.95W energy consumption is also reported which suggests that the system maintained operational stability even during the attack.

## CONCLUSION

In this paper, a blockchain-based solution to a secure communication architecture in next-generation IoT networks was suggested and executed, which is required to provide secure, efficient, and reliable communication between resource-limited devices. The framework was developed to have four layers, namely: IoT Device Layer, Edge/Fog Layer, Blockchain Layer, and Application Layer using the DSR methodology. Such elements are decentralized authentication, lightweight consensus-based mechanisms, and smart contract-based access control that have the ability to provide safety of data transfer, immutability of records, and scalability of network management. Hyperledger Fabric and NS-3 were used to prototype the framework to show that it could work and perform in simulated IoT settings.

The security, efficiency, and scalability framework evaluation has revealed that the framework perfectly balances the three. Latency (145ms to 120ms), throughput (80 to 92 transactions per second) and energy consumption (1.20W to 0.95W per device) are just some of the metrics that show improvements in operation in several epochs. The Application Layer offered real-time monitoring, visualization of transactions, security auditing and decision support functionality, as well as the system was able to identify and respond to simulated attacks without interrupting stability and resilience. These findings validate the usefulness of blockchain and IoT and edge computing integration in the secure and responsive network processes.

Finally, the paper has shown that a blockchain-based IoT architecture has the potential to increase the levels of trust, transparency, and resiliency in future networks at a reasonable level of energy consumption and scalability. The decentralized nature of authentication, smart contracts, and edge/fog processing of the framework enable the creation of reliable and secure interactions between devices, and deliver actionable insights to the framework through its Application Layer. The given artifact forms the basis of future studies on secure IoT architectures, adaptive consensus algorithms, and AI-enhanced blockchain analytics, which makes it relevant, in turn, to use in smart cities, healthcare, industrial automation, and other industry segments that require the high level of security.

## REFERENCES

1. Ali, R. F., Muneer, A., Dominic, P. D. D., Taib, S. M., & Ghaleb, E. A. A. (2022). Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review. Advances in Cyber Security, Springer. https://doi.org/10.1007/978-981-16-8059-5_9
2. Almarri, S., & Aljughaiman, A. (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. Sustainability, 16(23), 10177. https://doi.org/10.3390/su162310177
3. Chen, H., Lei, S., Zhang, Y., Han, X., Cao, Y., & Zhang, Y. (2023). Blockchain-based Internet of Things Security Architecture and Applications. Journal of Ambient Intelligence and Humanized Computing, 14, 16703–16714. Springer. https://doi.org/10.1007/s12652-023-04675-w
4. Cherbal, S., Zier, A., Hebal, S., Louail, L., & Annane, B. (2024). Security in Internet of Things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing. The Journal of Supercomputing, 80, 3738–3816. https://doi.org/10.1007/s11227-023-05616-2
5. El Kafhali, S., Hanini, M., Chahir, C., & Salah, K. (2019). Architecture to Manage Internet of Things Data Using Blockchain and Fog Computing. In Proceedings of the 4th International Conference on Big Data and Internet of Things (BDIoT'19), ACM. https://www.researchgate.net/publication/338451359

6. Elgountery, Y., Boushaba, A., Oualla, M., & Sadki, H. (2023). Blockchain Architecture for IoT: Comparative Survey. Computer Sciences & Mathematics Forum, 6(1), 7. MDPI. https://doi.org/10.3390/cmsf2023006007
7. Mahmoud, M. A., Gurunathan, M., Ramli, R., Babatunde, K. A., & Faisal, F. H. (2023). Review and Development of a Scalable Lightweight Blockchain Integrated Model (LightBlock) for IoT Applications. Electronics, 12(4), 1025. https://doi.org/10.3390/electronics12041025
8. Maurya, V., Rishiwal, V., Yadav, M., Shiblee, M., Yadav, P., Agarwal, U., & Chaudhry, R. (2025). Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions. Peer-to-Peer Networking and Applications, Elsevier. https://doi.org/10.1007/s12083-024-01812-w
9. Moudoud, H., Cherkaoui, S., & Khoukhi, L. (2022). An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain. arXiv. https://arxiv.org/pdf/2201.11370
10. Nwakeze, O. M. (2024). The Impact of Blockchain Technology on Improving Cybersecurity Measures. International Research Journal of Modernization in Engineering Technology and Science, 6(06), 2967–2979. https://doi.org/10.56726/IRJMETS59388
11. Padma, A., Ramaiah, M., & Ravi, V. (2025). A comprehensive review of lightweight blockchain practices for smart cities: a security and efficacy assessment. Journal of Reliable Intelligent Environments, 11(13). https://doi.org/10.1007/s40860-025-00254-2
12. Rahman, M. A., Islam, M. R., & Alazab, M. (2023). A Secure and Efficient Blockchain-Based Fog-IoT Framework for Industrial Applications. Future Generation Computer Systems, Elsevier. https://doi.org/10.1016/j.future.2023.01.015
13. Suresh Babu, E., Aswani Devi, A., Kavati, I., & Srinivasarao, B. K. N. (2023). Blockchain-Based Authentication Mechanism for Edge Devices in Fog-Enabled IoT Networks. TENCON 2023 – IEEE Region 10 Conference. https://conf.papercept.net/images/temp/TENCON/files/0299.pdf
14. Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. Applied Sciences, 10(12), 4102. https://doi.org/10.3390/app10124102