INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

An Intelligent Blockchain Framework for Secure Communication in IOT Environments

Neeraj Kumar Gautam[1], Sharad Kumar[1], Md. Arif[1]

[1]School of Engineering & Technology, Shri Venkateshwara University, Gajraula, Uttar Pradesh, India

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150500274

Received: 29 May 2026; Accepted: 03 June 2026; Published: 24 June 2026

ABSTRACT

IOT (Internet of Things) is rapidly expanding with the creation of smart environments around agriculture, healthcare, industrial automation and transportation. However, as the number of sensitive data exchanges between different IoT devices increases, the number of privacy and security challenges is also growing. These challenges include unauthorized access to, or tampering of, data; identity spoofing; and cyberattacks. Most traditional security models are centralized and are either too slow due to their inherent scalability limitations or possess a single point of failure which makes them unsuitable for IoT ecosystems of a large-scale and dynamic nature. This intelligent framework will allow for decentralized blockchain architectures coupled with intelligent security mechanisms to provide for secure, transparent, and tamper-proof communications between devices on the Internet of Things as well as those on IoT networks. The framework will use ledger-like technology, smart contracts, lightweight encryption techniques, and intelligent authentication to increase the integrity of data, preserve the privacy of that data, and create trust management options among all devices connected by their respective IoT networks. Edge-enabled blockchain processing will also be included within the framework to reduce the computational overhead in processing transactions and to increase the efficiency of real-time communications. The experimental analysis of the intelligent blockchain framework will demonstrate how it can substantially improve security for communication over other forms of conventional IoT security models and reduce risk of unauthorized access to information, increase reliability in the transaction process, and decrease vulnerabilities to each network compared to other traditional models of security in the Internet of Things.

Keywords: Internet of Things (IoT), Blockchain Technology, Secure Communications, Smart Contracts, Edge Computing, Cybersecurity, Distributed Ledger, Data Privacy, Authentication.

INTRODUCTION

Digital communication technologies and smart computing systems are advancing rapidly, which has accelerated the development of the Internet of Things (IoT) on many fronts such as healthcare, industrial automation, smart transportation, agriculture, environmental surveillance and smart city infrastructures. IoT allows devices to interact with each other and exchange information to perform automated intelligent processes by allowing ongoing communications between devices, sensors & data sharing. An increasing amount of IoT devices have created highly connected, data-rich environments that demand reliable, scalable and secure communication mechanisms to facilitate efficient performance of systems and trustful exchange of information between all parties. In spite of the many benefits offered by IoT systems, security and privacy issues represent significant and ongoing challenges to the current state of IoT ecosystems. Most IoT devices communicate over open, distributed networks through the use of publicly available frequency bands, which results in a large volume of sensitive data being transmitted constantly among devices, gateways, edge nodes and cloud systems. Due to limitations of a centralised security architecture (i.e., single points of failure or lack of transparency) and cyber-attacks (e.g., data tampering, identity spoofing, Denial-of-Service attacks, unauthorised access, and malicious intrusions) traditional centralised security approaches are not capable of protecting IoT ecosystems. Moreover, the resource-constrained nature of IoT devices means that complex protection mechanisms cannot readily be implemented, making IoT ecosystems extremely vulnerable to communication and privacy threats. As a result of these challenges, blockchain has emerged as a potential solution for securing distributed modes of communication. Mazaud et al. [1] proposed a framework for providing secure communication between IoT

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

devices via a blockchain mechanism. Their research aimed to build security into the exchange of data among interconnected IoT devices via decentralised blockchain mechanisms. Rather than relying on central authorities to store and process data, blockchains provide a decentralized, tamper-proof environment in which people share and transact with secure data on a distributed ledger that allows for both transparent transaction management and trusted communication. The distributed ledger mechanism assures that all transactions recorded on it will remain unchanged and that each will be verified for integrity before being recorded on the ledger and across all connected IoT devices. In addition, smart contracts allow for automatic authentication, access control, and management of secure communication within the dynamic IoT space. When integrated into IoT environments, blockchain technology provides numerous benefits such as improved security, enhanced transparency, reduced risk by increasing trust, and improved reliability. While conventional methods for implementing blockchains pose a number of challenges for resource-limited IoT systems, including computational complexity, increased storage requirements, lack of scalability, and increased communication delays, large-scale IoT environments require intelligent methods to manage device-to-device communications in real time, to handle dynamic device interactions and heterogeneous network architectures, and to meet real-time security requirements with very low computational demands. Recent work in this area has focused on the development of lightweight blockchain architectures, edge-assisted blockchain implementations, and intelligent security mechanisms that can be used for applications in IoT. Goyal et al. [2] proposed blockchain-based security frameworks that could be applied to IoT-enabled smart communication networks. They discussed the need for decentralized authentication, secure data sharing, and trust management in large-scale IoT environments. However, many challenges remain to be solved including the need for secure, decentralized authentication; efficient consensus algorithms; adaptive communication management; energy-efficient blockchains operations; and scalable security frameworks for heterogeneous IoT environments. In this paper, the authors propose an intelligent blockchain framework that enables secure communication within IoT environments illustrated by figure one below. The intelligent blockchain framework integrates a decentralized blockchain architecture, authentication through smart contracts, lightweight mechanisms for encryption and intelligent communication management strategies to provide a secure and trusted environment for exchanging data between IoT devices. The intelligent blockchain framework, using edge-assisted processing for the blockchain, is designed to reduce communication overhead, increase efficiency of transactions, and improve performance of real-time systems.

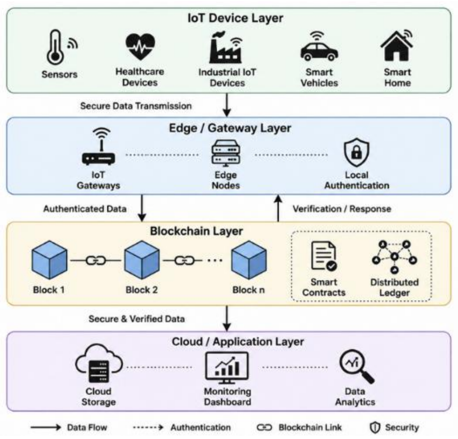

Fig. 1. Proposed Intelligent Blockchain Framework for Secure Communication in IoT Environments

The remainder of this paper is structured as follows. Section II provides an overview of the literature and prior studies on blockchain-enabled security frameworks and methods of secure communication in IoT networks. Section III covers the proposed intelligent blockchain framework and methodology used by the authors. Section IV covers the experimental setup and the parameters used to evaluate the performance of this study. Section V includes a summary of the results presented and suggests possible directions for continued research regarding intelligent, scalable, secure blockchain-enabled communication systems for IoT.

LITERATURE SURVEY

In recent years, technologies related to the Internet of Things (IoT) and distributed communication systems have advanced rapidly. At the same time, there has also been an increase in requirements for the trusted, secure, and

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

scalable ways of communicating data. To meet these demands, Reddy et al. [3] developed an Artificial Intelligence (AI) and blockchain-supported framework for securely transmitting IoT data between devices. This method utilized AI analytic capabilities combined with blockchain technology to create secure communication channels, detect anomalies in data, and authenticate data transmitted. Kant et al. [4] explored how to utilize blockchain technology within IoT security systems to establish securely distributed networks. Their research examined how blockchain allowed for the establishment of decentralized communication networks within multiple and diverse types of IoT systems, creating more authentic communication, trust, and the attainment of a high level of data integrity. Priya et al. [5] constructed a framework that integrated blockchain technology into the creation of secure methods of communicating between autonomous drones. The researchers demonstrated the effectiveness of their blockchain communications network by using decentralized means of verifying the data shared between drone systems. Sheetal et al. [6] proposed an architecture based upon the principles of blockchain to facilitate secure communications and data transmission within the IoT. Their proposed architecture focuses upon the establishment of secure means for communicating, establishing secure means of protecting sensitive data, and preventing unauthorized access to distributed IoT environments. Investigating how deep learning can be used to detect and protect against malicious and encrypted traffic traveling through communication networks, Reddy et al. [7] identified intelligent security analytics as a critical part of recognizing cyber threats and therefore creating an environment that allows for the protection of networked infrastructures from unauthorized access. Similarly, Huang [8] built a secure framework to use blockchain technology for distributed data storage and transmission in IoT-cloud environments in order to create improved security for communication and decentralized data management through the integration of blockchain with cloud technologies. Pothineni et al. [9] developed a framework to allow for secure and scalable blockchain-based data sharing solutions in IoT environments. This work addressed issues associated with secure information sharing, scalability of communications, and management of distributed trust. Gondhalekar et al. [10] established an improved security framework for global IoT communication over Software Defined Networks (SDNs) in adversarial networks. Their research provided intelligent traffic management, adaptive security policies, and network level communication protection for distributed IoT. Lastly, Veeraiah et al. [11] proposed an IoT framework implemented within a blockchain-based environment. The work integrated blockchain capabilities into cloud-assisted IoT communications to create secure data storage, decentralized authentication, and reliable data transmission. Sharma and Kumar [12] discussed the function of AI in smart city environments for improving safety and/or privacy through intelligent monitoring, detecting anomalies, and privacy preservation for safeguarding IoT system-related sensitive data. Additionally, they stated that an AI-based security framework can significantly enhance secure communication infrastructures of smart cities. Reddy et al. [13] proposed an intrusion detection and response system based on blockchain technology for secure Industrial IoT (IIoT). Their framework uses blockchain verification in conjunction with intelligent intrusion detection/response methods to detect malicious behaviour in communication between IIoT devices. Vikas et al. [14] designed an intrusion detection system using a hybrid deep-belief network and using Harris Hawks optimization (HHO) for wireless sensor networks (WSNs). Their focus was on improving detection performance of attacks as well as network security using intelligent optimization and deep-learning methods. Dash et al. [15] proposed a new multi-level blockchain security mechanism to ensure secure communications in next-generation IoT networks by implementing multiple blockchain security layers, decentralized authentication mechanisms, and methods of managing intelligent communications to enhance network security and protect data privacy.

PROPOSED METHODOLOGY

The main purpose of the proposed method is to create an infrastructure for secure, transparent, scalable, and tamper-resistant communication that will protect IoT networks from unauthorized access, malicious attacks, manipulated data, and vulnerabilities in communications received by the network.

IoT Device Layer & Data Communication Environment

The first level in this framework is called the IoT communication layer, which includes various interconnected smart devices within different types of networks. Devices included in the IoT layer comprise things like wearable devices, environmental sensors, industrial monitoring systems, as well as smart healthcare devices, surveillance systems, smart transportation, and intelligent home appliances. These devices continuously transmit data and receive data in real-time using wireless communication protocols and distributed architectures. Due to the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

constraint of limited computing resources and limited amounts of memory and energy availability, traditional centralized communication models are highly susceptible to cyber threats, breaches of security, and failures due to lack of communication. In addition to classifying packets of communication data according to their level of importance, the framework also categorizes packets by their degree of sensitivity and by their level of security risk associated with them. For example, healthcare-related, industrial automation-related, and financial communication packets will be afforded additional security validation and appropriate level of encryption processing.

Blockchain-Based Secure Communication Architecture

The second step of the proposed approach incorporates a decentralized blockchain network architecture to manage secure communication in IoT ecosystems. The blockchain layer is made up of interlinked distributed nodes that are responsible for verifying transactions, authenticating communications, and securely recording data. Each communication event that occurs between two IoT devices is converted to a blockchain transaction and added to a distributed ledger block after being verified. The proposed method uses cryptographic hashing algorithms and distributed consensus mechanisms to help keep the integrity of the data and prevent any unauthorized alterations to the communication records. Each communication block contains transaction data, device identification data, timestamps, encrypted communication data, and hash values from all prior blocks. Chaining communication blocks creates an immutable and transparent record of all the communication transactions within the network. By eliminating single points of failure, the decentralized blockchain architecture can greatly improve the level of trust associated with communication in a distributed IoT environment. The proposed architecture also mitigates data integrity issues associated with data tampering and replay attacks by maintaining synchronised distributed ledger records across all network participants.

Intelligent Authentication & Threat Detection

Each connected IoT device will have a unique blockchain identity (identity) and a unique cryptographic key (token) assigned to use for verification - the token will be used to confirm that a message came from the device to which it claims to have originated. The devices connect to the blockchain for purposes of identity verification via blockchain authentication protocols before they can communicate with each other. Additional capabilities of the intelligent monitoring technology within the proposed framework enable analysis of patterns of communication, transaction behaviour, and network usage to aid in identifying communications that are believe to be suspicious or could be malicious. Considering that adaptability is part of the goal of the intelligent security technology, communication requests that do not fit normal patterns of behaviour or are found to cover transactions not authorized will be continuously monitored using adaptive security analysis. Any malicious communication activity will result in the framework blocking the transaction; devices performing actions believed to be malicious will be isolated from the connectivity of the network.

Edge-Assisted Blockchain Processing & Resource Optimization

In stage four of the proposed methodology, edge computing methods are utilized in conjunction with blockchain architecture to improve the efficiency of communication and decrease computing overhead for IoT environments. As traditional operations do not have the resources to support real-time systems, implementing a blockchain directly onto resource-constrained IoT devices is inefficient due to the high amount of computing and storage resources required for traditional block chain operations. To address this issue, the proposed framework proposes using edge nodes (or edge servers) between IoT devices and cloud infrastructures for localized blockchain processing and temporary communication management. Edge nodes will be used to verify blockchain transactions, execute all of the smart contracts, and store temporary ledgers and perform filtering operations of communications for nearby IoT devices. By implementing this type of processing mechanism on edge devices will greatly reduce the amount of time it takes for communications to occur, as well as reduce the amount of energy consumed and computing overhead within the IoT network. In addition, the framework uses adaptive resource allocation strategies to pave the way for the balancing of blockchain workloads across distributed edge nodes.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Performance Evaluation and Comparative Analysis

Analyses of multiple scenarios involving IoT communications and analyze how well the proposed intelligent blockchain framework compares to other traditional centralized security architectures as well as other currently used blockchain-based (IoT) architectures. The parameters of interest for evaluation purposes include communication latency, transaction verification time, attack detection accuracy, throughput of the network, overhead incurred for communication, authentication efficiency, integrity of data, and resource utilization by devices on the network. Communication latency will be measured as an amount of time taken by a secure transaction to be processed in addition to the amount of time required by the completion of all necessary data transferred over the IoT network. Authentication efficiency will be assessed as to how quickly and accurately our framework can identify individual device identities and authorize transactions with as little delay in the corresponding processing of validation by our framework as possible.

RESULT AND ANALYSIS

An experimental evaluation of the suggested framework was performed by comparing the suggested framework to both traditional, centralized security architectures for IoT and existing blockchain-enabled communication models while examining multiple networks, workload levels, and types of communications.

System Configuration and Experimental Environment

A new intelligent blockchain framework has been implemented and evaluated in a high-performance computing environment that enables blockchain-enabled IoT communications for experimental purposes (Xu et al., 2021). The experimental environment consisted of an Intel® Core™ i7 (16 GB RAM) and a Ubuntu operating system. The proposed framework was created using various tools including; Hyperledger Fabric, Ethereum simulation, TensorFlow, Scikit-learn, NumPy, and Pandas. These libraries allow for the use of various Python-based blockchain simulation software as well as libraries for network/internet communication, transaction management, monitoring communication, and authenticating or validating transactions and performance within a blockchain using IoT. The IoT experimental environment consisted of multiple smart devices connected to an IoT network (e.g., healthcare sensors, industrial monitoring devices, smart transportation systems, wearable devices, and environmental sensors) to allow for IoT device smart monitoring and communications. To verify communications, manage transactions/validate transactions, and synchronize distributed ledgers within and across the IoT networks, distributed edge nodes and blockchain verification nodes were deployed and used. In the proposed blockchain framework, the data transmission between IoT devices was secured through the use of lightweight cryptocurrencies and smart contracts. The experiments were conducted under a variety of conditions including varying numbers of connected devices, rate of transaction generation, rates of communications workload, etc., to measure the efficiency of the proposed blockchain framework in a dynamic IoT environment.

Performance Evaluation Metrics

The performance analysis of the proposed intelligent blockchain framework was conducted using multiple security and communication-related evaluation metrics represented through equations (1) to (5). Authentication Accuracy (AC) determines the percentage of correctly authenticated communication requests within the IoT network:

$$\mathrm{AC} = \frac{\text{Authenticated Requests}}{\text{Total Authentication Requests}} \times 100 - - - (1)$$

Communication Latency (CL) evaluates using transaction verification time (TVT) and transmission delay (TD):

$$\mathrm{CL} = \mathrm{TVT} + \mathrm{TD} - - - - - - - - - - (2)$$

Throughput measures the successful processing rate of blockchain transactions within the IoT network:

$$\text{Throughput} = \frac{\text{Total Processed Transactions}}{\text{Total Execution Time}} - - (3)$$

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Attack Detection Rate (ADR) evaluates the capability of the proposed framework to identify malicious communication activities:

$$\mathrm{ADR} = \frac{\text{Detected Attacks}}{\text{Total Attack Instances}} \times 100 - - - - - (4)$$

Communication Overhead (CO) measures the additional communication traffic generated during blockchain transaction management:

$$\mathrm{CO} = \frac{\text{Control Communication Packets}}{\text{Total Network Packets}} \times 100 - -(5)$$

Comparative Analysis of Communication Security Performance

The experimental analysis compares the communication security performance of conventional IoT security models, blockchain-assisted communication systems, and the proposed intelligent blockchain framework.

Comparative Security Performance Analysis of IoT communication Frameworks

Communication Framework	**Authentication Accuracy (%)**	**Attack Detection Rate (%)**	**Data Integrity (%)**
Traditional IoT Security Model	82.4	79.6	84.1
Conventional Blockchain Framework	89.7	87.9	90.4
Hybrid Blockchain Security Model	93.2	91.5	94.3
Proposed Intelligent Blockchain Framework	97.6	96.8	98.1

The intelligent blockchain framework developed in this research delivers higher authentication accuracy, detection of attacks, and data integrity than those found in other communication security systems (as shown in TABLE I). By combining distributed blockchain verification, intelligent methods of authentication, and smart contracts to govern communication, the intelligent blockchain framework has improved its ability to prevent unauthorized communication (or malicious network activities). Also, the intelligent blockchain framework has increased the level of trustworthiness of communications by maintaining immutable records of distributed ledgers across all IoT devices that are interconnected.

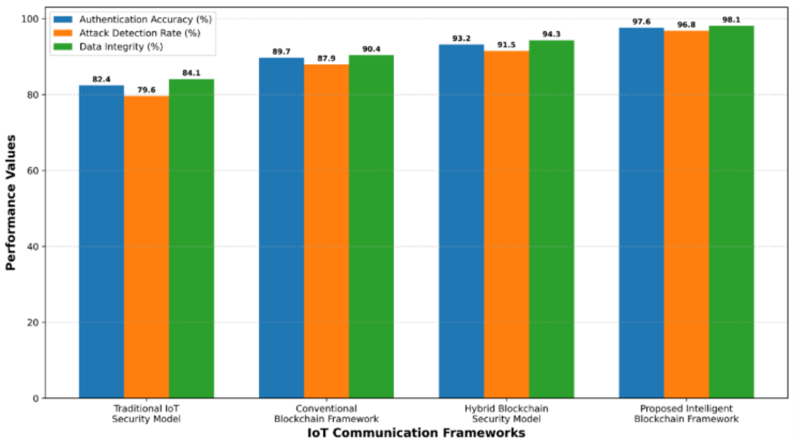

Fig. 2. Comparative Security Performance Analysis of IoT Communication Frameworks

INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING,
MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Fig. 2 demonstrates that the proposed intelligent blockchain framework consistently outperforms conventional communication security architectures across all security evaluation metrics.

Communication Latency and Throughput Analysis

The latency and throughput analysis evaluates the communication efficiency of the proposed framework under varying blockchain transaction loads and IoT communication conditions.

Commmunication Latency & Throughput Analysis of Blockchain-Enabled IoT Frameworks

Framework	**Average Latency (ms)**	**Throughput (Transactions/s)**	**Verification Time (ms)**
Centralized IoT Framework	214	382	196
Conventional Blockchain System	168	524	143
Edge-Assisted Blockchain Model	121	698	104
Proposed Intelligent Blockchain Framework	83	914	72

As illustrated in TABLE II, the intelligent blockchain framework developed by this study has achieved the lowest levels of communication latency and transaction verification time while providing the highest levels of throughput performance. The use of edge-assisted processing of blockchain transactions has allowed for localized transaction verification and intelligent workload management, thereby reducing delays in communicating with other IoT devices. Additionally, the use of distributed verification of blockchain transactions in conjunction with edge-assisted processing helps to reduce the amount of congestion in a network and, as a result, increases the efficiency of communications within large IoT environments.

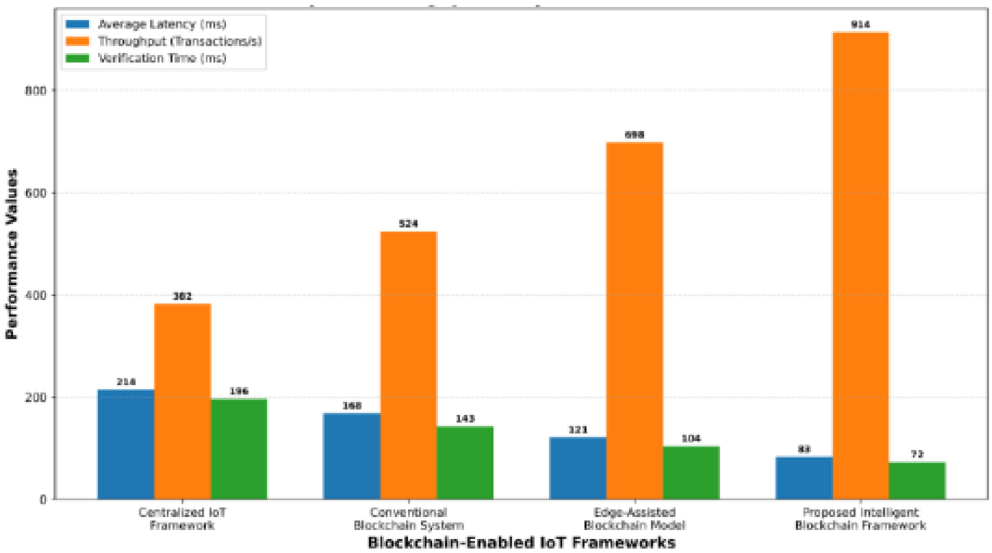

Fig. 3. Comparative Communication Latency and Throughput Analysis of Blockchain-Based IoT Frameworks

Fig. 3 illustrates that the proposed framework provides superior real-time communication performance and transaction processing efficiency for secure IoT applications.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Scalability and Communication Overhead Analysis

The scalability analysis evaluates the capability of the proposed framework to maintain secure communication performance under increasing numbers of IoT devices and blockchain transactions.

Scalability & communication Overhead Analysis Under Different Iot Network Loads

Number of IoT Devices	Centralized Framework Overhead (%)	Blockchain Framework Overhead (%)	Proposed Framework Overhead (%)
500 Devices	28.4	22.1	14.3
1000 Devices	31.7	24.8	15.9
2000 Devices	36.5	27.6	17.4
4000 Devices	41.2	31.3	19.1
6000 Devices	46.8	35.7	21.5

According to the scalability analysis results, the intelligent blockchain framework remains capable of maintaining minimal communication overhead and stable performances on the network as an increasing number of IoT devices connect to the network shown in TABLE III. The intelligent workloads creation and the assistance of the edge when verifying blockchain transactions have effectively minimized unnecessary communication traffic and maximized the efficiency of blockchain transaction processing within the overall network.

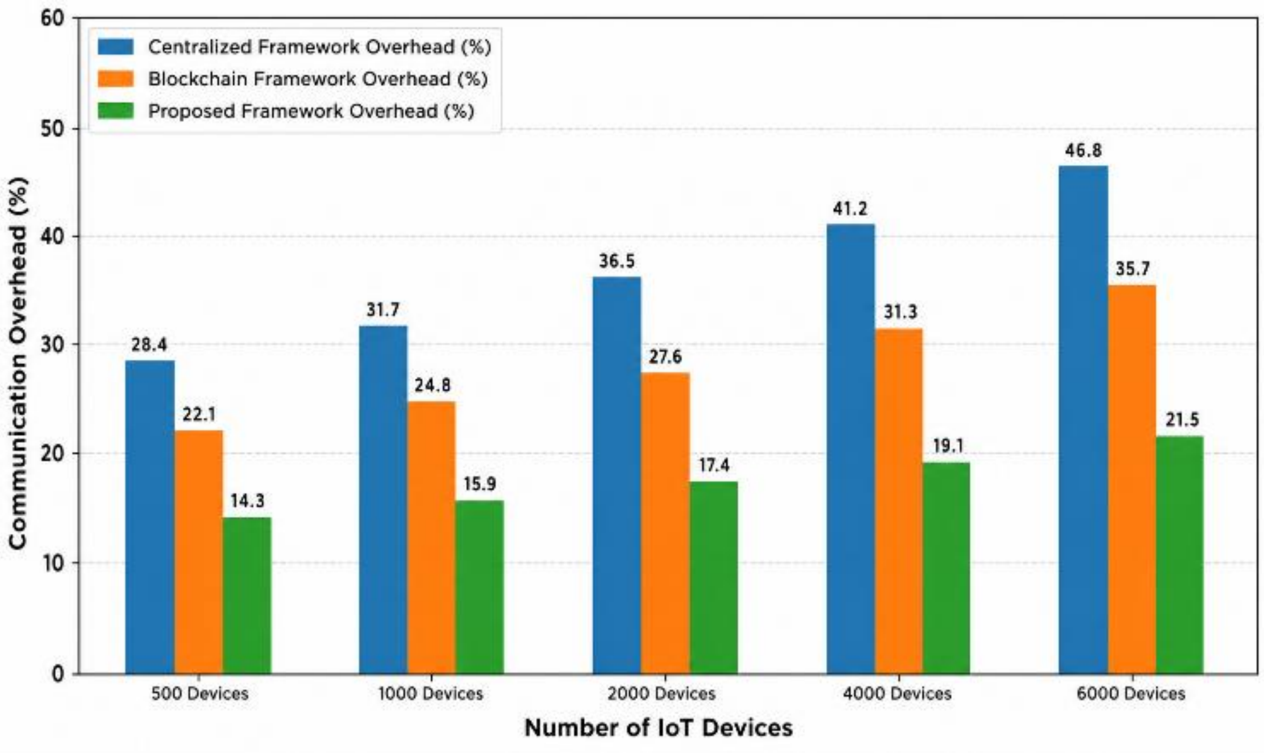

Fig. 4. Scalability and Communication Overhead Analysis of Blockchain-Based IoT Communication Frameworks

The findings presented in fig. 4 verify that intelligent blockchain framework demonstrates superior levels of scalability, reliability of secure communication, and computational efficiency than do other frameworks being developed as next-generation IoT networks continue to be created due to ever-growing numbers of connected devices in dynamic, large-scale environments.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

CONCLUSION AND FUTURE SCOPE

The proposed framework significantly improved secure communication reliability, reduced communication vulnerabilities, increased transaction verification efficiency, and reduced network overhead vs. traditional centralized IoT security frameworks and traditional blockchain-based communication systems. The experimental results showed that the proposed framework provides an overall authentication accuracy of 97.6%, an overall attack detection rate of 96.8%, and an overall data integrity performance of 98.1%, which is significantly better than traditional IoT security frameworks. The proposed model also outperformed traditional models for communication efficiency with an overall lowest latency of 83 ms, highest throughput of 914 transactions/s, and minimum transaction verification time of 72 ms due to intelligent edge-assisted blockchain processing and adaptive communication management. The scalability analysis showed that the framework maintained stable communication performance at only 21.5% communication overhead, even when tested in a large-scale IoT environment containing 6000 connected devices. Overall, the results validate that the proposed intelligent blockchain framework is a secure, scalable, and computationally efficient solution for next-generation IoT communication infrastructures. Future work could include extending the proposed framework through integrating AI-based predictive threat analysis, federated learning mechanisms, lightweight consensus protocols, quantum resistant cryptographic methods, and software-defined networking architectures to further enhance autonomous security management, communication scalability, energy efficiency, and resistance to cyberattacks in heterogeneous smart IoT ecosystems and industrial communication environments.

REFERENCES

1. T. Mazaud, M. D'Hérouville, L. Hauszler, D. H. Pohren, A. D. S. Roque and E. P. De Freitas, "A Blockchain-Based Framework for Secure IoT Device Communication," 2025 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Chisinau, Moldova, Republic of, 2025, pp. 1-4, doi: 10.1109/BlackSeaCom65655.2025.11193938.
2. K. Goyal, V. R. Chintha, P. Kumar, S. S. K. Sundaresan, A. Ashirova and A. Jain, "Blockchain-Based Security Frameworks for IoT-Enabled Smart Communication Networks," 2025 International Conference on Intelligent and Secure Engineering Solutions (CISES), Greater Noida Gautam Budh Nagar, India, 2025, pp. 977-981, doi: 10.1109/CISES66934.2025.11265248.
3. S. M. Reddy, K. Mahesh, K. GnanaPraneeth and S. Rajula, "Blockchain-Integrated AI for Secure Data Transmission in IoT Ecosystems," 2025 2nd International Conference on Recent Trends in Electrical, Electronics and Computing Technologies (ICRTEECT), Warangal, India, 2025, pp. 1-5, doi: 10.1109/ICRTEECT67512.2025.11448725.
4. R. Kant, S. Sharma, V. Vikas, S. Chaudhary, A. K. Jain and K. K. Sharma, "Blockchain – A Deployment Mechanism for IoT Based Security," 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 2023, pp. 739-745, doi: 10.1109/CICTN57981.2023.10140715.
5. S. S. Priya, S. Srinivas Vellela, V. R. B, S. Javvadi, K. B. Sk and R. D, "Design And Implementation of An Integrated IOT Blockchain Framework for Drone Communication," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1-5, doi: 10.1109/CONIT59222.2023.10205659.
6. Sheetal, V. Kumari and V. S. Badiger, "Securing the internet of things communication and data transmission by using Blockchain based Architecture," 2025 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bangalore, India, 2025, pp. 1-5, doi: 10.1109/IITCEE64140.2025.10915455.
7. P. C. S. Reddy, P. Shirley Muller, S. N Koka, V. Sharma, N. Sharma and S. Mukherjee, "Detection of Encrypted and Malicious Network Traffic using Deep Learning," 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE), Ballari, India, 2023, pp. 1-6, doi: 10.1109/AIKIIE60097.2023.10390386.
8. Z. Huang, "A Blockchain-Based Secure Framework for Distributed Data Storage and Transmission in IoT-Cloud Environments," 2025 8th International Conference on Computer Information Science and Application Technology (CISAT), Kunming, China, 2025, pp. 935-939, doi: 10.1109/CISAT66811.2025.11181722.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

9. B. Pothineni et al., "Secure and Scalable Data Sharing in IoT Environments with Blockchain Integration," 2025 10th International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, Malaysia, 2025, pp. 222-226, doi: 10.1109/ICCCE66530.2025.11474215.
10. G. Gondhalekar, V. G, L. D. Isaac, R. K. Vyas, A. R. S R and A. K. N, "An Optimized Security Framework for Global IoT Communication using Software-Defined Networking (SDN) in Adversarial Environments," 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2023, pp. 100-109, doi: 10.1109/I-SMAC58438.2023.10290515.
11. V. Veeraiah, V. Talukdar, S. B. Talukdar, J. Kotti, M. K. Dharani and A. Gupta, "IoT Framework in a Blockchain dependent Cloud Environment," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10308158.
12. V. Sharma and S. Kumar, "Role of Artificial Intelligence (AI) to Enhance the Security and Privacy of Data in Smart Cities," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 596-599, doi: 10.1109/ICACITE57410.2023.10182455.
13. B. L. Reddy et al., "Blockchain-Based Intrusion Detection and Response Framework for Secure Industrial IoT Networks," 2025 International Conference on Communication and Smart Devices (ICCoSD), Ranchi, India, 2025, pp. 1-6, doi: 10.1109/ICCoSD66074.2025.11348276.
14. Vikas, R. P. Daund, D. Kumar, P. Charan, R. S. K. Ingilela and R. Rastogi, "Intrusion Detection in Wireless Sensor Networks using Hybrid Deep Belief Networks and Harris Hawks Optimizer," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, pp. 1631-1636, doi: 10.1109/ICESC57686.2023.10193270.
15. S. Dash, P. S. R. Rao and L. Sujihelen, "A Novel Multi-Level Blockchain Security Model for Secure Communication in Next-Generation IoT Networks," 2025 15th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2025, pp. 1-5, doi: 10.1109/MACS68476.2025.11453390.