

A Scalable Blockchain Framework for Secure IoT Communication

Sudipta Majumder*

Dept. of CSE, DUIET, Dibrugarh University, Assam, India

Email: sudipta2020@dibru.ac.in

ORCID ID: <https://orcid.org/0000-0002-1748-8685>

*Corresponding Author

Received: 04 October, 2024; Revised: 11 January, 2025; Accepted: 20 March, 2025; Published: 08 August, 2025

Abstract: The rapid proliferation of Internet of Things (IoT) devices has revealed weaknesses in its centralized communication architectures, rendering them vulnerable to security risks such as Distributed Denial of Service (DDoS) attacks. This scenario highlights the need for secure and efficient communication frameworks to safeguard IoT networks. In this paper, we present a blockchain-based framework designed to improve IoT communication networks' security, scalability, and performance. Our methodology utilizes decentralized architecture to mitigate risks linked to centralized sources of failure while enhancing performance metrics, including latency, throughput, energy consumption, and transaction success rates. We present an innovative approach that integrates a plateau effect in latency and consensus time, guaranteeing performance stability as the number of devices increases. The proposed model demonstrates decreases in latency by 26.57% and reductions in energy usage by 35.29% compared to existing Ethereum frameworks, based on extensive simulations conducted under diverse network conditions with one thousand devices, underscoring the framework's effectiveness in managing network congestion. This research offers a viable answer to the problems of IoT communication, facilitating future investigations into the optimization of blockchain integration for improving IoT security and efficiency.

Index Terms: Internet of Things, Blockchain, Consensus Mechanism, Performance Optimization, Decentralization, Network Security

1. Introduction

The Internet of Things (IoT) has revolutionized a variety of sectors, such as healthcare, transportation, and smart communities, by facilitating the seamless exchange of data among a multitude of devices. This expansion poses security and efficiency challenges. This is especially true for centralized communication models. Centralized systems have weak spots. They can fail easily. These types of networks face risks like DDoS attacks, data leaks, and unauthorized access [1]. Developing robust decentralized communication frameworks has become more crucial as the number of interconnected devices increases. Traditional IoT systems rely on cloud servers for device communication. This can cause higher latency and lower resilience during network disruptions. This reliance can cause delays in data transmission. It also hampers real-time processing and essential for applications like disaster response, industrial automation, and critical infrastructure management. Furthermore, implementing centralized systems frequently necessitates substantial resources to ensure security and manage significant data volumes, which complicates the process of scaling [2,3].

Blockchain technology offers an effective solution. It improves IoT communication security and efficiency. Blockchain provides a decentralized ledger. It securely records transactions. This reduces risks from single points of failure. It is challenging for malicious actors to manipulate an immutable chain formed by each transaction being cryptographically secured and linked to previous ones. Blockchain is decentralized. It promotes transparency [4,5]. Devices can interact freely. No central authority is needed. Implementing blockchain in IoT systems has challenges despite its potential. IoT devices have resource limits. They struggle with processing power, memory, and energy use [6,7]. This makes it hard to use traditional blockchain protocols. Also, consensus mechanisms in blockchain can add latency. This makes real-time data exchange more complicated. Besides, Blockchain ensures that every node on a network stores a copy of a ledger which results in large storage requirements. This requirement can be particularly costly for IoT devices as they have very little storage space. Innovative approaches are needed to be developed to optimize performance and security.

Numerous studies on leveraging blockchain technology for IoT communication have been conducted [1-7], focusing on improving security, decentralization, and data integrity. However, there is a lack of research on integrating blockchain into IoT systems in a manner that simultaneously addresses scalability, latency, energy efficiency, and transaction throughput. In addition, previous studies were limited because they often emphasized theoretical models or specific applications without providing holistic frameworks capable of managing real-world challenges like network congestion and unauthorized access. This paper addresses these gaps by proposing a blockchain-based framework that enhances the scalability, security, and efficiency of IoT communication networks. The framework tackles critical issues such as high latency, energy constraints, and throughput instability while incorporating proactive mechanisms to mitigate security risks, offering a comprehensive solution for modern IoT systems. The system uses a new consensus algorithm. It reduces latency and energy use. It also boosts throughput and success rates for transactions. The system achieves stability in performance as the number of devices increases by integrating a plateau effect into measurements related to latency, consensus time, and energy consumption. This approach fortifies the network against centralized design vulnerabilities while improving efficiency. Extensive simulations are undertaken to evaluate the performance of the proposed framework under diverse scenarios. Critical parameters such as latency, throughput, energy consumption, consensus duration, and security (assessed by unauthorized access attempts) are evaluated, demonstrating substantial enhancements. The findings underscore the capacity of blockchain technology to revolutionize IoT connectivity, enhancing both efficacy and security.

We start in Section 1 with an introduction outlining the necessity of blockchain-based secure and scalable IoT connection. Section 2 presents related work that emphasizes recent advancements and challenges in the areas of security, interoperability, scalability, and the use of blockchain technology in IoT network. Section 3 outlines the methodology, including the proposed framework and algorithm. Section 4 presents the results, including enhancements in performance. Section 5 provides a conclusion and future work of the findings and proposes avenues for future investigation.

2. Related Work

Enabling seamless interactions between an ever-expanding multitude of interconnected devices, the Internet of Things (IoT) has fundamentally transformed the landscape of device communication. This technology revolution brings many communication challenges. We must address these to ensure secure data exchange among IoT devices. There are four main challenges: security, interoperability, resource limits, and network management. Each area has its own challenges. We must overcome them to unlock IoT's full potential.

Security is a significant challenge in IoT communication. Numerous IoT devices are implemented with a "security second, functionality first" approach, which frequently results in substantial vulnerabilities [8]. Issues such as "default credentials" are never modified and insufficient encryption protocols for data transmission are the consequence of this absence of security measures. IoT networks are open and interconnected. This makes them vulnerable. They face many cyber threats [9,10]. Denial-of-Service (DoS) attacks flood devices with traffic. Data interception captures sensitive information during transmission [11]. Strong security measures are becoming more and more necessary as the number of IoT devices keeps growing. Without proper security, data breaches and loss of trust increase. It's crucial to create safer systems. One solution to improve security in IoT communications is using blockchain technology. It provides a decentralized and immutable framework for secure data exchanges. Blockchain can help with security issues in IoT. This idea is getting attention from researchers and industry.

Another big problem in IoT is interoperability [12,13]. IoT devices are diverse. They use different communication protocols. This makes it hard for different makers of devices to work together smoothly. This lack of standardization causes compatibility issues. It hinders communication and collaboration between devices. To solve the interoperability issue, there is a growing focus on creating universal communication protocols [14]. These frameworks help different IoT devices interact easily. Standardization is key. It helps devices work together in IoT systems. This boosts their potential [15].

Resource constraints are another challenge for IoT communication. IoT devices use little power. This limits their processing and communication [16]. These limits can cause problems. Data transmission may be slow. Connections can be unreliable, especially in crowded areas with many devices. Devices need to talk often. This can use up their resources. It may cause delays. These challenges that can be addressed using techniques like pruning, sharding as well as off chain storage solutions. These approaches are used to reduce the amount of data stored on a blockchain while maintaining the reliability and efficiency of the system the blockchain is serving. Various researchers are also tackling resource challenges. They are looking into edge computing, which processes data closer to its source [17,18]. They are also using lightweight communication protocols. These helps reduce resource use and enable effective data exchanges. These strategies improve IoT systems. They use resources better. Performance gets better [19].

Good network management is key for IoT applications. Managing a complex network needs smart methods. This ensures data routing and resource use are efficient. Software-defined networking and Machine-to-Machine communication provide good ways to handle IoT networks [20]. These technologies allow control of network resources. They help change network settings based on real-time data. They bring new challenges. Real-time data processing is

needed. Network configurations must adapt to changing conditions. These management solutions show promise. They need more research and development. This ensures they work well in real life [21,22].

Centralized IoT models raise more security concerns. Centralized architectures have benefits. They simplify management and aggregate data. However, they also have vulnerabilities. These can compromise data integrity and confidentiality. Centralized IoT models face a big security issue. There are single points of failure (SPoF). All data goes through a central server or cloud service. This centralization poses a risk. If the main server is breached, the whole system suffers. An attacker can access the central hub. They can manipulate or steal a lot of data. This can lead to serious problems for users and organizations. Any downtime or failure of the central server can disrupt the whole IoT system. This affects availability and reliability [23,24].

Data privacy is a key issue in centralized IoT models. These systems require sensitive data to be sent and stored on third-party servers. This raises concerns about unauthorized access and data breaches. Data on a central server is a target for cybercriminals [24,25]. Attacking a server can expose personal information. It also risks sensitive business data. These systems often limit user control over data. This can lead to privacy issues and unclear data usage [26]. Relying on third-party services for data management adds security risks. Centralized IoT models depend on cloud providers for data storage and processing [27]. This can create vulnerabilities tied to the provider's security practices. A security breach at a cloud provider can compromise the data of all its clients. Relying on outside entities makes it hard to follow data protection rules. Organizations may struggle to ensure their data is managed legally [28]. Centralized IoT models simplify management. They help with data processing. But they bring security risks. These are single points of failure. Also, data privacy concerns exist. There are risks with third-party dependencies. Fixing these problems is crucial for safely using IoT systems. This requires looking into decentralized systems. They can reduce risks by spreading data and processing over many nodes.

Blockchain technology offers a strong solution for the security issues in IoT systems. Its decentralized and immutable nature boosts data integrity, privacy, and authentication in IoT settings [29]. Blockchain technology ensures data integrity. It prevents tampering effectively. Centralized IoT models store data on one server [30]. This makes it easy for unauthorized access and manipulation. Blockchain uses a distributed ledger. Data is recorded on many nodes. Decentralization means changing one piece of data needs agreement from most nodes. This cuts down the chance of tampering. Using cryptographic algorithms in blockchain boosts data security. It allows for secure authentication and identity management. This is key for protecting sensitive IoT data [31,32]. Blockchain can boost privacy in IoT networks. More devices mean more data. This raises worries about privacy and unauthorized access. Blockchain offers a clear and safe way to share data. Smart contracts on blockchain enforce access control. They define who can access data and under what conditions. This ensures sensitive information is available only to authorized users. Data control matters a lot in healthcare. Keeping patient data private is crucial [29]. Blockchain helps IoT devices talk securely. Traditional IoT systems use centralized servers for communication. This can lead to bottlenecks and single points of failure. Blockchain lets IoT devices talk directly. This makes the network stronger and more reliable. This decentralized model boosts efficiency. It also lowers the risk of DDoS attacks. There's no central point to target [33,34].

Integrating blockchain into IoT systems has challenges. Scalability is a big issue. Blockchain needs a lot of computing power and storage. This is tough for IoT devices with limited resources. Researchers are exploring lightweight blockchain solutions. They are looking at hybrid models. These combine blockchain with other technologies, like fog computing. The goal is to tackle scalability issues while keeping security intact. Ongoing research and development are crucial. Innovative solutions can unlock blockchain's potential in IoT applications [35,36]. Blockchain integration in IoT affects performance. It's an important factor to consider. Blockchain boosts security, transparency, and data integrity. However, it adds complexities that can affect IoT system performance. Key performance factors are scalability, latency, consensus methods, and resource limits. Scalability is a big challenge. More IoT devices mean more transactions. Traditional blockchain systems often have trouble with high transaction volume. This causes delays and bottlenecks. Blockchain networks depend on consensus mechanisms. These can limit large-scale IoT applications. Researchers are looking into hybrid consensus methods and lightweight blockchain protocols. These aim to meet the specific needs of IoT settings. The goal is to improve scalability while keeping security intact [37-41].

Lesser latency is important for efficient performance. Consensus and transaction validation consume time. This can delay data processing and communication between IoT devices. This is a big issue for time-sensitive applications such as autonomous vehicles or industrial automation. Real-time data exchange is required for such application. The necessity for rapid consensus in real-time data sharing can conflict with the fundamental attributes of blockchain, such as decentralization, security, and immutability. A blockchain assisted network needs many nodes to validate transactions. This results in more latency. Edge computing and off-chain processing are being explored to solve such problems. They help reduce latency. Certain transactions can be processed outside the blockchain. Security and integrity remain intact [42-49]. The consensus mechanism affects blockchain performance in IoT. Consensus algorithms have different resource needs and performance traits. Proof-of-work (PoW) mechanisms use a lot of computing power. They may not work well for IoT devices with limited resources. Lightweight consensus protocols like proof-of-stake (PoS) and delegated proof-of-stake (DPoS) may provide efficient options. They may lessen the computational load on IoT devices and keep security intact. Researchers are working on hybrid consensus mechanisms. The goal is to optimize performance [50-66].

Despite advancements in utilizing blockchain for IoT security, considerable deficiencies persist in the literature. Most current research emphasizes theoretical models or particular applications, with little focus on holistic frameworks

that tackle security and performance issues in practical contexts. Zubaydi et al. conducted a thorough literature study on blockchain's function in enhancing security and privacy for IoT; however, they need to present a comprehensive architecture that integrates these elements with performance measures such as latency and energy consumption Zubaydi et al. [67]. Similarly, Sagirlar et al. address the design of cooperative blockchains for IoT. However, they need to offer an in-depth analysis of how these architectures might be optimized for practical applications [68].

Moreover, limited research has successfully included techniques to maintain performance measures while improving throughput and transaction success rates. For instance, whereas Vg presents a blockchain-based framework for intrusion protection in IoT fog computing, it fails to consider the equilibrium between security measures and the performance requirements of IoT applications [69]. Similarly, Bobde's research on improving industrial IoT network security via blockchain integration underscores the significance of security but fails to explore the ramifications for system performance [70]. The gap is crucial, as the operational efficiency of IoT systems is essential for their effective implementation. This study addresses these deficiencies by introducing an innovative blockchain-based system to enhance performance metrics while guaranteeing strong security for IoT communications. This approach will tackle the dual issues of ensuring security and improving performance by utilizing insights from existing literature, including the necessity for lightweight consensus mechanisms and proactive security measures. As Khan et al. proposed, integrating lightweight consensus techniques can diminish energy consumption and latency while preserving transaction integrity [71]. Furthermore, integrating automatic responses to security risks, as articulated by Sharma, might augment the resilience of IoT systems without detracting from their performance .

3. Methodology

The framework outlines a method for IoT communication using blockchain technology, detailing how IoT devices engage with it to facilitate secure and efficient data exchange. Multiple IoT devices collect and generate data from their respective environments. These devices act as points in the network and collect real-time data. The data is sent to the blockchain, serving as the first input into the system. The main part of the system represents the Blockchain layer, which performs several important functions:

- A. Consensus Mechanism: This layer ensures that all participating devices agree on the validity of data or transactions. It maintains network integrity by verifying transactions using Proof of Stake consensus protocols. The consensus process guarantees that only valid and confirmed transactions are included in the blockchain.
- B. Smart Contracts: These are contracts programmed into the blockchain, automatically executing specific rules when certain conditions are satisfied. In IoT, smart contracts can automate tasks such as data sharing, managing devices, or controlling access based on the information received from IoT devices.

After the consensus mechanism confirms a transaction, it is recorded in the Immutable Ledger, which securely keeps all verified data or transactions in a format that cannot be altered or tampered with. All IoT devices, including IoT Device N, can access this ledger to maintain transparency and traceability. Fig.1 shows the proposed Blockchain Framework for Secure IoT Communication.

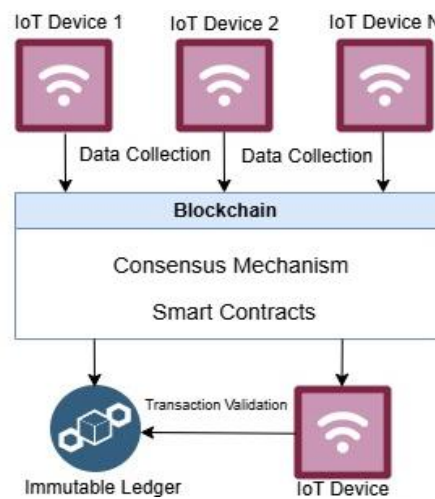


Fig. 1. Blockchain Framework for Secure IoT Communication

Fig.2 describes the communication and data flow between an IoT device and a blockchain network. An IoT device collects data from its environment or sensors. The collected data is formatted into a specific structure, usually using JSON (JavaScript Object Notation), a standard format for transmitting structured data between devices. After formatting

the data correctly, it is transmitted to the Blockchain Network, where it is included in a transaction for processing. When a transaction is received, the blockchain starts its Consensus Mechanism, which is essential for making sure that all nodes involved agree on the transaction's validity. This method checks the data's integrity and authenticity, ensuring that only valid transactions are processed.

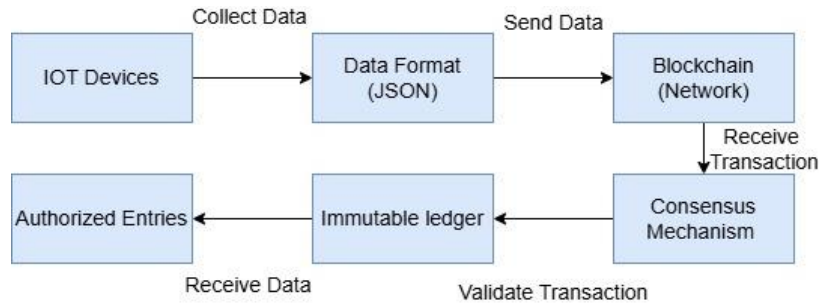


Fig. 2. IoT Device Communication and Data Flow in the proposed Blockchain Framework

Once the consensus process is complete, the validated transaction is stored permanently in the immutable ledger, which serves as a secure and tamper-proof record of all verified transactions. The immutable ledger guarantees that once data is recorded, it remains unchanged and cannot be deleted, ensuring transparency and trust throughout the network. Authorized Entities, including other IoT devices, applications, or users, can access and retrieve data in the ledger that have permission to interact with the blockchain. This guarantees a secure and clear exchange of information, enabling reliable communication and data sharing among IoT devices and the wider network, while protecting the system's integrity.

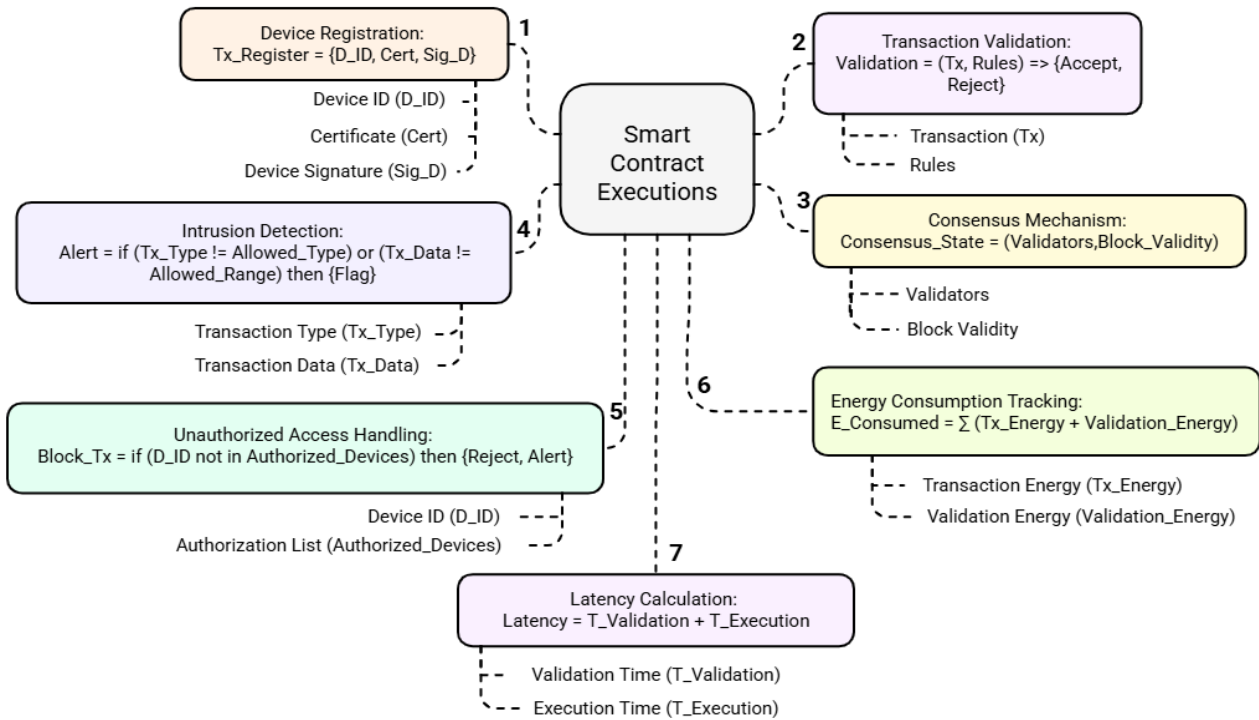


Fig. 3. Smart contract implementation and execution steps

The proposed blockchain-based IoT model uses the features, such as immutable ledgers, audit trails, smart contract-based monitoring and consensus mechanism alerts, respectively, to achieve effective Unauthorized access detection. This immutable ledger guarantees that any transaction, once recorded, cannot be changed or deleted, thus building a solid and tamper-proof audit trail. Through this trail, we know that there are anomalies, such as repeated failed attempts for authentication or irregular transaction patterns, which could be an indication of unauthorized access attempts. The ledger keeps a complete and chronological record of all activities to support post-incident analysis and forensic investigations. Security monitoring has been further automated with smart contract-based monitoring to detect suspicious behavior. Depending on the usage context, smart contracts specify and enforce rules to verify the identity of the devices that interact, for example whether a device is registered or whether the device activities are within permitted roles. The smart contract blocks the transaction and sends alerts if a transaction violates defined rules, for example an unregistered device attempts access. Also, the role played by the consensus mechanism is of accorded importance in

identifying any unauthorized access. In this process, validators check if each transaction is fine by verifying it or not. The transaction is rejected if the presence of tampered or malicious data is found and the attempt is flagged. These mechanisms ensure real-time detection and quick response to unauthorized activities, which enhances overall system security. Fig.3., Fig.4. and Fig.5. show the smart contract implementation and executions, IOT device integration and unauthorized access handling mechanism of the proposed framework respectively.

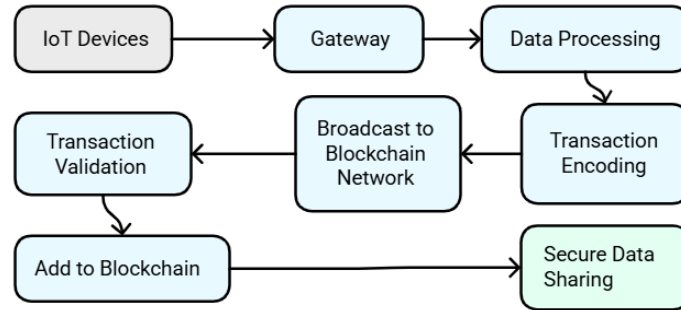


Fig. 4. IOT device integration in the block chain framework

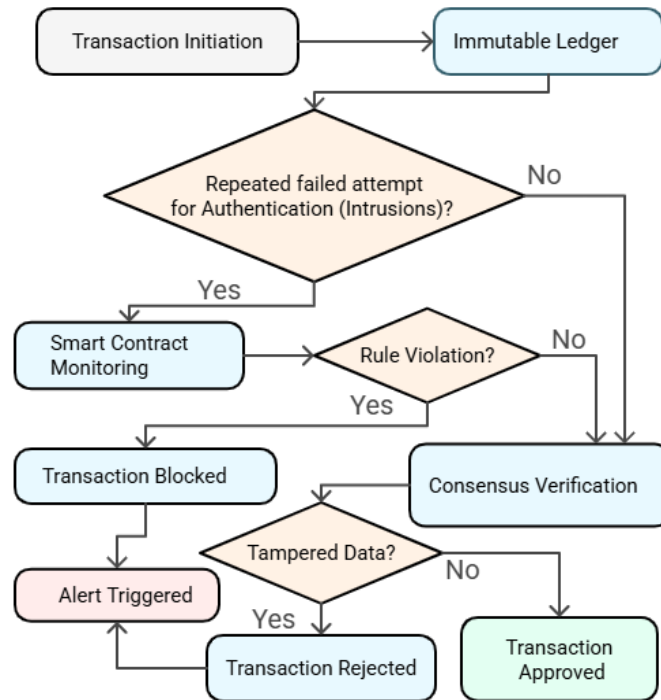


Fig. 5. Unauthorized access handling mechanism

For implementing the proposed framework, we have generated data programmatically and used them to model IoT communication parameters such as device count etc. Data points were created using random number generation with controlled variations to simulate real-world scenarios. Based on these communication parameters and data points, simulations for latency, throughput, unauthorized access attempts, energy consumptions and transaction rate are carried out. The simulations are conducted using python. Libraries such as NumPy and matplotlib are used for mathematical computations and data visualizations respectively. A few essential simulation environment and test conditions considered for the above simulation are shown in Table 1.

Table 1. System Parameters

Description	Value (Range)
Maximum number of devices	1000
Total time steps for unauthorized access	100
Maximum validators	50
Maximum congestion level (transactions per second)	1000
Range of devices for plotting (step size of 100)	10 to 1000
Range of validators for consensus time simulation	5 to 50
Time delay in communication (ms)	10 to 50 ms
Range of network congestion levels for transaction rate	100 to 1000
Number of trials for Confidence Interval observation	100

Table 2 shows the Algorithm for the proposed Scalable Blockchain Framework for Secure IoT Communication.

Table 2. Algorithm for Scalable Blockchain Framework for Secure IoT Communication

1	Initialize IoT Devices
	I. Start IoT Device 1, IoT Device 2, ..., IoT Device N. II. Each IoT device collects data (e.g., environmental, sensor data).
2	Data Collection and Transmission
	For each IoT device ($i = 1$ to N): I. Collect data. II. Structure the data as a transaction (e.g., device ID, timestamp, sensor data). III. Transmit the transaction to the Blockchain Layer.
3	Blockchain Layer: Consensus and Verification
	I. Receive data from IoT devices. II. Create a block: a. Include multiple transactions in the block. b. Add metadata like a timestamp, block number, and previous block's hash. III. Proof of Stake (PoS) Consensus Mechanism: a. Validate the block from IoT devices using PoS. b. Ensure validators with higher stakes participate in block validation. c. Verify all transactions using the PoS mechanism. IV. If transaction is valid: a. Move to Smart Contracts. Else b. Reject the transaction. c. Return feedback to IoT devices for retransmission or adjustment.
4	Authentication and Rule Violation Monitoring
	I. Check authentication for repeated failures: a. Trigger smart contract monitoring if failures persist. II. Identify and flag suspicious transactions or rule violations. a. Include violation details in a separate flagged data structure for auditing. III. Continue to tampered data validation if required.
5	Tampered Data Validation
	I. Validate transactions in the block: a. Compare transaction hashes against their original values to detect tampering. b. If tampered, reject the transaction and flag it. c. Else, proceed to consensus validation. II. Append valid data to the block for storage.
6	Smart Contracts Execution
	For each verified transaction: I. Execute predefined conditions in smart contracts. II. If conditions are met, process the transaction. Else, mark the transaction as incomplete and append its status to the block.
7	Immutable Ledger Storage
	I. Finalize the block by: a. Calculating its hash (based on transactions, metadata, and previous block's hash). b. Linking it to the previous block in the blockchain using the hash. II. Store the completed block in the blockchain's distributed ledger.
8	Access by Authorized Entities
	For each authorized entity (e.g., IoT devices, applications, or users): I. Query the blockchain for a specific transaction, block, or data point. II. Retrieve and verify the data by checking its hash and block number.
9	Feedback Loop
	For each authorized entity or user request: I. Send feedback to IoT devices or applications. II. Request additional data as needed. III. Adjust the data collection or transmission processes based on block insights (e.g., patterns detected in flagged or failed transactions).
10	Performance Evaluation and Metrics Collection
	I. Monitor latency, throughput, energy consumption, unauthorized access attempts, consensus time, and transaction success rate. II. Trigger alerts for authentication failures, rule violations, or tampered data.
11	Repeat
	Loop back to Step 2 for continuous data collection, validation, and communication

4. Results

The “Latency vs. Number of Devices (with confidence interval)” in Fig.6 shows an initial rise in latency. After 200 devices, it stabilizes. It stays around 50ms, even with more than 800 devices. This highlights the framework's scalability and ability to manage a large number of IoT devices with little degradation in performance. The framework's resilience in various situations is demonstrated by its capacity to keep latency levels constant even under rising demand, with 95 % confidence interval. Fig.7, depicting Throughput versus the Number of Devices, with 95% confidence interval, indicates that throughput consistently hovers around 500 transactions per second (Tx/sec) across all device quantities. This signifies the framework's stability and efficiency. The framework guarantees a high and stable transaction processing rate, irrespective of the number of connected devices, showcasing its capacity to handle extensive IoT connectivity without a decline in throughput. The Security (Unauthorized Access Attempts) versus Time Fig.8 illustrates variations in unauthorized access attempts, fluctuating between 0 and 10. The framework's capacity to monitor and manage these variations indicates a robust security mechanism for identifying and addressing real-time risks. This adaptive security mechanism underscores the framework's proactive strategy for securing IoT networks, rendering it a viable solution for protecting sensitive data. The framework effectively balances scalability, performance, and security, establishing it as a dependable platform for IoT connectivity.

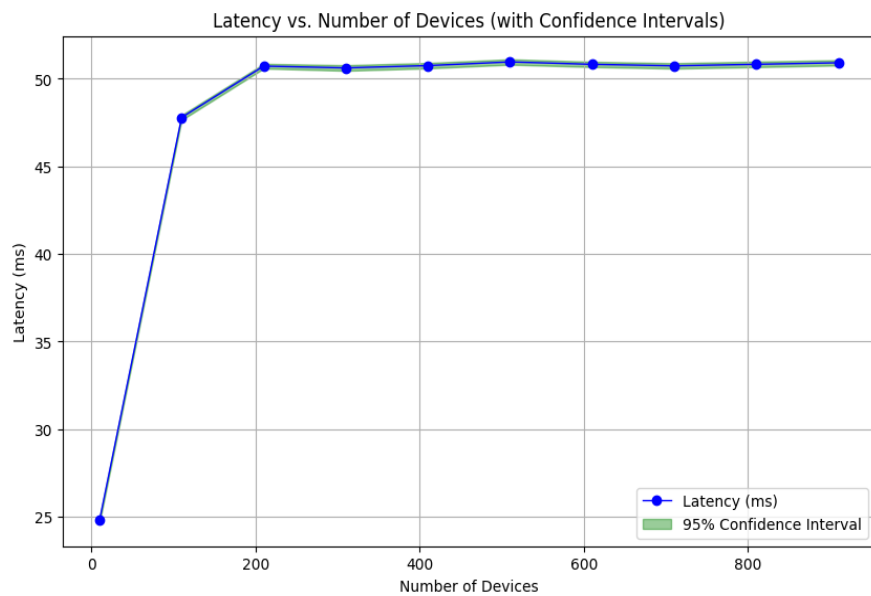


Fig. 6. Latency vs. Number of Devices (with 95% Confidence Interval)

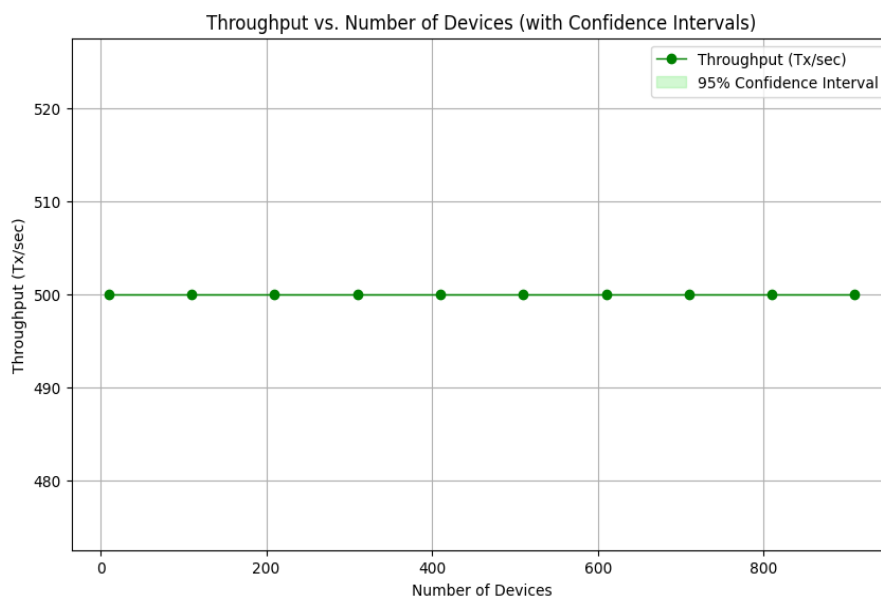


Fig. 7. Throughput of the system as the numbers of devices increases (with 95% Confidence Interval)

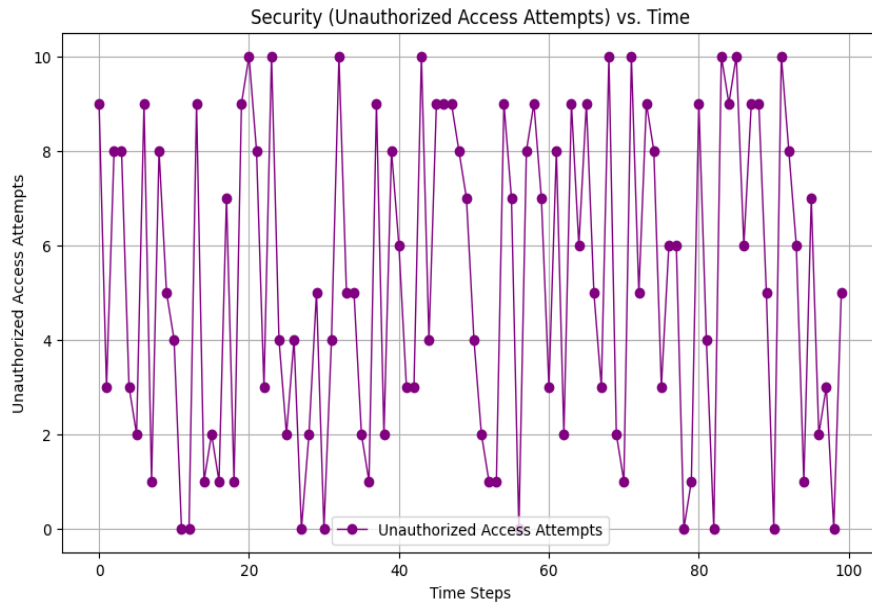


Fig. 8. Unauthorized access attempts

Fig.9, "Energy Consumption per Device vs. Number of Devices (with confidence interval)" illustrates that energy consumption per device remains largely constant, exhibiting a slight increase when the number of devices escalates. This indicates that the blockchain protocol effectively regulates energy consumption, even with the integration of additional IoT devices, rendering it a viable solution for extensive IoT networks. The capacity to scale without substantially augmenting energy demands is vital for sustainable IoT implementations. According to Fig.10, "Consensus Time vs. Number of Validators (with confidence interval)," consensus time rises as the number of validators does, but the rise is controlled and gradual. The advantageous point is that, despite having a network of 50 validators, the consensus time is approximately 8 seconds, demonstrating that the architecture can accommodate more extensive networks without significant delays. This illustrates the framework's scalability while ensuring efficient consensus times, which are essential for secure and prompt IoT connection. As shown in Fig.11, until a sufficient congestion level is reached, the transaction success rate stays high (>90%). Even amongst moderate to severe congestion (up to 800 transactions per second), the system sustains robust performance, exhibiting a significant reduction at extreme congestion levels. This signifies that the blockchain infrastructure is resilient under standard and considerably elevated transaction volumes, providing dependable communication and transaction validation in practical IoT applications.

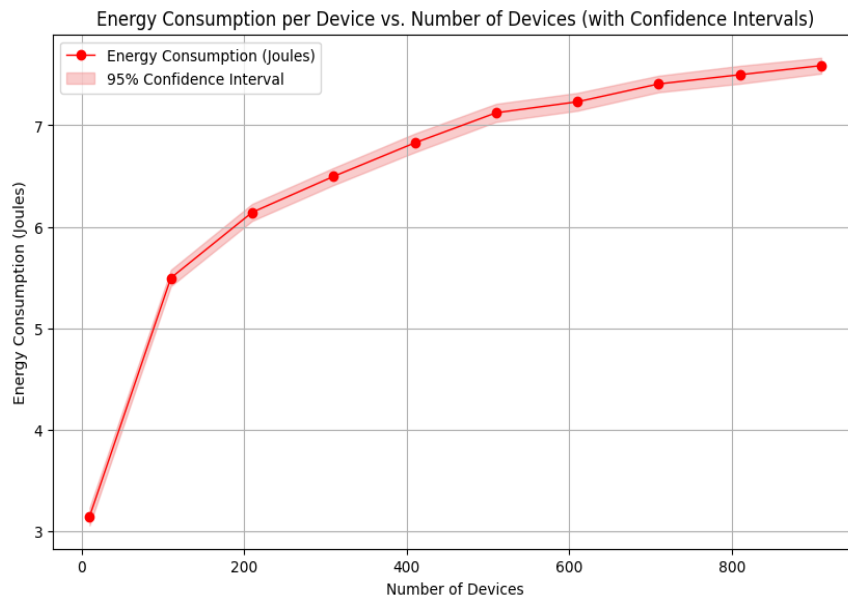


Fig. 9. Energy Consumption per Device vs. Numbers of Devices (with 95% Confidence Interval)

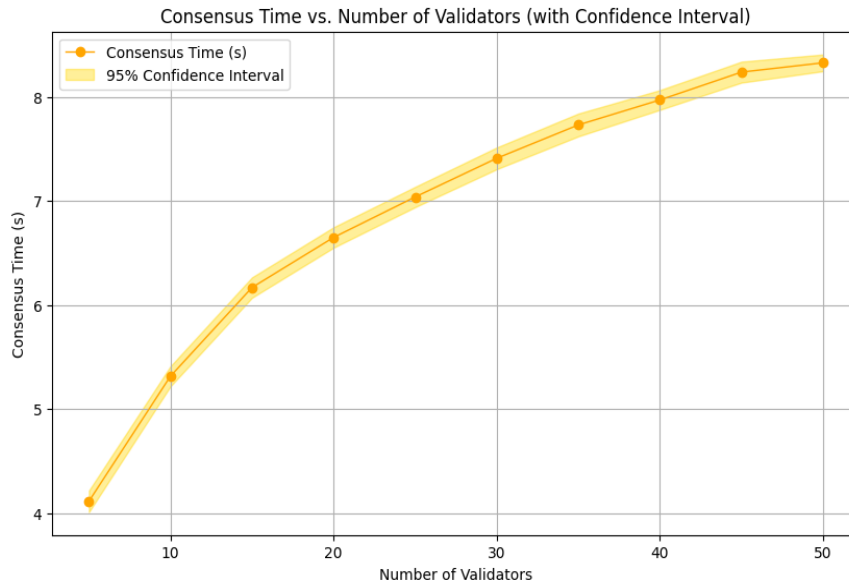


Fig. 10. Consensus Time vs. Number of Validators (with 95% Confidence Interval)

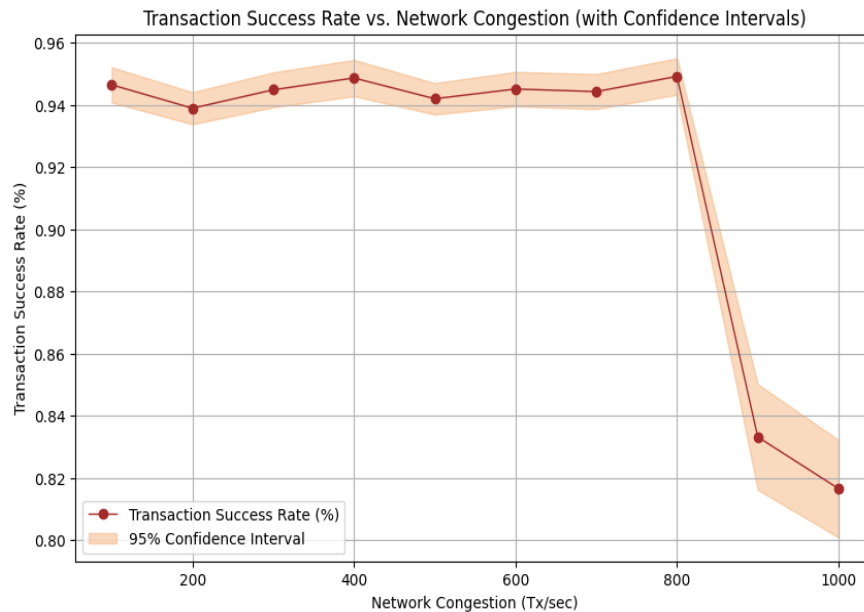


Fig. 11. Transaction success rate and network congestion (with 95% Confidence Interval)

Fig.12., Fig.13. and Fig.14. compares the performance of the proposed model with existing Ethereum block chain model. The comparison is made in terms of Latency, Energy Consumptions and consensus time. The Proposed model shows better performance in the areas of latency and Energy consumption. This mentioned performance is better specially when the number of devices connected to the network are higher. The average latency of the proposed model is 26.57% better than Ethereum for up to 1000 numbers of devices. Additionally, the average energy consumption of the proposed model is 35.29% lower than Ethereum. The consensus time of the model is initially lower than Ethereum's consensus time but it increases when number of validators count crosses 24. It signifies that while the proposed framework initially takes more time in the consensus mechanism, it achieves better overall latency and energy efficiency compared to Ethereum.

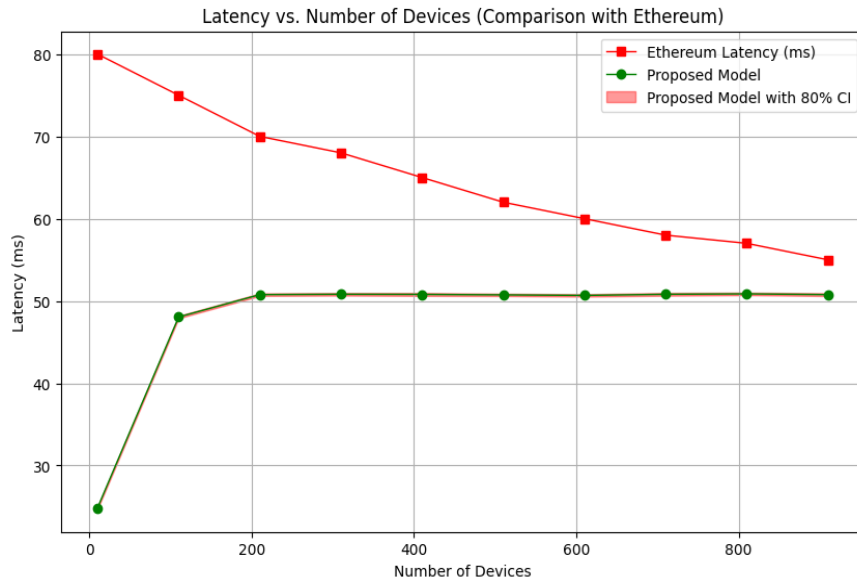


Fig. 12. Latency comparison between proposed model and Ethereum

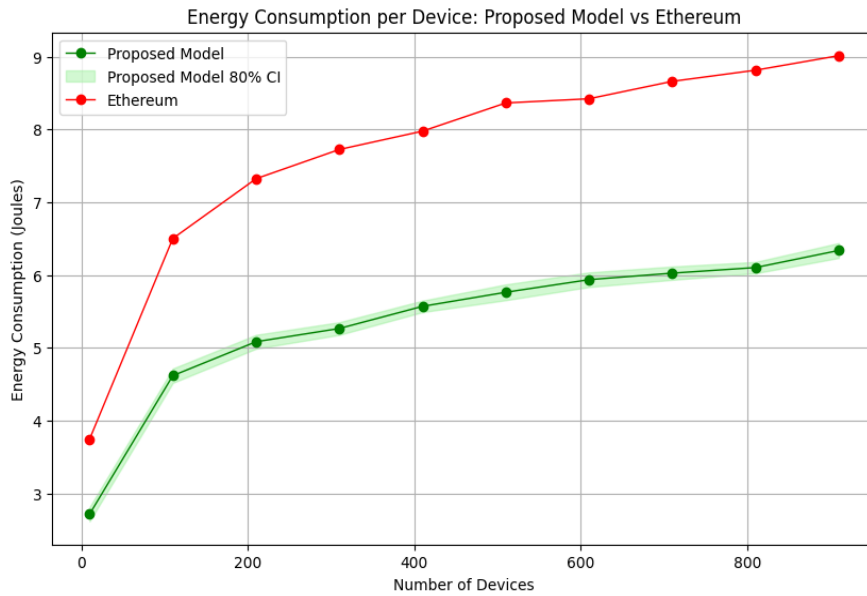


Fig. 13. Energy consumption comparison between proposed model and Ethereum

To analyze storage overhead, we use blocks of 100 transactions each with a transaction size average of 1.0 KB when comparing our model to Ethereum. We use these assumptions to determine storage requirements for varied device counts by using 10 transactions as the average per device. We observed that the proposed model and Ethereum require nearly the same storage overhead; however, the proposed model demonstrates slightly lower overhead as evident from Fig. 15.

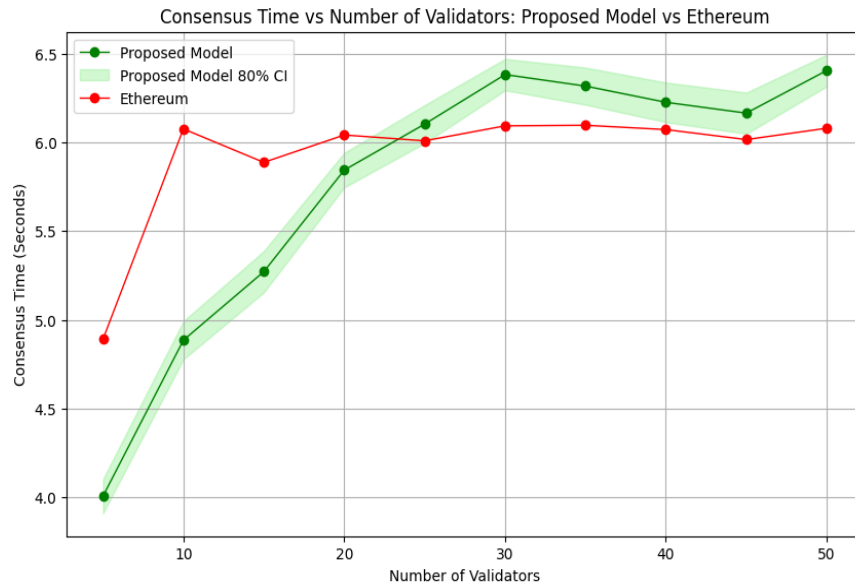


Fig. 14. Consensus time between proposed model and Ethereum

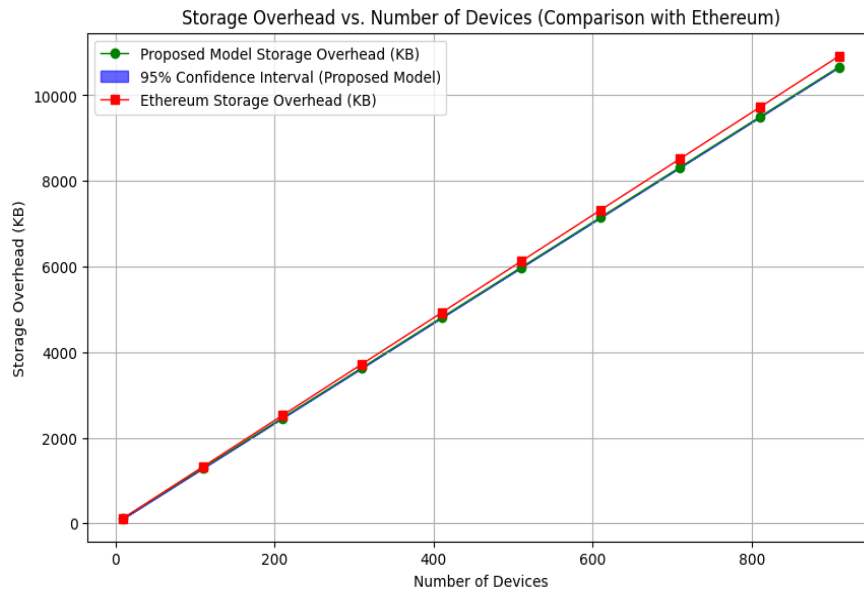


Fig.15. Storage overhead comparison of the proposed model with Ethereum

5. Conclusion and Future Work

The proposed blockchain system effectively resolves significant difficulties in IoT connectivity, such as scalability, performance, and security. The framework utilizes blockchain's decentralized architecture to eradicate central points of failure and guarantees trust via an immutable ledger. The system reliably sustains stable performance while handling extensive IoT networks, showcasing its capacity to accommodate rising device loads without sacrificing efficiency. The system efficiently identifies and mitigates illegal access attempts, ensuring robust protection for critical IoT data. Its adaptive security protocols provide real-time risk management, rendering it a formidable tool for protecting IoT environments. The architecture ensures energy efficiency and scales seamlessly with the increasing number of devices, which is crucial for sustainable IoT implementations. Despite expanding network size, consensus times stay within acceptable thresholds while maintaining elevated communication and transaction validation rates throughout different degrees of network congestion.

Future research should investigate the optimization of the consensus method to improve performance in ultra-large-scale networks, as well as the integration of sophisticated security features, like decentralized identity management and AI-driven intrusion detection. Also, offloading block chain related computation using edge and fog computing may improve the performance of the system.

Declaration

In preparing this manuscript, I have utilized generative artificial intelligence (AI) tools solely to enhance the language and readability of the text. The use of AI was conducted under careful human oversight and control. All content has been thoroughly reviewed and edited to ensure accuracy, completeness, and alignment with the intended scholarly standards.

No generative AI tools or AI-assisted technologies were involved in the conceptualization, data analysis, or interpretation of the research findings presented in this manuscript.

References

- [1] Y. Harbi, Z. Aliouat, A. Refoufi, & S. Harous, "Recent security trends in internet of things: a comprehensive survey", *IEEE Access*, vol. 9, p. 113292-113314, 2021. <https://doi.org/10.1109/access.2021.3103725>
- [2] K. Noh, J. Park, & J. Park, "Data transmission direction-based routing algorithm for improving network performance of IOT systems", *Applied Sciences*, vol. 10, no. 11, p. 3784, 2020. <https://doi.org/10.3390/app10113784>
- [3] H. Zhang, B. Di, K. Bian, & L. Song, "Iot-u: cellular internet-of-things networks over unlicensed spectrum", *IEEE Transactions on Wireless Communications*, vol. 18, no. 5, p. 2477-2492, 2019. <https://doi.org/10.1109/twc.2019.2904269>
- [4] A. Falayi, "Survey of distributed and decentralized iot securities: approaches using deep learning and blockchain technology", *Future Internet*, vol. 15, no. 5, p. 178, 2023. <https://doi.org/10.3390/fi15050178>
- [5] W. Zhou, "A blockchain-based privacy-preserving and fair data transaction model in iot", *Applied Sciences*, vol. 13, no. 22, p. 12389, 2023. <https://doi.org/10.3390/app132212389>
- [6] M. Parmar, "Internet of things-blockchain integration: a robust data security approach for end-to-end communication", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 2, p. 1050, 2023. <https://doi.org/10.11591/ijeecs.v32.i2.pp1050-1057>
- [7] S. Meisami, S. Meisami, M. Yousefi, & M. Aref, "Combining blockchain and iot for decentralized healthcare data management", *International Journal on Cryptography and Information Security*, vol. 13, no. 1, p. 35-50, 2023. <https://doi.org/10.5121/ijcis.2023.13102>
- [8] B. Bryant and H. Saiedian, "Key challenges in security of iot devices and securing them with the blockchain technology", *Security and Privacy*, vol. 5, no. 5, 2022. <https://doi.org/10.1002/spy2.251>
- [9] A. Ghali, R. Ahmad, & H. Alhussian, "A framework for mitigating ddos and dos attacks in iot environment using hybrid approach", *Electronics*, vol. 10, no. 11, p. 1282, 2021. <https://doi.org/10.3390/electronics10111282>
- [10] R. Alhamarneh, "Strengthening internet of things security: surveying physical unclonable functions for authentication, communication protocols, challenges, and applications", *Applied Sciences*, vol. 14, no. 5, p. 1700, 2024. <https://doi.org/10.3390/app14051700>
- [11] M. Adam, "A survey on security, privacy, trust, and architectural challenges in iot systems", *Ieee Access*, vol. 12, p. 57128-57149, 2024. <https://doi.org/10.1109/access.2024.3382709>
- [12] L. AlSuwaidan and N. Almegren, "Validating the adoption of heterogeneous internet of things with blockchain", *Future Internet*, vol. 12, no. 6, p. 107, 2020. <https://doi.org/10.3390/fi12060107>
- [13] M. Noaman, M. Khan, M. Abrar, S. Ali, A. Alvi, & M. Saleem, "Challenges in integration of heterogeneous internet of things", *Scientific Programming*, vol. 2022, p. 1-14, 2022. <https://doi.org/10.1155/2022/8626882>
- [14] Z. Valadkhani, F. Lotfi, & B. Rodić, "A vision of the internet of things: a review of critical challenges", *International Journal of Computer and Information Technology (2279-0764)*, vol. 10, no. 4, 2021. <https://doi.org/10.24203/ijcit.v10i4.121>
- [15] M. Mansour, A. Gamal, A. Ahmed, L. Said, A. Elbaz, N. Herencsáret al., "Internet of things: a comprehensive overview on protocols, architectures, technologies, simulation tools, and future directions", *Energies*, vol. 16, no. 8, p. 3465, 2023. <https://doi.org/10.3390/en16083465>
- [16] F. Pereira, R. Correia, P. Pinho, S. Lopes, & N. Carvalho, "Challenges in resource-constrained iot devices: energy and communication as critical success factors for future iot deployment", *Sensors*, vol. 20, no. 22, p. 6420, 2020. <https://doi.org/10.3390/s20226420>
- [17] M. Khan, O. Alhazmi, M. Javed, H. Ghandorh, & K. Aloufi, "Reliable internet of things: challenges and future trends", *Electronics*, vol. 10, no. 19, p. 2377, 2021. <https://doi.org/10.3390/electronics10192377>
- [18] L. Tello-Oquendo, S. Lin, I. Akyildiz, & V. Pla, "Software-defined architecture for qos-aware iot deployments in 5g systems", *Ad Hoc Networks*, vol. 93, p. 101911, 2019. <https://doi.org/10.1016/j.adhoc.2019.101911>
- [19] T. Nguyen and D. Hoang, "S-manage protocol for software-defined iot", In *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1-6. IEEE, 2018. <https://doi.org/10.1109/atnac.2018.8615336>
- [20] A. Ateya, A. Algarni, M. Hamdi, A. Koucheryavy, & N. Soliman, "Enabling heterogeneous iot networks over 5g networks with ultra-dense deployment—using mec/sdn", *Electronics*, vol. 10, no. 8, p. 910, 2021. <https://doi.org/10.3390/electronics10080910>
- [21] V. Quy, N. Hoai, L. Manh, L. Ngoc, & G. Jeon, "Wireless communication technologies for iot in 5g: vision, applications, and challenges", *Wireless Communications and Mobile Computing*, vol. 2022, p. 1-12, 2022. <https://doi.org/10.1155/2022/3229294>
- [22] M. Bataineh, W. Mardini, Y. Khamayseh, & M. Yasin, "Novel and secure blockchain framework for health applications in iot", *Ieee Access*, vol. 10, p. 14914-14926, 2022. <https://doi.org/10.1109/access.2022.3147795>
- [23] Y. Li, Y. Tu, J. Lu, & Y. Wang, "A security transmission and storage solution about sensing image for blockchain in the internet of things", *Sensors*, vol. 20, no. 3, p. 916, 2020. <https://doi.org/10.3390/s20030916>
- [24] A. Maftei, A. Lavric, A. Petrariu, & V. Popa, "Massive data storage solution for iot devices using blockchain technologies", *Sensors*, vol. 23, no. 3, p. 1570, 2023. <https://doi.org/10.3390/s23031570>
- [25] M. Abidin, S. Suhaad, K. Mashiko, & N. Ismail, "Ethereum blockchain network implementation for iot platform", *International Journal of Integrated Engineering*, vol. 11, no. 7, 2019. <https://doi.org/10.30880/ijie.2019.11.07.001>

- [26] S. Algarni, F. Eassa, K. Almarhabi, A. Almalaise, E. Albassam, K. Alsubhiet al., "Blockchain-based secured access control in an iot system", *Applied Sciences*, vol. 11, no. 4, p. 1772, 2021. <https://doi.org/10.3390/app11041772>
- [27] R. Jmal, W. Ghabri, R. Guesmi, B. Alshammari, A. Alshammari, & H. Alsaif, "Distributed blockchain-sdn secure iot system based on ann to mitigate ddos attacks", *Applied Sciences*, vol. 13, no. 8, p. 4953, 2023. <https://doi.org/10.3390/app13084953>
- [28] H. Emira, "Blockchain-enabled security framework for enhancing iot networks: a two-layer approach", *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 10, 2023. <https://doi.org/10.14569/ijacsa.2023.0141059>
- [29] A. Hwaitat, "A new blockchain-based authentication framework for secure iot networks", *Electronics*, vol. 12, no. 17, p. 3618, 2023. <https://doi.org/10.3390/electronics12173618>
- [30] K. Arachchige, "Evaluation of blockchain networks' scalability limitations in low-powered internet of things (iot) sensor networks", *Future Internet*, vol. 15, no. 9, p. 317, 2023. <https://doi.org/10.3390/fi15090317>
- [31] Gulia, Preeti, et al., "Exploring the potential of blockchain technology in an iot-enabled environment: a review", *Ieee Access*, vol. 12, p. 31197-31227, 2024. <https://doi.org/10.1109/access.2024.3366656>
- [32] U. Khalid, M. Asim, T. Baker, P. Hung, M. Tariq, & L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for iot systems", *Cluster Computing*, vol. 23, no. 3, p. 2067-2087, 2020. <https://doi.org/10.1007/s10586-020-03058-6>
- [33] R. Singh, H. Sharma, T. Choudhury, A. Mor, S. Mohanty, & S. Mohanty, "Blockchain for iot-enabled healthcare", *Eai Endorsed Transactions on Pervasive Health and Technology*, vol. 9, 2023. <https://doi.org/10.4108/eetpht.9.3348>
- [34] M. Bhavsingh, "A blockchain-based approach for securing network communications in iot environments", *International Journal of Computer Engineering in Research Trends*, vol. 10, no. 10, p. 37-43, 2023. <https://doi.org/10.22362/ijcert/2023/v10/i10/v10i106>
- [35] P. Schmid, A. Schaffhauser, & R. Kashef, "Iotbchain: adopting blockchain technology to increase plc resilience in an iot environment", *Information*, vol. 14, no. 8, p. 437, 2023. <https://doi.org/10.3390/info14080437>
- [36] K. Arachchige, "An analysis of blockchain-based iot sensor network distributed denial of service attacks", *Sensors*, vol. 24, no. 10, p. 3083, 2024. <https://doi.org/10.3390/s24103083>
- [37] K. Sharma, "Securing iot devices from ddos attacks through blockchain and multi-code trust framework", *E3s Web of Conferences*, vol. 472, p. 03001, 2024. <https://doi.org/10.1051/e3sconf/202447203001>
- [38] S. Koppu, K. Kumar, S. Somayaji, M. Iyapparaja, W. Wang, & C. Su, "Fusion of blockchain, iot and artificial intelligence - a survey", *Ieice Transactions on Information and Systems*, vol. E105.D, no. 2, p. 300-308, 2022. <https://doi.org/10.1587/transinf.2021bcr0001>
- [39] S. Abdulrahman and M. Useng, "Blockchain and distributed ledger technologies for iot security: a survey paper", *Mesopotamian Journal of Computer Science*, p. 5-8, 2022. <https://doi.org/10.58496/mjcs/2022/006>
- [40] M. Mohammed, "Enhancing iot data security with lightweight blockchain and okamoto uchiyama homomorphic encryption", *Computer Modeling in Engineering & Sciences*, vol. 138, no. 2, p. 1731-1748, 2024. <https://doi.org/10.32604/cmescs.2023.030528>
- [41] R. Xu, Y. Chen, and E. Blasch, "Microchain: A light hierarchical consensus protocol for IoT systems," in *Blockchain Applications in IoT Ecosystem*, Springer, 2021. doi: https://doi.org/10.1007/978-3-030-65691-1_9.
- [42] M. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, A. Μαγλαράς, & H. Janicke, "Blockchain technologies for the internet of things: research issues and challenges", *Ieee Internet of Things Journal*, vol. 6, no. 2, p. 2188-2204, 2019. <https://doi.org/10.1109/jiot.2018.2882794>
- [43] A. Sadawi, M. Hassan, & M. Ndiaye, "A survey on the integration of blockchain with iot to enhance performance and eliminate challenges", *Ieee Access*, vol. 9, p. 54478-54497, 2021. <https://doi.org/10.1109/access.2021.3070555>
- [44] V. KARTHIKA and S. JAGANATHAN, "Iledger: a lightweight blockchain framework with new consensus method for iot applications", *Ieice Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. E106.A, no. 9, p. 1251-1262, 2023. <https://doi.org/10.1587/transfun.2022eap1088>
- [45] X. Hu, Y. Su, & R. Guo, "Iot adaptive dynamic blockchain networking method based on discrete heartbeat signals", *Sensors*, vol. 20, no. 22, p. 6503, 2020. <https://doi.org/10.3390/s20226503>
- [46] S. Alrubei, E. Ball, & J. Rigelsford, "HDPoA: Honesty-based distributed proof of authority via scalable work consensus protocol for IoT-blockchain applications," *Computer Networks*, vol. 217, p. 109337, 2022. <https://doi.org/10.1016/j.comnet.2022.109337>
- [47] S. Misra, A. Mukherjee, A. Roy, N. Saurabh, Y. Rahulamathavan, & M. Rajarajan, "Blockchain at the edge: performance of resource-constrained iot networks", *Ieee Transactions on Parallel and Distributed Systems*, vol. 32, no. 1, p. 174-183, 2021. <https://doi.org/10.1109/tpds.2020.3013892>
- [48] Z. Lee, R. Chua, S. Keoh, & Y. Ohba, "Performance evaluation of big data processing at the edge for iot-blockchain applications", *IEEE Global Communications Conference (GLOBECOM)*, Waikoloa, HI, USA, 2019, pp. 1-6, 2019. <https://doi.org/10.1109/globecom38437.2019.9013329>
- [49] S. Brotsis, N. Kolokotronis, K. Limnietis, & S. Shialeles, "On the security of permissioned blockchain solutions for iot applications", *6th IEEE Conference on Network Softwarization (NetSoft)*, Ghent, Belgium, 2020, pp. 465-472, 2020. <https://doi.org/10.1109/netsoft48620.2020.9165480>
- [50] B. Cao, Y. Li, L. Zhang, Z. Long, S. Mumtaz, Z. Zhouet al., "When internet of things meets blockchain: challenges in distributed consensus", *Ieee Network*, vol. 33, no. 6, p. 133-139, 2019. <https://doi.org/10.1109/mnet.2019.1900002>
- [51] X. Lu and C. Jiang, "Teedag: a high-throughput distributed ledger based on tee and directed acyclic graph", *Electronics*, vol. 12, no. 11, p. 2393, 2023. <https://doi.org/10.3390/electronics12112393>
- [52] S. Alghamdi, "Enabling a secure iot environment using a blockchain-based local-global consensus manager", *Electronics*, vol. 12, no. 17, p. 3721, 2023. <https://doi.org/10.3390/electronics12173721>
- [53] H. F. Atlam, A. Alenezi, M. O. Alassafi, & G. Wills, "Blockchain with Internet of Things: Benefits, challenges, and future directions," *International Journal of Intelligent Systems and Applications*, vol. 10, no. 6, pp. 40-48, 2018.
- [54] J. Hu, M. Reed, M. Al-Naday, & N. Thomos, "Hybrid blockchain for iot—energy analysis and reward plan", *Sensors*, vol. 21, no. 1, p. 305, 2021. <https://doi.org/10.3390/s21010305>

- [55] M. Uddin, A. Stranieri, I. Gondal, & V. Balasubramanian, "Blockchain leveraged decentralized iot ehealth framework", *Internet of Things*, vol. 9, p. 100159, 2020. <https://doi.org/10.1016/j.iot.2020.100159>
- [56] M. Uddin, M. Muzammal, M. Hameed, I. Javed, B. Alamri, & N. Crespi, "Cbciot: a consensus algorithm for blockchain-based iot applications", *Applied Sciences*, vol. 11, no. 22, p. 11011, 2021. <https://doi.org/10.3390/app112211011>
- [57] V. Upadhyay, A. Vaish, & J. Kokila, "The need for lightweight consensus algorithms in IoT environment: A review," *Proceedings of the 2024 Sixteenth International Conference on Contemporary Computing*, 2024.
- [58] H. Lee, H. Seo, & W. Choi, "Fast and scalable distributed consensus over wireless large-scale internet of things network", *Ieee Internet of Things Journal*, vol. 9, no. 11, p. 7916-7930, 2022. <https://doi.org/10.1109/jiot.2021.3118928>
- [59] L. Li, D. Huang, & C. Zhang, "An efficient DAG blockchain architecture for IoT," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1286-1296, Jan. 15, 2023. <https://doi.org/10.1109/JIOT.2022.3206337>
- [60] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng et al., "Direct acyclic graph-based ledger for internet of things: performance and security analysis", *Ieee/Acm Transactions on Networking*, vol. 28, no. 4, p. 1643-1656, 2020. <https://doi.org/10.1109/tnet.2020.2991994>
- [61] Z. Auhl, N. Chilamkurti, R. Alhadad, & W. Heyne, "A comparative study of consensus mechanisms in blockchain for iot networks", *Electronics*, vol. 11, no. 17, p. 2694, 2022. <https://doi.org/10.3390/electronics11172694>
- [62] T. Cai, H. Lin, W. Chen, Z. Zheng, & Y. Yan, "Efficient blockchain-empowered data sharing incentive scheme for internet of things", *International Journal of Software and Informatics*, vol. 11, no. 3, p. 287-313, 2021. <https://doi.org/10.21655/ijsi.1673-7288.00264>
- [63] H. Guo, W. Li, & M. Nejad, "A hierarchical and location-aware consensus protocol for iot-blockchain applications", *Ieee Transactions on Network and Service Management*, vol. 19, no. 3, p. 2972-2986, 2022. <https://doi.org/10.1109/tnsm.2022.3176607>
- [64] M. Alaslani, F. Nawab, & B. Shihada, "Blockchain in iot systems: end-to-end delay evaluation", *Ieee Internet of Things Journal*, vol. 6, no. 5, p. 8332-8344, 2019. <https://doi.org/10.1109/jiot.2019.2917226>
- [65] Y. Xu, F. Luo, M. Haider, Z. Chen, & Y. Li, "Efficient byzantine consensus mechanism based on reputation in iot blockchain", *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, 2021. <https://doi.org/10.1155/2021/9952218>
- [66] H. Zubaydi, P. Varga, & S. Molnár, "Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: a systematic literature review", *Sensors*, vol. 23, no. 2, p. 788, 2023. <https://doi.org/10.3390/s23020788>
- [67] G. Sagirlar, J. D. Sheehan, & E. Ragnoli, "On the design of co-operating blockchains for IoT," *3rd International Conference on Information and Computer Technologies (ICICT)*, San Jose, CA, USA, vol. 3, pp. 548-552, 2020. <https://doi.org/10.1109/ICICT50521.2020.00093>
- [68] P. VG, "Blockfog: a blockchain-based framework for intrusion defense in iot fog computing", *Scalable Computing Practice and Experience*, vol. 25, no. 3, p. 1950-1962, 2024. <https://doi.org/10.12694/scpe.v25i3.2686>
- [69] Y. Bobde, "Enhancing industrial iot network security through blockchain integration", *Electronics*, vol. 13, no. 4, p. 687, 2024. <https://doi.org/10.3390/electronics13040687>
- [70] A. Khan, A. Laghari, M. Dootio, & S. Karim, "The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises", *Scientific Reports*, vol. 13, no. 1, 2023. <https://doi.org/10.1038/s41598-023-28707-9>
- [71] S. Sharma, "Streamlining iot-driven data using blockchain", *Int Res J Adv Engg Mgt*, vol. 2, no. 05, p. 1509-1514, 2024. <https://doi.org/10.47392/irjaem.2024.0204>

Authors' Profiles



Sudipta Majumder earned his B.Tech in Computer Science and Engineering from NERIST in 2009, followed by an M.Tech in Information Technology and a PhD in Network Security from the Department of Electronics and Communication Engineering. His research interests include the Internet of Things (IoT), optimization, machine learning, wireless networks, and network security. Currently, he serves as a Senior Assistant Professor in the Department of Computer Science and Engineering at DUIET, Dibrugarh University. He is also a life member of the Computer Society of India (CSI).

How to cite this paper: Sudipta Majumder, "A Scalable Blockchain Framework for Secure IoT Communication", *International Journal of Information Engineering and Electronic Business(IJIEEB)*, Vol.17, No.4, pp. 26-40, 2025. DOI:10.5815/ijieeb.2025.04.03