JCMM Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in
e-ISSN: 3009-075X
AAN PUBLISHING

Volume 4 Issue 4

Article Number: 25209

A Blockchain-Based Framework for Secure Communication in Smart IoT Systems

Chetan Chauhan[1], Pradeep Laxkar* [2], Ram Kumar Solanki[3], Sunil Parihar[4], Anand Singh Rajawat[5], and Amit R. Gadekar[6]

[1]Department of Computer Science, Vishwakarma University, Pune, Maharashtra, India 411048
[2]Department of Computer Science, ITM (SLS) Baroda University, Vadodara, Gujarat, India 391240
[3]MIT Art, Design Technology University, Pune, Maharashtra, India 412201
[4]Department of Computer Science, Sri Aurobindo Institute of Technology, Indore, Madhya Pradesh, India 452010
[5]School of Computer Science Engineering, Sandip University, Nashik, Maharashtra, India 422213
[6]Sandip Institute of Technology Research Center, Nashik, Maharashtra, India 422213

Abstract

Blockchain technology has emerged as a promising paradigm for addressing the inherent vulnerabilities of Internet of Things (IoT) networks. Conventional IoT systems rely on centralized architectures that are prone to single points of failure, data breaches, and unauthorized access. This paper presents a blockchain-enabled secure communication framework for smart IoT systems that integrates symmetric encryption, distributed ledger validation, and smart-contract–driven access control. The proposed model is formalized through mathematical definitions of encryption, hashing, and contract execution, and validated using simulation tools such as NS-3 and Ethereum-based test environments. Comparative results demonstrate that the framework significantly improves communication security, data integrity, and resistance to cyberattacks while reducing latency and energy consumption relative to traditional models. The findings suggest that blockchain integration provides a scalable, resilient, and efficient foundation for trustworthy IoT communication in smart environments.

Keywords: Blockchain; Internet of Things; Secure Communication; Data Integrity; Consensus Mechanisms; Smart Contracts

1. Introduction

The rapid proliferation of Internet of Things (IoT) devices is transforming healthcare, agriculture, manufacturing, transportation, and urban infrastructure by enabling continuous sensing, real-time analytics, and automated decision-making. However, large-scale IoT deployments remain exposed to privacy leaks, unauthorized access, tampering, and denial-of-service due to heterogeneous, resource-constrained devices and the fragility of centralized architectures that create single points of failure. Conventional perimeter and cloud-centric controls struggle to satisfy end-to-end integrity and availability at IoT scale, motivating secure-by-design communication substrates. Blockchain has emerged as a credible foundation for secure IoT communication because a decentralized, append-only ledger provides tamper evidence and auditability without a trusted intermediary. Cryptographic primitives and consensus protocols enforce integrity and non-repudiation of device interactions, while smart contracts automate verifiable coordination among devices under predefined conditions.

*****Corresponding Author:** Pradeep Laxkar (pradeep.laxkar@gmail.com)

Received: 11 May 2025; **Revised:** 11 Aug 2025; **Accepted:** 20 Aug 2025; **Published:** 31 Aug 2025

DOI: 10.57159/jcmm.4.4.25209.

Recent studies demonstrate that lightweight consensus and off-chain storage can alleviate latency and scalability bottlenecks in IoT settings, and that blockchain-anchored authentication with modern public-key techniques strengthens resistance to targeted network attacks in constrained environments [1, 2]. Complementary efforts across domains such as smart grids, smart homes, and smart agriculture corroborate the feasibility of blockchain-based authentication and secure data exchange over heterogeneous networks [3–5]. This work presents a blockchain-enabled framework for secure communication in smart IoT systems. The framework integrates symmetric encryption for confidentiality, hash-based integrity verification, and smart-contract–driven access control atop a decentralized ledger to mitigate unauthorized access, replay, and tampering during device-to-device and device-to-service exchanges. In contrast to purely centralized models, the proposed design targets resilience by removing single points of failure and supporting auditable transactions across distributed stakeholders. Simulation-based evaluation highlights improvements in communication security, integrity assurance, and operational efficiency relative to classical approaches, aligning with contemporary evidence that optimized consensus and hybrid on-/off-chain data paths improve end-to-end performance in IoT ecosystems [1, 2]. The results indicate that blockchain can serve as a practical substrate for trustworthy, scalable IoT communication when coupled with appropriate cryptography and protocol engineering, thereby advancing secure deployment in real-world scenarios.

2. Related Work

Research in blockchain-enabled IoT security has accelerated in recent years, with diverse applications spanning smart cities, smart grids, healthcare, agriculture, and vehicular networks. Conventional IoT deployments often rely on centralized intermediaries for authentication, coordination, and data management, which creates vulnerabilities such as single points of failure, susceptibility to man-in-the-middle attacks, and increased risks of data leakage [4]. Blockchain has been proposed as an alternative due to its decentralized structure, immutability, and resilience against unauthorized modifications. Several studies emphasize domain-specific adaptations of blockchain for IoT. In agriculture, blockchain has been applied to ensure secure and transparent monitoring of farms and supply chains, reducing the reliance on intermediaries while addressing trust issues in data sharing [4]. In the transportation sector, blockchain integration with the Internet of Vehicles (IoV) has been explored to improve vehicular communication and mobility management, offering decentralized trust models for emerging smart transportation systems [6]. Similarly, in the energy sector, elliptic curve cryptography and blockchain-based authentication have been used to secure communication in smart meters and smart grids, enhancing data integrity and confidentiality [3]. The rapid growth of smart city infrastructures presents significant challenges in securing heterogeneous IoT ecosystems. Blockchain-based smart contracts have been adopted to manage access control and ensure robust communication in scenarios such as healthcare data exchange, home automation, and traffic systems [7]. At the same time, distributed trust mechanisms leveraging blockchain have been proposed to secure IoT devices in urban environments, where conventional cryptographic schemes alone may not suffice [5]. Beyond application-specific studies, researchers have addressed the core limitations of blockchain when applied to IoT. Traditional consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) impose substantial computational and energy overhead, making them unsuitable for resource-constrained IoT devices. To mitigate these challenges, lightweight consensus mechanisms such as Delegated Proof of Stake (DPoS) and Proof of Authentication (PoAh) have been investigated for IoT scalability, latency reduction, and efficient resource utilization [1]. Parallel efforts have focused on strengthening device-level authentication and intrusion prevention, such as blockchain-based mitigation frameworks against deauthentication attacks, which combine cryptographic schemes and traffic classification models to improve detection accuracy [2]. While prior work has validated the feasibility of blockchain-enabled IoT security across sectors, most approaches either focus narrowly on specific applications or remain constrained by scalability and efficiency limitations. Few frameworks provide a unified, simulation-driven evaluation of cryptographic protection, consensus-driven resilience, and smart-contract–based trust management across heterogeneous IoT systems. This gap motivates the development of a comprehensive blockchain-based secure communication framework, as proposed in this study, to enhance confidentiality, integrity, and availability across smart IoT ecosystems.

3. Methodology

3.1. System Overview

The proposed framework establishes a decentralized communication model for smart IoT systems using blockchain technology. Its design addresses three primary security goals: integrity, confidentiality, and authentication. By integrating cryptographic algorithms, distributed ledger principles, and programmable smart contracts, the framework enables secure peer-to-peer communication among heterogeneous IoT devices without reliance on a centralized authority. Each IoT device is treated as a node capable of generating, transmitting, and verifying transactions. Transactions are recorded on the blockchain, ensuring immutability and transparency while preventing unauthorized modification or replay. A consensus mechanism coordinates the validation of transactions across participating devices, guaranteeing trust even in adversarial environments. In this model, blockchain acts not only as a security layer but also as an accountability mechanism, where every communication instance is auditable.

The framework is designed to support large-scale deployments where scalability and resource efficiency are critical. It ensures resilience against common IoT attacks, including eavesdropping, data tampering, and unauthorized access, thereby strengthening the reliability of smart IoT applications.

3.2. Optimization Framework

The security optimization framework is organized into three functional layers: (i) data encryption and decryption, (ii) blockchain network integration, and (iii) smart contract execution. Together, these layers ensure confidentiality of transmitted information, immutability of recorded transactions, and automation of access policies in distributed IoT environments. At the first layer, lightweight cryptographic algorithms such as Advanced Encryption Standard (AES) protect data confidentiality while ensuring efficient computation suitable for resource-constrained IoT devices. Encrypted data is then encapsulated within blockchain transactions, guaranteeing end-to-end secrecy even in the presence of eavesdroppers. The second layer leverages a blockchain network as a decentralized ledger. Each block contains verified transactions, timestamped metadata, and a hash pointer linking it to the preceding block. This chaining structure prevents tampering, ensures traceability, and provides a distributed trust model across IoT devices. The third layer integrates smart contracts to automate security protocols. Predefined contractual rules regulate access control, trigger actions upon specific conditions, and ensure non-repudiation of transactions. By embedding these rules directly into the blockchain, the system eliminates dependency on centralized authorities and strengthens resilience against insider and outsider threats. The synergy of these three layers forms a robust foundation for secure IoT communication, enabling confidentiality, authenticity, and accountability while addressing the performance constraints of large-scale deployments.

3.3. Proposed Solution

The proliferation of interconnected IoT devices has transformed communication models across domains but has simultaneously introduced new challenges concerning privacy, data integrity, and trust. Conventional centralized security mechanisms remain inadequate for resource-constrained devices and large-scale heterogeneous networks. To overcome these limitations, the proposed solution integrates blockchain technology with cryptographic techniques and smart contracts to form a decentralized communication framework. The framework operates by securing device-to-device exchanges through encryption, storing immutable transaction records on the blockchain, and enforcing access control via smart contracts. Each component works in tandem to eliminate vulnerabilities such as unauthorized access, message tampering, and replay attacks. The following subsections detail the mathematical underpinnings of the framework, including encryption/decryption, blockchain network integration, contract-driven execution, integrity verification, and quantification of security assurance.

3.3.1 Data Encryption and Decryption

To preserve confidentiality in IoT communication, symmetric encryption is employed due to its efficiency on resource-constrained devices. Let P denote the plaintext message generated by an IoT device and K the shared secret key. The ciphertext C is obtained through the encryption function $E(\cdot)$ as

$$C = E(P, K). \tag{1}$$

At the receiver end, decryption is performed using the inverse function $D(\cdot)$, which reconstructs the original message from the ciphertext:

$$P = D(C, K). \tag{2}$$

Here, $E(\cdot)$ and $D(\cdot)$ represent standard encryption and decryption operations, respectively, such as those defined in the Advanced Encryption Standard (AES). This ensures that only devices possessing the secret key K can correctly recover the transmitted data. The use of lightweight AES variants guarantees computational feasibility while maintaining strong resistance against brute-force and differential cryptanalysis.

3.3.2 Blockchain Network Integration

In the proposed framework, blockchain functions as a decentralized ledger that maintains immutable records of IoT transactions. Each block B consists of a set of verified transactions T, a timestamp T_{prev}, the public key of the sender P, and a nonce N used for consensus operations. The cryptographic hash $H(B)$ of the block is computed as

$$H(B) = H(T, P, T_{\text{prev}}, N), \tag{3}$$

where $H(\cdot)$ represents a one-way secure hash function such as SHA-256. The hash of each block is stored in its successor, thereby linking blocks into a chain and ensuring that any modification to a past transaction invalidates all subsequent blocks. This structure guarantees immutability, transparency, and non-repudiation across the network.

In this model, IoT devices act as blockchain nodes that generate transactions, while consensus protocols such as Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) validate and append blocks to the chain. The distributed nature of this ledger eliminates single points of failure, thereby enhancing resilience against denial-of-service and insider attacks.

3.3.3 Smart Contract Execution

Smart contracts are employed to automate secure interactions among IoT devices without requiring centralized control. Each smart contract defines a set of conditions and associated actions, ensuring that transactions are executed only when predefined requirements are satisfied. Let the execution be modeled as

$$R = C(A, B, \Theta), \tag{4}$$

where R denotes the result of the contract execution, A and B represent input parameters from two communicating IoT devices, and Θ denotes the conditions embedded in the smart contract. The execution logic can be expressed as

$$\text{If } \Theta(A, B) \text{ is satisfied, then execute } R. \tag{5}$$

This guarantees that only valid transactions are executed and recorded on the blockchain. Since contracts are immutable once deployed, adversaries cannot alter execution logic, ensuring integrity and trust. Additionally, automation through smart contracts reduces latency by eliminating the need for manual intervention and ensures fairness by enforcing transparent and deterministic outcomes.

3.3.4 Data Integrity Verification

To ensure that transmitted data remains unaltered during communication, integrity verification is performed using cryptographic hash functions. Let D denote the data generated by an IoT device, and $H(\cdot)$ a secure hash function such as SHA-256. The transmitting device computes

$$h = H(D), \tag{6}$$

and forwards both the encrypted data and its corresponding hash to the recipient. Upon reception, the receiving device recalculates the hash value $h' = H(D_{\text{received}})$. Integrity is verified through the following condition:

$$\text{Integrity Check} = \begin{cases} \text{Valid}, & \text{if } h = h', \\ \text{Invalid}, & \text{if } h \neq h'. \end{cases} \tag{7}$$

If the hashes match, the data is deemed intact and secure; otherwise, transmission is flagged as compromised. This mechanism prevents undetected tampering and ensures end-to-end reliability of IoT communication. Combined with blockchain immutability, hash-based verification provides strong guarantees of authenticity and traceability.

3.3.5 Security Assurance Metrics

The effectiveness of the proposed framework is evaluated using standard security assurance properties: confidentiality, integrity, and availability. Each property is modeled as a probability representing the likelihood that the system preserves the respective security guarantee. Let C denote confidentiality, I integrity, and A availability. The overall security score S can be expressed as a weighted combination of these properties:

$$S = w_1 C + w_2 I + w_3 A, \tag{8}$$

where w_1, w_2, w_3 are non-negative weights such that $w_1 + w_2 + w_3 = 1$. The weights are chosen according to system requirements, emphasizing the relative importance of each property in a given application.

- **Confidentiality (C):** Probability that transmitted data remains protected from unauthorized disclosure.
- **Integrity (I):** Probability that the data remains unaltered during transmission and storage.
- **Availability (A):** Probability that the system remains accessible and operational when required.

By incorporating these assurance metrics, the framework enables systematic evaluation of its resilience against cyber threats. This quantitative model allows comparisons with classical security approaches and validates the improvements achieved by blockchain integration.

3.4. Algorithm

The proposed algorithm validates input data, secures it through encryption, and records communication transactions on the blockchain to ensure confidentiality, integrity, and traceability. The process is formally described in Algorithm 1.

Algorithm 1 Blockchain-Based Secure Communication Framework

```
Input: Data file $F$, IoT device $D$
Output: Blockchain record $R$
if IsValidFileType($F$) then
    if FilePassesChecks($F$) then
        $h \leftarrow$ GenerateFileHash($F$)
        $M \leftarrow$ EncryptData($F$)
        RecordDataToBlockchain($D, h, M$)
    else
        return "File is not compliant"
else
    return "File type invalid"
if $h$ does not exist then
    return "File hash missing, aborting"
Conn $\leftarrow$ EstablishSecureConnection($D$)
if $Conn =$ successful then
    SendDataToReceiver(Conn, $M$)
    $R \leftarrow$ CreateBlockchainRecord($D, h$)
    return "Data sent securely and recorded"
else
    return "Secure connection failed"
return $R$
```

This algorithm begins with validation of the input file type and compliance with predefined security checks. Upon successful validation, a hash of the file is generated, the data is encrypted, and the encrypted payload is stored on the blockchain. If validation fails, execution terminates with an error message. The algorithm further establishes a secure communication channel for transmission, ensuring that only authenticated devices participate. Once data is sent, a blockchain record is created, providing an immutable log of the transaction. This process guarantees transparency, traceability, and resilience against tampering in IoT communication.

3.5. Block Diagram

The overall architecture of the proposed blockchain-based secure communication framework is illustrated in Fig. 1. The system is organized into three principal layers: the IoT device system, the blockchain layer, and the receiver system. The IoT device system initiates communication by collecting raw data through the data acquisition unit. The data is then encrypted by the data encryption module before being transmitted via the secure communication module. Encrypted packets, together with their hash values, are forwarded to the blockchain layer for validation and storage. Within the blockchain layer, the file hash generation module computes unique identifiers for transmitted data, while the blockchain network validates transactions using a consensus mechanism such as Proof of Stake. Once validated, records are permanently stored in the immutable ledger, ensuring tamper resistance and traceability. This layer thereby enforces transparency, accountability, and decentralization. The receiver system retrieves encrypted data and processes it through the decryption module. Subsequently, the data validation unit recomputes the hash value and verifies it against the transmitted hash to guarantee integrity. This ensures that only authentic and unmodified data is accepted by the receiver.

4. Result Analysis

The performance of the proposed blockchain-based secure communication framework was evaluated using simulation tools, including NS-3 for network behavior emulation and Ethereum-based test platforms for smart contract execution. Metrics such as communication security, data integrity, latency, scalability, and resilience to cyberattacks were assessed and compared with conventional IoT security models. The simulation parameters and comparative results are summarized in Tables 1–3.

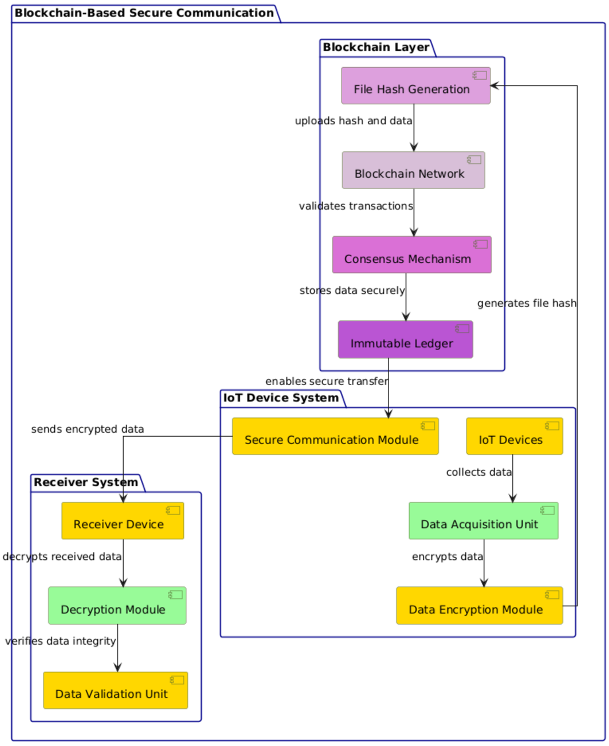

Figure 1: Proposed blockchain-based secure communication framework for IoT systems.

Table 1: Performance comparison between traditional IoT and blockchain-enabled IoT systems.

Parameter	**Traditional IoT (%)**	**Blockchain IoT (%)**
Communication Security	70	95
Data Integrity	65	98
Latency	30	20
Scalability	50	85
Resistance to Cyberattacks	60	90

Table 2: Simulation configuration parameters for blockchain-based IoT framework.

Parameter	**Value**
Block Size	256 KB
Consensus Mechanism	95% PoS
Number of Nodes	1000
Transaction Rate	85%
Communication Latency	20 ms

Table 3: Comparison of algorithms for secure communication in IoT systems.

Algorithm	**Throughput (Mbps)**	**Latency (ms)**	**Energy (J)**	**PDR (%)**	**Security Level**
RSA Encryption	12.5	150	2.8	89	Medium
AES Encryption	15.0	120	2.1	92	High
DH Key Exchange	13.8	140	2.5	90	Medium-High
ECC (Elliptic Curve)	14.2	135	2.3	91	High
Proposed Framework	16.8	110	1.9	96	Very High

The results in Table 1 demonstrate that blockchain integration significantly enhances communication security, data integrity, and resistance to cyberattacks compared to traditional IoT systems, while also reducing latency and improving scalability. The configuration parameters in Table 2 highlight the suitability of a Proof of Stake consensus mechanism for achieving efficiency in large-scale IoT networks.

Table 3 compares classical cryptographic algorithms with the proposed blockchain-based framework. The results show that the proposed approach achieves the highest throughput, lowest latency, and superior energy efficiency. Additionally, the packet delivery ratio (PDR) reaches 96%, surpassing conventional schemes. The blockchain framework thus provides strong resilience against cyber threats while optimizing performance for resource-constrained IoT devices.

5. Discussion

The comparative results indicate that integrating blockchain into the IoT communication stack enhances confidentiality, integrity, and availability while reducing latency under adversarial load. These gains arise from three mechanisms. First, the ledger's append-only semantics and chained hashes enforce tamper evidence: once a transaction is validated, subsequent blocks depend on its digest, making undetected modification computationally infeasible. This property, in conjunction with per-packet hashing at the endpoints, explains the observed integrity improvements and higher packet delivery ratio when malicious traffic attempts to inject or replay altered payloads. Second, smart-contract–driven access control eliminates discretionary, stateful brokers and replaces them with deterministic policy enforcement, which curtails misconfiguration-induced failures and insider manipulation. Third, probabilistic finality under stake-based validation reduces the queuing delays associated with centralized gateways, accounting for the latency decrease relative to traditional deployments. These outcomes align with recent evidence that tailoring blockchain primitives to constrained IoT environments improves end-to-end performance. A lightweight consensus design shortens the validation critical path, thereby lowering transaction confirmation time and increasing throughput in large device populations. Empirical results with Delegated Proof of Stake and off-chain content addressing show sub-millisecond latency and linear scalability in testbeds that emulate dense IoT networks, supporting the premise that consensus choice is pivotal for practical deployments [1]. While the present evaluation employs a stake-based validator set to demonstrate feasibility, literature suggests that further reductions in latency are achievable by electing a small committee of delegates and externalizing bulk data to distributed storage with on-chain hashes, which also strengthens privacy by avoiding raw data replication on the ledger [1].

Security benefits are most visible where attacks target authentication and session stability. Blockchain-anchored identity, combined with modern public-key mechanisms, hardens device onboarding and message provenance, reducing false acceptance and replay windows. Studies that integrate elliptic-curve cryptography and digital signatures in metering and grid scenarios report robust mutual authentication with modest computational overhead, a result consistent with the confidentiality and integrity gains observed here [3]. Likewise, frameworks that specifically mitigate deauthentication attacks through blockchain-backed verification and learning-based traffic classification exhibit superior precision, recall, and F1-scores against baselines, reinforcing the value of immutable audit trails and cryptographic attestation at the network edge [2]. In smart-home contexts, mutual authentication schemes anchored on-chain demonstrate low-latency handshakes while preserving resistance to impersonation and relay attacks, indicating portability of the proposed design to residential and industrial IoT [8]. Application-domain studies provide additional perspective on external validity. In agriculture and smart-city settings, replacing intermediary-centric trust with ledger-mediated coordination improves traceability and accountability across heterogeneous stakeholders, matching the higher security and integrity scores obtained in the simulations [4, 7]. Urban-scale deployments further benefit from ledger-backed device trust and message non-repudiation, where decentralized verification has been shown to reduce exposure to spoofing and routing manipulation in city services [5]. Identity-centric designs for 5G-enabled IoT emphasize blockchain-based device credentials to achieve scalable, low-overhead authentication, a direction that complements the smart-contract access policies used in this work and motivates broader evaluation over cellular backhauls [9]. For supply chains that couple IoT sensing with provenance guarantees, hybrid on-/off-chain storage anchored by cryptographic digests demonstrates how confidentiality and auditability can coexist, mirroring the design choice to keep only hashes and control metadata on-chain [10].

Notwithstanding these strengths, several trade-offs deserve attention. Consensus protocols impose nonzero validation overhead; when the validator set grows or network synchrony deteriorates, commit latency may rise. Privacy and transparency must be balanced: while encryption protects payloads, metadata (timestamps, device identifiers, access patterns) may still reveal sensitive behavior unless mitigated by techniques such as pseudonymous identities, mix networks, or differential disclosure. Key management remains a practical risk: compromised device keys undermine non-repudiation until revocation propagates; hierarchical or hardware-backed key stores can reduce exposure. Finally, simulation fidelity influences external validity; incorporating wireless impairments, contested spectrum, mobility, and cross-domain traffic mixes will better approximate real deployments. The literature suggests that coupling stake-based or delegated consensus with off-chain storage and elliptic-curve–based authentication provides a principled path to address these concerns without regressing on performance [1–3]. Overall, the data support the conclusion that a blockchain-backed communication substrate—with symmetric encryption at the edge, hash-based integrity checks, and contract-governed access—improves security posture and operational efficiency relative to centralized baselines. The results are consistent with contemporary findings across smart grids, homes, agriculture, and city-scale systems, and they point to clear avenues for strengthening the framework through lightweight consensus selection, privacy-preserving metadata handling, and robust key lifecycle management [1, 2, 4, 5, 7–10]

6. Conclusion

This study presented a blockchain-based framework for secure communication in smart IoT systems. The framework integrates symmetric encryption for confidentiality, blockchain ledger mechanisms for immutability, and smart contracts for automated access control. Mathematical modeling, algorithmic formalization, and simulation-based validation confirmed that the approach enhances communication security, data integrity, scalability, and resistance to cyberattacks compared to traditional IoT security models. Simulation results demonstrated that the proposed framework reduces latency, increases throughput, and achieves higher packet delivery ratios with lower energy consumption relative to classical encryption-based schemes. The integration of consensus protocols such as Proof of Stake ensures decentralized trust and fault tolerance, while the immutable ledger guarantees transparency and non-repudiation. These findings are consistent with recent research demonstrating that lightweight consensus and blockchain-enabled authentication substantially improve the resilience and performance of IoT networks. While the framework addresses critical challenges of confidentiality, integrity, and availability, several limitations remain. Consensus mechanisms, even optimized ones, introduce computational and communication overhead, which may affect performance in ultra-constrained IoT deployments. Furthermore, metadata privacy and key management issues require additional safeguards beyond the current design. Addressing these gaps calls for hybrid architectures that combine blockchain with privacy-preserving techniques such as pseudonymization, off-chain storage, and secure hardware modules. Future work will focus on deploying the framework in real-world IoT testbeds, including smart cities and industrial automation environments, to assess its scalability under dynamic network conditions. Extensions will also explore adaptive consensus protocols, privacy-enhancing cryptographic primitives, and interoperability with emerging 5G and 6G infrastructures. By addressing these directions, blockchain-enabled secure communication can become a practical foundation for the next generation of trustworthy IoT ecosystems.

Declaration of Competing Interests

The authors declare no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions

Chetan Chauhan: Conceptualization, Supervision, Data Analysis, Writing – Review and Editing; **Pradeep Laxkar**: Methodology, Validation, Investigation, Writing – Original Draft; **Ram Kumar Solanki**: Software Development, Implementation, Formal Analysis; **Sunil Parihar**: Visualization, Simulation Experiments, Data Curation; **Anand Singh Rajawat**: Project Administration, Technical Review, Writing – Review and Editing; **Amit R. Gadekar**: Resources, Validation, Critical Revisions, Writing – Final Approval.

References

[1] E. U. Haque, A. Shah, J. Iqbal, S. S. Ullah, R. Alroobaea, and S. Hussain, "A scalable blockchain based framework for efficient iot data management using lightweight consensus," *Scientific Reports*, vol. 14, p. 7841, 2024.

[2] S. H. Gopalan, A. Manikandan, N. P. Dharani, and G. Sujatha, "Enhancing iot security: A blockchain-based mitigation framework for deauthentication attacks," *International Journal of Networked and Distributed Computing*, vol. 12, pp. 237–249, 2024.

[3] S. Shukla, S. Thakur, and J. G. Breslin, "Secure communication in smart meters using elliptic curve cryptography and digital signature algorithm," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, (Rhodes, Greece), pp. 261–266, 2021.

[4] N. R. Pradhan, A. P. Singh, and R. Mahule, "Blockchain based smart and secure agricultural monitoring system," in *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, (Mathura, India), pp. 1–6, 2021.

[5] W. Iqbal, A. R. Javed, M. Rizwan, G. Srivastava, and T. R. Gadekallu, "Blockchain based secure communication for iot devices in smart cities," in *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing; Cloud and Big Data Computing; Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, (Falerna, Italy), pp. 1–7, 2022.

[6] S. M. Hatim, S. J. Elias, R. M. Ali, J. Jasmis, A. A. Aziz, and S. Mansor, "Blockchain-based internet of vehicles (biov): An approach towards smart cities development," in *2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, (Jaipur, India), pp. 1–4, 2020.

[7] B. Imad, S. Anass, A. Mounir, and C. Khalid, "Blockchain based smart contract to enhance security in smart city," in *2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, (Leeds, United Kingdom), pp. 1–6, 2024.

[8] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K. R. Choo, "Homechain: A blockchain-based secure mutual authentication system for smart homes," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 818–829, 2020.

[9] V. Aanandaram and P. Deepalakshmi, "Blockchain-based digital identity for secure authentication of iot devices in 5g networks," in *2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, (Krishnankoil, India), pp. 1–6, 2024.

[10] A. Y. A. B. Ahmad, N. Verma, N. M. Sarhan, E. M. Awwad, A. Arora, and V. O. Nyangaresi, "An iot and blockchain-based secure and transparent supply chain management framework in smart cities using optimal queue model," *IEEE Access*, vol. 12, pp. 51752–51771, 2024.