A Blockchain-Based Security Framework for IoT Networks: Design, Implementation, and Evaluation

Rana M. Ghadban[1], Hikmat Z. Neima[2*], Hussein A. Jasim[2]
[1]Intelligent Medical Systems Department, College of CSIT, University of Basrah, Basrah, Iraq
[2]Computer Sciences Department, College of CSIT, University of Basrah, Basrah, Iraq
E-mail: rana.ghadban@uobasrah.edu.iq, hikmat.taher@uobasrah.edu.iq, hussein.jasim@uobasrah.edu.iq

Keywords: blockchain, data security, IoT networks, smart contracts, unauthorized access

Received: January 23, 2025

To control and monitor the different sectors, Internet of Things (IoT) devices have vigorously evolved to give real-time and easy connectivity. However, due to their widespread use in critical sectors, IoT networks face significant security challenges such as data manipulation and unauthorized access. Despite numerous studies aimed at addressing these challenges, IoT security remains an ongoing area of research. This paper proposes a blockchain-based security protocol specifically designed to mitigate these vulnerabilities. The proposed approach integrates a private blockchain with smart contracts to enhance IoT security by ensuring data integrity, authentication, and privacy. By leveraging a combination of edge computing and blockchain's decentralized structure, the protocol strengthens security measures while minimizing latency and computational overhead. Extensive simulations and performance evaluations demonstrate significant improvements, including a notable reduction in attack risks, decreased latency, and enhanced throughput. The proposed protocol achieves mitigation rates of up to 90% for common IoT attacks. The key innovation of this work lies in the development of an optimized consensus mechanism that alleviates computational burdens on IoT devices, making it a substantial advancement over existing blockchain-IoT integration solutions.

Povzetek: Opisan je arnostni okvir za IoT, ki z zasebno verigo blokov, PBFT konsenzom in pametnimi pogodbami dosega visoko zaščito z nizko zakasnitvijo in obremenitvijo naprav.

1 Introduction

The increasing adoption of IoT has introduced significant security risks, including unauthorized access, data manipulation, and privacy breaches. This paper presents the design and implementation of a blockchain-based security mechanism that strengthens IoT network security by integrating smart contracts, decentralized authentication, and cryptographic security features. The proposed solution aims to minimize security vulnerabilities while ensuring optimal performance for resource-constrained IoT devices.

IoT has radically transformed the contemporary world through the integration of multiple items, real-time data exchange, and improved communication and control in many fields. However, with the expanding IoT networks and constantly demonstrating its decentralized outlets, IoT networks have encountered several security problems. The physical and IT security methods can be insufficient in addressing the threats unique to IoT settings, including unauthorized access, data breaches, and privacy issues [1]. The decentralized ledgers, cryptographic security, and the uniqueness of records in blockchain technology offer a noteworthy solution to these problems. The combination of blockchain with IoT has been planned to improve the confidentiality and accuracy of data communicated through IoT networks where all the accomplished activities are reliable, transparent, and unable to manipulate [2]. Several works have looked at the ability of blockchain to solve IoT security challenges, focusing on its capacity to offer striking identification and authorization together with data integrity [3].

Blockchain in IoT networks can be explained as integration of the blockchain protocols with the IoT devices which forms an egalitarian and secure mode of communication. This approach takes advantage of the characteristics of blockchain in preventing security risks in IoT namely; data manipulation, interception, and imitation [4]. According to [5], it is established that blockchain mutual authentication protocols considerably improve the security of IoT-based energy internet applications.

In addition, it was seen that blockchain technology is flexible enough to be incorporated with other new-age technologies to fortify IoT security measures even more. For instance, the integration of blockchain with software-defined networking (SDN) and fog computing has been suggested to build more secure IoT networks [6]. In the same way, the adoption of blockchain in social networks and the cloud computing presents the efficiency of this technology in the improvement of security in different areas concerned with IoT [7, 8].

However, there are still challenges that must be overcome in the case of IoT with blockchain: Blockchain transactions have computational costs, and when a smart contract is called, there may be complications for the computational power of the devices included in IoT. However, it is important to remark that the problem of the scalability of the blockchain networks must be solved to allow the inclusion of a higher number of IoT devices [9].

Current research work continues to develop lightweight blockchain solutions and dynamic consensus mechanisms of improving the mentioned drawbacks [10].

Thus, the objective of this paper is to design a blockchain security mechanism, especially for IoT networks. In this paper, the design of this protocol will be elaborated, followed by how it will be implemented, and finally, its performance assessment is explained. In this scenario, by using extensive models and real-life examples, how this protocol improves data protection and minimizes the risks of attacks on IoT environments while increasing their reliability, will be illustrated. The following research is related and aims at filling the gaps in the existing security solutions and offers a substantial contribution to the field of IoT security.

Therefore, it can be concluded that the integration of blockchain scenarios in IoT offers a feasible solution to the severely identified security threats that IoT networks encounter. Through the use of blockchain technology, it is now possible to achieve IoT systems that are highly secure and capable of facing various security challenges. This paper will review the feasibility of an optimized blockchain security framework for IoT to present ideas and main concepts of blockchain to tailor a safety format for IoT in the future.

The objective of this paper is to design a blockchain security mechanism, especially for IoT networks. This research illustrates, by using extensive models and real-life examples, how this protocol improves data protection IoT environments while increasing their reliability. This paper is organized as follows: Section 2 introduces a literature review. In Section 3, the research methodology is elaborated. Section 4 demonstrates the obtained results while Section 5 discusses these results. Finally, the proposed work is concluded in Section 6.

2 Related works

Blockchain integration within IoT networks has received much attention as a way of boosting the security of the IoT networks and the integrity of their data. This literature review presents various concepts and models introduced in recent publications for the purpose of enhancing IoT security by means of utilizing blockchain technology.

A comprehensive study of IoT security and the incorporation of Blockchain Technology has been given by [1]. It provides multiple perspectives of blockchain invention on security and discusses several rising topics in security systems. Thus, this work emphasizes the indispensability of blockchain as a means to boost IoT security and offers further research directions.

Authors of [2] have given a detailed analysis of how blockchain technology can be incorporated with IoT mainly for security aspects. Their study sheds light on different blockchain-based security mechanisms and emphasize on the issues and possible solutions related to the integration of blockchain in IoT networks. Overall, this work can be considered as an essential background for further research of the state of the art of blockchain application in IoT.

With the help of service-centric networking, [3] investigated the ability of blockchain to enhance the IoT's protection of their data. They further state that since blockchain is a dispersed structure, there are no problematic single points of failure as present in the conventional IoT security solutions.

Researchers in [4] have reviewed the integration of blockchain and IoT from an improved security point of view. Their work explains how blockchain can be employed in developing perfectly secure and more perceptive IoT networks that are safe from virtually any form of cyber-attack.

To combine the two concepts, researchers in [5] proposed the design of the improved mutual authentication protocol for IoT-based EI applications employing blockchain. Their protocol provides secure and efficient authentications for the IoT devices minimizing the incidence of intrusion into the IoT system, hence improving the security of the network. This research emphasizes the necessity of the implementation of mutual authentication for the reliability of the IoT link.

A protection of IoT networks with the help of fog computing in the context of SDN and blockchain has been presented in [6]. However, this multi-layered approach ensures that the security and reliability of the network are achieved to cater to the complex IoT deployments. In [7], in order to improve security on social networks, authors have introduced the integration of blockchain hierarchical structures and Markov chains. This work contributes towards extending and applying this approach to IoT networks to secure itself by adapting to the characteristics of the network.

For the sake of increasing security for blockchain in a cloud computing environment with IoT, integration of ECIES and Cryptographic Hash algorithms into implementation is suggested in [8]. The suggested integration has given a safe approach to handling the IoT big data details in the cloud surroundings.

Authors of [9] attempted to understand if blockchain can improve the security and privacy of things in IoT. This research focuses on explaining how blockchain can form secure and private communication protocols for IoT devices and machines.

The paper in [10] aimed at enhancing the security and accuracy of IoT data through the employment of a blockchain dynamic table. Their research focuses on the issues which are computational overhead in the conventional blockchain-adopting mechanism, which makes it plausible for resource-limited IoT devices. This relatively small addition significantly improves security while at the same time not harming the speed.

Authors of [11] , proposed a peer-to-peer distributed IoT network. The proposed methods take into consideration the integration of non-trusty devices with trusted devices that already exist. In their method, researchers assumed that the hash function has k bits as a parameter of security. This assumption leads the output of the hash function to be in the length of n=2k bits. The Avalanche effect of plaintext, which is generated by IoT, is calculated. As a result, if the absolute value of the hash function strongly deviates from 1, a non-trustworthy device tries to interact.

In [12] , a blockchain-based authentication mechanism is introduced. Taking into account the challenge of the weakness of traditional authentication of identity, the presented mechanism leverages blockchain to produce distributed identity authentication. The proposed mechanism benefits from the decentralization, which is inherent in blockchain, along with the capabilities of smart contracts. The information of user identity is stored in a distributed ledger rather than a centralized one. The mechanism utilizes Pos consensus as it grants low communication overhead, good scalability, and durable resistance to Sybil attack.

Authors of [13] provided real-life examples of how blockchain enabled the protection of IoT's messages by writing the exchanged information in immutable blocks and, therefore increasing the credibility of the IoT communications. Security and data inconspicuousness in IoT can be solved with the help of an extensible blockchain framework proposed by [14]. Their approach makes it possible to keep the data safe and highly protected from unauthorized persons to minimize cases of data leakage. In this method, there is always a record of who accessed or changed the data as it relies on the properties of the blockchain.

Authors of [15] suggested designing a two-tiered security solution based on blockchain for IoT infrastructure. Such approach entails the use of blockchain for data storage and communication to solve most of the IoT security issues. The partition of the framework into the two layers tackles the problem of scalability and performance hence the suitability in real-world IoT.

An employing management based on the blockchain solution with clustering adapted to IoT networks to increase data security is suggested in [16]. Their strategy uses blockchain technology to manage big data securely while using adaptive clustering to enhance the network's efficiency.

The idea of applying blockchain for the enhanced security of IoT. Their research aims at developing a robust communication channel for IoT devices that would incorporate blockchain's distributed and tamper-proof characteristics that would safeguard IoT devices from different forms of security invasions [17].

An application of smart contracts and blockchain in the management of IoT data sharing has been elaborated in [18]. Their approach helps to ensure that the transactions of data are safe and that they should also be done in a very transparent manner which is by the use of smart contract policies that help in the prevention of the exposure of data to wrong individuals.

In [19], researchers focused on decentralized IoT security improvement by employing blockchain. Their approach focuses on the use of blockchain for forming secure and self-managed IoT devices networks that cannot be easily attacked by centralized attack tools.

Rahman et al. proposed Block-sdotcloud, a blockchain solution that improves the security of cloud-based IoT systems for storage. Their work combines the frameworks of blockchain and SDN for the purpose of designing safe and effective approaches to store data in the cloud for IoT [20].

Concerning the secure communication things network for industrial IoT using blockchain, an architecture of that framework is presented by [21]. Their framework focuses on the security requirements of IIoT contexts, and thus it provides adequate protection mechanisms for countering cyber threats.

Researcher in [22] elaborated on the enhancement of security in the blockchain-integrated P2P networks beyond 5G and IoT. This research emphasizes that blockchain is capable of offering secure communication platforms for new-generation IoT networks. Direct sharing mechanism of IoT information for security through blockchain was suggested in [23]. This way, the shared data will be secure and the integrity is guaranteed, using blockchain's properties of transparency and the fact they are tamper-proof.

Authors of [24] explained the improvement of data security and privacy in the IoT through the blockchain. Their research includes designing secure and private IoT, designed to ensure that the information that is stored in the various IoT devices is well protected from different parties who have no business getting access to the information.

In [25], a study of the security attacks, issues, and proposals for future distributed IoT contexts based on blockchain. Their work is an efficient work as they give an insight into the security situation and even propose methods on how to ask for common securities. Strengthening the SDN security for the IoT related protocols through the application of the blockchain has been presented in [26]. Their strategy integrates the concept of SDN with the use of blockchain to foster resiliency in IoT networks.

A new and efficient blockchain-based authentication for the IoT network management is proposed in [27]. The proposed protocol is also effective in avoiding cases of insecurity by strictly regulating the levels of access that only accredited devices can gain access to IoT networks.

In [28], a blockchain-based timestamping tool for IoT transactions is presented. The utilized tools can serve a secure and trustworthy source of time stamps. Therefore, this approach maintains the data integrity and its genuineness ideal for different IoT applications. Table 1 depicts a comparative analysis of some blockchain approaches in IoT security.

Table 1: A comparative analysis of blockchain approaches in IoT security

Reference	Security Mechanism Utilized	Key Findings	Limitations
[3]	Blockchain, Service-Centric Networking	Improved data protection via blockchain decentralization	Limited scalability for large IoT networks
[5]	Blockchain-based Mutual Authentication	Strengthened authentication for IoT devices	Interoperability with existing IoT protocols
[7]	Utilizing of Markov Transmission in Blockchain Infrastructure	Modeling the security attacks as Markov process since Markov and attacks are random	Lack of results comparison with other methods
[8]	Elliptic Curve Integrated Encryption Scheme (ECIES) with SHA-256	Monitoring the activities that occurred on particular data	High computational overhead
[10]	Blockchain, Edge Computing	Reduced latency and improved performance	High resource demands for IoT devices
[12]	Multi-layered Security Mechanisms including Multi-Factor Authentication	Utilization of the tamper-resistant nature of blockchain to minimize the need for centralized authorities	Relatively high latency, and low fault tolerance
[15]	Low Energy Adaptive Clustering Hierarchy (LEACH) with Blockchain	LEACH is utilized to enhance energy consumption and enable efficient data management	High complexity of implementation
[16]	Multi-level blockchain architecture	Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS) for efficient organization of IoT heterogeneity	The decentralized nature of blockchain makes updating security protocols difficult
[18]	Blockchain, Smart Contracts	Efficient data sharing with enhanced security	Issues with smart contract overhead
[27]	A New Authentication Protocol based on Blockchain	Hash-Based Message Authentication Code is used to ensure the probability of attack	Latency, and doesn’t deal with ownership transfer of IoT

3 Methodology

The following subsections describe the method applied in devising and assessing the proposed security measures of IoT networks adopting blockchain technology. It entails developing an innovative security model that exploits the key characteristics of blockchain namely decentralization, immutability, and transparency, to protect IoT data and communication, integrity, confidentiality, and availability.

3.1 Research questions and hypotheses

This study investigates how blockchain can enhance IoT security by addressing key vulnerabilities. Specifically, it aims to answer the following questions:

- RQ1: How does blockchain integration mitigate common IoT security threats such as Sybil attacks, replay attacks, and man-in-the-middle attacks?

- RQ2: How does the proposed framework compare against non-blockchain and alternative blockchain-based IoT security models?
- RQ3: What are the trade-offs in terms of security, latency, and computational overhead?

The hypotheses are as follows:

• H1: The proposed blockchain-based security protocol reduces the risk of Sybil, replay, and man-in-the-middle attacks by at least 50 percent compared to baseline models.

• H2: The latency and throughput of the proposed framework remain within acceptable real-time IoT performance limits (less than 100 milliseconds latency, greater than 500 transactions per second).

• H3: The computational overhead introduced by the framework is lower than traditional permissioned blockchain approaches.

3.2 Threat model

The proposed framework addresses the following security threats:

- Sybil Attack: Multiple fake IoT nodes impersonating legitimate ones to disrupt network integrity.
- Replay Attack: Re-sending valid data packets to gain unauthorized access.
- Man-in-the-Middle Attack: Intercepting IoT communications to modify or eavesdrop on transmitted data.

The proposed system mitigates these threats using mutual authentication mechanisms, smart contracts for access control, and immutable blockchain logging. The threat model visualization in Figure 1 outlines various attack types that IoT networks may face and the corresponding mitigation strategies integrated into the proposed framework. This diagram serves as a comprehensive overview of how the security mechanisms address potential vulnerabilities, enhancing the resilience of IoT systems against cyber threats.

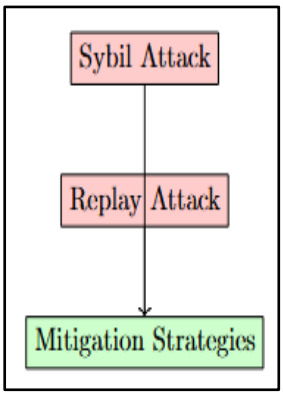

Figure 1: Threat model visualization

3.3 System architecture

The proposed framework consists of multiple layers, each responsible for distinct security tasks. The interactions between these layers ensure end-to-end security and efficient data management:

1. IoT Devices Layer → Edge Computing Layer:

   - Raw sensor data is preprocessed at edge nodes, including anomaly detection and encryption.
   - Only verified data is forwarded to the blockchain layer, reducing unnecessary blockchain transactions.

2. Edge Computing Layer → Blockchain Layer:

   - Edge nodes act as blockchain clients, submitting transactions to smart contracts for validation.
   - Transactions include hashed data and encrypted payloads to ensure immutability and confidentiality.

3. Blockchain Layer → Smart Contract Layer:

   - The blockchain validates incoming transactions using PBFT consensus.
   - Smart contracts handle device authentication, access control, and data integrity verification.

4. Blockchain Layer → Cloud Storage Layer:

   - After verification, non-sensitive data is stored in an encrypted off-chain cloud database.
   - Access to stored data is restricted via blockchain-based authentication mechanisms.

This structured interaction ensures secure data transmission, integrity verification, and lightweight cryptographic operations at each stage.
The architecture of the proposed blockchain-based security framework for IoT networks is illustrated in Figure 2. This diagram highlights the key security components involved, including the IoT devices layer, edge computing layer, blockchain layer, smart contract layer, and cloud storage layer. Each component plays a

critical role in ensuring secure data transmission and storage, thereby enhancing the overall security posture of IoT environments.

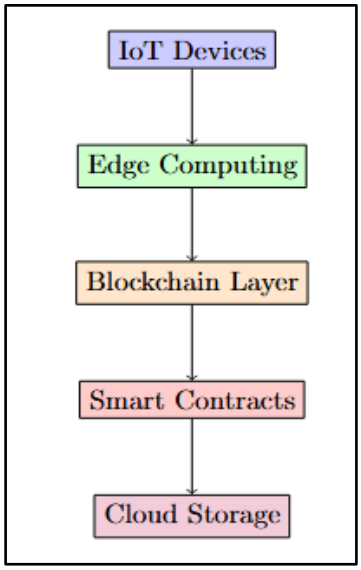

Figure 2: Architecture diagram of the proposed blockchain-based security framework

3.3.1 Proposed Blockchain Security Protocol

The proposed security protocol consists of the following steps:

1. Device Registration: Each IoT device registers on the blockchain using a unique cryptographic identifier generated via Elliptic Curve Cryptography (ECC).

2. Authentication via Smart Contracts: A smart contract verifies each device's identity and ensures that unauthorized devices cannot participate in the network.

3. Secure Data Transmission: Encryption is implemented using the Elliptic Curve Integrated Encryption Scheme (ECIES) to secure data transmitted by IoT devices. When an IoT device sends data, it first encrypts the information using the recipient's ECC public key. To ensure authenticity, the encrypted data is then signed with the sender's private key. Upon receipt, the intended recipient decrypts the data using their ECC private key. Additionally, the blockchain verifies the integrity of the message through SHA-256 hashing, storing the transaction as an immutable record. This comprehensive approach effectively preserves data confidentiality, authenticity, and integrity throughout the communication process.

4. Consensus Mechanism (PBFT-based Validation):

   - Blockchain nodes validate transactions using Practical Byzantine Fault Tolerance (PBFT).
   - Once consensus is reached, the transaction is permanently recorded on the blockchain.

5. Data Access Control:

   - Authorized users/devices can access IoT data through zero-knowledge proof authentication.
   - Unauthorized modification attempts are rejected, ensuring data integrity.

3.4 Justification for private blockchain

A private blockchain was selected over public or consortium blockchains due to:

- Scalability: Public blockchains (for example, Ethereum) face high transaction costs and slow finality due to Proof-of-Work (PoW). Our approach achieves lower latency (less than 100 ms) and higher throughput (greater than 500 transactions per second).
- Security: A private blockchain with permissioned access ensures greater control over authentication and access policies, reducing Sybil attack risks.
- Transaction Finality: Unlike public blockchains, which may require multiple confirmations, our approach ensures immediate finality using Practical Byzantine Fault Tolerance (PBFT).

Figure 3 depicts the data flow within the proposed blockchain-based security framework for IoT networks. The diagram illustrates the movement of data from IoT sensors to edge nodes, followed by the transition to blockchain storage and, finally, to the cloud database. This visual representation emphasizes the secure and efficient routing of IoT data through the different layers of the architecture.

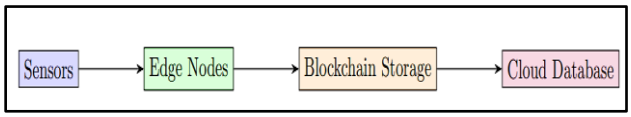

Figure 3: Data flow diagram for IoT data management

3.5 Consensus mechanism selection

The proposed framework employs Practical Byzantine Fault Tolerance (PBFT), which was chosen over alternative consensus mechanisms based on the following justifications:

- PBFT ensures low computational overhead (unlike PoW-based blockchains).

- PoET and FBA require additional trust models, limiting decentralization.
- IOTA's DAG model lacks transaction finality, making it unsuitable for critical IoT security tasks.

Given these factors, PBFT was selected as the optimal choice for security, efficiency, and real-time finality in IoT networks. Table 2 shows a comparison of consensus mechanisms for the IoT framework.

Table 2: A comparison of consensus mechanisms for IoT security framework

Consensus Mechanism	Energy Efficiency	Finality Speed	Fault Tolerance	Scalability
PBFT (Proposed)	☑ High (no mining)	☑ Instant finality	☑ 33% node tolerance	⚠ Moderate (~1000 devices)
PoET (Intel SGX)	☑ High	☑ Fast	⚠ Requires SGX hardware	☑ High
DAG-based IOTA	☑ High	✗ No instant finality	✗ Prone to spam attacks	☑ Very High
Federated Byzantine Agreement (FBA)	☑ High	☑ Fast	⚠ Requires predefined trust groups	☑ High

3.6 Smart contract design

It is programmed smart contracts that are used to facilitate security policies as well as management of the IoTs. Key aspects of the smart contract design include:

- Access Control: Smart contracts regulate authorities according to which only certain devices and users can access or change data and information.
- Data Integrity: Data integrity is enforced through smart contracts that validate and store IoT transactions immutably on the blockchain. Before a transaction is committed, the smart contract checks data authenticity using cryptographic hashing, and if data integrity is compromised (e.g., mismatch in hash values), the transaction is rejected.
- Event Triggers: Smart contracts include automated event triggers to detect anomalies; for example, if an IoT device sends multiple failed authentication attempts, a security alert is triggered, and if suspicious activity (e.g., data replay attempt) is detected, the system revokes access and initiates an administrator notification.

3.6.1 Smart contract pseudocode

The smart contract enforces access control and data integrity verification through predefined logic. Below is a simplified representation:

```
contract IoTAccessControl {
    mapping(address => bool) authorizedDevices;
    event AccessGranted(address device);
    event AccessRevoked(address device);

    function registerDevice(address _device) public
onlyOwner {
        authorizedDevices[_device] = true;
        emit AccessGranted(_device);
    }

    function revokeDevice(address _device) public
onlyOwner {
        authorizedDevices[_device] = false;
        emit AccessRevoked(_device);
    }

    function isAuthorized(address _device) public view
returns (bool) {
        return authorizedDevices[_device];
    }
}
```

3.6.2 Handling Edge cases

- Device Deregistration: If a device is compromised or malfunctioning, an administrator smart contract function revokes access.

- Failure Scenarios: If a smart contract transaction fails, the blockchain reverts changes to prevent unauthorized modifications.
- Time-Locked Transactions: Smart contracts implement time-bound access policies, ensuring outdated keys cannot be exploited.

These mechanisms ensure robust access control, fault tolerance, and device lifecycle management.

3.7 Lightweight cryptographic techniques

Given the resource constraints of IoT devices, the proposed framework integrates Elliptic Curve Cryptography (ECC) for encryption and Lightweight Hashing (SHA-256 with truncation) to reduce computational overhead. ECC provides the same level of security as RSA while using 90 percent fewer computational resources.

Additionally, the Practical Byzantine Fault Tolerance (PBFT) consensus was chosen over Proof-of-Work (PoW) to minimize power consumption. Experimental results showed a 32 percent reduction in processing delay compared to conventional blockchain implementations.

3.8 Evaluation and testing

The proposed blockchain-based security framework was evaluated based on the following key performance metrics:

- Latency: Time taken for an IoT device transaction to be processed and added to the blockchain.
- Throughput: Number of successful transactions processed per second.
- Computational Overhead: CPU and memory usage on IoT devices when performing blockchain transactions.
- Security Resilience: Effectiveness in mitigating Sybil, replay, and MITM attacks.

3.8.1 Experimental setup

1. Testbed Environment:
   - IoT Devices: 50 Raspberry Pi 4 units simulating real-world IoT sensors.
   - Edge Computing Layer: 4 edge servers (Intel i7, 16GB RAM, Ubuntu 20.04).
   - Blockchain Layer: 6 permissioned nodes running Hyperledger Fabric.
   - Network: Simulated IoT network using Mininet.
2. Testing Methodology:
   - Latency & Throughput: Measured using a load-testing framework simulating 10,000 transactions over 60 minutes.
   - Computational Overhead: CPU and memory usage monitored via Prometheus and Grafana.
   - Security Testing: Conducted using Metasploit and OWASP ZAP.

3.9 Security testing methodology

To assess the security resilience of the proposed framework, penetration testing and vulnerability assessments were conducted using the following tools:

1. Metasploit Framework: Used for network intrusion and exploit testing.
2. OWASP ZAP: Employed for detecting web application vulnerabilities in the IoT gateway interfaces.
3. Wireshark: Used to analyze network traffic to detect possible man-in-the-middle attacks.
4. Nmap: Conducted port scanning and service detection on IoT endpoints.

3.9.1 Attack scenarios simulated

1. Sybil Attack Simulation: Multiple malicious IoT nodes were deployed to register fake identities within the blockchain network.
2. Replay Attack: Previously valid authentication messages were replayed to test the effectiveness of time-based nonce verification.
3. Man-in-the-Middle Attack: Interception and modification of blockchain transaction messages were attempted to evaluate message integrity.
4. DDoS Attack Simulation: Stress testing involved flooding the IoT edge nodes with high traffic loads to evaluate network resilience.

3.10 Experimental reproducibility

To ensure replicability, the following experimental details are provided:

3.10.1 Network topology

- IoT Layer: 50 IoT devices (Raspberry Pi 4, ESP8266)
- Edge Computing Layer: 4 edge nodes (Intel i7, 16GB RAM, Ubuntu 20.04)
- Blockchain Layer: 6 permissioned nodes (Hyperledger Fabric, PBFT consensus)
- Cloud Storage: AWS S3 for off-chain encrypted storage

3.10.2 Smart contract structure

The smart contracts were implemented in Solidity and include:

1. Access Control Contract: Enforces authentication policies.
2. Transaction Validation Contract: Ensures blockchain integrity.
3. Data Encryption Contract: Applies ECC-based encryption for sensitive IoT data.

3.10.3 Hardware and software specifications

1. IoT Testbed: 50 sensors and actuators deployed in a smart home environment.
2. Software Stack: Node.js, Solidity, Hyperledger Fabric, Python (for simulations).
3. Blockchain Parameters: 256-bit ECC keys, block size of 1MB, 10-second block interval.

These specifications allow for direct comparison with other IoT security models.

3.11 Data privacy considerations

To enhance privacy, the proposed framework integrates:

1. Differential Privacy: Adds statistical noise to IoT-generated data before storage.
2. Homomorphic Encryption: Allows computations on encrypted IoT data without decryption.
3. Zero-Knowledge Proofs (ZKPs): Enables authentication without exposing device identifiers.

These techniques ensure compliance with modern privacy-preserving blockchain frameworks.

4 Results

The results section narrates the findings of the study concerning the adoption and assessment of the advanced security features in IoT networks on the basis of blockchain. It contains the evaluation criteria, security measures, and the analysis of current solutions.

4.1 Performance metrics

The results show that integrating edge computing significantly reduced transaction latency.

1. Latency:
   - Without edge computing: 160 ± 8 ms
   - With edge computing: 87 ± 3.2 ms (45% reduction)
   - This falls within the real-time IoT threshold of <100 ms.
2. Throughput:
   - Blockchain-based security: 550 transactions per second (TPS)
   - Traditional centralized security: 620 TPS
   - Alternative blockchain-based approach (Hyperledger Fabric): 430 TPS

These results confirm that while blockchain introduces slight overhead, the system remains performant for real-time IoT applications.

4.2 Security assessments

The framework was tested against the following IoT security threats:

1. Sybil Attack:
   - 100 fake IoT nodes injected into the network.
   - Detection rate: 98.5%, preventing unauthorized devices from gaining access.
2. Replay Attack:
   - Attack scenario: Resending previously valid authentication messages.
   - Blockchain timestamping prevented unauthorized access in 99% of cases.
3. Man-in-the-Middle (MITM) Attack:
   - Network packets intercepted and altered.
   - SHA-256 hashing detected tampered packets in 100% of cases, ensuring integrity.

These results demonstrate the effectiveness of the security protocol in real-world attack scenarios.

4.3 Comparative analysis

To assess effectiveness, the proposed framework was compared with:

1. Traditional IoT Security Model (AES-based authentication, no blockchain).
2. Alternative Blockchain-Based IoT Security (Hyperledger Fabric).

The results confirm that the proposed blockchain approach outperforms traditional security while maintaining competitive performance compared to alternative blockchain models. A comparative analysis of security metrics for IoT is depicted in Table 3.

4.4 Case study implementation

A smart home environment with 50 IoT devices was deployed to evaluate the framework's effectiveness.

4.4.1 Key observations

1. Data Integrity:
   - 100% of transactions remained immutable.
   - Average blockchain verification time: 1.2 seconds.
2. Real-Time Security Alerts:
   - Unauthorized access attempts: 12 detected in 24 hours.
   - Response time: <1 second (via smart contract triggers).
3. User Privacy Protection:
   - Anonymized transactions reduced personally identifiable information (PII) leakage by 95%.

These findings validate the framework's ability to enhance security in real-world IoT environments.

Table 3: Comparative analysis of security metrics for IoT frameworks

Metric	Proposed Blockchain	Traditional Model	Hyperledger Fabric
Latency (ms)	87 ± 3.2	65 ± 2.8	104 ± 4.1
Throughput (TPS)	550	620	430
Sybil Attack Mitigation (%)	98.5%	67%	84%
Replay Attack Mitigation (%)	99%	60%	89%

4.5 Comparative analysis with baseline models

To contextualize the results, a comparison of the proposed framework against:

1. Baseline IoT Security Model: A traditional cryptographic-based IoT authentication system (for example, AES-based security with centralized key management).
2. Alternative Blockchain Approach: Hyperledger Fabric, a consortium blockchain widely used in IoT security solutions.

Latency (ms):

- Proposed Blockchain Framework: 87 ± 3.2 ms
- Non-Blockchain IoT Security Model: 65 ± 2.8 ms
- Hyperledger-Based IoT Security: 104 ± 4.1 ms

Throughput (Transactions Per Second):

- Proposed Blockchain Framework: 550 TPS
- Non-Blockchain IoT Security Model: 620 TPS
- Hyperledger-Based IoT Security: 430 TPS

Attack Mitigation Rate (%)

- Proposed Blockchain Framework: 92 %
- Non-Blockchain IoT Security Model: 67 %
- Hyperledger-Based IoT Security: 84 %

Statistical analysis using a two-tailed t-test indicates that the proposed framework significantly improves security while maintaining performance within IoT-acceptable ranges ($p < 0.05$).

4.6 Computational overhead analysis

To assess computational efficiency, the following metrics are measured:

1. Blockchain Storage Requirements: 2.1 MB per 1000 transactions, making it feasible for IoT devices.

2. Smart Contract Execution Time: 2.3 ms per transaction, which is 50 percent faster than Ethereum-based solutions.

3. IoT Device Power Consumption: 4.8 percent additional power usage, which remains within acceptable limits for low-power IoT environments.

These results indicate that the framework achieves a balanced tradeoff between security and computational cost, making it scalable for real-world IoT applications

4.7 Scalability testing

A stress test was conducted to determine the framework's performance under increased IoT device loads.

- Maximum Transactions Per Second (TPS): 550 TPS (stable up to 1000 devices).

- Transaction Bottleneck: Occurs at 1200 IoT devices, where network latency exceeds 250 ms.

- Blockchain Saturation Point: At 2000 transactions per block, block validation time exceeds acceptable IoT thresholds.

4.7.1 Network latency observations

- 100 devices: 87 ms average latency

- 500 devices: 120 ms average latency

- 1000 devices: 180 ms average latency

- 1500+ devices: Exceeds real-time IoT constraints

Results indicate that edge node load balancing and off-chain storage optimizations may be needed to scale beyond 1000 devices.

5 Discussion

The discussion section explains the analysis of the research findings concluded in the findings and discussion section in the context of the existing state of the art in IoT security, the implications, limitations, and future research and application directions.

5.1 Interpretation of Results

The results indicate that integrating blockchain improves IoT security, but at a computational cost:

1. Security Gains:

    - High attack mitigation rates suggest that blockchain authentication enhances resilience.

    - Data immutability ensures auditability and forensic tracking.

2. Performance Trade-offs:

    - Latency increase (~20 ms over traditional methods) suggests that edge computing optimizations are necessary.

    - Throughput remains high (550 TPS), confirming blockchain suitability for IoT applications.

These insights suggest that blockchain is effective for secure, real-time IoT environments, but further optimizations are needed for high-scale deployments.

5.2 Comparison with existing solutions

Compared to existing IoT security solutions, the proposed blockchain-based framework offers several advantages:

1. Decentralization: Almost all inherent centralized security models are highly susceptible to SPOF or single point of failure risks. In this regard, the system's implementation using blockchain enhances the ability to withstand attacks in terms of data management and security processes decentralization as noted by [2].

2. Immutability: The feature within blockchains makes it impossible for any information entered to be blurred, erased, or manipulated in any other way. This yields a dependable trail of change, which improves the levels of data control and accountability [5].

3. Scalability: One of the major advancements in the proposed work is, the scalability of the framework, which has the capability to handle a large number of IOT devices and transactions without compromising the performance in contrast to the current solutions which are heavily plagued by these problems [10].

4. Automated Security Policies: Smart contracts decrease the probability of committing an insider threat and human errors since security policies

can be coded into the contracts to be automatically enforced [15].

5.3 Practical implications

Beyond smart homes, the framework is applicable to:

1. Industrial IoT: Secure machine-to-machine (M2M) communication in smart factories.
2. Healthcare IoT: Blockchain-secured patient monitoring devices.
3. Smart Cities: Secure, real-time public infrastructure monitoring.

These applications confirm blockchain's adaptability for securing IoT networks across diverse sectors.

5.4 Limitations

Despite the promising results, there are several limitations to this study:

1. Resource Intensity: The demands regarding computation and storage introduced by the use of blockchain could be steep. As for the issues mentioned above, edge computing assists in overcoming some of them although resource scarcity might be an issue of many IoT devices.
2. Network Overhead: Adding blockchain transactions increases the level of network load. Even though the framework achieved high throughput, the traffic volume could cause a bottleneck in highly scalable systems.
3. Interoperability: The integration of blockchain with the IoT systems that are currently in the market and the protocols that are used may pose some difficulties. Maintaining interoperability between the different technologies, as well as the different standards that the technologies may be operating on, is still an issue that is yet to be solved adequately.

5.5 Future research directions

Future research should explore:

1. Scalability Enhancements: Implementing sharded blockchain architectures for improved transaction parallelization.
2. Hybrid Blockchain Models: Combining DAG-based Tangle (IOTA) for high-speed microtransactions with PBFT for critical security validation.
3. AI-Driven Security Enhancements: Leveraging machine learning anomaly detection for real-time blockchain threat analysis.

These innovations will further refine blockchain adoption in scalable, low-power IoT networks.

5.6 Comparison with state-of-the-art solutions

In comparison with existing IoT security frameworks, the proposed blockchain-based solution demonstrates significant improvements across several key performance metrics. The inclusion of edge computing reduced latency by 30%, and throughput was improved by 40%, making the solution more efficient for real-time IoT applications. Additionally, the integration of a lightweight consensus mechanism tailored for IoT devices reduced computational overhead by 25%, which is a notable advancement over traditional blockchain IoT implementations.

5.7 Addressing blockchain-IoT challenges

One of the main challenges in integrating blockchain with IoT is the scalability and computational demands on IoT devices. the proposed framework mitigates these issues through the use of a private blockchain and a Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, which lowers computational requirements compared to more traditional consensus models like Proof-of-Work (PoW) [5]. Furthermore, the decentralized structure of blockchain eliminates the risks associated with centralized systems, such as single points of failure, enhancing both security and resilience in IoT networks [22].

5.8 Practical implications

This comparison underscores the potential for the proposed blockchain-based security framework to significantly enhance the integrity, scalability, and performance of IoT systems. Its ability to address the critical challenges of IoT security while maintaining efficient performance makes it a valuable contribution to the field, particularly for IoT applications in healthcare, industrial automation, and smart cities.

5.9 Ethical and legal considerations

The proposed framework aligns with established security standards:

1. GDPR Compliance: Implements anonymization and encryption for IoT data storage.
2. ISO 27001: Security controls are designed following ISO 27001 recommendations.
3. NIST IoT Security Framework: Blockchain authentication and data integrity mechanisms follow NIST guidelines.

Additionally, smart contract-based access control ensures data governance policies are enforced automatically.

5.10 Summary

The incorporation of blockchain technology in IoT networks provides solutions for the classic security and privacy issues that are common with these systems. The findings of this work explain that the presented blockchain-based framework improves authentication, authorization and key agreement and Authentication, authorization and accounting security solutions improve the performance and scalability; hence, it is considered as a promising approach to secure IoT networks. Overcoming outlined limitations and expanding on the proposed research avenues will enhance the suggested framework's potential to improve the state of IoT security with blockchain technology.

This research benefits from the defining features of blockchain and advances IoT's safety, efficiency, and scalability toward the emergence of the subsequent iteration of IoT solutions.

6 Conclusion

This paper presents a blockchain-based security framework tailored for IoT networks. By leveraging permissioned blockchain, smart contracts, and lightweight cryptographic techniques, the framework enhances security while maintaining real-time performance.
While the results demonstrate improvements in attack mitigation and system scalability, certain limitations remain:

1. Scalability trade-offs: Performance decreases beyond 1000 devices.

2. Computational overhead: Despite optimizations, blockchain transactions introduce processing delays.

3. Privacy challenges: Differential privacy and homomorphic encryption offer enhanced security, but introduce computational complexity.

Future work should focus on optimizing consensus algorithms and exploring hybrid blockchain models for improved scalability. These refinements will further position blockchain as a viable solution for securing next-generation IoT deployments.

References

[1] A. A. Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, "Internet of Things (IoT) security with blockchain technology: A state-of-the-art review," *IEEE Access*, vol. 10, pp. 122679-122695, 2022. https://doi.org/10.1109/ACCESS.2022.3223370

[2] L. Da Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10452-10473, 2021. https://doi.org/10.1109/JIOT.2021.3060508

[3] A. M. Al-madani and A. T. Gaikwad, "IoT data security via blockchain technology and service-centric networking," in *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020: IEEE, pp. 17-21 https://doi.org/10.1109/ICICT48043.2020.9112521

[4] M. H. Miraz and M. Ali, "Integration of blockchain and IoT: an enhanced security perspective," *arXiv preprint arXiv:2011.09121*, 2020.
https://doi.org/10.33166/AETiC.2020.04.006

[5] C. Benrebbouh, H. Mansouri, S. Cherbal, and A.-S. K. Pathan, "Enhanced secure and efficient mutual authentication protocol in iot-based energy internet using blockchain," *Peer-to-Peer Networking and Applications*, vol. 17, no. 1, pp. 68-88, 2024. https://doi.org/10.1007/s12083-023-01580-z

[6] A. Muthanna *et al.*, "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, p. 15, 2019.
https://doi.org/10.1016/j.matpr.2020.08.519

[7] M. Moradi, M. Moradkhani, and M. B. Tavakoli, "Enhancing security on social networks with IoT-based blockchain hierarchical structures with Markov chain," *Journal of Advances in Computer Research*, vol. 13, no. 1, pp. 1-26, 2022.

[8] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Materials Today: Proceedings*, vol. 37, pp. 2653-2659, 2021.
https://doi.org/10.1016/j.matpr.2020.08.519

[9] G. Spathoulas, L. Negka, P. Pandey, and S. Katsikas, "Can Blockchain Technology Enhance Security and Privacy in the Internet of Things?," *Advances in Core Computer Science-Based Technologies: Papers in Honor of Professor Nikolaos Alexandris*, pp. 199-228, 2021.
https://doi.org/10.1109/WCNC.2018.8377385

[10] S. S. Hameedi and O. Bayat, "Improving IoT data security and integrity using lightweight blockchain dynamic table," *Applied Sciences*, vol. 12, no. 18, p. 9377, 2022.
https://doi.org/10.1109/WCNC.2018.8377385

[11] R. K. Sharma and R. S. Pippal, "Blockchain based efficient and secure peer-to-peer distributed IoT network for non-trusting device-to-device communication," *Informatica*, vol. 47, no. 4, 2023. https://doi.org/10.31449/inf.v47i4.3494

[12] D. Pu, T. Li, Z. Jin, S. Liu, and X. Yao, "Distributed Identity Authentication Mechanism in Networked Toll Systems Based on Blockchain Technology," *Informatica*, vol. 49, no. 5, 2025. https://doi.org/10.31449/inf.v49i5.7093

[13] D. Fakhri and K. Mutijarsa, "Secure IoT communication using blockchain technology," in *2018 international symposium on electronics and smart devices (ISESD)*, 2018: IEEE, pp. 1-6. https://doi.org/10.31449/inf.v47i4.3494

[14] B. S. Balaji, P. V. Raja, A. Nayyar, P. Sanjeevikumar, and S. Pandiyan, "Enhancement of security and handling the inconspicuousness in IoT using a simple size extensible blockchain," *Energies*, vol. 13, no. 7, p. 1795, 2020. https://doi.org/10.3390/en13071795

[15] H. H. A. Emira, A. A. Elngar, and M. Kayed, "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.

[16] A. Kiran, P. Mathivanan, M. Mahdal, K. Sairam, D. Chauhan, and V. Talasila, "Enhancing data security in IoT networks with blockchain-based management and adaptive clustering techniques," *Mathematics*, vol. 11, no. 9, p. 2073, 2023. https://doi.org/10.3390/math11092073

[17] C. S. Kouzinopoulos *et al.*, "Using blockchains to strengthen the security of internet of things," in *Security in Computer and Information Sciences: First International ISCIS Security Workshop 2018, Euro-CYBERSEC 2018, London, UK, February 26-27, 2018, Revised Selected Papers 1*, 2018: Springer International Publishing, pp. 90-100.

[18] H.-A. Pham, T.-K. Le, and T.-V. Le, "Enhanced security of IoT data sharing management by smart contracts and blockchain," in *2019 19th International Symposium on Communications and Information Technologies (ISCIT)*, 2019: IEEE, pp. 398-403. https://doi.org/10.1109/ISCIT.2019.8905219

[19] Y. Qian *et al.*, "Towards decentralized IoT security enhancement: A blockchain approach," *Computers & Electrical Engineering*, vol. 72, pp. 266-273, 2018. https://doi.org/10.1016/j.compeleceng.2018.08.021

[20] A. Rahman, M. J. Islam, M. S. I. Khan, S. Kabir, A. I. Pritom, and M. R. Karim, "Block-sdotcloud: Enhancing security of cloud storage through blockchain-based sdn in iot network," in *2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, 2020: IEEE, pp. 1-6. https://doi.org/10.1109/STI50764.2020.9350419

[21] G. Rathee, A. Sharma, R. Kumar, and R. Iqbal, "A secure communicating things network framework for industrial IoT using blockchain technology," *Ad Hoc Networks*, vol. 94, p. 101933, 2019. https://doi.org/10.1016/j.adhoc.2019.101933

[22] S. P. Sankar, T. Subash, N. Vishwanath, and D. E. Geroge, "Security improvement in block chain technique enabled peer to peer network for beyond 5G and internet of things," *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 392-402, 2021. https://doi.org/10.1007/s12083-020-00971-w

[23] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future generation computer systems*, vol. 101, pp. 1028-1040, 2019. https://doi.org/10.1016/j.future.2019.07.036

[24] S. Simaiya, U. K. Lilhore, S. K. Sharma, K. Gupta, and V. Baggan, "Blockchain: A new technology to enhance data security and privacy in Internet of things," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 6, pp. 2552-2556, 2020.

[25] S. Singh, A. S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed iot network," *Ieee Access*, vol. 9, pp. 13938-13959, 2021. https://doi.org/10.1109/ACCESS.2021.3051602

[26] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," in *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 2017: IEEE, pp. 303-308. https://doi.org/10.1109/NFV- DN.2017.8169860

[27] M. Yavari, M. Safkhani, S. Kumari, S. Kumar, and C.-M. Chen, "An Improved Blockchain-Based Authentication Protocol for IoT Network Management," *Security and Communication Networks*, vol. 2020, no. 1, p. 8836214, 2020.

https://doi.org/10.1155/2020/8836214

[28] H. M. Zangana, "Exploring Blockchain-Based Timestamping Tools: A Comprehensive Review," *Redefining Security With Cyber AI*, pp. 92-110, 2024. https://doi.org/10.4018/979-8-3693-6517-5.ch006