

Blockchain-Based Security Frameworks for IoT Edge Networks

Priya Sharma¹, Subodh Tiwari²

Associate Professor¹, Assistant Professor²

Department of CSE

Sunrise College of Engineering

Corresponding Author Email: Priyasharma457@yahoo.com¹

ABSTRACT

The proliferation of the Internet of Things (IoT) has led to a massive increase in connected devices, particularly in edge networks where computing is distributed closer to data sources. While IoT edge networks offer low latency and improved bandwidth utilization, they also pose significant security challenges due to the heterogeneous and resource-constrained nature of edge devices. Blockchain technology has emerged as a promising solution to enhance the security and privacy of IoT edge networks through decentralization, immutability, and transparency. This review explores blockchain-based security frameworks tailored for IoT edge networks, examining consensus mechanisms, lightweight cryptographic techniques, and hybrid architectures integrating blockchain with other security measures. The paper also discusses performance trade-offs, implementation challenges, and future directions, aiming to provide a comprehensive reference for researchers and practitioners in this field.

KEYWORDS: *Blockchain, IoT, Edge Networks, Security Frameworks, Decentralization, Lightweight Cryptography*

INTRODUCTION

The Internet of Things (IoT) has transformed modern technology landscapes, enabling applications ranging from smart homes and healthcare monitoring to industrial automation and smart cities. According to recent reports, over **50 billion IoT devices** are expected to be deployed by 2030, generating enormous volumes of data at the network edge. Edge computing

has emerged as a solution to reduce latency and bandwidth consumption by processing data closer to the source rather than relying on centralized cloud servers.

However, the integration of IoT and edge computing introduces several security and privacy challenges. Edge devices are often resource-constrained, lacking robust computational power, memory, and energy to implement traditional security mechanisms. Moreover, the distributed nature of edge networks makes centralized security approaches less feasible, creating vulnerabilities to attacks such as Distributed Denial of Service (DDoS), data tampering, spoofing, and unauthorized access.

Blockchain, originally introduced as the underlying technology for cryptocurrencies, provides a decentralized, tamper-resistant, and transparent ledger system that can strengthen IoT security. Its potential in IoT edge networks lies in its ability to secure transactions, ensure data integrity, and facilitate trust among devices without relying on a centralized authority.

This paper reviews existing blockchain-based security frameworks designed for IoT edge networks. We explore consensus protocols, lightweight blockchain architectures, hybrid security approaches, and practical implementation strategies, highlighting their advantages, limitations, and research gaps.

BACKGROUND

IoT edge networks have emerged as a critical component of modern distributed computing, driven by the exponential growth of connected devices and the need for real-time data processing. This section elaborates on the structure, characteristics, and security challenges of IoT edge networks, and introduces blockchain as a potential solution.

1. IoT Edge Networks

IoT edge networks refer to a computing paradigm in which data generated by IoT devices is processed locally at the network edge, rather than being fully transmitted to a centralized cloud server. By performing data analysis closer to the source, edge computing reduces latency, conserves network bandwidth, and enables real-time decision-making in applications such as autonomous vehicles, industrial automation, smart healthcare, and environmental monitoring.

Edge networks are typically composed of multiple layers:

1. **Device Layer:** Sensors, actuators, and IoT-enabled devices that generate data.
2. **Edge Layer:** Edge servers, gateways, or micro data centers that aggregate, filter, and process data locally.
3. **Cloud Layer:** Centralized servers or cloud platforms used for large-scale storage, analytics, and long-term decision-making.

The **key characteristics** of IoT edge networks include:

- **Heterogeneity:** Edge networks often consist of devices with varying hardware capabilities, operating systems, and communication protocols. For instance, an industrial IoT network may include temperature sensors, robotic controllers, and mobile devices, all communicating using different protocols such as MQTT, CoAP, or HTTP. Managing such heterogeneity is a major challenge for system designers.
- **Resource Constraints:** Many IoT edge devices have limited computational power, memory, and battery life. This restricts their ability to perform heavy cryptographic operations or complex analytics, making lightweight and efficient security mechanisms crucial.
- **High Scalability:** IoT edge networks can scale to include hundreds or thousands of devices in a single deployment. Scalability affects data processing, communication overhead, and security management, as every new node increases the potential attack surface.
- **Dynamic Topology:** Devices in edge networks can join or leave dynamically, either due to mobility (e.g., wearable devices or autonomous vehicles) or temporary network outages. This dynamic behavior complicates network management, authentication, and trust establishment among devices.

Edge computing in IoT networks provides significant advantages over traditional cloud-based architectures, including:

- **Reduced Latency:** Critical for applications such as autonomous driving or real-time health monitoring.
- **Bandwidth Efficiency:** Only relevant or aggregated data is transmitted to the cloud, reducing network congestion.
- **Improved Reliability:** Local processing allows continued operation even when cloud connectivity is intermittent.

Despite these benefits, edge networks are highly vulnerable to security threats due to their distributed nature and resource limitations, which is discussed next.

2. Security Challenges in IoT Edge Networks

Security is a major concern in IoT edge networks because the combination of distributed nodes, heterogeneous devices, and constrained resources makes traditional security measures insufficient. Key challenges include:

- **Data Integrity Threats:** Data transmitted from sensors to edge nodes or between edge nodes can be intercepted or altered by attackers. This can lead to incorrect decisions, such as faulty readings in industrial systems or medical monitoring errors.
- **Unauthorized Access:** Weak authentication mechanisms on edge devices allow attackers to impersonate legitimate devices. For example, a hacker could gain control over a smart home device or an industrial actuator if identity verification is inadequate.
- **Distributed Denial of Service (DDoS) Attacks:** Malicious nodes or compromised devices can flood the network with unnecessary requests, overwhelming the system and causing network downtime or service degradation. Edge networks, due to their smaller scale compared to centralized clouds, can be particularly vulnerable to DDoS attacks.
- **Privacy Leakage:** Sensitive data, such as health information, financial transactions, or personal location data, can be exposed if proper encryption or anonymization mechanisms are not applied. Even edge devices with local processing may transmit raw data to cloud servers, creating potential privacy risks.
- **Physical Attacks:** Edge devices are often deployed in unsecured or remote environments, making them susceptible to tampering or theft. Physical compromise can allow attackers to inject malicious data or extract cryptographic keys.

These security challenges highlight the need for robust, decentralized security mechanisms that are lightweight and compatible with the constraints of IoT edge networks.

3. Blockchain Overview

Blockchain technology provides a promising solution to the security challenges of IoT edge networks. It is a distributed ledger system in which transaction records are stored in immutable

blocks, each cryptographically linked to the previous block. This ensures that data cannot be altered retroactively without consensus from the network.

Key features of blockchain relevant to IoT edge security include:

- **Decentralization:** Blockchain eliminates the need for a centralized authority by distributing control across multiple nodes. This reduces single points of failure and makes the network more resilient to attacks.
- **Immutability:** Once a block is recorded on the blockchain, its data cannot be modified or deleted without network consensus. This ensures data integrity, preventing tampering by malicious actors.
- **Transparency and Auditability:** All nodes in the network can access the ledger and verify transactions. This transparency enhances trust between devices and enables auditing of historical actions without relying on a central server.
- **Smart Contracts:** These are programmable scripts embedded in blockchain networks that automatically execute predefined rules when certain conditions are met. For IoT edge networks, smart contracts can enforce access control policies, automate authentication, and trigger security actions without human intervention.
- **Cryptographic Security:** Blockchain relies on cryptographic techniques such as hash functions, digital signatures, and public-private key infrastructure (PKI) to secure transactions and verify node identities.

By leveraging these properties, blockchain can address multiple IoT edge security issues:

- Ensuring **data integrity** by recording sensor readings in immutable blocks.
- Enforcing **authentication and access control** through smart contracts.
- Enhancing **privacy** by allowing selective verification using techniques such as zero-knowledge proofs or encryption of sensitive payloads.

In essence, blockchain transforms the trust model of IoT edge networks from centralized authority-based systems to decentralized, verifiable, and resilient frameworks, making it a suitable candidate for securing next-generation edge computing infrastructures.

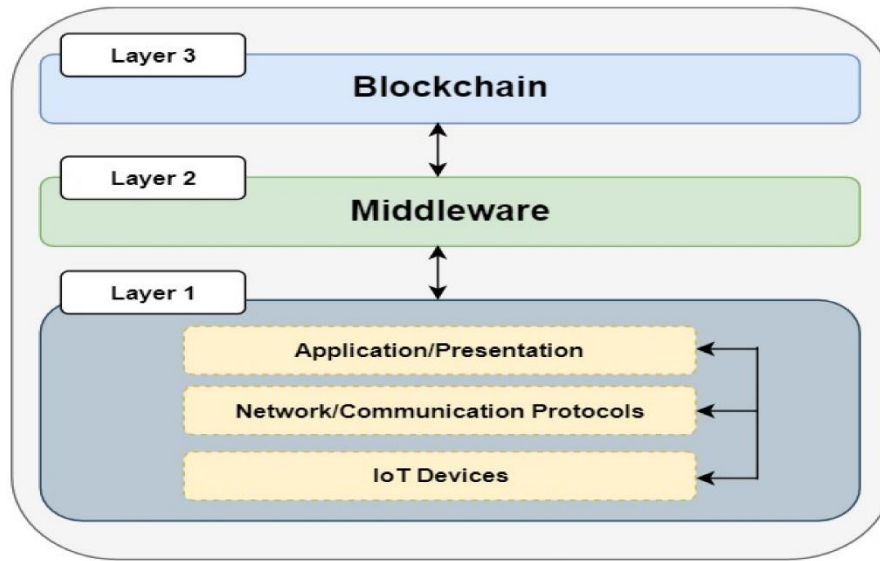


Figure 1: Blockchain-based IoT Edge Network Architecture

BLOCKCHAIN-BASED SECURITY FRAMEWORKS FOR IOT EDGE NETWORKS

IoT edge networks are highly vulnerable due to their distributed nature, heterogeneous devices, and resource constraints. Traditional security mechanisms relying on centralized authorities or cloud-based authentication often fail to meet the real-time and scalability requirements of edge networks. Blockchain technology has emerged as a promising solution to address these limitations.

Blockchain-based frameworks for IoT edge networks aim to:

- Enable **secure and decentralized authentication** of devices.
- Enforce **data integrity** and immutability.
- Implement **access control policies** in a transparent and tamper-proof manner.
- Provide **auditability** for system actions and transactions.

These frameworks can be classified based on architecture, consensus mechanism, and integration with existing IoT protocols.

1. Decentralized Authentication and Access Control

Authentication and access control are critical in IoT edge networks to prevent unauthorized devices from entering the network or accessing sensitive data. Conventional approaches often rely on centralized servers, which are vulnerable to attacks and create a single point of failure.

Blockchain-based solutions replace these centralized mechanisms with **decentralized identity management** and **smart contract-based access control**, offering a scalable and secure alternative.

Key Concepts:

- **Decentralized Identity Management:**

Each IoT device is assigned a blockchain-based identity stored on the distributed ledger. This identity includes cryptographic keys, device metadata, and trust attributes. Devices authenticate themselves by signing transactions with their private keys, and other nodes can verify their legitimacy using public keys stored on the blockchain. This approach eliminates the need for a central certificate authority and reduces the risk of identity spoofing.

- **Access Control Using Smart Contracts:**

Smart contracts are self-executing programs stored on the blockchain that automatically enforce access control policies. For example, a smart contract may define which devices can access a temperature sensor, the frequency of access, or the data that can be read or modified. Once deployed, these contracts operate autonomously and cannot be altered without consensus, ensuring tamper-proof enforcement.

Example Framework – BACIoT:

- **BACIoT (Blockchain-based Access Control for IoT)** is a framework that integrates smart contracts for role-based access control (RBAC) in IoT edge networks.
- **Architecture:** Edge devices register their identities on a permissioned blockchain network. A smart contract encodes access rules based on device roles. When a device requests access to a resource, the smart contract validates the request, ensuring that only authorized devices can interact with sensitive components.
- **Advantages:**
 - Tamper-resistant access control
 - No single point of failure
 - Scalable to large IoT deployments
- **Limitations:**
 - Smart contract execution may consume computational resources
 - Permissioned blockchain setup may require trusted validators

Table 1: Comparison of Blockchain-based Access Control Frameworks

Framework	Consensus	Edge Overhead	Key Feature	Security Level
BACIoT	PoW	Medium	Smart contract RBAC	High
IoT-Chain	PoS	Low	Lightweight consensus	Medium
EdgeBlock	PBFT	High	Fast authentication	High

2. Consensus Mechanisms for Edge Networks

In blockchain systems, **consensus mechanisms** are protocols that ensure all nodes in the network agree on the current state of the distributed ledger. They are critical for maintaining **data integrity, trust, and fault tolerance**. In traditional blockchain networks such as Bitcoin, **Proof-of-Work (PoW)** is used, where nodes (miners) solve complex computational puzzles to validate blocks. While PoW is highly secure, it is **extremely resource-intensive**, requiring significant CPU power and energy, making it unsuitable for **resource-constrained IoT edge networks**.

Edge networks typically include low-power devices with limited processing capability and battery life. Therefore, lightweight consensus mechanisms are necessary to achieve **efficient, secure, and scalable blockchain operation** in such environments. The most commonly used alternatives include **Proof-of-Stake (PoS)**, **Delegated Proof-of-Stake (DPoS)**, and **Practical Byzantine Fault Tolerance (PBFT)**.

a) Proof-of-Stake (PoS)

Proof-of-Stake is a consensus mechanism where the likelihood of a node being selected to validate the next block is proportional to its stake in the network. “Stake” can refer to cryptocurrency holdings, reputation, or other measurable contributions to the network.

How it works in IoT Edge Networks:

1. Each edge device is assigned a stake based on its reliability, past behavior, or resource contribution.
2. Nodes with higher stakes are more likely to be chosen as validators for the next block.
3. Once a validator proposes a block, other nodes verify it. If valid, the block is appended to the blockchain.

Advantages:

- **Low energy consumption:** Unlike PoW, PoS does not require solving complex puzzles.
- **Scalability:** Can handle larger numbers of devices without significant computation overhead.
- **Security:** Higher stake nodes have a strong incentive to maintain network integrity.

Limitations:

- Risk of **centralization** if a few nodes hold most of the stake.
- Requires a **mechanism to assign and adjust stakes** in heterogeneous IoT networks.

Example: In a smart factory edge network, machines with high uptime and reliable data processing could be assigned higher stakes, allowing them to validate transactions more frequently.

b) Delegated Proof-of-Stake (DPoS)

DPoS is an evolution of PoS that further improves efficiency by introducing **delegates**, a small set of trusted nodes responsible for validating transactions and creating blocks on behalf of the network.

How it works:

1. IoT nodes vote for delegates based on trustworthiness, performance, or stake.
2. Only selected delegates participate in consensus and block validation.
3. The blockchain network achieves consensus when a majority of delegates approve a block.

Advantages:

- **High efficiency:** Reduces the number of nodes involved in validation, lowering communication overhead and latency.
- **Faster transaction throughput:** Ideal for real-time IoT applications where rapid confirmation is critical.
- **Resource-friendly:** Non-delegate nodes do not perform heavy computations.

Limitations:

- **Trust dependency:** Security relies on the honesty of delegates.
- Potential for **voting manipulation** if nodes collude to select malicious delegates.

Example: In a smart grid edge network, a few trusted substations act as delegates to validate energy usage data from hundreds of smart meters, ensuring low-latency verification.

c) Practical Byzantine Fault Tolerance (PBFT)

PBFT is a consensus protocol designed for **small to medium-sized networks** where nodes may behave maliciously (Byzantine faults). PBFT allows nodes to reach agreement even if up to one-third of nodes are faulty or compromised.

How it works in IoT Edge Networks:

1. A node proposes a new block to the network.
2. All nodes exchange messages to verify the block through multiple phases: pre-prepare, prepare, and commit.
3. Once a supermajority (typically 2/3) of nodes agree, the block is added to the blockchain.

Advantages:

- **Fast consensus:** Suitable for low-latency edge networks.
- **Resilient to malicious nodes:** Can tolerate a significant fraction of faulty or compromised nodes.
- **Deterministic finality:** Unlike PoW or PoS, blocks are immediately final once consensus is reached, eliminating the risk of forks.

Limitations:

- **Communication overhead:** Requires extensive message exchanges, which may become challenging as network size grows.
- **Limited scalability:** Best suited for networks with tens or hundreds of nodes, rather than thousands.

Example: In an industrial IoT setup, PBFT can secure a network of 50–100 edge devices managing critical machinery, ensuring that even if a few devices are compromised, operations continue securely.

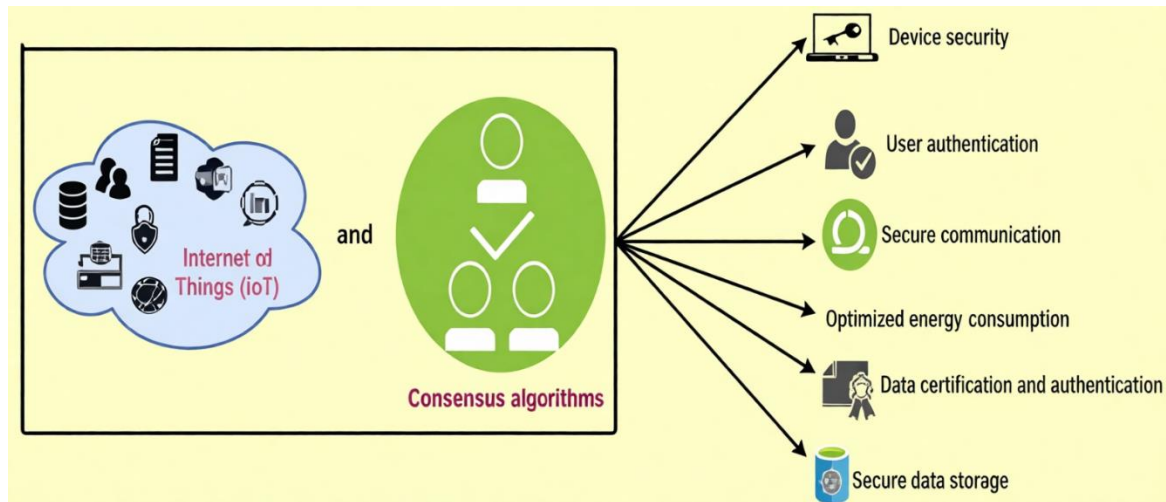


Figure 2: Lightweight Consensus Flow in IoT Edge Blockchain

3. Data Integrity and Privacy Preservation

In IoT edge networks, the integrity and privacy of sensor data are critical because devices generate continuous streams of information that may include sensitive personal, industrial, or environmental data. Blockchain naturally supports **data integrity** by recording transactions in immutable blocks linked with cryptographic hashes. Any tampering of previously stored data becomes easily detectable because a change in a block would alter its hash, breaking the chain. However, blockchain alone does not guarantee **privacy**, since all transaction data may be visible to nodes in the network. To address this, several mechanisms are applied in blockchain-based IoT frameworks:

a) Encryption of Payloads

Before storing data hashes on the blockchain, the actual sensor payload can be encrypted using symmetric or asymmetric cryptography.

- **Symmetric encryption** (e.g., AES) is computationally efficient and suitable for resource-constrained devices.
- **Asymmetric encryption** (e.g., RSA, ECC) provides secure key distribution but may require more processing power.

Example: A smart healthcare device encrypts patient heart-rate readings before submitting a hash to the blockchain. Edge nodes verify the authenticity of the data without exposing raw patient information.

b) Zero-Knowledge Proofs (ZKP)

ZKP allows one party to prove the validity of information to another without revealing the actual data. In IoT edge networks, ZKP can be used to confirm that sensor readings meet expected criteria while keeping raw data confidential.

- **Example Framework: IoT-PrivacyChain**

- IoT devices generate proofs for sensor readings.
- Edge nodes or blockchain validators verify these proofs without accessing the underlying data.
- This ensures compliance with privacy regulations while maintaining data integrity.

c) Homomorphic Encryption

Homomorphic encryption allows computation on encrypted data without decryption. This is particularly useful in edge networks where analytics or aggregation is required without exposing raw data.

- **Use Case:** Multiple IoT sensors in a smart city encrypt traffic or pollution data. The edge server performs analytics on encrypted data and submits the results to the blockchain for audit and verification.

Advantages of Combining Blockchain with Privacy Techniques:

- Ensures **tamper-proof records** while keeping sensitive information confidential.
- Enhances **regulatory compliance**, for example with GDPR or HIPAA.
- Enables **secure collaborative analytics**, where multiple parties contribute data without revealing raw inputs.

4. Hybrid Blockchain Architectures

To improve scalability, performance, and security in IoT edge networks, researchers have proposed hybrid architectures that combine blockchain with other technologies, including edge-cloud integration and AI-based security systems.

a) Edge-Cloud Hybrid Blockchain

In this architecture, blockchain responsibilities are split between **edge nodes** and **cloud servers**:

- **Edge Layer:** Edge devices handle **lightweight consensus** and validate local transactions,

ensuring low latency and efficient real-time processing.

- **Cloud Layer:** Central servers store the **full blockchain ledger**, providing long-term storage, auditability, and global synchronization.

Benefits:

- Reduces computation and storage burden on edge devices.
- Maintains immutability and traceability of data through centralized ledger storage.
- Supports large-scale IoT deployments without overloading the network.

Use Case: A smart manufacturing plant uses edge nodes to validate sensor readings from machinery, while cloud servers maintain the complete blockchain to ensure compliance with industry safety standards.

b) Blockchain + AI-based Intrusion Detection

Integrating **machine learning (ML) or deep learning** with blockchain enhances security by enabling proactive threat detection.

• **Mechanism:**

- ML models at edge nodes monitor device behavior for anomalies such as unusual traffic patterns, unauthorized access attempts, or sensor data inconsistencies.
- Blockchain stores alerts immutably, ensuring that detected attacks cannot be tampered with.
- Smart contracts can trigger automated responses, such as blocking a malicious device or alerting administrators.

Benefits:

- Enhances **real-time security monitoring** without relying solely on central servers.
- Provides **tamper-proof audit logs** for forensic analysis.
- Supports **adaptive security**, where the system learns from new threats over time.

Table 2: Hybrid Blockchain Security Approaches

Hybrid Model	Blockchain Role	Additional Technique	Benefits	Challenges
Edge-Cloud	Ledger storage	Edge preprocessing	Low latency, reduced storage	Synchronization issues

Hybrid Model	Blockchain Role	Additional Technique	Benefits	Challenges
AI-Blockchain	Audit logs	ML intrusion detection	Immutable threat records	Training overhead
Fog-Blockchain	Consensus & auth	Fog orchestration	Fast, decentralized auth	Scalability for large networks

IMPLEMENTATION CHALLENGES

While blockchain offers robust security, practical implementation in IoT edge networks faces several challenges:

- 1. Resource Constraints:** Many IoT devices cannot perform intensive cryptographic operations.
- 2. Latency:** Consensus mechanisms introduce delays, which may impact real-time applications.
- 3. Scalability:** Large IoT networks may overwhelm blockchain nodes.
- 4. Interoperability:** Devices with different protocols may struggle to participate in the same blockchain network.
- 5. Regulatory Compliance:** Privacy laws such as GDPR can conflict with immutable ledgers.

PERFORMANCE EVALUATION METRICS

To evaluate blockchain frameworks in IoT edge networks, common metrics include:

- **Throughput:** Number of transactions processed per second.
- **Latency:** Time taken to validate and record a transaction.
- **Energy Consumption:** Power used per transaction.
- **Storage Overhead:** Memory required for blockchain data.
- **Security Level:** Resistance against attacks such as DDoS or tampering.

FUTURE DIRECTIONS

Future research can focus on:

- **Ultra-lightweight blockchain protocols** optimized for microcontrollers.
- **Integration with 5G/6G networks** to improve real-time communication.

- **Cross-chain interoperability** to allow secure data exchange between different IoT networks.
- **Energy-efficient consensus** using AI to predict validator selection.
- **Post-quantum cryptography** to prepare for emerging threats.

CONCLUSION

Blockchain-based security frameworks offer a promising solution to the challenges of securing IoT edge networks. By leveraging decentralization, immutability, and smart contracts, these frameworks can provide robust authentication, data integrity, and privacy preservation without relying on centralized authorities. Lightweight consensus mechanisms and hybrid architectures address the limitations of resource-constrained edge devices. However, challenges related to latency, scalability, and interoperability remain significant. Ongoing research into optimized consensus, hybrid models, and integration with AI and next-generation networks will further enhance the applicability of blockchain in IoT edge environments.

REFERENCES

1. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog Computing for the Internet of Things: Security and Privacy Issues. *IEEE Internet Computing*, 21(2), 34–42.
2. Dorri, A., Kanhere, S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. *IEEE Internet of Things Journal*, 4(6), 1–14.
3. Nguyen, G., Kim, K., & Kim, J. (2019). A Survey on Blockchain-Based IoT Security Frameworks. *Journal of Network and Computer Applications*, 122, 85–99.
4. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303.
5. Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's Adoption in IoT: The Challenges, and a Way Forward. *Journal of Network and Computer Applications*, 125, 251–279.
6. Sharma, P., & Mehta, A. (2020). Lightweight Blockchain-Based Security Frameworks for Resource-Constrained IoT Devices. *International Journal of Computer Applications*, 176(14), 25–35.
7. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On Blockchain and Its

8. Integration with IoT. *Challenges and Opportunities. Future Generation Computer Systems*, 88, 173–190.
9. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*, 107, 841–853.
10. Bera, B., Misra, S., & Saha, R. (2020). Edge Computing for IoT: A Secure Blockchain Framework. *Journal of Information Security and Applications*, 55, 102646.
11. Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2018). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5), 1250–1258.