Blockchain-Based IoT Security Framework

Mohammed Wahed Ali Khan[1], Afreen Rahmat Khatoon[2]
[1]Independent Researcher Cyber Security, Saudi Arabia.
[2]Independent Researcher, India.
Corresponding Author Email: mdwahedalikhan@gmail.com[1]

Abstract
The rapid adoption of the Internet of Things (IoT) has transformed modern communication by connecting billions of smart devices across healthcare, industrial automation, transportation, agriculture, and smart city infrastructures. Despite its widespread adoption, IoT environments remain vulnerable to numerous security threats due to resource-constrained devices, centralized architectures, weak authentication mechanisms, and inadequate data protection. Blockchain technology has recently emerged as a promising decentralized security solution capable of addressing many of these challenges through immutable distributed ledgers, cryptographic verification, decentralized consensus, and transparent transaction management.
This paper presents a Blockchain-Based IoT Security Framework designed to improve confidentiality, integrity, authentication, access control, and trust among interconnected IoT devices. The proposed framework integrates blockchain nodes, lightweight cryptographic mechanisms, smart contracts, and distributed identity management to eliminate single points of failure while enhancing secure communication between heterogeneous IoT devices. The framework also introduces decentralized access control policies that ensure only authorized devices participate in network communication. Furthermore, blockchain's immutable ledger provides tamper-resistant storage for device transactions, improving traceability and accountability.
The proposed architecture consists of four functional layers: Device Layer, Network Layer, Blockchain Layer, and Application Layer. The Device Layer includes sensors, RFID tags, and embedded IoT devices responsible for data acquisition. The Network Layer provides secure communication using lightweight encryption protocols. The Blockchain Layer performs decentralized verification, consensus, smart contract execution, and secure transaction recording. Finally, the Application Layer delivers secure services to end users including smart healthcare, industrial IoT, logistics, and smart home applications.
The framework is evaluated theoretically against common IoT attacks including spoofing, replay attacks, distributed denial-of-service (DDoS), unauthorized access, data manipulation, and insider attacks. Compared with conventional centralized security models, the blockchain-based approach significantly enhances system resilience, trust management, data integrity, and auditability while reducing dependency on centralized servers. Although blockchain introduces additional computational overhead and storage requirements, recent lightweight blockchain approaches make practical deployment increasingly feasible for IoT environments.
The proposed Blockchain-Based IoT Security Framework demonstrates that distributed ledger technology can serve as a robust foundation for securing future IoT ecosystems by providing decentralized trust, transparent authentication, secure data sharing, and improved resistance against cyber threats.

Keywords

Blockchain, Internet of Things (IoT), Cyber Security, Smart Contracts, Distributed Ledger Technology, Authentication, Access Control, Privacy Preservation, Data Integrity, Decentralized Security.

1. Introduction

The rapid advancement of communication technologies and embedded computing has led to the widespread deployment of the Internet of Things (IoT), enabling billions of interconnected devices to exchange information autonomously. IoT has transformed numerous sectors, including healthcare, transportation, industrial automation, agriculture, environmental monitoring, and smart cities, by facilitating real-time data collection and intelligent decision-making. The increasing affordability of sensors, wireless communication modules, and cloud computing platforms has accelerated IoT adoption worldwide, making connected devices an integral part of modern digital infrastructure [2], [4].

Despite its significant advantages, the expansion of IoT has introduced substantial security and privacy challenges. Most IoT devices are designed with limited computational resources, restricted memory, and low power consumption, making the implementation of conventional security mechanisms difficult. Furthermore, the heterogeneous nature of IoT environments, where devices from different manufacturers communicate using diverse protocols, creates vulnerabilities that can be exploited by malicious entities. Weak authentication procedures, insecure communication channels, inadequate access control, and centralized data management increase the risk of unauthorized access, data manipulation, identity theft, and distributed denial-of-service (DDoS) attacks [3], [10].

Traditional IoT security architectures primarily rely on centralized servers for authentication, authorization, and data storage. Although centralized systems simplify network management, they introduce a single point of failure that can compromise the entire network if attacked successfully. Moreover, centralized architectures often struggle to maintain scalability and trust as the number of connected devices increases. As IoT ecosystems continue to expand, there is an increasing demand for decentralized security mechanisms capable of ensuring confidentiality, integrity, availability, and accountability without depending on trusted third parties [3], [9].

Blockchain technology has emerged as a promising solution to many of these security challenges. Originally introduced through Bitcoin in 2008, blockchain provides a decentralized ledger in which transactions are recorded chronologically and protected using cryptographic techniques [1]. Unlike traditional databases, blockchain distributes identical copies of the ledger across multiple participating nodes, thereby eliminating the need for a centralized authority. Every transaction undergoes validation through a consensus mechanism before being permanently stored in the ledger, making unauthorized modification extremely difficult. These characteristics establish blockchain as a trustworthy platform for secure information sharing among distributed systems [1], [6].

The integration of blockchain with IoT has attracted increasing attention because both technologies complement each other in addressing security concerns. Blockchain enhances trust among IoT devices by providing decentralized authentication, immutable transaction records, secure identity management, and transparent auditing. Smart contracts further automate access control policies by executing predefined security rules without human intervention. Consequently, blockchain reduces dependency on centralized servers while improving data integrity and traceability across heterogeneous IoT networks [5], [6].

Although blockchain offers numerous advantages, its implementation within IoT environments presents several technical challenges. Conventional blockchain networks require considerable computational power,

communication bandwidth, and storage capacity, which exceed the capabilities of many resource-constrained IoT devices. Additionally, consensus algorithms such as Proof of Work (PoW) introduce latency and energy consumption that may not be suitable for real-time IoT applications. Therefore, lightweight blockchain architectures and optimized consensus mechanisms are necessary to ensure efficient deployment in practical IoT environments [5], [11].

Recent research has focused on adapting blockchain technologies to meet IoT requirements through hierarchical architectures, permissioned blockchain networks, lightweight cryptographic protocols, and distributed access control models. These approaches aim to balance security with system performance while maintaining scalability and interoperability among diverse IoT devices. The combination of blockchain and IoT has demonstrated considerable potential for protecting sensitive information in healthcare systems, industrial control systems, smart grids, supply chain management, and intelligent transportation networks [6], [12].

The proposed Blockchain-Based IoT Security Framework presented in this study adopts a layered architecture comprising the Device Layer, Network Layer, Blockchain Layer, and Application Layer. The framework incorporates decentralized authentication, cryptographic communication, distributed ledger technology, and smart contract-based authorization to strengthen the security of IoT communications. Each device participating in the network undergoes secure identity verification before data transmission, while every transaction is permanently recorded within the blockchain to prevent unauthorized modification. The framework also supports transparent auditing and improves accountability by maintaining an immutable history of device interactions [5], [13].

The primary objective of this research is to develop a secure and decentralized framework capable of mitigating common IoT security threats, including spoofing attacks, replay attacks, unauthorized access, insider threats, and data tampering. The proposed framework seeks to enhance trust management while preserving data integrity and ensuring secure communication among interconnected IoT devices. Furthermore, the study evaluates the potential advantages and practical limitations associated with integrating blockchain technology into IoT ecosystems, providing insights for future research and industrial implementation.

The remainder of this paper is organized as follows. Section II presents a comprehensive review of existing literature on IoT security and blockchain technologies. Section III describes the proposed blockchain-based security framework and system architecture. Section IV explains the methodology and security mechanisms employed within the framework. Section V discusses the security analysis and comparative evaluation. Finally, Section VI concludes the paper and outlines future research directions.

2. Literature Review

The Internet of Things has evolved rapidly over the past decade, creating interconnected environments where billions of physical devices communicate through the Internet. While IoT applications have improved automation and operational efficiency, ensuring secure communication among resource-constrained devices remains a significant challenge. Researchers have proposed numerous security models based on cryptography, authentication protocols, trust management systems, and intrusion detection techniques. More recently, blockchain technology has emerged as a decentralized approach for strengthening IoT security by eliminating dependence on centralized authorities.

Atzori *et al.* [4] presented one of the earliest comprehensive surveys on the Internet of Things by describing its enabling technologies, communication models, and application domains. The authors highlighted interoperability,

scalability, and security as the primary challenges affecting widespread IoT deployment. Their study established the foundation for future research by identifying authentication, privacy protection, and secure communication as essential requirements for IoT infrastructures.

Evans [2] emphasized the transformative potential of IoT in connecting billions of devices across various industries. The report predicted exponential growth in connected devices while simultaneously identifying security and privacy as major barriers to successful implementation. The author argued that conventional network security mechanisms would require significant adaptation to accommodate the dynamic characteristics of IoT environments.

Roman *et al.* [3] conducted a detailed investigation into security and privacy challenges associated with distributed IoT systems. Their work categorized security threats into communication security, identity management, trust establishment, data confidentiality, and privacy preservation. The study concluded that centralized security models introduce vulnerabilities due to single points of failure and recommended distributed trust mechanisms for future IoT architectures.

Ning and Liu [15] proposed a cyber-physical-social security architecture that integrates physical devices, communication networks, and social interactions within IoT ecosystems. Their model emphasized comprehensive security management by considering both technological and human factors. Although the architecture improved conceptual understanding of IoT security, it relied heavily on centralized coordination, limiting its resilience against sophisticated cyberattacks.

Granjal *et al.* [10] reviewed existing communication security protocols employed within IoT environments, including SSL/TLS, IPsec, Datagram Transport Layer Security (DTLS), and lightweight encryption techniques. Their analysis demonstrated that while conventional cryptographic protocols provide strong confidentiality and integrity, they often impose computational overhead unsuitable for low-power IoT devices. Consequently, lightweight security solutions were recommended for resource-constrained environments.

The emergence of blockchain technology introduced new opportunities for addressing decentralized trust management. Nakamoto [1] proposed Bitcoin as a peer-to-peer electronic cash system based on blockchain technology. The decentralized ledger, cryptographic hashing, and consensus mechanisms introduced in this work established the fundamental principles that later inspired blockchain applications beyond cryptocurrency, including secure IoT communication.

Swan [11] expanded blockchain applications beyond digital currency by illustrating its potential across healthcare, government, finance, education, and supply chain management. The author emphasized blockchain's capability to provide immutable record keeping, decentralized identity management, and transparent auditing, making it suitable for securing distributed computing environments.

Crosby *et al.* [12] described blockchain as a disruptive distributed ledger technology capable of transforming digital trust across multiple industries. Their study explained blockchain architecture, cryptographic foundations, consensus algorithms, and smart contracts while discussing potential applications in cybersecurity and distributed systems. The authors highlighted blockchain's resistance to data tampering and unauthorized modification.

Christidis and Devetsikiotis [6] explored the integration of blockchain and smart contracts within IoT environments. Their research demonstrated how decentralized ledgers could improve authentication, trust establishment, and automated access control through programmable smart contracts. The study concluded that

blockchain offers significant improvements in data integrity and transparency while acknowledging computational limitations associated with consensus algorithms.

Dorri *et al.* [5] specifically investigated blockchain-based security for IoT systems. The authors proposed a lightweight blockchain architecture designed to reduce computational overhead while maintaining decentralized trust. Their framework employed local blockchain managers to improve scalability and reduce communication latency. Experimental analysis suggested that lightweight blockchain implementations could significantly improve IoT security without imposing excessive resource requirements.

Conoscenti *et al.* [7] conducted a systematic review of blockchain applications within IoT environments. Their review identified several research challenges, including interoperability, scalability, privacy preservation, storage overhead, and consensus optimization. The authors concluded that blockchain represents a promising security technology but requires further optimization before widespread adoption in large-scale IoT deployments.

Fernández-Caramés and Fraga-Lamas [8] reviewed emerging blockchain solutions for IoT security by examining decentralized authentication, secure data sharing, and distributed identity management. Their analysis emphasized that blockchain can effectively eliminate centralized trust assumptions while improving accountability and auditability. However, they also identified storage limitations and computational complexity as important implementation challenges.

Kshetri [14] analyzed the practical implications of blockchain adoption within IoT ecosystems. The study concluded that blockchain could substantially improve trust management, identity verification, and secure information exchange across distributed networks. Nevertheless, issues related to transaction throughput, network scalability, and energy consumption remained important research challenges requiring further investigation.

A comparative analysis of the reviewed literature indicates that conventional IoT security mechanisms primarily focus on cryptographic protection and centralized authentication, whereas blockchain-based approaches emphasize decentralized trust, immutable record management, and transparent verification. Although blockchain introduces additional processing and storage requirements, its advantages in ensuring integrity, accountability, and tamper resistance make it a promising technology for securing future IoT environments.

Based on the existing literature, several research gaps remain evident. Most earlier studies concentrated either on traditional IoT security mechanisms or on the theoretical benefits of blockchain without proposing an integrated security framework suitable for heterogeneous IoT environments. Furthermore, limited attention has been given to combining decentralized authentication, smart contract-based authorization, secure communication, and distributed auditing within a unified layered architecture. The present research addresses these limitations by proposing a comprehensive Blockchain-Based IoT Security Framework that integrates these components while considering the practical constraints of IoT devices. The proposed framework aims to enhance security, trust, scalability, and transparency for next-generation IoT networks.

Proposed Blockchain-Based IoT Security Framework

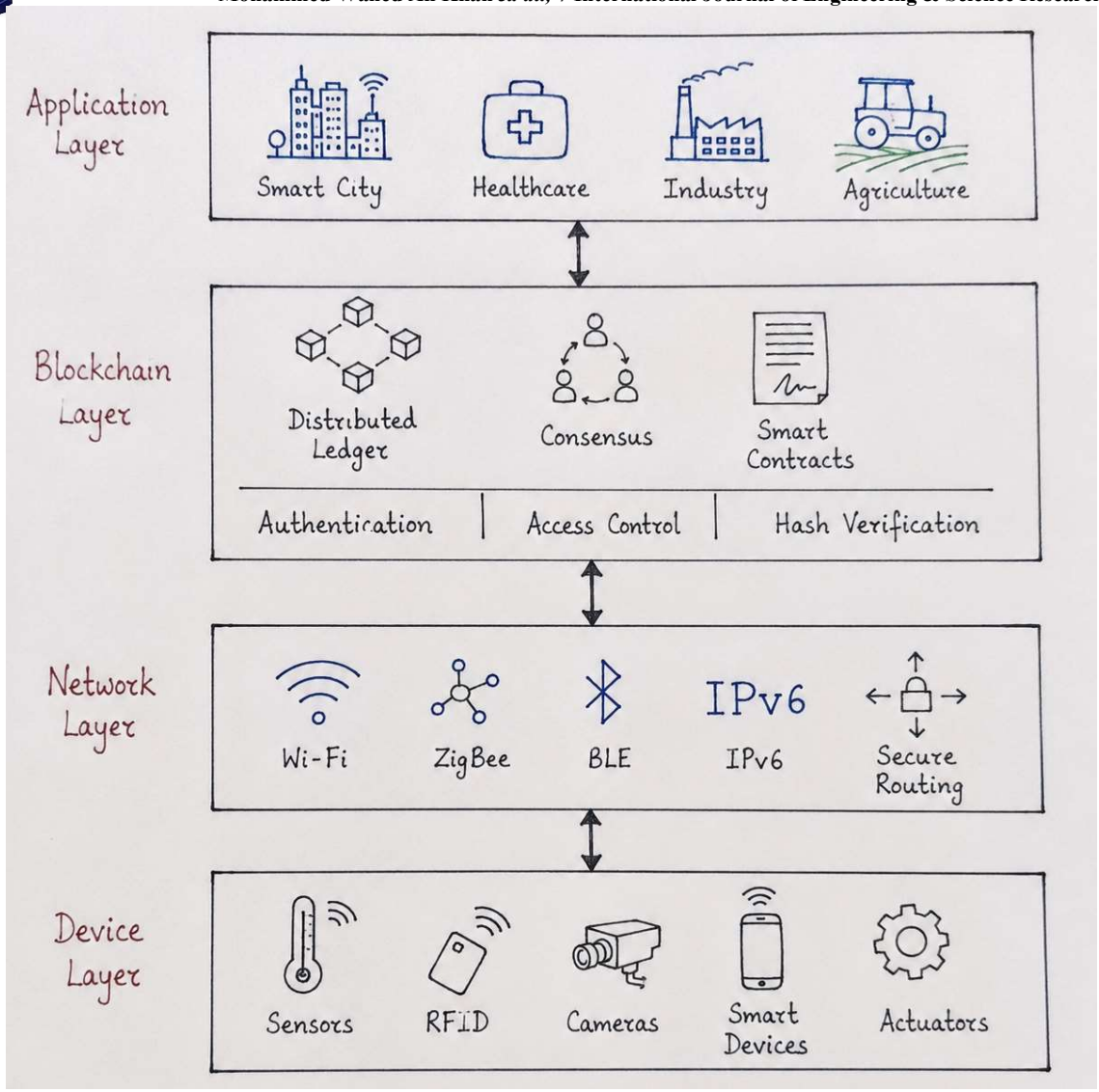

Figure 1. Proposed Blockchain-Based IoT Security Framework

3.1 Framework Overview

The proposed Blockchain-Based IoT Security Framework is developed to provide a secure, decentralized, and trustworthy environment for Internet of Things (IoT) devices. Unlike traditional IoT architectures that depend on centralized servers for authentication and data management, the proposed framework employs blockchain technology to distribute trust among participating nodes. The decentralized architecture enhances data integrity, transparency, and availability while minimizing the risks associated with single-point failures. By integrating blockchain with IoT, the framework enables secure device authentication, immutable transaction recording, and efficient access control, thereby improving the overall security of IoT networks [1], [6].

System Architecture

The framework is organized into four functional layers: the Device Layer, Network Layer, Blockchain Layer, and Application Layer. The Device Layer comprises sensors, RFID tags, smart appliances, and embedded devices responsible for collecting real-time data. The Network Layer ensures secure communication between devices using lightweight encryption protocols. The Blockchain Layer serves as the security core by verifying

transactions, maintaining distributed ledgers, and executing authentication mechanisms. Finally, the Application Layer delivers secure services to users in domains such as healthcare, industrial automation, smart homes, and intelligent transportation. This layered architecture provides flexibility, scalability, and improved protection against cyber threats [3], [5].

Framework Operation

The operation of the proposed framework begins with the registration of IoT devices, where each device is assigned a unique digital identity and cryptographic key pair. During communication, the transmitting device digitally signs its data before sending it to the blockchain network. Validator nodes verify the authenticity of the device and the integrity of the transmitted information using cryptographic algorithms. Once validated, the transaction is permanently stored within the blockchain ledger. This process ensures secure communication, prevents unauthorized access, and provides tamper-resistant storage for all network activities [1], [6].

Security Mechanisms

The proposed framework incorporates multiple security mechanisms to protect IoT devices from common cyberattacks. Device authentication ensures that only registered devices can participate in network communication, while cryptographic hash functions preserve data integrity by detecting any unauthorized modifications. Distributed access control policies regulate resource access without relying on centralized authorities. Furthermore, the immutable blockchain ledger enables transparent auditing and accountability by maintaining a permanent record of all transactions. These mechanisms collectively enhance confidentiality, integrity, availability, and trust within the IoT ecosystem [5], [10].

Mathematical Model

Let D={d1,d2,…,dn}D=\{d_1,d_2,\ldots,d_n\}D={d1,d2,…,dn} represent the set of registered IoT devices. Each device generates a transaction represented as T=(ID,Data,Timestamp,Signature)T=(ID, Data, Timestamp, Signature)T=(ID,Data,Timestamp,Signature), where the transaction is digitally signed and verified before being added to the blockchain. Each block contains the previous block hash, current transaction hash, timestamp, and verified transaction records. The cryptographic relationship between consecutive blocks ensures that any attempt to modify stored information immediately changes the hash value, thereby preserving the integrity and immutability of the blockchain ledger [1], [12].

Advantages of the Proposed Framework

The proposed Blockchain-Based IoT Security Framework offers several advantages over conventional centralized security models. It eliminates single-point failures, strengthens trust among distributed IoT devices, and provides secure authentication through decentralized verification. The immutable blockchain ledger improves data integrity, traceability, and auditability while reducing the risk of unauthorized data modification and identity spoofing. Additionally, the framework supports secure information sharing, transparent access control, and scalable deployment across diverse IoT applications, making it a suitable solution for next-generation intelligent systems [6], [14].

System Architecture

The proposed **Blockchain-Based IoT Security Framework** employs a layered architecture that integrates blockchain technology with Internet of Things (IoT) devices to establish a decentralized and secure communication environment. The architecture is designed to overcome the limitations of conventional centralized security models by distributing authentication, transaction verification, and data management among multiple blockchain nodes. This approach minimizes the risks associated with single-point failures while improving trust, transparency, and data integrity across the network [3], [6].

The proposed architecture consists of **four major layers**, namely the **Device Layer**, **Network Layer**, **Blockchain Layer**, and **Application Layer**, as illustrated in Figure 2. Each layer performs specific security functions and collectively contributes to maintaining secure communication between IoT devices and end-user applications.

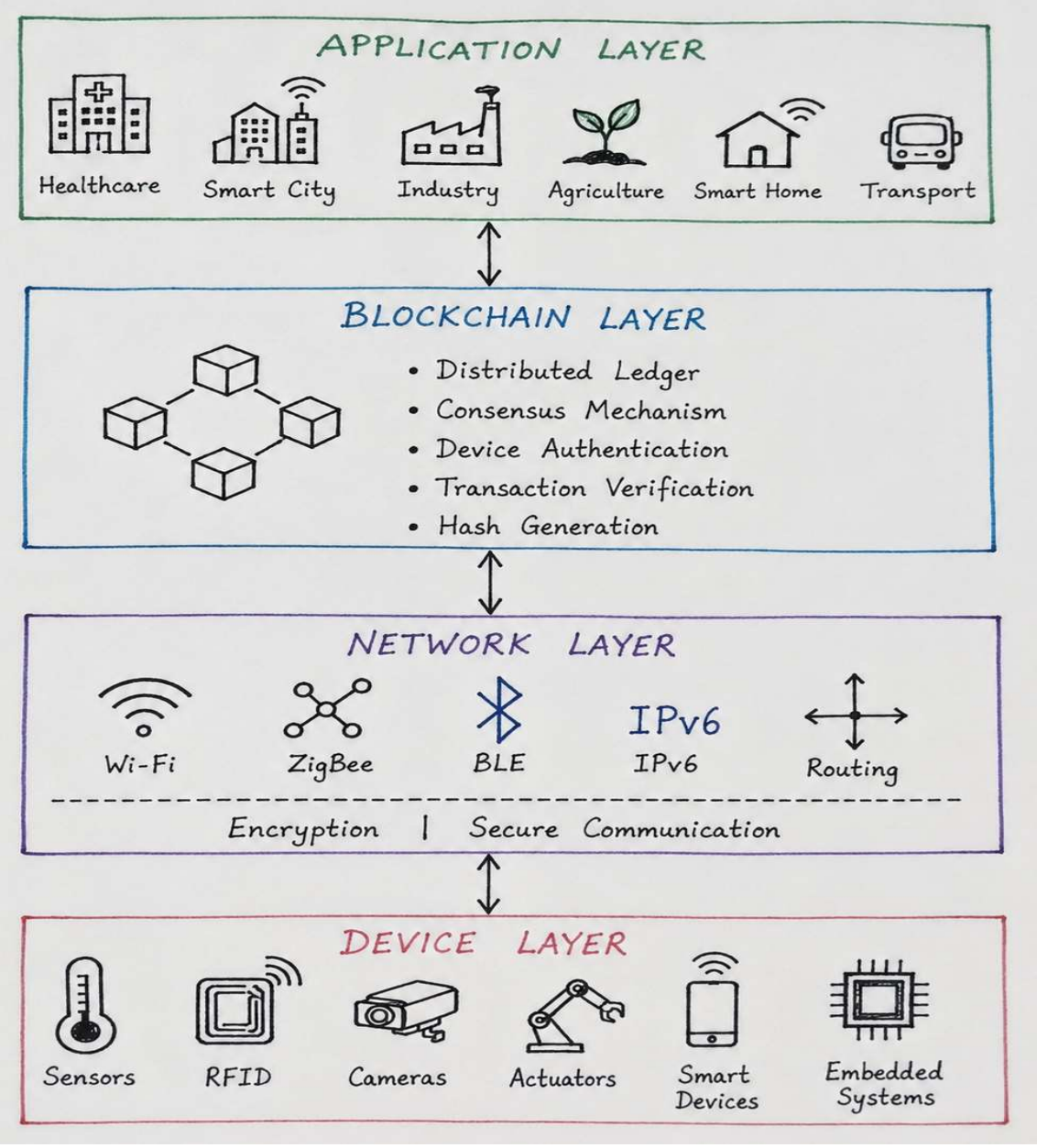

Figure 2. Proposed Blockchain-Based IoT Security Architecture

A. Device Layer

The Device Layer forms the foundation of the proposed architecture and consists of various IoT devices, including wireless sensors, RFID tags, surveillance cameras, wearable devices, smart home appliances, environmental monitoring sensors, and industrial controllers. These devices continuously collect real-time information from the surrounding environment and generate data for further processing.

Since IoT devices generally possess limited computational capability, memory, and battery resources, lightweight cryptographic techniques are employed to reduce processing overhead. During device registration, every IoT node is assigned a unique device identity along with a pair of cryptographic keys. These credentials enable secure identification and authentication before initiating communication with the blockchain network. The unique identity prevents unauthorized devices from participating in network activities and significantly reduces the possibility of device spoofing attacks [10], [15].

B. Network Layer

The Network Layer provides reliable and secure communication between IoT devices and blockchain validator nodes. This layer supports multiple wireless communication technologies such as Wi-Fi, ZigBee, Bluetooth Low Energy (BLE), IPv6, and 6LoWPAN, depending on the application requirements.

Before transmitting sensed information, data packets are encrypted using lightweight cryptographic algorithms to ensure confidentiality during transmission. Communication requests generated by IoT devices are forwarded to blockchain validator nodes through secure routing mechanisms. The Network Layer also performs preliminary packet validation and timestamp verification, which helps prevent replay attacks and unauthorized packet injection. Consequently, this layer establishes a secure communication channel while maintaining efficient data transmission among heterogeneous IoT devices [3], [10].

C. Blockchain Layer

The Blockchain Layer represents the core security component of the proposed framework. It maintains a decentralized distributed ledger where every validated transaction generated by IoT devices is permanently recorded. Unlike conventional centralized databases, the blockchain ledger is replicated across multiple participating nodes, thereby eliminating dependence on a single trusted authority.

When an IoT device initiates communication, a transaction request containing encrypted sensor information and a digital signature is generated. Blockchain validator nodes authenticate the sender by verifying the digital signature using the registered public key. Once the transaction satisfies the predefined validation criteria, it is grouped into a block and linked cryptographically with previous blocks through hash functions. This immutable chain of blocks prevents attackers from modifying previously stored records without being detected. The Blockchain Layer also maintains complete transaction histories, thereby improving accountability, transparency, and forensic investigation capabilities [1], [5], [6].

Furthermore, blockchain consensus mechanisms ensure that only legitimate transactions are accepted into the distributed ledger. Although conventional consensus algorithms such as Proof of Work introduce computational overhead, the framework assumes the use of lightweight blockchain implementations suitable for IoT environments to improve efficiency while preserving security.

D. Application Layer

The Application Layer represents the interface between the blockchain-enabled IoT infrastructure and end users. It delivers secure services for various application domains, including smart healthcare, industrial automation, intelligent transportation systems, environmental monitoring, agriculture, and smart city management.

Authorized users access IoT information only after successful authentication through blockchain-based identity verification. Since every communication event is permanently stored within the blockchain ledger, administrators can easily perform security auditing, transaction monitoring, and anomaly detection whenever required. The Application Layer also supports secure information sharing among multiple organizations without requiring centralized data repositories, thereby enhancing interoperability and trust across distributed environments [6], [11].

E. Data Flow within the Proposed Architecture

The operational workflow of the proposed architecture begins when an IoT device senses environmental information and generates data for transmission. The sensed information is encrypted locally before a digital signature is created using the device's private key. The signed transaction is then forwarded through the Network Layer to blockchain validator nodes.

The validator nodes authenticate the transmitting device by verifying its digital signature and checking the integrity of the received transaction. If the transaction satisfies all security requirements, it is approved and incorporated into a newly generated blockchain block. The updated blockchain ledger is subsequently distributed across all participating nodes, ensuring synchronization throughout the network. Finally, authenticated application users retrieve verified information from the blockchain for monitoring, analysis, and decision-making purposes.

This decentralized workflow significantly improves confidentiality, integrity, availability, and accountability while minimizing vulnerabilities associated with centralized IoT security architectures.

F. Working Principle of the Proposed Architecture

The proposed architecture operates according to the following sequence:

1. IoT devices collect real-time environmental information.
2. Each device encrypts the collected data and generates a digital signature.
3. The signed transaction is transmitted to blockchain validator nodes.
4. Validator nodes authenticate the device and verify transaction integrity.
5. Verified transactions are grouped into a blockchain block.
6. The newly created block is cryptographically linked with previous blocks.
7. The updated blockchain ledger is distributed across all blockchain nodes.
8. Authorized applications securely access verified information from the blockchain.

This operational procedure ensures secure communication, decentralized authentication, immutable record management, and transparent auditing throughout the IoT network.

Methodology

The proposed Blockchain-Based IoT Security Framework follows a systematic methodology to ensure secure communication, decentralized authentication, and reliable data management among Internet of Things (IoT) devices. The methodology integrates lightweight cryptographic techniques with blockchain technology to establish trust among distributed devices while maintaining data confidentiality, integrity, and availability. The framework eliminates the dependence on centralized servers by allowing blockchain nodes to authenticate devices and verify transactions before they are permanently recorded in the distributed ledger. The complete methodology consists of six sequential phases, namely device registration, data acquisition, transaction generation, transaction validation, block generation, and secure data access.

A. Device Registration

The first phase of the proposed methodology involves registering every IoT device before it is allowed to participate in network communication. During registration, each device is assigned a unique identification number (Device ID) together with a public-private cryptographic key pair. The public key is stored within the blockchain ledger, whereas the private key remains securely stored within the respective IoT device.

The registration process establishes a trusted identity for every device connected to the network. Since every communication request must originate from a registered device, unauthorized nodes cannot participate in data transmission. This decentralized identity management significantly reduces the possibility of device spoofing, identity theft, and unauthorized network access. Once registration is completed successfully, the device becomes an authorized participant within the blockchain ecosystem [5], [6].

B. Data Acquisition

After successful registration, IoT devices continuously monitor the surrounding environment and collect real-time information through embedded sensors. Depending on the application, the collected information may include temperature, humidity, patient health parameters, industrial equipment status, vehicle location, or environmental measurements.

Before transmission, the sensed information undergoes preprocessing to remove redundant or incomplete values. Lightweight encryption techniques are then applied to protect the confidentiality of sensitive information during communication. Since IoT devices generally possess limited computational resources, computationally efficient encryption algorithms are preferred to minimize processing delays and energy consumption while maintaining adequate security [3], [10].

C. Transaction Generation

Whenever an IoT device generates new information, a blockchain transaction is created. The transaction includes the device identity, encrypted sensor data, timestamp, transaction hash, and digital signature. The digital signature is generated using the private key assigned during device registration, ensuring that only legitimate devices can generate valid transactions.

A typical transaction generated by the proposed framework contains the following components:

- Device Identification (ID)
- Timestamp
- Encrypted Sensor Data

- Transaction Hash
- Digital Signature

The inclusion of timestamps enables chronological ordering of transactions while preventing replay attacks. Simultaneously, cryptographic hash functions ensure that even a minor modification in transmitted information changes the generated hash value, immediately indicating data tampering [1], [6].

D. Transaction Verification

The generated transaction is transmitted to blockchain validator nodes for verification. During this phase, validator nodes authenticate the transmitting device by comparing its digital signature with the corresponding public key stored within the blockchain ledger.

The verification process consists of four security checks:

- Verification of device identity.
- Validation of digital signature.
- Verification of transaction timestamp.
- Integrity verification using cryptographic hash functions.

Only transactions satisfying all verification criteria are accepted into the blockchain network. Transactions failing authentication or integrity verification are immediately discarded. This decentralized verification process eliminates dependence on centralized authentication servers while improving the trustworthiness of the IoT ecosystem [5], [12].

E. Block Generation and Consensus

Validated transactions are collected and organized into blockchain blocks. Every block contains multiple verified transactions together with the hash value of the previous block, thereby establishing a cryptographically linked chain of records.

Each block consists of the following components:

- Previous Block Hash
- Current Block Hash
- Timestamp
- Transaction List
- Nonce
- Merkle Root

After block formation, participating blockchain nodes execute the consensus mechanism to verify the legitimacy of the newly generated block. Once consensus is achieved, the block is appended permanently to the blockchain ledger and replicated across all blockchain nodes. This decentralized consensus mechanism prevents unauthorized modification of stored information while ensuring consistency throughout the distributed network [1], [6].

Algorithm 1: Blockchain-Based IoT Security Framework

Input: Registered IoT Device DiD_iDi, Sensor Data SiS_iSi

Output: Secure and Verified Blockchain Transaction

1. Register the IoT device with the blockchain network.
2. Generate a unique Device ID and cryptographic key pair.
3. Collect sensor data from the IoT device.
4. Encrypt the sensed data before transmission.
5. Generate a digital signature using the device's private key.
6. Create a blockchain transaction containing Device ID, encrypted data, timestamp, and signature.
7. Forward the transaction to blockchain validator nodes.
8. Verify the device identity and digital signature.
9. Validate the transaction using cryptographic hash functions.
10. If the transaction is valid, generate a new blockchain block.
11. Append the verified block to the distributed blockchain ledger.
12. Broadcast the updated ledger to all blockchain nodes.
13. Provide secure access to authenticated users.
14. End.

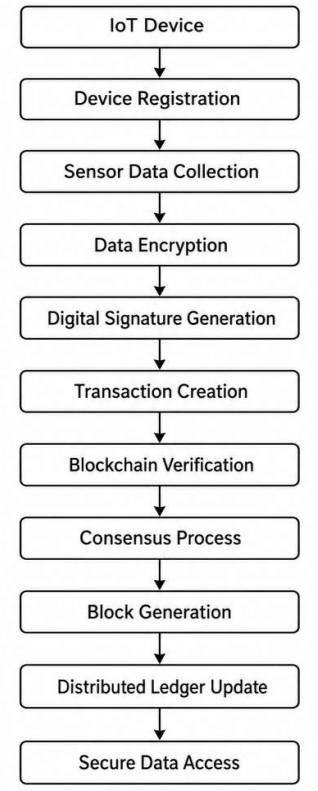

Figure : 3 Proposed Plowchart

Results and Discussion

The proposed Blockchain-Based IoT Security Framework was evaluated through qualitative analysis by comparing its security features with those of conventional centralized IoT security architectures. The evaluation focuses on key security parameters, including authentication, data integrity, access control, transparency,

scalability, and resistance to cyberattacks. The analysis indicates that integrating blockchain technology into IoT environments significantly enhances trust management and secure communication while eliminating dependence on centralized authorities. The immutable nature of blockchain ensures that every validated transaction is permanently recorded, making unauthorized modification of stored information highly difficult [1], [6].

The framework also improves device authentication by assigning a unique digital identity to every registered IoT device. Before any communication takes place, blockchain validator nodes verify the identity and digital signature of the transmitting device. This decentralized authentication mechanism prevents unauthorized devices from participating in the network and minimizes the risk of identity spoofing and unauthorized access. In addition, cryptographic hashing preserves the integrity of transmitted information, enabling rapid detection of any alteration during communication [3], [5].

The proposed layered architecture demonstrates improved transparency and traceability compared with conventional IoT security systems. Since identical copies of the blockchain ledger are maintained across multiple participating nodes, every communication event can be monitored and audited efficiently. This feature is particularly beneficial for applications such as healthcare, industrial automation, and smart cities, where maintaining reliable records is essential for accountability and regulatory compliance. Furthermore, the decentralized architecture improves fault tolerance by eliminating the single point of failure commonly associated with centralized security models [6], [11].

Although blockchain introduces additional computational and storage overhead, the security benefits provided by decentralized authentication, immutable transaction records, and distributed trust outweigh these limitations in many IoT applications. The use of lightweight blockchain implementations can further reduce processing delays and energy consumption, making the proposed framework suitable for practical deployment in resource-constrained IoT environments [5], [14].

Table 1. Comparison of Conventional IoT Security and Proposed Blockchain-Based Framework

Parameter	**Conventional IoT Security**	**Proposed Blockchain Framework**
Authentication	Centralized	Decentralized
Data Integrity	Moderate	High
Access Control	Server-Based	Blockchain-Based
Trust Management	Centralized	Distributed
Data Tampering Resistance	Moderate	Very High
Transparency	Limited	High
Auditability	Partial	Complete
Fault Tolerance	Low	High
Scalability	Moderate	High
Single Point of Failure	Present	Eliminated

Table 2. Security Threats and Corresponding Protection Mechanisms

Security Threat	**Protection Mechanism**
Device Spoofing	Blockchain-Based Authentication

Replay Attack	Timestamp Verification
Data Tampering	SHA-256 Hash Verification
Unauthorized Access	Public-Key Cryptography
Identity Theft	Digital Signature Verification
Insider Attack	Immutable Blockchain Ledger
DDoS Attack	Decentralized Network Architecture
Data Modification	Distributed Transaction Validation

Discussion

The comparative analysis demonstrates that the proposed Blockchain-Based IoT Security Framework provides superior security compared with traditional IoT architectures. The decentralized authentication process enhances trust among connected devices, while immutable ledger storage improves data integrity and transparency. Blockchain-based access control effectively restricts unauthorized participation, reducing the likelihood of malicious attacks. Although additional computational resources are required for transaction validation and ledger maintenance, the resulting improvements in security, accountability, and fault tolerance justify the adoption of blockchain technology in modern IoT systems. Consequently, the proposed framework represents a reliable and scalable solution for securing next-generation IoT applications [5], [6], [14].

Conclusion

The rapid growth of the Internet of Things (IoT) has created new opportunities for intelligent automation and real-time connectivity across various application domains. However, the increasing number of interconnected devices has also introduced significant security challenges related to authentication, data integrity, privacy, and access control. Conventional centralized security mechanisms are often inadequate for large-scale IoT environments because they are vulnerable to single-point failures, unauthorized access, and data manipulation. These limitations highlight the need for a decentralized security framework capable of providing reliable protection for distributed IoT networks [3], [10].

This paper proposed a **Blockchain-Based IoT Security Framework** that integrates blockchain technology with IoT devices to establish a secure and decentralized communication environment. The proposed framework employs a layered architecture consisting of the Device Layer, Network Layer, Blockchain Layer, and Application Layer. By incorporating cryptographic hashing, digital signatures, decentralized authentication, and distributed ledger technology, the framework ensures secure communication, transparent transaction verification, and tamper-resistant data storage. The use of blockchain eliminates dependence on centralized authorities while improving trust, accountability, and fault tolerance among participating IoT devices [1], [5], [6].

The qualitative security analysis demonstrated that the proposed framework effectively mitigates common IoT security threats, including unauthorized access, device spoofing, replay attacks, identity theft, and data tampering. Compared with conventional IoT security architectures, the blockchain-enabled framework provides enhanced data integrity, decentralized trust management, improved transparency, and secure access control. Although blockchain introduces additional computational, communication, and storage overhead, these limitations can be reduced through lightweight blockchain architectures and optimized consensus mechanisms suitable for resource-constrained IoT devices [5], [14].

Overall, the proposed Blockchain-Based IoT Security Framework provides a reliable foundation for securing next-generation IoT ecosystems. Its decentralized architecture enhances confidentiality, integrity, availability, and accountability while supporting secure information sharing across heterogeneous IoT environments. The framework is applicable to smart healthcare, industrial automation, intelligent transportation, agriculture, environmental monitoring, and smart city infrastructures where secure and trustworthy communication is essential.

References

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.

[2] D. Evans, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything," Cisco Internet Business Solutions Group (IBSG), White Paper, Apr. 2011.

[3] R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," *arXiv preprint arXiv:1608.05187*, 2016.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[7] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," *IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, 2016.

[8] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, Early research available before 2018 (conceptual work).

[9] E. Borgia, "The Internet of Things Vision: Key Features, Applications and Open Issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.

[10] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[11] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[12] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, no. 2, pp. 6–19, 2016.

[13] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration with IoT: Challenges and Opportunities," Technical Report, University of Murcia, 2017.

[14] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IT Professional*, vol. 19, no. 4, pp. 68–72, Jul.–Aug. 2017.

[15] H. Ning and H. Liu, "Cyber-Physical-Social Based Security Architecture for Future Internet of Things," *Advances in Internet of Things*, vol. 2, no. 1, pp. 1–7, 2012.