JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 26 Issue 04, 2023 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

ENHANCING SECURITY IN IOT DATA TRANSMISSION WITH AN INNOVATIVE BLOCK-CHAIN APPROACH

Monika
Research Scholar, CSE Deptt. BMU, Haryana, India

Dr.Brij Mohan
Professor, CSE Dept. BMU, Haryana, India

Dr.Vinit Kumar
Assistant Professor, CSE Dept. VCE, Rohtak, Haryana, India

Abstract- The increasing adoption of Internet of Things (IoT) devices has raised concerns about their security and privacy. Traditional security mechanisms are often inadequate for the diverse and expansive IoT ecosystem, leading to vulnerabilities and potential threats. To address these challenges, researchers and practitioners have proposed various approaches and frameworks. In this paper, we analyze and evaluate these existing methodologies, considering their strengths, limitations, and key considerations for designing secure IoT environments. Based on the insights gained from the literature review, we propose a novel model for securing IoT environments using blockchain technology. Through extensive experimentation and analysis, we demonstrate the effectiveness and efficiency of our proposed model in mitigating common security threats in IoT environments. Our model offers scalability and interoperability, allowing seamless integration with existing IoT infrastructures. This research paper contributes to the ongoing efforts in securing IoT systems by providing a comprehensive review of existing approaches and presenting a novel blockchain-based model that enhances security and enables the widespread adoption of trustworthy IoT deployments in various domains.

Keywords: Blockchain, IoT Security, deep blockchain-based trustworthy privacy-preserving secured structure, blockchain-based federated learning

1. Introduction

The introduction of IoT-based technology has ushered in a new era of possibilities across various domains, including intelligent transport, smart homes, smart cities, and healthcare. The convergence of embedded device hardware and network technology has led to the emergence of large-scale, autonomous IoT systems. These systems generate and exchange vast quantities of crucial data, making network security a pressing concern, particularly in wireless sensor networks deployed in unattended locations.

Although many current IoT solutions rely on cloud services over the Internet, providing elastic computing and data storage capabilities, they still face significant security challenges. One major drawback is the single point of vulnerability introduced by the expansive and

Submitted: 22/11/2023 **Accepted**: 30/12/2023

interconnected nature of IoT architectures, compromising the availability of IoT systems and making them susceptible to malicious attacks such as data tampering and privacy breaches.

To address these security concerns, we propose a solution that leverages blockchain technology to protect IoT data. Blockchain technology, originally developed for cryptocurrency applications, offers inherent security features such as decentralization, immutability, and cryptographic algorithms. By integrating blockchain into IoT data transmission, we aim to establish a secure and trusted framework that safeguards the integrity and confidentiality of IoT data.

This research paper focuses on the design, implementation, and evaluation of our proposed blockchain-based solution for IoT data protection. Through a comprehensive review of the existing literature, we explore the current state of IoT security and the challenges associated with data transmission over the Internet. Building upon this foundation, our solution seeks to mitigate these challenges by leveraging the unique properties of blockchain technology.

Blockchain technology comprises several key components that form the foundation of its decentralized and secure nature. Below is an overview of the essential components of blockchain.

- Distributed Ledger: The distributed ledger is a decentralized database that records and stores all transactions across multiple nodes in the network. It serves as the backbone of the blockchain, ensuring transparency, immutability, and data consistency. Each transaction is grouped into blocks and added to the chain in a sequential manner.
- Consensus Mechanism: Consensus mechanisms are algorithms used to achieve agreement among network participants on the validity of transactions and the state of the blockchain. They ensure that all nodes in the network reach a consensus on the order and integrity of the transactions. Common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS).
- Cryptographic Hash Functions: Cryptographic hash functions are essential cryptographic algorithms used to secure data within the blockchain. They generate a unique fixed-size hash value for each input, ensuring the integrity of the data stored in the blocks. Any alteration to the data results in a different hash value, alerting the network to potential tampering.
- Public-Key Cryptography: Public-key cryptography, also known as asymmetric cryptography, is a cryptographic system that uses a pair of cryptographic keys (public and private keys) to encrypt and decrypt data. The public key is shared with others, while the private key is kept confidential. It enables secure authentication, digital signatures, and encryption of data within the blockchain.
- Smart Contracts: Smart contracts are self-executing contracts with the terms and conditions directly written into code within the blockchain. They automatically execute predefined actions when specific conditions are met. Smart contracts enable the automation of transactions, agreements, and processes, eliminating the need for intermediaries and enhancing efficiency and transparency.

- Peer-to-Peer Network: Blockchain utilizes a peer-to-peer (P2P) network architecture, where participating nodes communicate directly with each other. This decentralized network structure eliminates the need for a central authority and reduces the risk of a single point of failure. P2P networking ensures the distributed nature of the blockchain and enhances its resilience and fault tolerance.
- Mining: Mining is the process by which new transactions are validated, and new blocks are added to the blockchain. Miners, equipped with computational power, solve complex mathematical puzzles to validate transactions and compete to be the first to add a new block. Mining ensures the security, integrity, and decentralization of the blockchain network.

These components work in harmony to create a secure, transparent, and decentralized system within the blockchain. They collectively contribute to the trustworthiness, immutability, and resilience of the data stored and transmitted across the network. Understanding these components is crucial for comprehending the underlying principles and advantages of blockchain technology.

Blockchain or distributed ledger technology is presently among the most optimistic technological revolutions with huge potential for a variety of applications that can transparently respond to a number of issues for Internet security. The amount of security that blockchain technology offers has recently increased its use. Data manipulation is much more difficult with blockchain becauseit uses distributed databases. Initially bitcoin was introduced as a legal currency for transaction in electronic form and the technology running behind bitcoin was blockchain. In blockchain data is stored in a distributed ledger. Participants in the blockchain network may create, read, and verify transactions that are stored in a distributed ledger because of the integrity and availability provided by the blockchain technology. Moreover blockchain do not allow modifying or deleting the data stored in ledger. Cryptographic protocols and primitives, such as digital signatures and hash functions, are used to maintain and safeguard the blockchain system. Theblockchain technology also requires a consensus mechanism, which is simply a set of rules to be followed by every member, in order to produce a globally united perspective because it operates as a dispersed network and must enable all participants to agree on a single record.

Constructing a blockchain involves several crucial steps. First, the architecture must be designed, determining the type of blockchain, consensus mechanism, and block structure. Next, network nodes are established, each maintaining a copy of the distributed ledger. The chosen consensus mechanism is then implemented to enable decentralized decision-making among nodes. Transactions are validated and grouped into blocks, with references to previous blocks. Cryptographic security measures, such as encryption techniques, are implemented to ensure data integrity and confidentiality. Finally, the network is deployed, the initial genesis block is created, and blockchain operations commence. By following these steps, a secure and decentralized blockchain network can be constructed, capable of supporting various applications and fostering trust in data and transactions.

A. IoT Architecture

The architecture of the IoT plays a crucial role in enabling the seamless integration of devices, sensors, and systems to facilitate efficient data transmission and communication. This section provides an overview of the typical components and layers of IoT architecture.

Perception Layer: The perception layer consists of physical devices and sensors that collect data from the surrounding environment. These devices include sensors, actuators, RFID tags, and wearable devices. They gather real-time information such as temperature, humidity, location, and various other parameters.

Network Layer: The network layer facilitates the communication between the IoT devices and the IoT platform. It includes wired and wireless communication protocols, such as Wi-Fi, Bluetooth, Zigbee, and cellular networks. This layer ensures reliable and secure data transmission between devices and networks.

IoT Platform: The IoT platform serves as the middleware that connects and manages the communication between the perception layer and the application layer. It provides essential functionalities such as data storage, device management, security, and data analytics. The platform acts as a bridge between the physical devices and the higher-level applications.

Application Layer: The application layer encompasses the end-user applications and services built on top of the IoT platform. These applications utilize the collected data to provide various functionalities and services, such as smart home automation, industrial monitoring, healthcare applications, and environmental monitoring.

Cloud Computing: Cloud computing plays a vital role in IoT architecture by providing scalable storage and computational resources. It enables the processing and analysis of vast amounts of IoT data, facilitating real-time decision-making and advanced analytics. Cloud services also offer data storage, backup, and access control for IoT applications.

Edge Computing: Edge computing brings computational capabilities closer to the IoT devices themselves. By processing data locally at the edge of the network, edge computing reduces latency, conserves network bandwidth, and enables real-time data analysis. It enhances the responsiveness and efficiency of IoT systems, particularly in time-sensitive applications.

Security and Privacy: Security and privacy are critical considerations in IoT architecture. Measures such as access control, encryption, authentication, and data anonymization are implemented at various layers to ensure the confidentiality, integrity, and availability of IoT data. Security mechanisms protect against unauthorized access, data breaches, and malicious attacks.

B. IoT Attacks

This section highlights some of the common types of attacks that target IoT devices and networks, posing significant security challenges.

Denial-of-Service (DoS): In this attacks, threat actors flood IoT devices or networks with a massive volume of requests, overwhelming their resources and causing service disruption. These attacks can render critical IoT systems, such as healthcare monitoring or industrial control systems, inoperable, leading to severe consequences.

Botnets: These are networks of compromised IoT devices controlled by malicious actors. These botnets can be used to launch various attacks, including DDoS attacks, spreading malware, and conducting coordinated cyber-attacks. Botnet-based attacks exploit vulnerabilities in IoT devices with weak security measures, using them as entry points into larger networks.

Device Exploitation: IoT devices often have inherent security vulnerabilities, including weak authentication mechanisms, outdated software, and insecure communication protocols. Attackers exploit these weaknesses to gain unauthorized access, take control of devices, or intercept and manipulate IoT data.

Data Breaches and Unauthorized Access: IoT devices collect and transmit sensitive data, making them targets for data breaches. Attackers may intercept or manipulate data during transmission, gain unauthorized access to devices or networks, or exploit vulnerabilities in cloud or edge servers where IoT data is stored.

Physical Attacks: Physical attacks involve tampering with or manipulating IoT devices physically. This includes unauthorized access to device hardware, theft, tampering with sensors, or compromising the integrity of the device's firmware. Physical attacks can lead to unauthorized control, data manipulation, or even the extraction of sensitive information.

Man-in-the-Middle (MitM): In MitM attacks, attackers intercept and manipulate the communication between IoT devices, compromising the confidentiality and integrity of data. Attackers can eavesdrop on communications, inject malicious code, or alter data packets, leading to unauthorized actions or unauthorized access to sensitive information.

Firmware and Software Exploitation: IoT devices rely on firmware and software for their operation. Attackers can exploit vulnerabilities in device firmware or software to gain unauthorized control, inject malicious code, or execute arbitrary commands, potentially compromising the entire IoT ecosystem.

Social Engineering: Social engineering attacks target human users in the IoT ecosystem, exploiting their trust, lack of security awareness, or gullibility. Attackers may deceive users into providing sensitive information, sharing login credentials, or unknowingly installing malicious applications or firmware updates.

It is crucial for IoT stakeholders to be aware of these attack vectors and implement robust security measures to safeguard IoT devices and networks. This includes regular patching and updating of device firmware, implementing strong authentication mechanisms, encrypting data transmission, and employing intrusion detection and prevention systems to detect and mitigate attacks in real-time.

2. Related Works

The Saba et al. [1] aimed to address the cybersecurity challenges in IoT networks by developing an AI-based model for intrusion detection. To achieve this, they utilized seven datasets from the TON-IoT telemetry dataset, namely Thermostat, GPS Tracker, Garage Door, and Modbus datasets. These datasets were representative of IoT network traffic and provided valuable dinsights into potential intrusions. The proposed model observed the traffic across the IoT-based system and utilized embedded artificial intelligence techniques to forecast possible intrusions. By leveraging machine-learning algorithms, including several machine-learning classifiers and a deep learning model, the authors aimed to generate accurate outputs from the complex and extensive dataset. The authors trained and tested their proposed intrusion detection system using the seven datasets mentioned earlier. Through the implementation of a voting classifier, the model achieved an impressive accuracy rate of 99.7%. This demonstrated the effectiveness of the AI-based approach in detecting anomalies and potential intrusions within IoT networks.

Jeong et al. [2] focuses on improving the security and reliability of personal medical information in the context of intelligent self-diagnosis and healthcare. The authors propose the use of blockchain technology to enhance the management of personal information. They develop a monitoring system that analyzes individual biometric data, incorporating blockchain and Internet of Things (IoT) technologies. The system successfully detects abnormal movements and analyzes biosignals such as blood pressure and heart rate. Through experiments, the authors demonstrate the effectiveness of the system, achieving a high classification accuracy of 97.2%. They emphasize the importance of continued advancements, including the integration of ultrasmall biometric sensors, patient positioning functions, and the development of predictive algorithms for fall accidents. Overall, the paper highlights the application of blockchain technology in improving reliability, confidentiality, and real-time monitoring of personal medical information.

Joshi et al. [3] presents an AI-based model for intrusion detection in IoT networks using seven datasets of TON-IoT telemetry datasets. The model utilizes embedded artificial intelligence to observe traffic across the IoT-based system and predict possible intrusions. It achieves a high accuracy of 99.7% using a voting classifier on the tested datasets. The authors emphasize the need for secure and significant monitoring of IoT networks in various applications, including smart cities. They propose the integration of blockchain technology to enhance reliability and confidentiality in managing personal medical information. The accumulation and real-time monitoring of this information are achieved using IoT sensors and a smartphone interface. To improve the effectiveness of intrusion detection systems for IoT networks, the authors employ machine learning algorithms and evaluate their performance using the TON-IoT dataset. The SVM algorithm demonstrates an average error rate of 2% in analyzing biosignals, while the system achieves an overall classification accuracy of 97.2%. They also discuss potential future enhancements, such as incorporating ultrasmall biometric sensors and developing algorithms for predictive analysis.

Alabdali et al. [4] introduces a novel design for a smart refrigerator system that integrates IoT technology, smart mobile device applications, machine learning, and blockchain technology. The proposed system aims to achieve automatic self-checking and self-purchasing capabilities, providing users with real-time updates on the refrigerator's contents and enabling efficient purchasing decisions. The authors implement the system using the Blynk platform and leverage artificial intelligence to automate decision-making processes. They utilize machine learning classifiers to make automatic decisions regarding repurchasing products and consider various features for enhanced performance. The integration of blockchain technology ensures data security and privacy. The experiments conducted evaluate the proposed system using information retrieval metrics and visualization tools. The results demonstrate the system's ability to save effort, time, and money, offering users an easier, faster, and healthier lifestyle.

In this study, Subhi et al. [5] developed a new architecture that combines edge computing, AI, IoT devices, and blockchain. The system was tested using the COVID-19 pandemic as a use case, demonstrating its ability to monitor and predict the spread of the virus with 95% accuracy. The architecture ensures data integrity, provides continuous AI prediction, and enables secure sharing of outcomes on a blockchain platform. It is robust, low-cost, and has minimal impact on device power consumption. The proposed architecture outperforms related studies in terms of AI data integrity and accuracy. The authors highlight the flexibility of tuning blockchain solutions for specific applications. Overall, the study presents a secure and efficient system for AI-enabled IoT applications at the edge.

Ayub et al. [6] conducted a study on the integration of blockchain technology with the Industrial Internet of Things (IIoT) and identified the challenges related to information preservation, communication, trust, and security in the industrial domain. They proposed a blockchain hyperledger sawtooth-enabled framework that ensures secure execution and communication in industrial activities. The framework utilizes on-chain and off-chain communication channels to manage transactions and incorporates pseudo-chain codes and consensus protocols to address resource adaptation. The authors concluded that their framework provides a promising solution for industrial applications, enhancing provenance, integrity, transparency, and reliability. They also discussed the future deployment of the framework in industrial environments, such as manufacturing and production.

Sagu et al. [7] proposed a hybrid model for detecting attacks in IoT environments. The model consists of three stages: feature extraction using higher-order statistical features and information theory-based features, attack detection using Gated Recurrent Unit (GRU) and Bidirectional Long Short-Term Memory (Bi-LSTM) models, and optimization of Bi-LSTM weights using a self-upgraded Cat and Mouse Optimizer (SU-CMO). The performance of the proposed model was evaluated using two datasets, and it outperformed traditional and state-of-the-art techniques in terms of classification accuracy, f-measure, and Matthews Correlation Coefficient (MCC). The conclusion highlights the superior accuracy achieved by the proposed hybrid model and suggests further improvements by combining it with different deep learning models. Future work includes addressing multiclassification of attacks and exploring diverse deep learning approaches.

Amit et al. [8] introduced two metaheuristic optimization algorithms, SAEHO and SU-CMO, for training deep learning (DL) models to detect security threats in IoT environments. They designed and tuned two hybrid DL classifiers, CNN + DBN and Bi-LSTM + GRU, using these optimization algorithms, which resulted in improved model accuracy. The performance of the proposed approach was evaluated using two datasets, and it outperformed both conventional and state-of-the-art methods in terms of accuracy, rand index, f-measure, and MCC. The conclusion emphasized the importance of optimization in training machine learning models and presented the SAEHO and SU-CMO algorithms as effective options. The proposed frameworks demonstrated better results compared to existing approaches and showed potential for enhancing the accuracy of various DL models. However, the authors acknowledged that there is no guarantee of finding the optimal solution and suggested future work to evaluate the optimization algorithms in terms of time complexity and search space.

In their paper, [9] Kim et al. focused on developing a privacy-preserving distributed machine learning (DML) model on a permissioned blockchain. They addressed the privacy, security, and performance issues in existing DML models by proposing a new model based on the Hyperledger Fabric architecture. Their model utilized a differentially private stochastic gradient descent method and an error-based aggregation rule to ensure privacy preservation and prevent attacks on the accuracy of DML models. Experimental results demonstrated that their model outperformed majority-based aggregation rules, particularly in a differentially private scenario, providing stronger resilience against adversarial attacks. The model also exhibited lower time complexity and offered time savings compared to permissionless blockchain-based DML systems, highlighting its usability and advantages.

Biswas et al. [10] proposed a security framework that integrates blockchain technology with smart devices to ensure secure data communication in a smart city. They recognized the potential benefits of smart cities in terms of improved services and resource utilization but highlighted the challenges related to information security and privacy. To address these challenges, they proposed leveraging blockchain technology, which offers resilience against various threats and provides unique features such as reliability, fault tolerance, efficiency, and scalability. The integration of blockchain with smart devices would create a secure and distributed communication platform for all devices in a smart city. The authors concluded by mentioning future work focusing on designing a system-level model to investigate interoperability and scalability among different platforms used in smart cities.

Jung et al. [11] aimed to enhance the session key-based security scheme in the existing LTE mobile system by proposing a packet key-based security management scheme on the blockchain control plane. They addressed the limitations of both the vertical model and the SDN-based horizontal model in achieving end-to-end security management. The proposed blockchain-based security management (BSM) scheme allowed peers to easily obtain the necessary parameters for managing the packet key-based security system. The BSM scheme featured a renewal process that enabled different packet data streams to use distinct security parameters, ensuring robust security against active attacks. The authors compared the BSM scheme with the existing vertical model, highlighting its advantageous effects on latency, achieving around 200% better performance. The BSM scheme leveraged blockchain technology to enhance security, facilitate parameter exchange, and provide secure end-to-end data transfer in the context of packet key-based security systems.

Table 1 below summarize the literature review.

Authors	Objective	Methodology	Key Findings

Saba et al. [1]	Develop an AI-based model for intrusion detection in IoT networks	Utilized seven datasets from TON-IoT telemetry dataset, employed machine learning classifiers and deep learning model	Achieved 99.7% accuracy in detecting anomalies and potential intrusions in IoT networks
Jeong et al. [2]	Enhance security and reliability of personal medical information using blockchain technology	Developed a monitoring system integrating blockchain and IoT technologies, analyzed biometric data	Achieved 97.2% classification accuracy in detecting abnormal movements and biosignals
Joshi et al. [3]	Develop an AI-based intrusion detection model and explore the integration of blockchain technology in managing personal medical information	Utilized seven datasets from TON-IoT telemetry dataset, employed machine learning algorithms	SVM algorithm achieved 2% average error rate in analyzing biosignals, overall classification accuracy of 97.2%
Alabdali et al. [4]	Design a smart refrigerator system integrating IoT, machine learning, and blockchain technology	Implemented the system using the Blynk platform, utilized machine learning classifiers	Demonstrated the system's ability to save effort, time, and money in managing refrigerator contents
Subhi et al. [5]	Develop an architecture combining edge computing, AI, IoT devices, and blockchain for monitoring and predicting the spread of COVID-19	Tested the system using COVID-19 as a use case, employed blockchain for data integrity and secure sharing	Achieved 95% accuracy in monitoring and predicting the virus spread
Ayub et al. [6]	Investigate the integration of blockchain technology with IIoT for addressing information preservation, communication, trust, and security challenges	Proposed a blockchain-enabled framework for secure execution and communication in industrial activities	Demonstrated enhanced provenance, integrity, transparency, and reliability in industrial applications
Sagu et al. [7]	Propose a hybrid model for detecting attacks in IoT environments using GRU, Bi-LSTM, and SU-CMO	Conducted feature extraction, attack detection using GRU and Bi-LSTM, optimized Bi-LSTM weights using SU-CMO	Outperformed traditional and state-of-the-art techniques in terms of classification accuracy, f-measure, and MCC

Mingxin Ma et al. [8]	Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario	Designed Hierarchical access control for blockchain based cloud is discussed	Achieved improved accuracy compared to conventional and state-of-the-art methods
Kim et al.[9]	Develop a privacy-preserving distributed Ledger (DL) model on a permissioned blockchain	Proposed a new DL model based on the Hyperledger Fabric architecture. Utilized a differentially private stochastic gradient descent method and an error-based aggregation rule.	Outperformed majority-based aggregation rules, especially in a differentially private scenario. Provided stronger resilience against adversarial attacks. Lower time complexity and transaction latency.
Biswas et al. [10]	To overcome issues like those mentioned above, we propose a unique deep blockchain-based trustworthy privacy-preserving secured structure (DBTPPS).	Leverage blockchain technology to ensure information security and privacy in a smart city.	Highlighted the benefits of blockchain technology in terms of resilience, reliability, fault tolerance, efficiency, and scalability. Future work includes investigating interoperability and scalability among different platforms.
Jung et al. [11]	Enhance the session key-based security scheme in the existing LTE mobile system by proposing a packet key-based security management scheme on the blockchain control plane	Proposed a blockchain-based federated Learning (BFL) scheme. Enable easy acquisition of necessary parameters for managing the packet key-based security system.	Achieved robust security against active attacks. Compared to the existing vertical model, demonstrated advantageous effects on latency, around 200% better performance. Leveraged blockchain technology for secure end-to-end data transfer.

3. Proposed Methodology

A public and auditable record of all consumer-to-consumer transactions is maintained via blockchain technology. When any form of commerce is controlled by the consciousness of a significant number of customers who are participating in something within the system, distributed existence becomes a real possibility. The design of the Internet of Things blockchain ecosystem was developed in response to concerns about data security. This body of research tackles the central questions and optimal states that pertain to blockchain development. The Stuff Server Website calls for the creation of a new blockchain user account, complete with information about the community and data about the answers. The web address of the community application is saved in the storage database by the The equipment internet server, which also provides the address to the application. While the model sensor is operating, it is gathering the code and loading it onto the webserver through the use of a file protocol. On the blockchain, by selecting the location at which the data should be saved or thelocation at which a block should be constructed, and then checking that they are a component of the blockchain location on the dataset. The transaction necessitates the generation of a block in order to store the dataset information that is obtained from the sensor. The information that has been gathered from the sensor will then be relayed, and if it has not been recorded on the blockchain server before the block is formed, it will be done so at that time. The user goes to the Internet of Things Directory as a member id as soon as an implementation block is formed. This allows the user to accept the details included in the block via the blockchain knowledge, which, if linked to the database, will be exhibited on the user application. It is not possible to alter it.

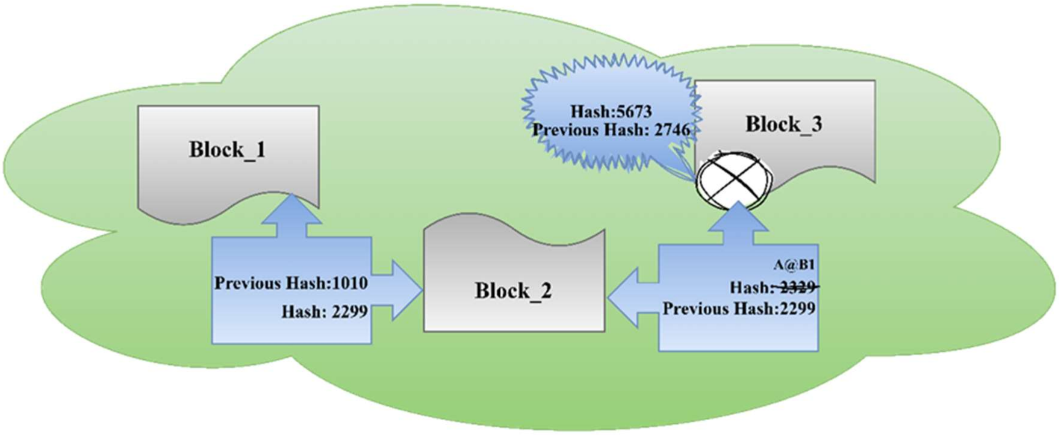


Figure 1. Block Chain Design

The data will not be deleted, but they will be eliminated by altering the status of the repository. The data will not be deleted. Because the functions are separated, there will not be a single point of failure because this will guarantee that all of the duties will be completed. Users are going to generate the trustworthy root of the data so that they are aware of where the data may be found. The proposed approach was implemented in terms of both the application server and the database server. Due to the fact that everyone still has access to the data despite the data protection measures that have been put into place, no one will view any of the data that has been protected here. The confidentiality of the data and its protection are both preserved. Since we have previously decided how to display and save data, there won't be a shortage of shared practices to address any issues that may arise. hybrid system based on the cloud A blockchain that ensures the confidentiality of Internet of Things data. It makes use of a private cloud to store information related to the Internet of Things (IoT), and it employs a blockchain overlay to keep track of all data transfers and events related to IoT interactions. It provided a trustworthy environment for sharing resources between clouds, as well as a blockchain to record all of the transactions, and it had the potential to address problems with data fusion and data security.

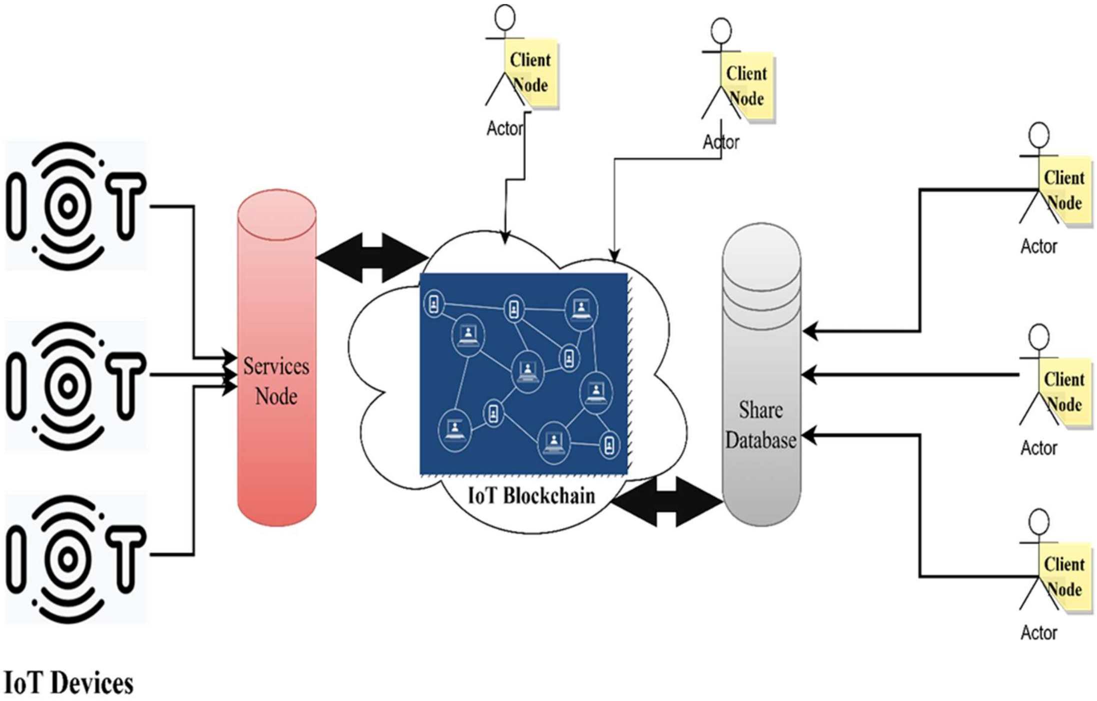


Figure 2. Proposed Algorithm

These are mathematical functions that give a description, much like an identifier of the data. On a single dataset, a unique output is able to be generated, despite the fact that the likelihood of the event is extremely remote. The use of hash in the verification of the integrity of data is one of the most widespread uses of hash. It is vital to always have the same value regardless of the size of the data that is being hashed, while the hash output size can vary based on the technique that is being utilised. There are various different hash algorithm explanations provided by the SHA-256 algorithm. The following are some of the specialised characteristics that hash algorithms should have:

Deterministic: Hash functions should be deterministic, meaning that for any given input, they should always yield the same output. The cryptographic operations are guaranteed to be consistent and reliable because to this characteristic.

Collision Resistance is achieved by designing the hash function in such a way that it is computationally impossible to find two separate inputs that result in the same output.

This assures that the output hash value will be radically different if there is even the slightest change in the data that was supplied.

The Algorithm of Consensus Efficiency: governs how efficiently transactions are verified and submitted to the block-chain through measuring how effective of the consensus algorithm used in the block-chain network. This algorithm governs how transactions are loaded to the block-chain.

Preimage Resistance: Given a hash value, it should be computationally impossible to retrieve the initial input that was used to generate that hash value. This is what is meant by "preimage resistance." Because of this characteristic, it is impossible to reconstruct the original data using only the hash value as a starting point.

Avalanche Effect: A relatively minor alteration to the input ought to create a substantially greater shift in the hash value that is produced. This characteristic assures that even a slight change in the input will result in an entirely different hash output. This is the case even if the input is just slightly modified.

Protection: The hash method should be immune to a wide variety of cryptographic attacks, including collision attacks, preimage attacks, and birthday assaults. The integrity of the data and durability against attacks on the algorithm should both be preserved by this solution.

If you have the hash values and want to figure out what the input was, it must be a really difficult task.

Compression: In an ideal world, the scale of a hash would only reflect a very small portion of the whole data.

Diffusion: In order to prevent the method from being reverse-engineered, the hash output can be changed from some bits to around 60 percent if just one bit of the input is changed.

Proposed Algorithm

Input	Plain Text Data Sets
Process	Generate the hashing algorithm function funH=Shuffle(Plain Text)*mutation(Plain Text)
	Find the hash data H_Data=funH(Plain Text)
	i. Arrange the hash function according to each block B_1={Hash(0),other parameter, data} B_2={Hash(1),other parameter, data} : : B_n={Hash(n),other parameter, data} ii. Compute the raw data through hash function Secure_Data=Advanced_sha(sha256hash=SHA256.create(B1…Bn))
Output	Return generated the secure string

4. Result and Discussion

This section explains the findings and elaborates on the advanced methods used to measure performance.

The necessary setup for running the simulation is window 10,OS, Intel(R) Core (TM)-i5 CPU @ 2.21GHz-4.4GHz , 8.00GB RAM, 1TB ROM , 512GB SSD and Matlab 2018.

The blockchain is a distributed ledger in which data is stored in chronological order, with each block representing a completed transaction. Each block's header undergoes a cryptographic hash using SHA256 to provide a hash value.Sensor data sets are collected and require a transactional block to be created.

Key Generation outcome

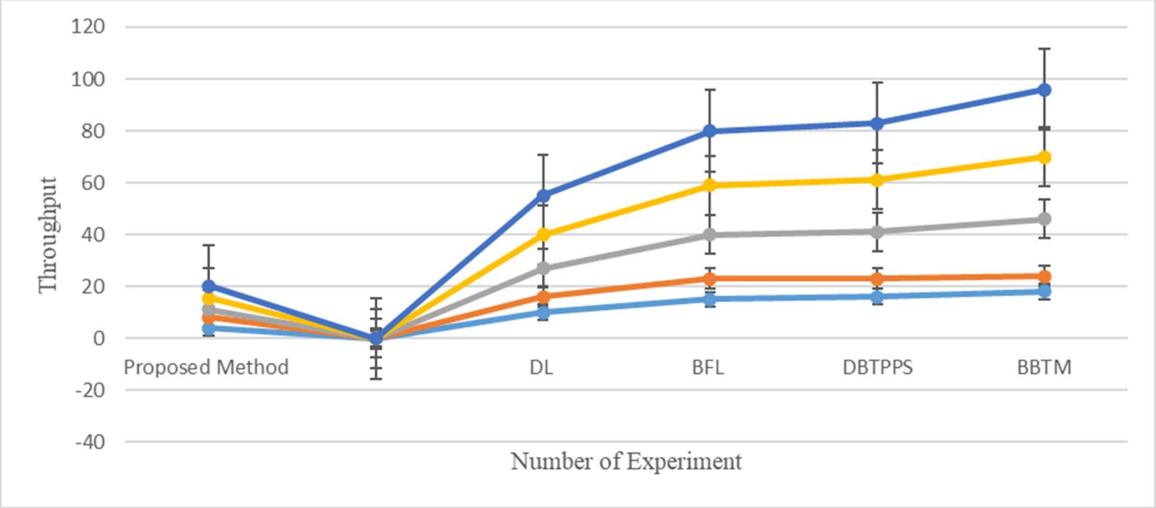
```
{Private key: “2d83caf8381226e5da9141ee9f39a316772affc2”}
{Public key: “40fd87b9fb54d950c1df0b9791282496”}
{Address:
“f37d0015c842fccddbc815a590dce7108f468fef”}
```

Outcome of crossponding raw data generated in each block with other parameter like index, time stamp, nonce, number of bits, merkle root tree head, block verision as :

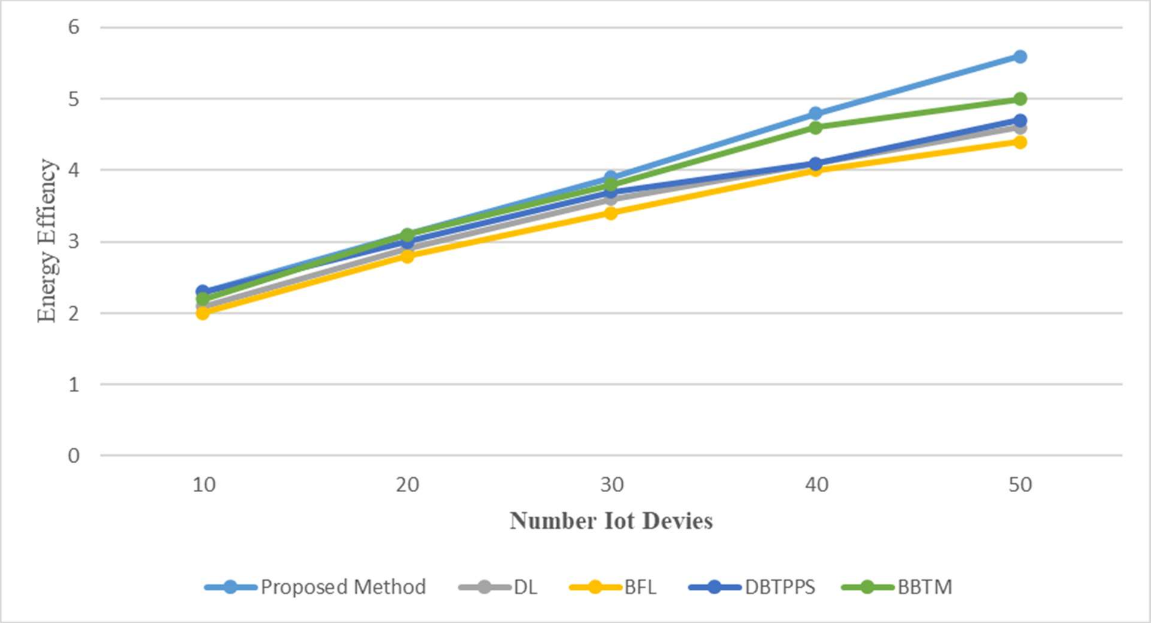
```
{Block:
Block chain Version: Blockchain 3.0: Decentralized Enterprise Level Applications
Index: 0000 1111
Time Stamp: 00:01:01:10
Data:   “my name is monika”
Hash: 343a50ea61e0695cb9c837dcffcab45477eefced
Previous Hash: 349c3a68780f0a47eb6110400a9951f55afe4b04
}
{Block:
Hash: 528e4a9dbf9065ff0c5338dc4bb3fcc769442266
Previous Hash: 343a50ea61e0695cb9c837dcffcab45477eefced
}
{Block:
Hash: edc10afa589816eee3bd35b59b5ce63c5cc809ff
Previous Hash: 528e4a9dbf9065ff0c5338dc4bb3fcc769442266
}
```

The process of calculating a block’s hash is similar to bitcoin’s. the has before this block only includes 4 zeros because our difficulty is set rather low. We just threw it into the array of transaction hashes to keep things simple. Matlab is used to simulate a blockchain platform with a large number of complex transactions, with a block size of 4 bytes and some code acess through python.

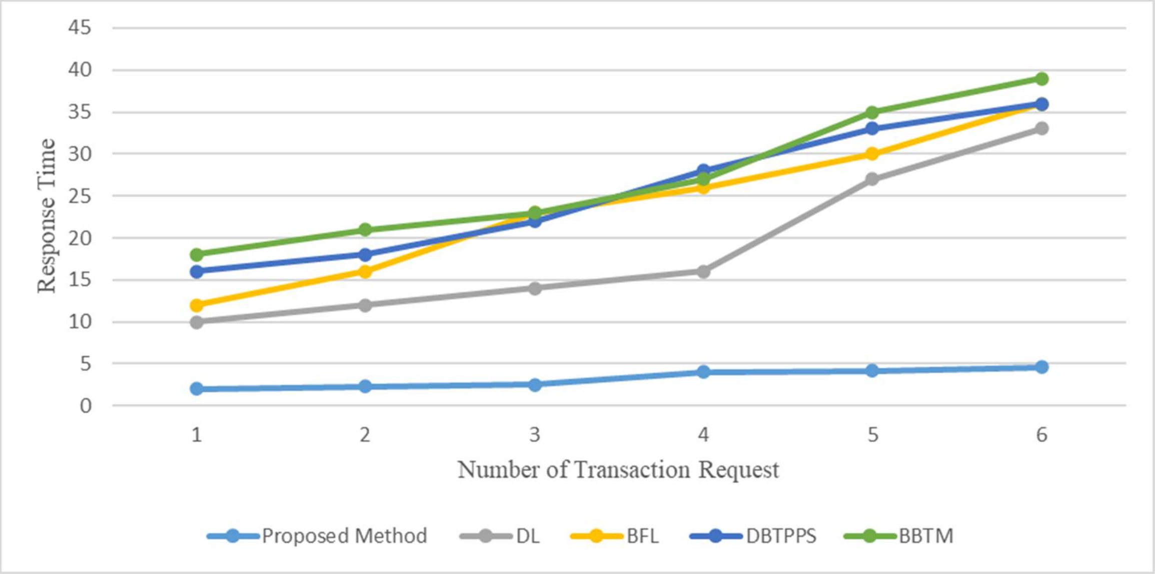
Each block header undergoes a cryptographic hash using SHA256 to generate a hash value. The process of calculating the hash of a block is similar to that of Bitcoin. The hash before this block only includes 4 zeros because our difficulty is set rather low. This makes it simpler for miners to grasp the basic concept and may be generated in a matter of seconds. Additionally, the tx field in Bitcoin encodes the hash of the transaction's root node in the Merkle tree. We just threw it into the array of transaction hashes to keep things simple. Bitcoin's algorithm relies on the string representation of the number +Nouce in the block header, which is hashed using the Secure Hash Algorithm 56 (SHA56). The header information is simplified by the use of a "simple blockchain," but the underlying process and Bitcoin remain unchanged. The blockchain data is kept in a local file.


120
100
80
60
40
20
0
-20
-40
Throughput
Proposed Method
DL
BFL
DBTPPS
BBTM
Number of Experiment

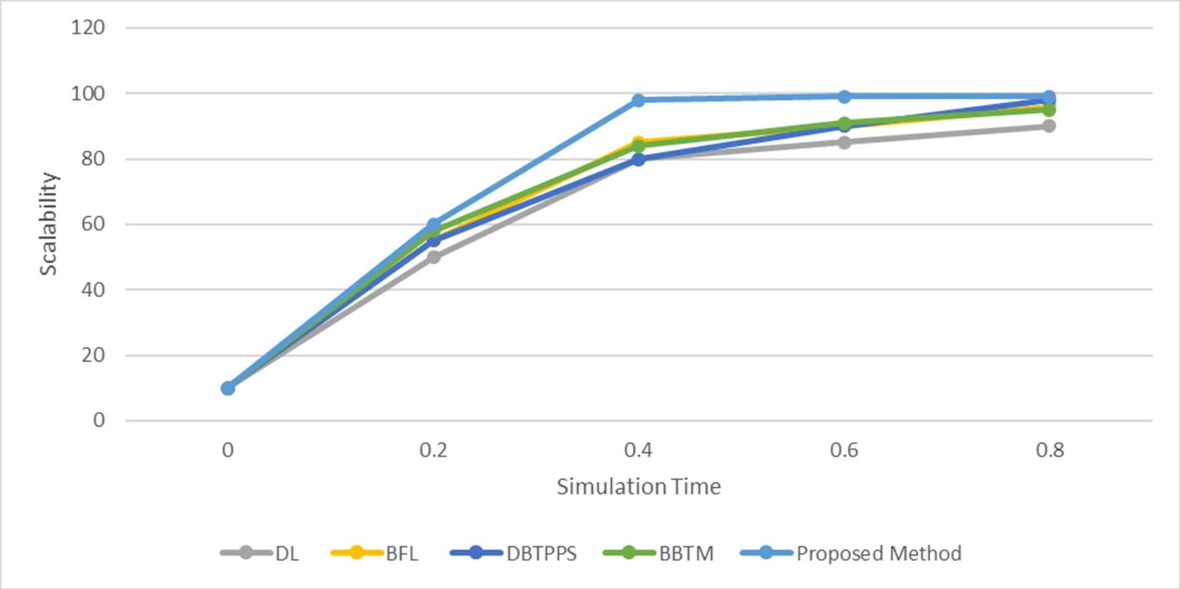
(a)


6
5
4
3
2
1
0
Energy Effiency
10
20
30
40
50
Number Iot Devies
Proposed Method
DL
BFL
DBTPPS
BBTM

(b)



(c)



(d)

Figure 3 Comparative analysis with proposed technique (a) Throughput (b) Energy Efficiency (c) Response Time (d) Scalability

Since the production of a block is tied to the transaction data, the block data is also saved during the saving process. The mining incentive will be the very first transaction in the blockchain, and will incentivize miners to participate. The block that is mined is its own reward. The miner also receives the total sum of all the payments made within the block. The certified transactions will be sorted according to predetermined criteria such as blockage, transaction fee, transaction amount, and so on. We merely implemented prizes to keep things simple throughout rollout. The current process will receive the prize. We can make a new process if the old one doesn't work. P2P (Peer-to-Peer, end-to-end) describes the blockchain network topology. For the actual enactment, we employ the python language within the anaconda framework. While maintaining the longest possible chain, the new node will synchronise all of the data from the other node's blockchain

5. Conclusion

In this work, we provide a recent piece on the blockchain and the Internet of Things. We outline the specific needs and problems of the five main building blocks of an IoT blockchain architecture. We also find gaps that prevent a solid foundation for the Internet of Things (IoT) blockchain from developing. This article delves into the concept of using a blockchain to secure the exchange of data between IoT devices in order to ensure data integrity. Improve the data transfer security with apply advanced hash function with use shuffle and mutation operation on input datasets and get a good result corresponding various performance parameter such throughput, energy efficiency, response time and scalability. Future scope of regarding generated data through sensor apply different deep learning and machine tool to perform complex task with smart block.

References

[1] T. Saba, A. R. Khan, T. Sadad, and S. Hong, “Securing the IoT System of Smart City against Cyber Threats Using Deep Learning,” Discrete Dyn. Nat. Soc., vol. 2022, p. e1241122, Jun. 2022, doi: 10.1155/2022/1241122.

[2] S. Jeong, J.-H. Shen, and B. Ahn, “A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain,” Wirel. Commun. Mob. Comput., vol. 2021, p. e9932091, May 2021, doi: 10.1155/2021/9932091.

[3] S. Joshi et al., “Unified Authentication and Access Control for Future Mobile Communication-Based Lightweight IoT Systems Using Blockchain,” Wirel. Commun. Mob. Comput., vol. 2021, p. e8621230, Dec. 2021, doi: 10.1155/2021/8621230.

[4] A. M. Alabdali, “A Novel Framework of an IOT-Blockchain-Based Intelligent System,” Wirel. Commun. Mob. Comput., vol. 2022, p. e4741923, Jan. 2022, doi: 10.1155/2022/4741923.

[5] S. M. Alrubei, E. Ball, and J. M. Rigelsford, “A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer,” IEEE Access, vol. 10, pp. 18583–18595, 2022, doi: 10.1109/ACCESS.2022.3151370.

[6] A. Ayub 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, doi: 10.1109/ACCESS.2022.3223370.

[7] A. Sagu, N. S. Gill, P. Gulia, J. M. Chatterjee, and I. Priyadarshini, “A Hybrid Deep Learning Model with Self-Improved Optimization Algorithm for Detection of Security Attacks in IoT Environment,” Future Internet, vol. 14, no. 10, Art. no. 10, Oct. 2022, doi: 10.3390/fi14100301.

[8] M. Ma, G. Shi, and F. Li, “Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario,” IEEE Access, vol. 7, pp. 34045–34059, 2019, doi: 10.1109/ACCESS.2019.2904042.

[9] H. Kim, S.-H. Kim, J. Y. Hwang, and C. Seo, “Efficient Privacy-Preserving Machine Learning for Blockchain Network,” IEEE Access, vol. 7, pp. 136481–136495, 2019, doi: 10.1109/ACCESS.2019.2940052.

[10] K. Biswas and V. Muthukkumarasamy, “Securing Smart Cities Using Blockchain Technology,” in 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Dec. 2016, pp. 1392–1393. doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.

[11] “Sensors | Free Full-Text | Packet Key-Based End-to-End Security Management on a Blockchain Control Plane.” https://www.mdpi.com/1424-8220/19/10/2310 (accessed Jun. 26, 2023).