applied sciences

MDPI

Article

Improving IoT Data Security and Integrity Using Lightweight Blockchain Dynamic Table

Saleem S. Hameedi *,† and Oguz Bayat †

Department of Electrical and Electronics Engineering, Altinbas University, 34217 Istanbul, Turkey
* Correspondence: saleem.alshabebi@ogr.altinbas.edu.tr
† These authors contributed equally to this work.

Abstract: Over the past few years, the Internet of Things (IoT) is one of the most significant technologies ever used, as everything is connected to the Internet. Integrating IoT technologies with the cloud improves the performance, activity, and innovation of such a system. However, one of the major problems which cannot be ignored in such integration is the security of the data that are transferred between the client (IoT) and the server (cloud). Solving that problem leads to the use the of IoT technologies in more critical applications and fields. This paper proposes a new security framework by combining blockchain technology with the AES algorithm. Blockchain technology is used and modified to protect data integrity and generate unique device identification within minimal power consumption and best performance. The AES algorithm is used to improve the data confidentiality when being transmitted to the server. The outcomes demonstrated that the proposed solution improves the security system of the IoT healthcare data and proved its efficiency and power consumption compared to other methods.

Keywords: IoT; security; AES encryption; blockchain; private blockchain; dynamic table

Citation: Hameedi, S.S.; Bayat, O. Improving IoT Data Security and Integrity Using Lightweight Blockchain Dynamic Table. *Appl. Sci.* **2022**, *12*, 9377. https://doi.org/10.3390/app12189377

Academic Editor: Luis Javier Garcia Villalba

Received: 15 August 2022
Accepted: 13 September 2022
Published: 19 September 2022

1. Introduction

The IoT envisions a fully interconnected society in which tangible items may interact and communicate with quantifiable information. As a result, the actual world may be represented digitally, and several smart applications in many different sectors can be created, including those for smart homes, wearable technology, smart cities, healthcare, automobiles, the environment, smart water, and smart grid [1]. To accomplish the needed functionality, IoT devices can be remotely controlled. The exchange of information between the devices then occurs through a network using established communication protocols. Simple wearable accessories to big equipment are among the "things" that are smartly connected and incorporate sensor chips [2]. On the other hand, the IoT also exposes daily life data to many different types of security threats [3]. Therefore, in recent years, tremendous work has gone into addressing security concerns in the IoT paradigm; while some of these strategies try to address security concerns at a particular layer, others seek to offer end-to-end security for IoT [4]. However, security in the IoT context is regarded as crucial given the breadth of the application field, particularly in light of the end-nodes (usually) constrained computing, memory, power, and control capabilities and their physical exposure [5].

Before the advent of IoT, most security threats were just related to information leakage and the loss of service. With IoT, security threats have become closely related to non-virtual lives and they can directly influence physical security risks. Besides, user privacy will become more important in the IoT environment as a lot of personal information will be delivered and shared among connected things. The four qualities of information security are authentication, non-repudiation, integrity, and availability [6]. All large corporations have their security protection systems in place to establish a highly secure system. Using the manufacturer of an IoT device as an example, the manufacturer will keep the updated firmware file on a file server that is well protected to assure the file's security [7].

In recent years, blockchain technology has been designed as a high-security solution for many security-needs applications, including the IoT. Blockchain technology has been predicted by the business and scientific communities to be a disruptive technology that will have a significant impact on how IoT devices are managed, controlled, and most crucially, secured [8]. Furthermore, blockchain technology has attracted a lot of attention as it moves toward decentralized designs and addresses security, anonymity, traceability, and centralization. Using blockchain, entities and techniques are enforcing security and privacy attributes in various IoT security levels [9]. IoT systems may be built with a suitably distributed consensus-based architecture and security challenges resolved by integrating blockchain technology. Even if this is the perfect match, it is still a difficult task. The majority of current blockchain technologies are not compatible with the IoT environment and cannot satisfy its unique requirements. Because IoT settings are resource-constrained, computationally intensive, power-intensive, and storage-constrained, blockchain has a high computational complexity, a small amount of scalability, a large bandwidth overhead, and a high latency. Some devices are not recommended to be used with IoT [10]. Therefore, recent solutions have been trying to adopt the blockchain technology by modifying and optimizing the blockchain generating and managing techniques [11–13]. This paper has presented a new mechanism to improve the security and efficiency of IoT networks using a new blockchain mechanism.

Our suggested system makes the following contributions:

- We offer a multi-layer blockchain-based method for safeguarding the privacy and security of IoT devices while also increasing system scalability.
- Multiple-hashcode-based access control is utilized to provide safe communication with multiple organizations without Trusting Third Parties (TTP);
- We assess our approach by executing a prototype implementation to match the IoT criteria.

The findings reveal that our system is more effective and efficient in terms of transaction latency and throughput; we also conduct a security analysis of the suggested solution in comparison to other recent research in the literature.

2. IoT Architecture and Security Challenges

The IoT deployments contain heterogeneous uniquely identifiable, low power consuming, and limited computational power devices with embedded sensors interconnected through a network [2]. The device is designed to provide remote services for IoT users. Transmitting data through a network and hops is required to implement an encryption mechanism for data confidentiality. Moreover, storing data on the device expose the data to privacy violations and make the devices susceptible to attacks that can modify the stored data and affect the system's integrity.

The second security challenge when using IoT and cloud technology is the security of communication and the authentication of the network parties [14]. The device must be identified and authenticated before being used for the services and transmitting the data to the server. However, the heterogeneous architecture and environment of the IoT network required a powerful authentication and authorization system to tackle this diversity.

With the increasing number of IoT devices and the passage of time, as well as equipment ranging from small embedded processor chips to huge high-end servers, many security challenges at various architectural levels of embedded IoT devices must be addressed [15]. The security threats/issues relating to the IoT device deployment architecture are classified as follows: [16]:

1. Issues with low-level security;
2. Issues of security at the intermediate level;
3. Issues of high-level security.

Solving these security challenges can be easy without the resource-constrained and power consumption of the IoT devices [17]. Therefore, each instruction and algorithm

should be implemented within these limitations. This leads to an extra challenge, which is the power consumption of the attack protection. The attacker can exhaust the IoT resource by flooding the network with redundant forged requests. The most prominent and widely used identification and authentication mechanism for IoT device security is Open Authorization (OAuth) [18]. End users and IoT devices get tokens using OAuth, an open standard communication mechanism. Tokens are saved in a database or on a server. End users make use of the system's resources. Tokens are used to authenticate end users in the system. There are four actors in the open standard protocol: the data and resource owner are responsible for creating verified resources and granting users access to the server, respectively; the Open Authentication Server (OAS) generates tokens for safe communication with valid clients/users or other entities [19]; the database or resource server offers authenticated resources/data.

3. Blockchain Technology

Blockchain technology has been predicted by the industry and research community as a technology with future applications that can play a key role in the management and control of IoT devices as well as adding security features [20]. This section describes the basics that have been used in designing the proposed solution and integrating Blockchain technology into it and how blockchain is a technology that enables viable security solutions to today's challenging IoT security problems. First, the section provides a brief explanation of blockchain, then identifies open-research IoT security problems and challenges that blockchain may provide solutions to. The department also scans blockchain-based solution literature for IoT security problems.

As shown in Figure 1, a blockchain is essentially a decentralized, distributed, and shared database ledger with the inability to alter the transactions and records in it over a peer-to-peer (P2P) network [21]. After the data blocks are temporally sealed, they are restricted and validated by miners. By using Elliptical Curve Cryptography (ECC) and SHA-256 hashing, Blockchain provides strong encryption for data authentication and integrity [7]. The block data, as shown in Figure 2, contain a list of all transactions and a hash to the previous block. Having a complete record of all transactions in the blockchain makes it provide global trust distributed across borders. No matter how trusted third parties (TTP) or central authorities and services are, they can be disrupted, hacked, or malfunctioned. Misuse may also occur in the future.

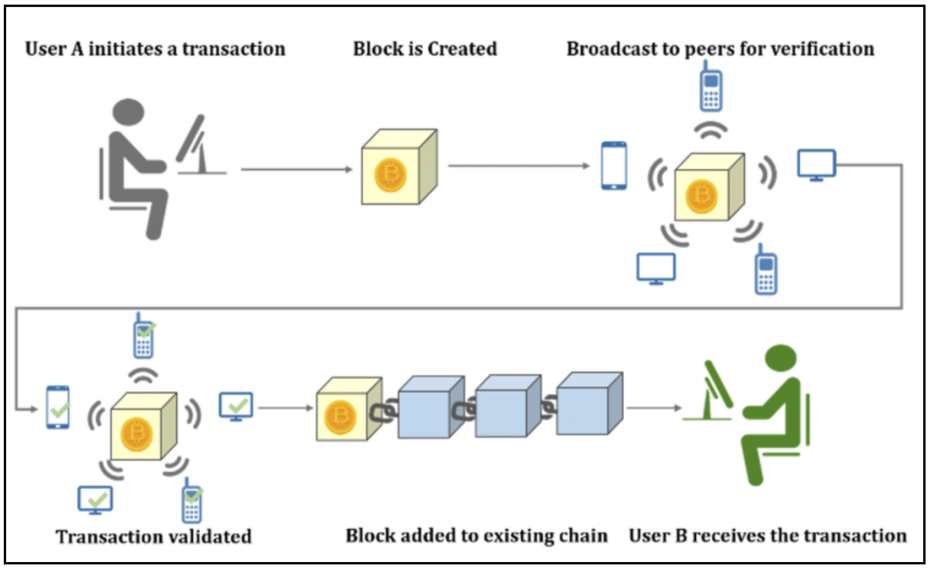

Figure 1. Blockchain architecture.

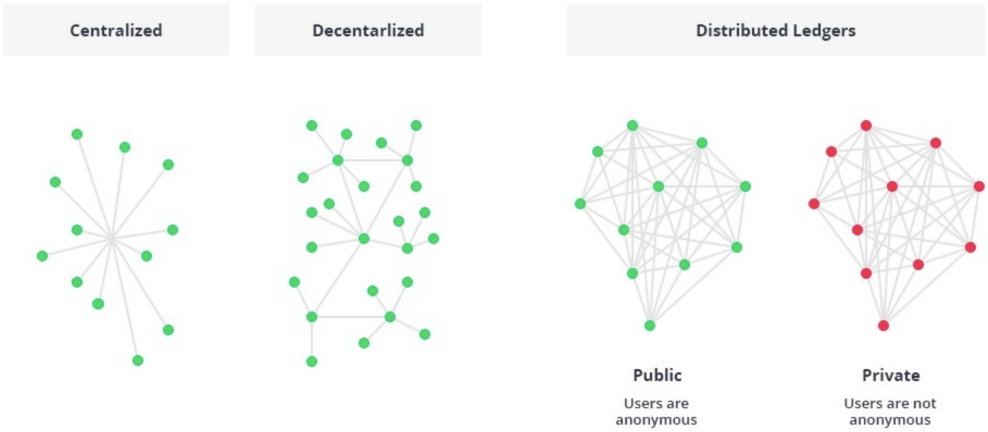

Figure 2. Blockchain ledger.

In the blockchain, every transaction in a shared public ledger is verified by the consensus of the majority of mining nodes that actively participate in the validation and verification of transactions. In the Bitcoin network [22], miners validate the block by calculating a hash with leading zeros to achieve the difficulty goal. Block data become immutable once transactions are validated and verified by consensus, which makes erasing or changing the data an impossible task. A Blockchain can be built as follows: (1) a licensed (or private) network that can be restricted to a specific group of participants (this is called a public blockchain) or (2) without permission or a public network that is open to anyone to join. Permission blockchains provide more privacy and improve access control and this is called the Local Blockchain.

Blockchain Platform in IoT

There are a variety of blockchain development platforms, such as Ethereum and Hyperledger, each with its own set of features [23]. Vitalik Buterin created the Ethereum blockchain platform [24]. The most significant distinction between Ethereum and Bitcoin is a smart contract, which enables Ethereum to deploy applications on the blockchain [25]. Ethereum can do a variety of tasks, such as playing games, according to various smart contracts. As a result, Ethereum is also known as "blockchain 2.0". Ethereum has paved the way for a new generation of blockchain developers. Ethereum extends the remaining qualities of blockchain to mainstream apps, which are referred to as "Decentralized Applications" [26]. Ethereum is a relatively new platform among a range of platforms, with a high level of reliability and appeal. Hyperledger, on the other hand, is a Linux Foundation-supported blockchain interoperability application. It has a variety of platforms, including IBM's Fabric [27]. To accomplish privacy protection, the system takes into account the enterprise's structure and creates alternative protocols depending on different network topologies, such as "Byzantine Fault Tolerance (BFT)." Because it is more private, it is most commonly used in the financial business, which is concerned about personal privacy.

IOTA is a blockchain platform developed by Dominik Schiener's team [28]. It is mainly used on the Internet of Things, providing payment and file storage functions. The underlying layer uses decentralized ledger technology, called Tangle, to make transactions [29]. The speed is faster. Tangle is also the first decentralized ledger system that does not require a fee. By distributing the work of verifying transactions to each trader, Tangle has saved the commission, which in turn increases work efficiency. Compared with other platforms, IOTA has a shorter time and there are still some imperfections waiting for the development team to improve

The combination of blockchain and IoT, which have constrained power and storage capacity, presents a hurdle due to blockchain's complexity, which also includes significant

computational costs and delays. The difficulties encountered with managing IoT data on a blockchain are shown and outlined below:

1. **The trade-off between performance, security, and power consumption:**The development of these technology-based apps on resource-constrained devices has increased significantly due to the high computing power needed to execute blockchain algorithms [30]. Researchers have also questioned how well the blockchain performs while processing data from the Internet of Things and advised improving its core algorithms to produce more verified blocks per second [31]. For instance, getting rid of the blockchain's PoW consensus algorithm can enhance efficiency and minimize power use [32]
2. **IoT Connectivity Challenges:** To exchange IoT data with possible stakeholders, the IoT devices are anticipated to be connected to high computational, storage, and networking capabilities [33]. The Internet of Things (IoT) has limited capacity to link with blockchain technology to offer fresh business prospects for the development of new applications and services in several domains.
3. **Data concurrency and throughput issue**: IoT systems have high concurrency because IoT devices transmit data continually [34]. Due to its intricate cryptographic security protocol and consensus procedures, the blockchain's throughput is constrained. Increased bandwidth is needed to quickly synchronize new blocks between blockchain nodes in a chain-structured ledger, which can increase blockchain throughput.
4. **Blockchain Regulating in IoT:** Decentralization, immutability, anonymity, and automation are some of the blockchain's promised security properties for a variety of IoT applications, but these traits taken together provide several new regulatory issues [35]. The distributed transaction ledger (DTL) immutability characteristic indicates that data are permanently published there and cannot be changed or removed. Additionally, because there is no governance, documents cannot be vetted to preserve privacy before being published on the blockchain.

In this paper, the local blockchain will be used to protect the IoT device's identity and data integrity.

4. Literature Review

According to [36], there are many security threats in IoT, which are categorized into two main threads: physical and logical threats. The proposed solution in this proposal is mainly focused on the logical threats; therefore, the literature review focuses on the logical threats of IoT devices, which contain security leaks and threads when storing and transmitting data from IoT devices to base stations in the cloud.

In 2016, Aafaf Quaddah et al. [37] defined a new blockchain framework for controlling the access of IoT. The first contribution of the framework consists of providing a reference model for the proposed solution in terms of objectives, models, and mechanisms of the IoT architecture. The second is the FairAccess for the fully decentralized pseudonymous and privacy-preserving characteristics. This contribution also gave a framework for authorization management. The authors indicated that the new FairAccess blockchain technique used different types of transactions, which is different from one that is used in bitcoin, which provides get, delegate, and revoke access. The framework had been tested and examined with a Raspberry PI device for a local blockchain. The main limitation of the proposed solution is the performance of the framework when used with a real-time IoT monitoring application.

In 2017, Yu, W. and Kose S. [38] worked on preventing stored secret key learning when using AES encryption by proposing a false key-based AES encryption technique. To hide the intermediate data during the reconstructing stage, Wave Dynamic Different Logic (WDDL) with an XOR gate has been utilized. The main objective of the proposed solution was to protect the data against Chosen Plaintext Attack (CPA) attack. However, the solution has not been tested against other AES attacks, such as brute force attacks and random key chaining (RCK).

Boudguiga et al. [39] also presented a blockchain-based technique for upgrading IoT device firmware by including various manufacturers and antivirus businesses into the blockchain system and obtaining firmware files from the system. Before it can be synchronized by other blockchain nodes in the system, it must be confirmed by the antivirus company node, and then IoT devices must request the files from the blockchain node. This design has been sent to an antivirus firm for verification. Because the number of verification nodes is so small, the verification node bears a significant strain. Furthermore, the attacker only needs to target a few nodes to do systemic damage.

In 2018, Mahdi H. Miraz and Maaruf Ali [40] studied the ability to use blockchain technology to enhance the IoT ecosystem security. They determine the main field of using blockchain to improve the security and privacy of IoT. The blockchain can be used and act as a catalyst by enhancing the security and reliability of IoT, as it works as a Machine-to-Machine (M2M) interaction mechanism. The study shows that it can track billions of devices connected to IoT systems by deploying blockchain technology. Furthermore, they explain how the threats to IoT security can be detected using the Shodan search engine, which they describe as "the world's first search engine for Internet-connected devices". Instead of a detailed explanation of how blockchain technology can be used to improve IoT security systems, they did not offer a clear mechanism of how to implement blockchain in the IoT. Furthermore, they did not show the impact of using blockchain on IoT performance.

In 2019, Naif J. R. et al. [41] proposed a lightweight security system using a chaotic system and AES encryption. They combine logistic and Lorenz chaotic systems to create a 5-D chaos system, which is used to generate the key of AES encryption. The AES that was used in the proposed solution had been modified by reducing the processing complexity, which results in improving the performance by 145%. However, the solution did not show the effects of using the chaos key on the security of the AES encryption and the efficiency of the security system against well-known IoT attacks. Furthermore, the new security system had been only compared with standard AES.

In 2019, Dorri A. et al. [42] presented a lightweight scalable blockchain security and privacy system for IoT called LSB. The proposed solution addressed the impact of computation of blockchain technology and the limitation of scalability, which overheads and delays the performance of IoT devices. The proposed solution optimized the blockchain to work with low-resource IoT devices. The LSB achieves the high-resource devices which are joined to the IoT network to manage the public blockchain and ensures the end-to-end security and privacy of the network. Furthermore, the solution optimized the performance by using lightweight consensus and the extensive simulations results show that LSB improves the performance of the IoT network and minimizes the packet overhead. However, the proposed solution did not use real blockchain technology management on the IoT devices, and most of the processing depended on the high-performance devices in the network.

In 2020, Du, M., Wang et al. [43] proposed a new three-dimensional blockchain architecture with a novel data structure to deal with heterogeneity and stability of IoT network and called it SpaceChain. The three-dimensional greasy heaviest-observed sub-tree (3D-GHOST) consensus mechanism was used for Spacechain to handle the issue of the network performance of IoT. The security mechanism is divided into two procedures: dynamic weight distribution and ready traversal. Moreover, the chain of the blocks is divided into two types: main chain and side chain. The solution with this dividing technique will only accept the first occurrence of a block after sorting the local ledger. The solution has been tested extensively to verify its performance and its security of the new solution.

In 2021, Houshyar H. Pajooh et al. [44] introduced a multi-layer blockchain-based security model of IoT. The proposed solution was designed to simplify blockchain implementation to protect the IoT network. The k-unknown clusters were used to facilitate the multi-layer concept besides the hybrid evolutionary computation algorithm. The simulated annealing and genetic algorithm were used in the clusters to protect the private blockchain

communication which occurred between the cluster heads and relevant base stations. The authentication mechanism and security had been enhanced with the blockchain approach when they were adopted by base stations and enabled secure communication among them. The comparison between the traditional blockchain and the proposed lightweight blockchain shows a better balance in the network latency and throughput. However, the multi-layer solution with many heavy algorithms has not been analyzed in terms of power consumption, as using such an algorithm will overhead the IoT devices' performance.

In 2022, Ahmed Imran et al. [45] looked at the interaction between blockchain technology and AI, a singular force behind the development of intelligent and sustainable IoT applications. They mainly talked about how blockchain technology has advantages that might help the growth and development of sustainable IoT applications. They established a clever and sustainable conceptual framework that processes and gathers essential data using cloud computing, IoT devices, and artificial intelligence. To support multiple applications, the system offers digital analytics and stores outcomes in decentralized cloud repositories. A sustainable incentive structure is also made possible by the layer-based design, which may help safe and protected smart city applications. However, the proposed solution has not been examined in terms of power consumption, as using an AI algorithm requires extensive computational power.

In 2022, Marah Bataineh et al. [46], to solve the issues posed by the constrained IoT resources when adopting the Blockchain mining process in IoT systems, proposed an IoT-Blockchain integration architecture employing an Ethereum Blockchain infrastructure within a rich-thin client IoT approach. The architecture relies on how the resources are loaded. Devices with fewer resources are called thin clients, whereas those with more resources are called rich clients. Both clients can access the blockchain and gather data, but the rich client is limited to carrying out the mining operation. Additionally, they put into place a healthcare system that performs surgical process management based on the suggested design. By testing and evaluating the design against other well-known IoT-based blockchain architectures, they also demonstrate the effectiveness of our solution.

5. Proposed Solution

The proposed solution has been designed to protect the IoT devices using two layers that works based on the two main different technology.

5.1. Dynamic Blockchain Table (DBT)

The dynamic blockchain table (DBT) is a new mechanism to protect the data and identification of IoT devices. It will solve the two main issues in the blockchain to be suited and compatible with the IoT devices specification and does not overhead the IoT network. First, it will preserve the data security of the content of the blockchain by using multipart AES encryption. Second, it will use the dynamic table that will be changed with the data which are being generated by the IoT devices.

Combining both technologies provides a full mechanism to protect the data and prevent intruder attacks. The main idea of the proposed system, as shown in Figure 3, is to generate unique identifiers for each device and protect the data at the same time. At the beginning, the device within the network generates a unique random array of 256 bytes and stores this within its data. When the device senses new data and needs to send it to the cloud, the first step is to convert the data into a separate set of bytes, then XOR merges the data and the array it generated to form a new array. The new sensed data are merged with the new array to be a single data block. This block represents the data that will be added to the chain, thus dispensing with the complex processing of hashing algorithms and at the same time creating a unique device identifier.

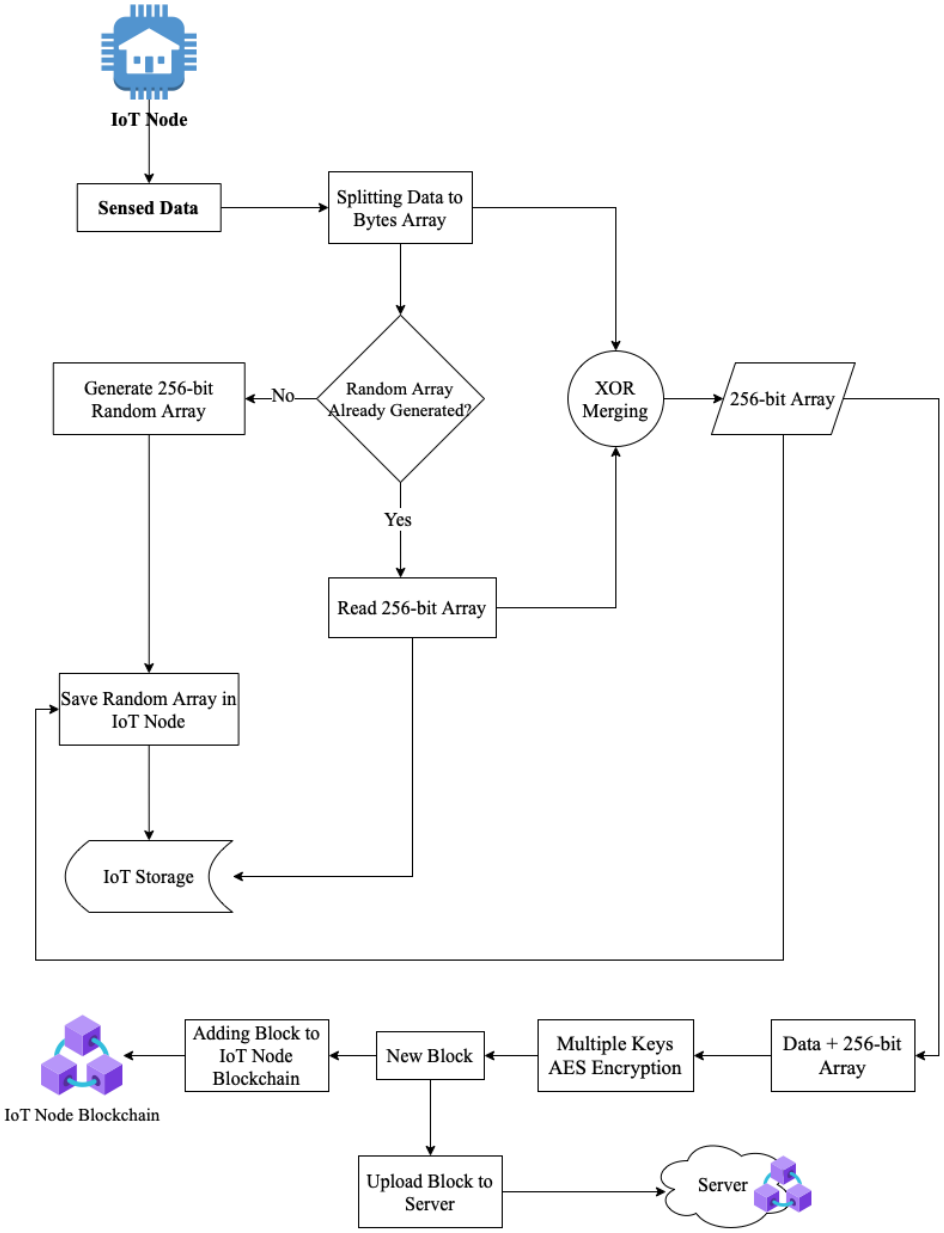

Figure 3. Dynamic blockchain table architecture.

5.2. Smart Contract

To keep the data management process running smoothly, the smart contract was created using the solidity programming language. The proposed solution uses a simple implementation of a smart contract on the server side. This implementation replicates the real-world method for collecting sensed data. The contract is composed of three parts:

- The data processing tasks that are called at each event include the production of sensed data records, data date and time, and IoT device ID, which is represented by a dynamicTable 256-bit.
- A database with a dynamic table from an Internet of Things device to store the detected data. ID, IoT ID, sensed data, and sensed data date/time are among these data.
- Functions, which contain all the functions needed to proceed with the event. Which are:
  1. Data creation: add the sensed data to the array with the basic information mentioned before.
  2. Block verification: when the dynamic table has confirmed the validity of the data with the previous dynamic table.

The smart contract solution is used mainly to confirm and store transaction data. However, the proposed solution has focused on the security of transferring data using blockchain. Nevertheless, the standard smart contract has been integrated on the server side to generate smart contract information for each IoT device information.

5.3. Multiple AES Encryption

At the beginning of its work, the device needs to send its unique array to the cloud using multiple encryptions, which we will talk about in the next section. On the cloud side, the cloud will decrypt the block and regenerate the array based on the data it has access to and using the array it owns. The generated array must match the array sent by the IoT. When matching occurs, the new array will be stored as a new device identifier. In the event of inconsistency, the received data will be discarded. Using this method will make it impossible to guess the device ID, as it changes every time, which gives the system additional layers of protection against attacks. On the other hand, any modification to the data will lead to a wrong result in generating the matrix, and this is what makes the protection of data integrity among the points covered by the proposed work.

Multiple data encryption is a method that has been proposed to reduce the amount of processing required in encryption while maintaining the level of security. The idea as shown in Figure 4 is to split data into multiple parts and encrypt each part with a different, small-sized key. In the proposed system, the data will be hashed into parts of 64 bytes and then four AES keys of the same size are generated, and then each piece of data is encrypted with a separate key. This method will also increase the data protection against Brute Force attacks, because the attacker will need to guess four keys instead of one. In addition, the result of the data after encryption will be easy to send without increasing the load on the network, because its size is smaller than the data encrypted with a long key.

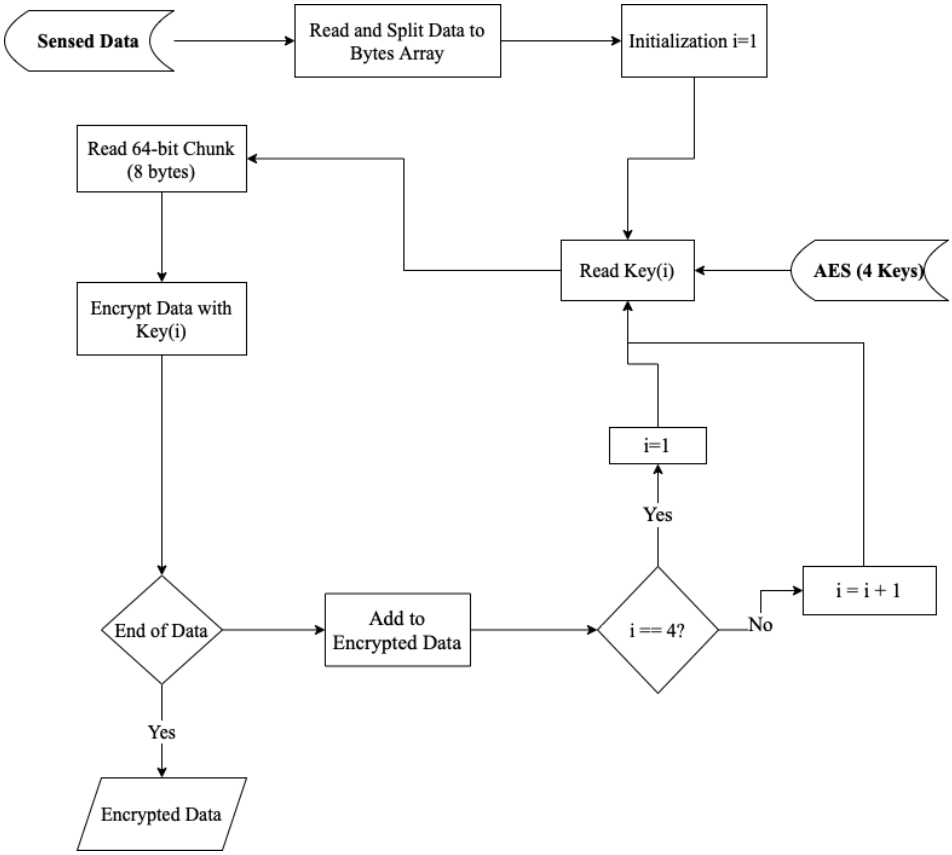

Figure 4. Multiple AES encryption architecture.

There is a strong likelihood that adversaries will use packet sniffing as a technique to launch an assault on wireless transmission systems. A transceiver is used by the attacker to intercept packets that are sent between gateways and nodes or the other way around. The integrity of the network and the validity of the data being compromised by the prospect of the attackers introducing these recorded packets back into the system. Furthermore, a Man-In-The-Middle attack is also a threat that should be handled for any new security solution for IoT. However, a solution can be proposed that protects both the block and dynamic table. First, each block is encrypted with four AES keys; therefore, extracting the data and dynamic array from the transfer packet requires guessing the four keys first. Second, the array is changed with every sensed data and sent to the server, which verifies each block before being accepted. Any block that does not pass the block checking mechanism will be dropped.

5.4. Key Exchange Mechanism

One of the core cryptographic building blocks, key exchange (KE), allows users to establish secure communication by exchanging symmetric keys. Therefore, to establish data encryption and blockchain generation, an AES key has to be generated and exchanged between the server and IoT node [47].

In the proposed solution, the data have been encrypted with four key parts to maximize the security and efficiency as mentioned before. This is required to exchange those keys between the server and IoT node in a secure mechanism.

First, both the server and IoT node generate new ECC public and private keys. Then, the server generates the four keys of AES with 64 bits. The IoT nodes send the ECC public key to the server so it can use it to encrypt the four AES keys and then re-send it to the IoT nodes. The data encryption using the ECC algorithm is heavier than data decryption, as it requires more mathematical operations; therefore, such a heavy technique will be performed on the server side to ensure that it does not affect the efficiency of the IoT node. In addition, for the best performance, the TinyECC algorithm was used [48].

Figure 5 summarizes the key exchange mechanism in the proposed solution using the TinyECC algorithm.

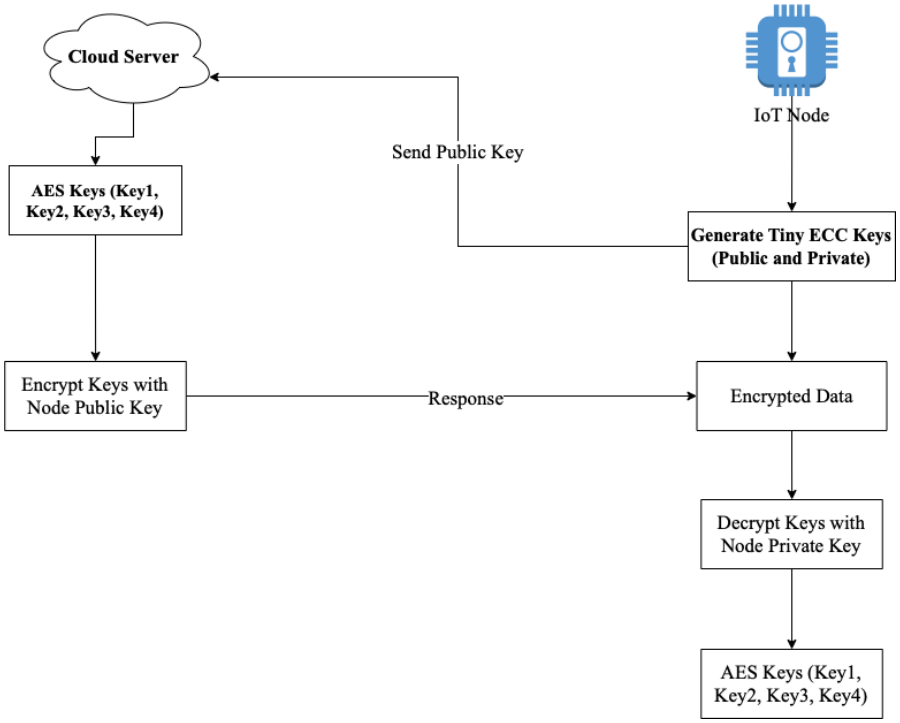

Figure 5. Key exchange mechanism.

6. Materials and Methods

To examine the performance of the proposed solution, we evaluate the proposed lightweight blockchain solution in two parts. First, the solution has been tested with a real IoT device, which is the Z1 (as shown in Figure 6), powered by an MSP430F2617 low-power microcontroller with a strong 16-bit RISC CPU running at 16 MHz, built-in clock factory calibration, 8 KB RAM, and 92 KB Flash memory. The well-known CC2420 transceiver, which is IEEE 802.15.4-compatible and works at 2.4 GHz with an effective data rate of 250 Kbps, is also included. The Z1 hardware selection ensures optimum efficiency and robustness at the lowest possible energy cost.

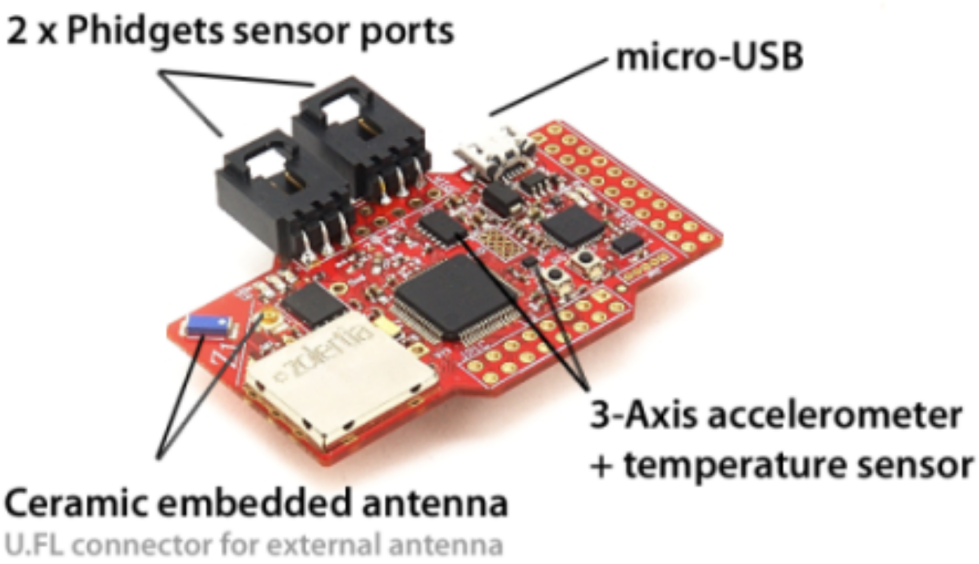

Figure 6. Z1 IoT device.

Second, Cooja simulation has been used to test the multi-situation of the IoT network with the new solution. Contiki is a Linux-based operating system that focuses on low-power Internet of Things devices, while Cooja is a Contiki-based network emulator. Cooja can mimic both big and small networks of IoT motes. Its simulation depicts several types of sensor nodes (heterogeneous networks). It uses a few functions to operate and evaluate a Contiki system. For example, the simulator can tell the Contiki system how to handle an event or retrieve the whole memory of the Contiki system for examination.

7. Evaluation and Analysis

Three main security requirements must be addressed by any security design, namely confidentiality, integrity, and availability, otherwise known as CIA. Confidentiality makes sure that only an authorized user can read the message. Integration makes sure that the message sent at the destination is received without any change, and availability means that every service or data point is available to the user when they need it. To increase the availability of a smart home, devices are protected from malicious requests. This is achieved by limiting the accepted transactions to those entities with which each device has created a shared key. Transactions from the overlay are authorized by the miner before being forwarded to the devices. Furthermore, it can be argued that our BC-based framework offers only a marginal increase in transaction processing delays compared to current smart home gateway products. There is also an additional one-time delay during initialization for the generation and distribution of shared keys. In short, the additional delays are not significant and do not affect the availability of smart home devices.

7.1. Security Analysis

Table 1 summarizes how the proposed framework met the above security requirements, as the proposed work was tested on two main types of attacks and threats to IoT. The first is a Distributed Denial of Service (DDOS) attack, where, to defeat a particular target node, the attacker uses several infected IoT devices. The second is a link attack, which puts the privacy of users at risk, as a link between multiple transactions or data books with the same PK is created by the attacker to find the real ID of an unknown user.

Table 1. Security requirements evaluation.

Requirement	Employed Safeguard
Confidentiality	Achieved using AES Encryption
Integrity	Blockchain Technology is employed for integrity achievement
User Control	Using logging transaction of Blockchain
Authorization	Achieved using Dynamic Blockchain Array

Compared with using standard blockchain technology over an encrypted channel (e.g., HTTPS), the proposed solution has much better security benefits. The following points are summarizing the main key differences:

- Using standard blockchain technology is much more costly than the proposed solution due to the hashing mechanism that is used with a standard blockchain, which is (SHA-2).
- Encrypting the transfer channel only with the HTTPS or SSL technique is not enough to secure the IoT data, because it requires encrypting data with a 256-bit AES key, which is much more costly than a 64-bit AES key. Moreover, it does not protect the network from message forwarding. The attacker can simply store and re-send IoT packets many times over the network to the server. On the other hand, the dynamic table mechanism provides a unique identity for each sent message.
- Using multi-part AES keys and a dynamic blockchain table, giving a different message each time even if the data are the same, which maximizes the encrypted data security against a brute-force attack.
- Last but not least, using the proposed solution provides a set of blocks that can be used to verify IoT nodes' data at any time, as each block is connected with a previous one.

7.2. Performance Evaluation

The BC-based architecture suffers from the computational and packet burden on smart home devices and miners to provide improved security and privacy. To assess this overhead, we simulated the scenario of data transmitted within the IoT network in the Cooja simulator. To compare the overhead of a BC-based architecture, we simulate another scenario that deals with transactions without encryption, hashing, and BC. We used IPv6 over Low Energy Wireless Personal Area Networks (6LoWPAN) as the primary communication protocol in our simulation, since it is well suited to the resource constraints of a smart home setup. We simulated three z1 mote sensors (simulating smart home devices), which send data directly to the home miner (also simulated as a z1 mote) every 10 s. Each simulation lasted for 3 min and the results presented over this duration were averaged. Cloud storage is directly connected to the miner to store data and save the transmitted block data. It is noteworthy that the overlay delay and its processing are not taken into account in our simulation. To provide a comprehensive assessment, we have simulated store and access transactions.

The following metrics have been implemented to evaluate the performance of the proposed system:

1. **Packet overhead**: Indicates the length of the sent packets.

2. **Time overhead**: Refers to the processing time for each transaction in the miner and is measured from the time the transaction is received in the miner until the appropriate response is sent to the server.
3. **Power consumption**: Refers to the power that the miner consumes in the hardware to process transactions. The miner is the most power-consuming device in the IoT network because it handles all transactions and does a lot of hashing and encryption. The power consumption of other devices is limited to coding for their transactions.

To understand the performance results, each result is discussed separately:

- Packets overhead: Table 2 shows the simulation results for packets in the network. The content of the table applies to both the access and storage parameters, as they both have the same packet size. The use of encryption and hashing increases the payload of packets due to the transformation of data from its explicit form to its encrypted form; however, given the lower layer headers (i.e., 6LowPAN), the increase in data payload has a relatively small impact, because multi-key encryption with an appropriate meta-array size in the data will result in a slight increase in the size of the transmitted data.

Table 2. Packet overhead (bytes) with standard blockchain.

Packet Flow	Base	Standard Blockchain	Proposed Solution
From device to cloud	5	512	128
From cloud to device	5	512	128

Table 3 shows the high performance of the proposed solution in terms of packet overhead compared with the recent solution presented in 2022 [19]. The results show that the proposed solution keeps the packet overhead four times lower than the compared solution. Such a low bytes usage keeps the energy consumption very low for the IoT device.

Table 3. Packet overhead (bytes) with recent solution.

Packet Flow	IoT Security	Proposed Solution
From device to cloud	1024	128
From cloud to device	1024	128

- Time overhead: Figure 7 shows the results of overtime. The BC-based design alone takes more time to process packets than the basic method due to additional coding and hashing, as the system needs more processing. However, comparing it with the previous works that used the blockchain technology, we find that the system has given a better time as a result of the presence of a simplified block technology in the proposed work, which helped reduce the effort significantly.
- Energy consumption: Clearly, the blockchain method in previous research increases the energy consumption by 0.07 (mJ), but in the proposed work, the amount of energy consumed was much better and very close to the basic work. Figure 8 and 9 show the power consumption of the three primary tasks a miner performs: CPU, Transmit (Tx), and Listen (Lx). CPU power consumption increased by approximately 0.002 (mJ) in the comparable design, but with the proposed work, the power increased by approximately 0.0004 due to the lightweight blockchain technique of the proposed solution and simple (xor) hashing. Sending longer data packets doubled the transmission power consumption of the method, we compared with the basic method, but with the proposed system, the consumption increased by less than 25%.

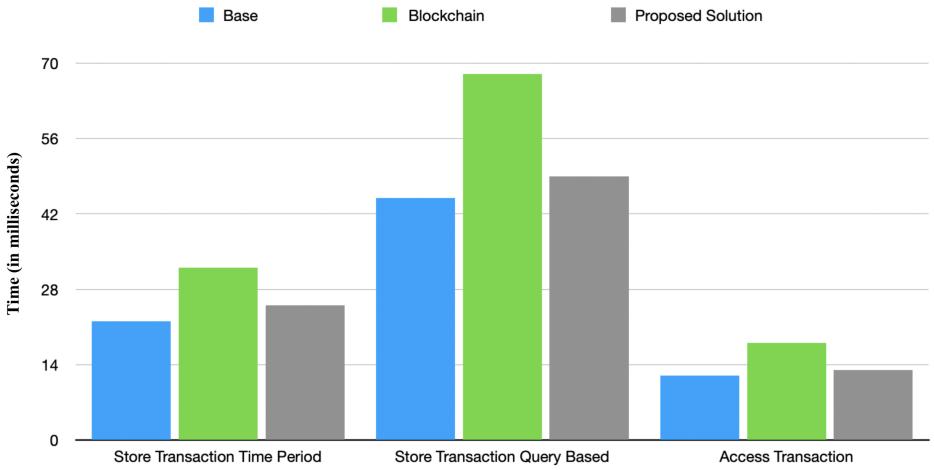

Figure 7. Time Overhead evaluation.

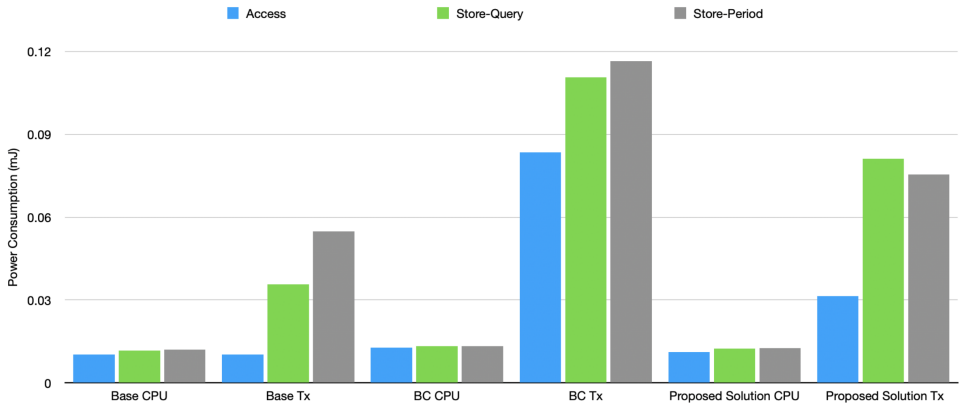

Figure 8. Energy consumption overhead (CPU and Tx).

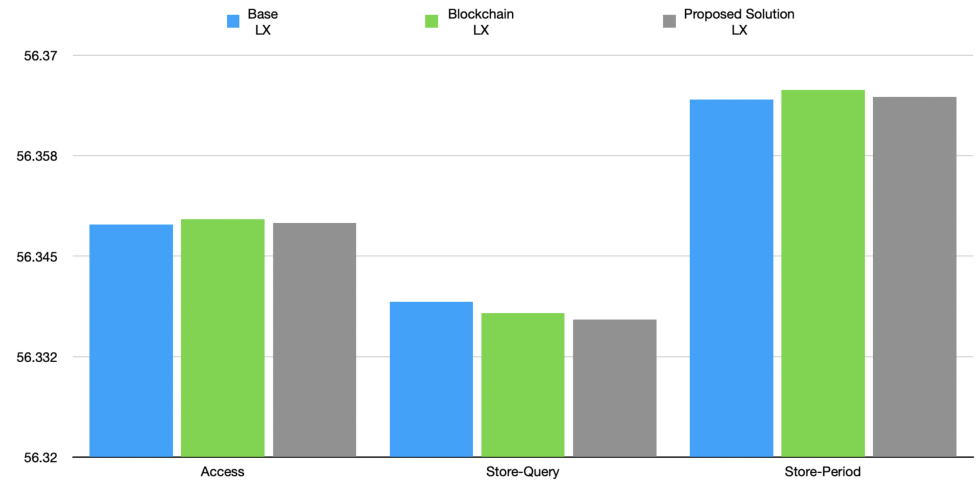

Figure 9. Energy consumption overhead (Lx).

7.3. Proposed Solution Analysis with Healthcare Application

To examine the proposed solution's integrity, efficiency, and performance with real-world IoT usages, such as smart cities, smart homes, and other applications, the healthcare IoT network has been integrated with the proposed solution. The scenario of the application and network has been inspired from [46] and modified to fit with the proposed solution settings. We picture a sizable, chaotic hospital that sees hundreds of patients every day and is tremendously busy. The hospital is constantly checked for patients and other community hospitals, hundreds of physicians and other staff members commute daily, and therapeutic supplies that need to be used right away are frequently recalled. Healthcare professionals are assisted by information technologies, yet real-time monitoring of patient and asset mobility is not always reliable. Therefore, it becomes challenging to recognize and respond to critical situations in this complicated and chaotic circumstance. The proposed solution has been tested with packet overhead and energy consumption.

In terms of packet overhead, as noticed in Table 4, it has been preserved with 128 bytes only compared with 1024 bytes of standard blockchain, as mentioned before.

In terms of energy consumption, the consumption of the proposed solution is much better and very close to the basic work. The table at the bottom of Figure 10 shows the power consumption of the three primary tasks a miner performs: CPU, Transmit (Tx), and Listen (Lx). The energy consumption is very low, with 0.005 mJ for the CPU and 0.08 for Tx, due to the blockchain's lightweight mechanism and simple hashing.

Table 4. Packet overhead (bytes) of healthcare.

Packet flow	Proposed solution
From device to cloud	128
From cloud to device	128

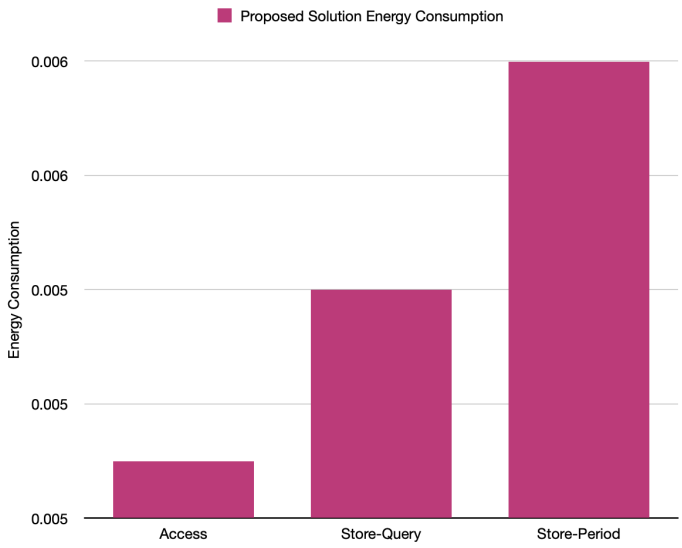

Figure 10. Energy consumption overhead (CPU and Tx) of healthcare application.

In terms of Lx, Figure 11 shows the power consumption, which is very low with 56.5 mJ at most in store-periods, 56.2 mJ in Store-Query, and 56.7 mJ in Access.

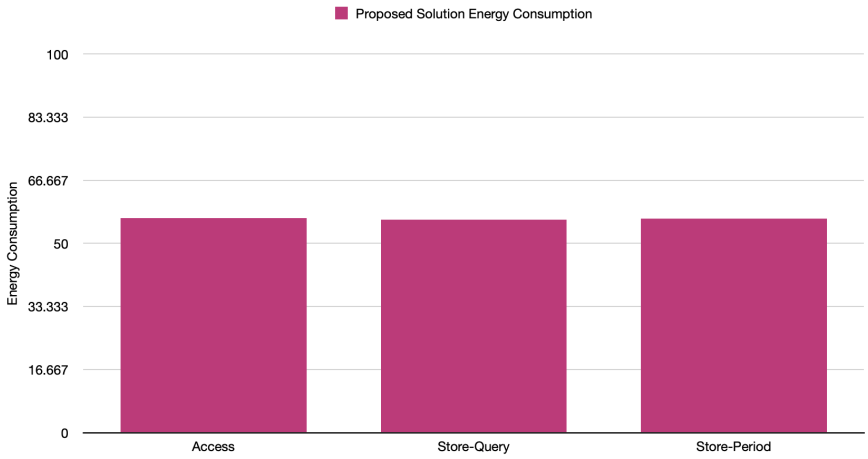

Figure 11. Energy consumption overhead (Lx) of healthcare application.

8. Conclusions

More complex security procedures are required as the number of IoT devices grows. This research uses blockchain technology to do multi-node firmware verification, allowing IoT device security to be achieved. In this proposal, a high-security monitoring system will be used to secure and integrate the transmitted data and preserve the identification of IoT devices. The system can be implemented and tested with various platforms to secure the data. Moreover, the AES algorithm and blockchain generator parameters can be improved to get optimal performance for each application and datatype.

Author Contributions: Methodology, S.S.H. and O.B.; software, S.S.H. and O.B.; validation, S.S.H. and O.B.; formal analysis, S.S.H. and O.B.; investigation, S.S.H. and O.B.; resources, S.S.H. and O.B.; data curation, S.S.H. and O.B.; writing—original draft preparation, S.S.H. and O.B.; writing—review and editing, S.S.H. and O.B.; visualization, S.S.H. and O.B.; supervision O.B.; project administration, S.S.H. and O.B.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no grant or funding from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nižetić, S.; Šolić, P.; González-de, D.L.d.I.; Patrono, L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *J. Clean. Prod.* **2020**, *274*, 122877. [CrossRef]
2. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
3. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
4. Noor, M.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]
5. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. *Internet Things* **2018**, *1*, 1–13. [CrossRef]
6. Gunduz, M.Z.; Das, R. Analysis of cyber-attacks on smart grid applications. In Proceedings of the 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), Malatya, Turkey, 28–30 September 2018; pp. 1–5.
7. Antonopoulos, A.M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2014.
8. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* **2022**, *11*, 630. [CrossRef]
9. Tanwar, S.; Gupta, N.; Iwendi, C.; Kumar, K.; Alenezi, M. Next Generation IoT and Blockchain Integration. *J. Sens.* **2022**, *2022*, 9077348. [CrossRef]

10. Rahman, M.S.; Islam, M.A.; Uddin, M.A.; Stea, G. A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges. *Internet Things* **2022**, *19*, 100551. [CrossRef]
11. Al_Barazanchi, I.; Murthy, A.; Al Rababah, A.A.; Khader, G.; Abdulshaheed, H.R.; Rauf, H.T.; Daghighi, E.; Niu, Y. Blockchain Technology-Based Solutions for IOT Security. *Iraqi J. Comput. Sci. Math.* **2022**, *3*, 53–63. [CrossRef]
12. Tsaur, W.J.; Chang, J.C.; Chen, C.L. A highly secure IoT firmware update mechanism using blockchain. *Sensors* **2022**, *22*, 530. [CrossRef]
13. Chauhan, C.; Ramaiya, M.K. Advanced Model for Improving IoT Security Using Blockchain Technology. In Proceedings of the 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 January 2022; pp. 83–89.
14. Sadeeq, M.M.; Abdulkareem, N.M.; Zeebaree, S.R.; Ahmed, D.M.; Sami, A.S.; Zebari, R.R. IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Acad. J.* **2021**, *1*, 1–7. [CrossRef]
15. Atlam, H.F.; Wills, G.B. IoT security, privacy, safety and ethics. In *Digital Twin Technologies and Smart Cities*; Springer: Cham, Switzerland, 2020; pp. 123–149.
16. Mohindru, V.; Garg, A. Security attacks in internet of things: A review. In Proceedings of the International Conference on Recent Innovations in Computing, Jammu, India, 20–21 March 2020; pp. 679–693.
17. Arshad, J.; Azad, M.A.; Abdeltaif, M.M.; Salah, K. An intrusion detection framework for energy constrained IoT devices. *Mech. Syst. Signal Process.* **2020**, *136*, 106436. [CrossRef]
18. Oh, S.R.; Kim, Y.G. AFaaS: Authorization framework as a service for Internet of Things based on interoperable OAuth. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720906388. [CrossRef]
19. Ahsan, T.; Khan, F.; Iqbal, Z.; Ahmed, M.; Alroobaea, R.; Baqasah, A.M.; Ali, I.; Raza, M.A. IoT devices, user authentication, and data management in a secure, validated manner through the blockchain system. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 8570064. [CrossRef]
20. Samuel, O.; Omojo, A.B.; Mohsin, S.M.; Tiwari, P.; Gupta, D.; Band, S.S. An Anonymous IoT-Based E-Health Monitoring System Using Blockchain Technology. *IEEE Syst. J.* **2022**, 1–12. [CrossRef]
21. Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
22. Li, X., Jiang, P., Chen, T., Luo, X., and Wen, Q; A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
23. Jyothilakshmi, K.; Robins, V.; Mahesh, A. A comparative analysis between hyperledger fabric and ethereum in medical sector: A systematic review. *Sustain. Commun. Netw. Appl.* **2022**, *93*, 67–86.
24. Zhao, Z. Comparison of Hyperledger Fabric and Ethereum Blockchain. In Proceedings of the 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, 14–16 April 2022; pp. 584–587.
25. Kushwaha, S.S.; Joshi, S.; Singh, D.; Kaur, M.; Lee, H.N. Systematic review of security vulnerabilities in ethereum blockchain smart contract. *IEEE Access* **2022**, *10*, 6605–6621. [CrossRef]
26. Six, N.; Herbaut, N.; Salinesi, C. Blockchain software patterns for the design of decentralized applications: A systematic literature review. *Blockchain Res. Appl.* **2022**, *3*, 100061. [CrossRef]
27. Sah, S.; Surendiran, B.; Dhanalakshmi, R.; Arulmurugaselvi, N. A Survey on Hyperledger Frameworks, Tools, and Applications. In *Internet of Things, Artificial Intelligence and Blockchain Technology*; Springer: Cham, Switzerland, 2021; pp. 25–43.
28. Dasgupta, K.; Rajasekhara Babu, M. A review on crypto-currency transactions using IOTA (Technology). In *Social Network Forensics, Cyber Security, and Machine Learning*; Springer: Singapore, 2019; pp. 67–81.
29. Shabandri, B.; Maheshwari, P. Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle. In Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 7–8 March 2019; pp. 1069–1075.
30. Schiller, E.; Niya, S.R.; Surbeck, T.; Stiller, B. Scalable transport mechanisms for blockchain IoT applications. In Proceedings of the 2019 IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium), Osnabruck, Germany, 14–17 October 2019; pp. 34–41.
31. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and iot integration: A systematic survey. *Sensors* **2018**, *18*, 2575.
32. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. An efficient selective miner consensus protocol in blockchain oriented IoT smart monitoring. In Proceedings of the 2019 IEEE International Conference on Industrial Technology (ICIT), Melbourne, Australia, 13–15 February 2019; pp. 1135–1142.
33. Petrut, I.; Oteşteanu, M. The IoT connectivity challenges. In Proceedings of the 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 17–19 May 2018; pp. 000385–000388.
34. Yu, F.; Rao, W.; Liu, C.; Wang, J.; Zhou, L. Architecture, Integrated Gateway Design, Furthermore, Performance Evaluation for High Concurrency Access of Power Internet of Things. *Mob. Inf. Syst.* **2022**, *2022*, 1260923.
35. Ellul, J.; Galea, J.; Ganado, M.; Mccarthy, S.; Pace, G.J. Regulating Blockchain, DLT and Smart Contracts: A technology regulator's perspective. *ERA Forum* **2020**, *21*, 209–220. [CrossRef]
36. Al Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]

37. Ouaddah, A.; Abou Elkalam, A.; Ait Ouahman, A. FairAccess: A new Blockchain-based access control framework for the Internet of Things. *Secur. Commun. Netw.* **2016**, *9*, 5943–5964. [CrossRef]
38. Yu, W.; Kose, S. A lightweight masked AES implementation for securing IoT against CPA attacks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2017**, *64*, 2934–2944. [CrossRef]
39. Boudguiga, A.; Bouzerna, N.; Granboulan, L.; Olivereau, A.; Quesnel, F.; Roger, A.; Sirdey, R. Towards better availability and accountability for iot updates by means of a blockchain. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 26–28 April 2017; pp. 50–58.
40. Miraz, M.H.; Ali, M. Blockchain enabled enhanced IoT ecosystem security. In Proceedings of the International Conference for Emerging Technologies in Computing, London, UK, 23–24 August 2018; pp. 38–46.
41. Naif, J.R.; Abdul-Majeed, G.H.; Farhan, A.K. Secure IOT system based on chaos-modified lightweight AES. In Proceedings of the 2019 International Conference on Advanced Science and Engineering (ICOASE), Duhok, Iraq, 2–4 April 2019; pp. 1–6.
42. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *J. Parallel Distrib. Comput.* **2019**, *134*, 180–197. [CrossRef]
43. Du, M.; Wang, K.; Liu, Y.; Qian, K.; Sun, Y.; Xu, W.; Guo, S. Spacechain: A three-dimensional blockchain architecture for IoT security. *IEEE Wirel. Commun.* **2020**, *27*, 38–45. [CrossRef]
44. Honar Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-layer blockchain-based security architecture for internet of things. *Sensors* **2021**, *21*, 772. [CrossRef]
45. Ahmed, I.; Zhang, Y.; Jeon, G.; Lin, W.; Khosravi, M.R.; Qi, L. A blockchain-and artificial intelligence-enabled smart IoT framework for sustainable city. *Int. J. Intell. Syst.* **2022**, *37*, 6493–6507. [CrossRef]
46. Bataineh, M.R.; Mardini, W.; Khamayseh, Y.M.; Yassein, M.M.B. Novel and Secure Blockchain Framework for Health Applications in IoT. *IEEE Access* **2022**, *10*, 14914–14926. [CrossRef]
47. Seyhan, K.; Nguyen, T.N.; Akleylek, S.; Cengiz, K.; Islam, S.H. Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security. *J. Inf. Secur. Appl.* **2021**, *58*, 102788. [CrossRef]
48. Tambe, V.; Bansod, G.; Khurana, S.; Khandekar, S. Reliability and availability of IoT devices in resource constrained environments. *Int. J. Qual. Reliab. Manag.* **2022**, *39*, 1648–1662. [CrossRef]