sensors

MDPI

Article

LBSS: A Lightweight Blockchain-Based Security Scheme for IoT-Enabled Healthcare Environment

Omar Said [1,2]

[1] Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; o.saeed@tu.edu.sa
[2] Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin Elkom 32511, Egypt

Abstract: Recently, global healthcare has made great progress with the use of Internet of Things technology. However, for there to be excellent patient care, there must be a high degree of safety for the IoT health system. There has been a massive increase in hacking systems and the theft of sensitive and highly confidential information from large health centers and hospitals. That is why establishing a highly secure and reliable healthcare system has become a top priority. In this paper, a security scheme for the IoT-enabled healthcare environment, LBSS, is proposed. This security scheme comprises three security mechanisms. The first mechanism is based on the blockchain technology and is used for transaction integrity. The second mechanism is used to store the healthcare system data in a secure manner through the distribution of its data records among multiple servers. The third mechanism is used to access the healthcare data after applying a proposed authorization test. To minimize the security overhead, the healthcare data is prioritized in regard to its importance. Therefore, each security mechanism has specific steps for each level of data importance. Finally, the NS3 package is used to construct a simulation environment for IoT-enabled healthcare systems to measure the proposed security scheme performance. The simulation results proved that the proposed healthcare security scheme outperformed the traditional models in regard to the performance metrics.

Keywords: blockchain; healthcare; IoT; IoT simulation; security; IoT security

check for updates

Citation: Said, O. LBSS: A Lightweight Blockchain-Based Security Scheme for IoT-Enabled Healthcare Environment. *Sensors* **2022**, *22*, 7948. https://doi.org/10.3390/s22207948

Academic Editor: Ju Wook Jang

Received: 9 September 2022
Accepted: 16 October 2022
Published: 18 October 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Healthcare can be defined as a large-scale ecosystem that includes many components, such as health insurance, medicine, health facilities, warehouses, robots, sensors, and more. Modern technologies have had the greatest impact on health practices and have transformed them from traditional practices to technological practices, such as monitoring human health using sensors and wearable devices such as smart watches and wristbands. This may be required for a group of patients, such as those with abnormal blood pressure or diabetes, who need periodic monitoring and rapid intervention by specialists to find quick and effective solutions [1,2].

The Internet of Things (IoT) technology connects a group of computers, tablets, mobile phones, and other devices that have a Central Processing Unit (CPU) to handle programs or applications. The main goal of IoT technology is to extend the function of the Internet in order to link the deaf things that are not equipped with CPUs, such as daily live tools, people, medical equipment, and other tracking sensors. Accordingly, there are many applications of IoT technology in various areas of life, such as the military, security, transportation, and economy. All of these fields contribute to the construction of smart cities, which leads to the promised goal of IoT technology, which is a smart world that considers the entire universe as one entity with autonomous management (i.e., without human intervention) [3].

There is a boom in the IoT market which is related to healthcare because of the presence of high-speed Internet. This leads to the creation of the appropriate conditions for healthcare

devices to work and operate in one big network as well as for the spread of sensors that support most healthcare devices and equipment. Furthermore, the medical environment is developed technologically and humanely to keep pace with this tremendous development in the information technology and artificial intelligence sectors. Moreover, devices and IoT applications that are gradually adapted to patients and healthcare workers are clearly increasing. Additionally, all components of healthcare, such as patients and doctors, benefit from IoT technology and its applications in monitoring, tracking, maintaining, treating, and more. The IoT-based healthcare system should cover many locations, which leads to a huge number of communicating devices that produce a massive number of gigabytes. The data produced are transmitted through many types of transmission media and processed by different types of users [4].

Sharing data within healthcare systems that are based on IoT technology is an important issue. In these systems, the data is usually shared through cloud-computing technology. Patient data is collected and uploaded to the cloud and is then available to users. Subsequently, it is distributed to authorized persons, such as specialists and administrators, according to the type of data and patients. After that, an initial diagnosis is proposed and then a treatment is prescribed where errors, which may arise because of the manual writing of data, are eliminated. Afterward, data may be sent or received in a real-time manner, if required, through the cloud-computing servers. Because of the presence of sensitive data on the cloud, it may be insecure for several internal or external reasons. For example, the authorized persons to manage the health data centers may be dishonest and tamper with this data. Therefore, there were great security challenges for healthcare systems that depend on the IoT technology, which has unique specifications such as a massive number of terabytes of data, a large number of cloud-computing servers, their extension in many locations, and a large number of users and huge transactions that may have occurred for health data within a short period [5]. The main contributions of this work:

- Apply blockchain technology for data transaction integrity in the IoT-enabled healthcare environment;
- Propose a security mechanism for data storing in the IoT-enabled healthcare environment;
- Propose a security mechanism for data access in the IoT-enabled healthcare environment;
- Construct a simulation for the IoT-enabled healthcare environment and examine the efficiency of the proposed security scheme;
- Finally, show and discuss the simulation results.

The organization of the paper is stated as follows: Section 2 introduces the related works. Section 3 demonstrates the design of the proposed security scheme. Section 4 presents the simulation construction in addition to the discussion of the results. Finally, the paper is concluded in Section 5.

2. Related Works

This paper focuses on the security issue for IoT-enabled healthcare environments. The research, which is related to healthcare and blockchain, is evaluated regarding four main factors. The first factor is “IoT Representation (IoT Rep.)”, which evaluates if the related work represented the IoT environment accurately. The second factor is “IoT Suitability (IoT Sut.)”, which evaluates if the related work was suitable for the IoT environment. The third factor is “Security Weakness (SW)”, which evaluates if the related work had security weakness(es). The fourth factor is “Review (Rev.)”, which means that the related work was just a review article. The related works are evaluated and categorized in Table 1.

Table 1. Summary of the related works.

Authors	Year	Ref.	Contributions	Limitation Factors			
				IoT Rep.	IoT Sut.	SW	Rev.
Wang et al.	2020	[6]	Proposed a security mechanism for healthcare systems. This mechanism combined the edge cloud and IoT technologies to secure the retrieval of data.	✔	✘	✔	✘
Fotouhi et al.	2020	[7]	Introduced an authentication scheme to prevent attacks targeted at wireless body area networks.	✔	✘	✘	✘
Wang et al.	2020	[8]	Demonstrated a parallel healthcare system in which the blockchain technology and care auditability were applied.	✔	✘	✘	✘
Ismail et al.	2019	[9]	Introduced a blockchain system for healthcare environments. It divided the network into clusters to apply its security model.	✔	✘	✔	✘
Haghparast et al.	2020	[10]	Proposed a security framework for IoT-based e-health systems. This framework consisted of four layers of sensors. Each layer achieved function(s) from the framework target.	✔	✘	✘	✘
Gupta	2017	[11]	Demonstrated a generalized architecture for the security and management of cloud servers in IoT healthcare systems. It divided the cloud centers into three categories to guarantee the secure communication of information.	✔	✘	✘	✘
Ning, et al.	2021	[12]	Demonstrated a blockchain framework for distributed traffic management in transportation systems. It analyzed this framework into two sub-problems to decrease its complexity.	✔	✘	✔	✘
Lakhan et al.	2022	[13]	Identified and ensured the fraud of medical data in addition to privacy preservation at local fog nodes and clouds, with minimum delay and energy consumption.	✔	✘	✔	✘
Manoharan et al.	2022	[14]	Presented a model to analyze the biomedical signals behavior and complete the output tracking mechanism of the transceiver results with low power consumption.	✔	✘	✔	✘
Selvarajan, et al.,	2022	[15]	Introduced a system to minimize the loss of functionalities in the biomedical signals. Additionally, an activation function was presented in the middle stage.	✔	✘	✔	✘
Anitha et al.	2021	[16]	Proposed a security method that detected the replication attack. This security method was for the healthcare system, which was based on a Wireless Sensor Network (WSN).	✘	✔	✔	✘
Benil et al.	2020	[17]	Demonstrated a security scheme to verify and audit medical cloud servers using blockchain technology.	✘	✔	✘	✘
Kong et al. [11]	2019	[18]	Introduced a security model using a neural network and the pre-classification of health data and dynamic gaming theory.	✘	✔	✘	✘
Wang et al. [12]	2020	[19]	Introduced a security framework used to evaluate the security specs of Internet of Health Things (IoHT).	✘	✔	✘	✘

Table 1. *Cont.*

Authors	Year	Ref.	Contributions	Limitation Factors			
				IoT Rep.	IoT Sut.	SW	Rev.
AbouNassar et al.	2020	[20]	Proposed a security model based on blockchain technology. It used a smart contract to enhance the Trustworthy Factor (TF) and establish trustworthy communications in the IoHT infrastructure.	✘	✔	✘	✘
Kavitha et al.	2019	[21]	Introduced a security framework to deal with the security flaws of the personal data records, which were found in healthcare systems. It used the hyperelliptic curve-based public key cryptosystem instead of the traditional cryptographic framework to ensure the group communications were secure.	✘	✔	✘	✘
Tai	2019	[22]	Introduced a security model for IoT healthcare data in which the control operations for the IoT system were adjusted and the user anonymity is considered to introduce an authentication model. Additionally, the control system for IoT has the ability to ensure reliable e-Health services.	✘	✔	✔	✘
Pawar et al.	2018	[23]	Demonstrated a system model that was based on the blockchain technology to manage the health data that were obtained from the medical devices.	✘	✔	✘	✘
Hasanova, et al.	2022	[24]	Presented an algorithm that was based on machine learning technology to predict heart diseases using the blockchain data.	✘	✔	✘	✘
Marwan et al.	2018	[25]	Proposed a security method to prevent unauthorized users from accessing healthcare records. This method used machine-learning technology.	✘	✘	✔	✘
Ding et al.	2019	[26]	Introduced a security system that handles the limited capabilities of sensors. It also verified data integrity and reduced the computation overhead cost.	✘	✘	✔	✘
Li et al.	2020	[27]	Introduced a framework to apply the blockchain technology to guarantee secure data sharing in addition to computing the sensitive data of patients.	✘	✘	✔	✘
Vedaraj et al.	2020	[28]	Provided an effective security framework for the health data in addition to predicting the patients' diseases. Additionally, it can encrypt and decrypt using a special security algorithm.	✘	✘	✔	✘
Wang et al.	2021	[29]	Introduced a system to quantify the freshness of information using critical-level changes. It was an optimized problem of minimization of the Age-of-Critical-Information (AoCI). Furthermore, an information-aware heuristic algorithm was introduced.	✘	✘	✔	✘

Table 1. *Cont.*

Authors	Year	Ref.	Contributions	Limitation Factors			
				IoT Rep.	IoT Sut.	SW	Rev.
Ning, et al.	2021	[30]	Used Unmanned Aerial Vehicles (UAV) to investigate Multi-access Edge Computing (MEC) that considered edge server deployment and offloading computation. Moreover, two learning algorithms were demonstrated to reach the Nash Equilibrium (NE).	✘	✘	✔	✘
Zarour et al.	2015	[31]	Introduced a study to determine the impact of using blockchain technology on the healthcare system from groups of experts and specialists.	✘	✘	✘	✔
Sharma et al.	2022	[32]	Introduced a literate review of the relationship between the blockchain technology, IoT technology, and the healthcare system.	✘	✘	✘	✔

3. Proposed Security Scheme

The proposed security scheme provided three security mechanisms: integrity, confidentiality, and availability. The integrity mechanism ensures that the healthcare data transactions are accomplished correctly; see Section 3.1. The confidentiality mechanism guarantees that those authorized to do so can only access sensitive healthcare data. The availability mechanism guarantees that the healthcare data should be available to those who need it; see Figure 1. For confidentiality and availability, see Section 3.2.

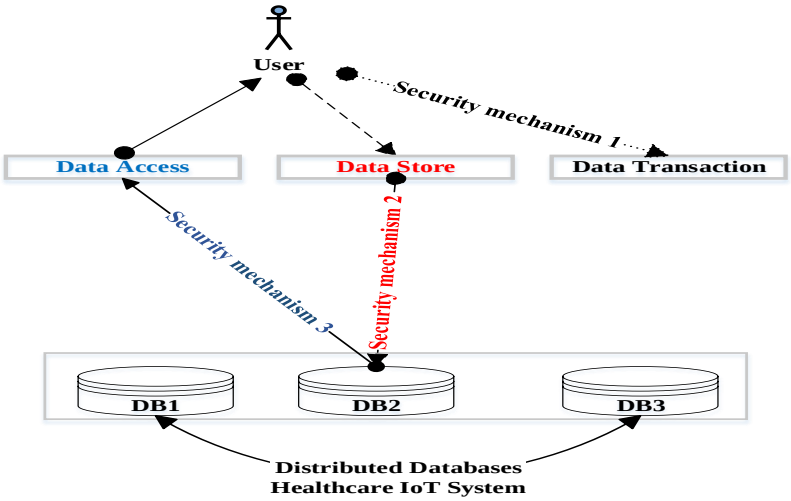


Figure 1. The three mechanisms of the proposed security scheme.

One of the challenges of IoT technology is scalability, which causes a huge number of heterogeneous things to suddenly join or leave this environment in addition to a massive number of terabytes of exchanged data within short periods. To face these challenges in the proposed security scheme, the IoT-based healthcare system is divided into many clusters. Each cluster may comprise heterogeneous or homogenous things (devices, tools, and users). The clustering process is achieved based on available network resources, size and type of transmitted data, number of things, and the level of importance of things and data. The clustering process, which is based on constructing a clustering-based attribute selection scale after partitioning the training sample into a number of clusters, is described in [33].

In the sections below, the three mechanisms are discussed in addition to mathematical notations.

3.1. Integrity

The healthcare system comprises different types of things. Each thing has a type of exchanged data. Therefore, the healthcare environment has many types of data with different levels of importance. Hence, healthcare data is classified into many levels depending on its importance such that each level can be handled with different procedures [34]. This concept can lead us to the core idea of the proposed integrity factor, and the blockchain technology is used to ensure that each transaction is correctly verified. First, each transaction can be stored as a block, each containing the hash function of the previous block. In case any transaction needs to be added to the chain, it should be verified by a group of persons which are called "miners". There are many mechanisms to prove the transaction, such as Proof of Work (PoW), Proof of Stake (PoS), and others [35]. As stated previously, the main challenge with the healthcare system based on IoT technology is the terabytes of data (stored, exchanged, and processed). This makes the use of one transaction verification mechanism so difficult (if not impossible). So, in the proposed blockchain mechanism, a mixture of transaction verification mechanisms is applied depending on the type of healthcare data (i.e., importance level). For more clarification, the proposed model classifies the healthcare data into "N" levels of importance such that the first level is assigned to the most important level of data, the second level is assigned to the next level of importance, and so on. This provides flexibility to create other levels of importance, especially for an IoT-based healthcare system. For an accurate determination of the importance of healthcare data, the data type should be combined with the thing's state. For example, in case of danger, a patient's status, such as cancer patients, prescriptions, and prescription changes, will have to be completed in an accurate manner and under the supervision of an expert (i.e., in most cases specialists are necessary but insufficient). On the contrary, a patient undergoing a simple general surgery must have accurate anesthesia calculations.

To clarify the model idea, three levels of importance are used and applied for data and things. These three levels of importance are critical, middle, and traditional. The first level of importance is assigned to the data package, which comprises the critical things described by critical data. The second level of importance is assigned to the data package, which comprises the critical things that are described by the data of middle importance in addition to the critical data, which is related to the things of middle importance. The third level of importance is assigned to the data package, which comprises the things of middle importance that are related to the data of middle importance, the data of middle importance that is related to the traditional things, the things of middle importance that are related to the traditional data, and the traditional data that is related the traditional things; see Figure 2.

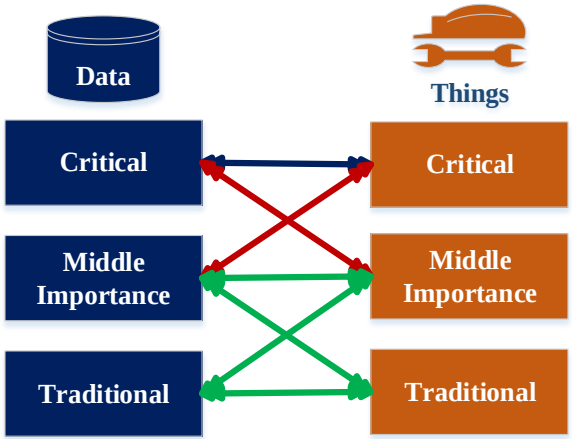


Figure 2. The levels of data importance for data combined with things.

The importance level of data may be changed by a time period. For example, the timing of blood pressure measurement for a hypertensive patient is sometimes crucial. This is because it can be performed as a routine or considered an important issue to the

point where it may save this patient from death. In addition, a certain result from forensic medicine may be used in court and change the direction of judgment, or it may be used only for experiments.

The classification of things and data should be achieved by a high-level committee which is constructed by an elected administration in the healthcare system. The output of the classification process may be changed by a change of committee or over time. Changing the specialists' committee may affect the outcome of the classification process because each specialist has a point of view about the importance of things and data. For example, there are specialists who consider the data of the medical analysis for a particular disease to be very important, and other specialists may consider this data as traditional. In addition, the time factor is important in changing the result of the classification process, as some data at a certain time can be considered important, while the same data at another time may become unimportant. Therefore, the process of things and data classification may be dynamically changed.

Each level of importance should have a group of miners. These miners can be elected, or it is possible to appoint them according to the protocol or regulations at the hospital. For example, the head of the oncology department, the head of the narcotics department, the director of the hospital, the head of the mental health department, the physician, and the pharmacist in charge of drugs in the hospital may be considered miners who verify the drug transactions. This idea provides scalability, which is one of the challenges of blockchain such that, in case of an extension of healthcare data, the number of miners should be decreased to include the most experienced specialists and high-level managers for critical cases. To differentiate between the old security systems, which verify the transaction through all the available miners, and our proposed scheme, the miners should be selected from different organizations in various locations. This miner selection rule came from IoT envisioning (i.e., the healthcare system that is based on IoT technology transforms many health organizations into one large organization to provide an advantage in selecting miners from different countries, which gives the transaction verification process more credibility and security; see Figure 3). As stated in the bitcoin blockchain system [36], the data is divided into blocks. Each block comprises a group of control fields in addition to the data. One of the most important fields in the data block is the hash function. Each data block has a hash function from the previous block. In the proposed scheme, a hash function is used to condense each transaction.

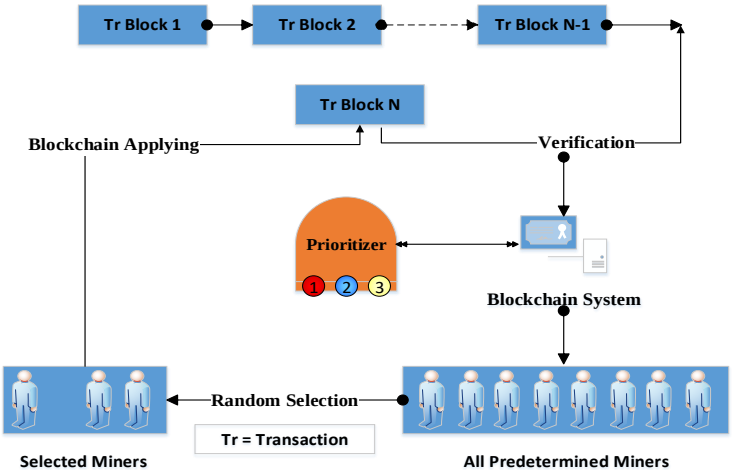


Figure 3. Data priority center, data blocks, and miners' relationship.

This function is complex because it consists of a number of simple hash functions. The complexity degree of the hash function depends on the data importance level on which the transaction took place. The number of simple hash functions equals the number of miners who are authorized to check the transactions. Every miner provides the system with its simple hash function in case of their agreement on the transaction.

The completion of the approval by all of the miners means that the simple hash functions are collected to create the complex hash function which, in turn, is used to test whether the transaction is accepted or not. If one miner does not pass the transaction, then their simple hash function is not sent to the security system. Therefore, the complex function will be considered incomplete, which means the transaction is rejected. There is a complex hash function that is assigned to each transaction block such that each miner uses a different simple hash function to test the current transaction and access the old complex hash functions in addition to their old simple hash functions to review the old transactions; see Figure 4. The simple and the complex hash functions are created using the "Hash Function Creator" component. For further description, see Algorithm 1.

Algorithm 1: Transaction Integrity

D_I Data Importance
L Importance Level
n Number of Importance Levels
H_{Tr} Hashed Transaction
H_C Complex Hash
m Number of Minors
H_S Simple Hash
SS Security Server

Algorithm Begin

1: D_I = L[i], 1 < i < n
2: For i = 1 to L
3: Begin
4: $H_{Tr} = H_C[i](T_r)$
5: $H_C[i] = \sum_{j=1}^{m} H_S[j]$
6: For j = 1 to m
7: $m_j \rightarrow H_S[j]$
8: While (T_r)
9: Begin
10: $m_j \rightarrow H_S[j] \rightarrow SS$
11: $SS = H_S[j] + H_S[j+1] \ldots H_S[m]$
12: IF $SS = \sum_{j=1}^{m} H_S[j]$
13: $T_r \rightarrow Succeed$
14: Else
15: $T_r \rightarrow Failed$
16: End
17: End
18: **End Algorithm**

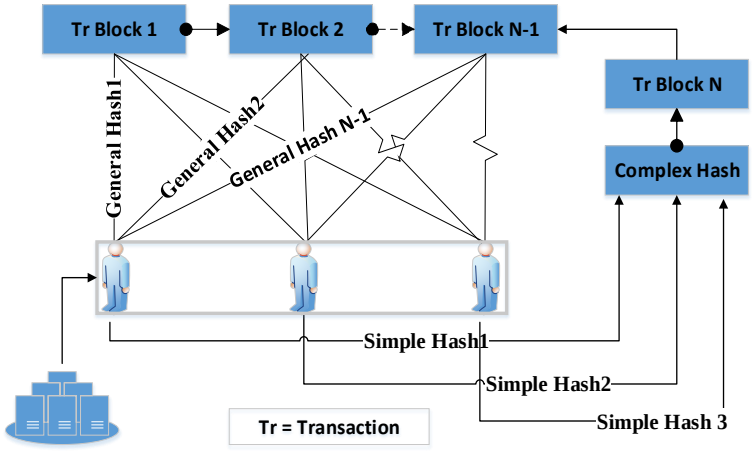


Figure 4. Using simple and complex hash functions.

3.2. Confidentiality and Availability

One of the most important security issues in the healthcare system is the protection of data from unauthorized viewing or accessing. Additionally, the proposed security scheme should guarantee, for authorized users, access to the system's resources. In traditional healthcare systems, the data that belongs to a healthcare organization is stored on its servers as complete units, which means that everything related to a specific patient is stored as a group of records in one storage database unit. This means any breach in the security system may allow access to patients' records. To avoid this security weakness, the proposed scheme used the data fragmentation idea. The patient's data is transformed into a group of records, and each patient record is divided into a group of blocks. These blocks are distributed by the "distributer" component over different servers inside or outside of the organization; see Figure 5.

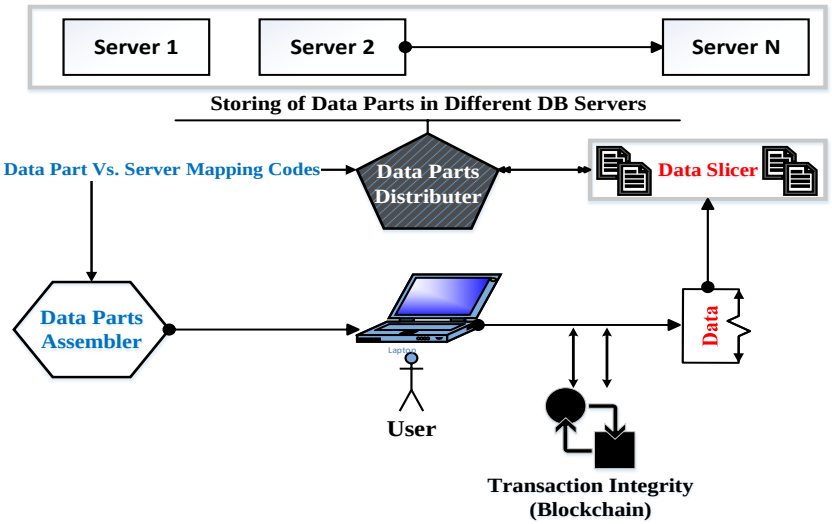


Figure 5. The general view of data distribution over servers.

To decrease the overload of the proposed mechanism—in the case of lower-importance data—its records will be directly distributed over the database servers without transformation into blocks. Therefore, the "prioritizer" component should be consulted to determine what will be conducted in the data fragmentation by the "slicer" component; see Figure 6. The function of the "prioritizer" component is achieved using the technique stated in [37] which used the queueing theory by assigning one queue for each importance level. The data in each queue is processed depending on available resources in the entire system.

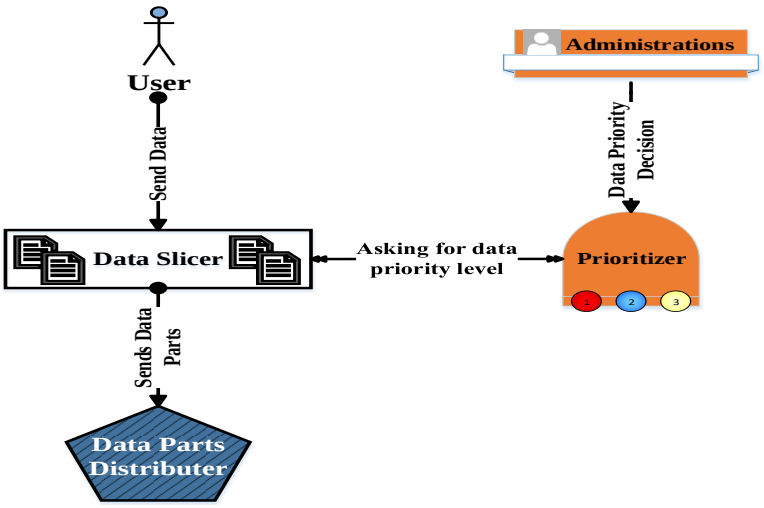


Figure 6. Prioritizer and slicer relationship.

Each block of data comprises a stamp of its related patient. This stamp may be a picture, a number, or a symbol. The process of choosing the stamp type should take into account that it does not represent an excessive overload on the packet or increase its complexity. This stamp is dynamically exchanged depending on the network status (i.e., available resources). Therefore, the stamp may be first selected as a number. Then, its difficulty is increased by the selection of a more complex form, such as a group of characters. After that, it is transformed into a picture and may be returned to a simple form again. This stamp is used by the "assembler" component to collect the data record after its fragmentation. The "assembler" data is encrypted. The request to access data is sent to the administrator, who, in turn, contacts the "prioritizer" asking about the importance level of the required data. Then, the administrator determines the requirements for this data to be accessed. After that, the administrator contacts the user asking about the required data authorization. Regarding the correct input of the data authorization, the administrator contacts the "assembler" to collect the data and sends it to the intended user; see Figure 7. Communication between the components of the proposed security scheme is achieved using management messages. The structure of these messages is similar to the messages of the Simple Network Management Protocol (SNMP) [38]. Each management message is simple. It comprises the source and destination IP addresses in addition to the required fields such as variables and their values. These management messages are encrypted. In the event of network starvation, the number of management messages will be decreased until the network is returned to its normal status. There are two types of management messages. The first type is called "query" and is used to access specific variables' values. The second type is called "response" and is used to send specific data to one or more scheme components.

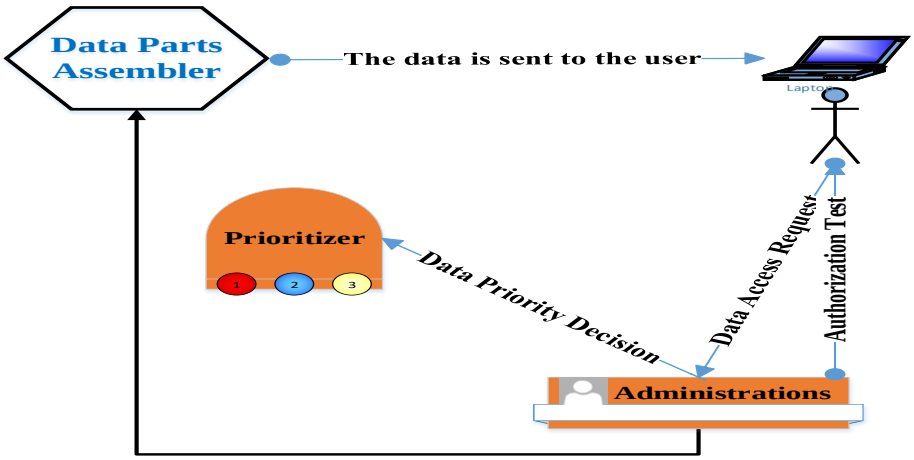


Figure 7. Healthcare data access mechanism.

The authorization data is directly related to its importance level (i.e., the authorization data is changed by adjusting the importance level). The application of this idea in our proposed security scheme can be stated as follows: Each data block (or record) comprises a digital signature of the authorized users. When the authorized user needs to access a healthcare data record, the system should receive the digital signature of that user. To be more accurate, as stated previously, there are several levels of importance for healthcare data. Therefore, each level of importance for the data will have a different security mechanism that should be applied for an access request. In the case of data with a high degree of importance, all users' electronic signatures must be required to access such data. Hence, the user who sends an access request either enters all of the digital signatures for the users who are authorized to access this type of sensitive data, or this user has a prior authorization deed from those users.

In the same way, electronic signatures will be reduced according to a reduction in the level of importance for the required data. Additionally, each user should determine

his/her security behavior, defined by the regular steps that are mostly accomplished within a specified time [39]. This security behavior will be applied as an additional security step for the most important data. So, if the unauthorized user tries to access data and knows the digital signatures of all of the authorized users related to that data, this unauthorized user does not have knowledge of their regular behaviors.

3.3. Mathematical Notations

This mathematical notation is based on [40]. Suppose that the number of miners equals "M", where "L" is the number of levels of importance. The contents of each data block "D_C" are determined using Equation (1), where "B^{Prev}" is the previous block, "H" is the hash function, "TS" is the timestamp (current time), "b" is the work proof difficulty, and "G" is the target. The "Merkle tree" and "nonce" are omitted from the contents of the block. This is because the time required to test the transaction depends on the predetermined number of miners with simple hashes created by the proposed security scheme. The validity of the transaction "T_V" is determined by Equation (2), where "P" is the number of blocks revised by the miners. The time required to add one transaction into the chain "T_T" is determined by Equation (3). The consumption time "C_T" is to ensure all system transactions are determined using Equation (4), where the number of transactions equals "T". The miner is selected from a group of predetermined persons. Additionally, $MN_L[i]$ is the set of miners, and "MNS" is the selected miners. The miners "M_S" are determined using Equation (5).

$$D_C = (H(B^{Prev\ [a]}) \oplus TS(t) \oplus b) \leq G, 1 < a < P \tag{1}$$

$$T_V = \sum_{P=1}^{D} \sum_{j=1}^{M_i} H_j \left(\left(H\left(B^{Prev} \right) \oplus TS(t) \oplus b \right) \right),\ 0 < i < L \tag{2}$$

$$T_T = P * \sum_{j=1}^{M_i} T_j \tag{3}$$

$$C_T = \sum_{k=1}^{L} \sum_{j=1}^{T} (P_k * \sum_{i=1}^{M} T_i) \tag{4}$$

$$M_S = \frac{P(MN_L[i]) * P(MN_L[i]|MNS)}{P(MN_L[i])} \tag{5}$$

4. Simulation and Evaluation

The simulation construction process for the healthcare environment, which is based on IoT technology, is demonstrated in the first section. Additionally, the results of the simulation are shown and discussed in the second section.

4.1. Simulation Infrastructure

The main challenge with IoT-based healthcare systems is how to represent the nature of the IoT environment. So, the simulation, stated in [41], is the most suitable to reflect the real specification of the IoT environment. This is because it comprises a presentation of three main networks: WSN, Radio-Frequency Identification (RFID), and Mobile Ad hoc Network (MANET). These networks communicate with each other using the Internet, which is also demonstrated. Moreover, this simulation used two alternative coverage methods: satellite and High-Altitude Platform (HAP). These coverage methods are used in case of limitation in the Internet coverage for a group of things. This will provide the healthcare system with representation flexibility through the consideration of the many heterogonous things that are found at many locations with a guarantee that these things will be communicated, even if they are passive things. The simulation scenario, in addition to the parameters' values for the networks and coverage tools, is stated in Figure 8.

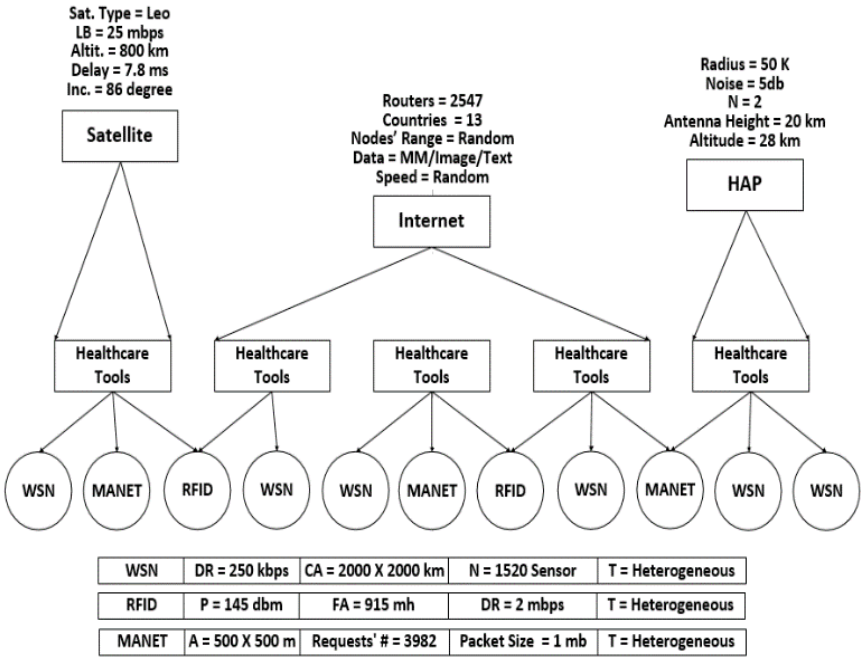


Figure 8. Simulation scenario with networks and coverage tools parameters.

The communication between different packets' header formats, which are raised due to the usage of different network types, is achieved using the packet transformation idea. Simply, this idea is discussed as follows: encapsulate the received packet with the header that is suitable for the received node. Hence, this node can translate this packet. In the event that the next node has the same type as its previous node, the additional header will remain (i.e., no encapsulation). However, if the next node is different, the header will be de-capsulated and another header will be added in the event that the received node is a new one.

The simulation model, which is used to measure the performance of the proposed security scheme, represented the nature of the IoT environment and is considered the first part of the simulation infrastructure. So, some changes are added to this simulation model to complete the representation of the real nature of healthcare systems, which is considered the second part of the simulation infrastructure. These changes are concluded in Table 2. The selected healthcare devices are the most common ones, such as surgery robotics and glucose monitoring for medical devices, laptops, and barcode readers and monitoring for inventory as well as chemical devices and laptops for pharmacy. Each device can be considered passive or active. The passive things are the things that are not supported by a CPU. However, the active things can connect to the Internet (or any other coverage tool) without additional hardware support. Furthermore, the third part of the simulation infrastructure is related to the representation of security specifications, which are stated in Table 3. The simulation of medical devices is taken from [42–44]. Notably, most of the healthcare security parameters are random, ranged values for an accurate representation of the IoT environment.

Table 2. Represented healthcare tools in the simulation environment.

Part	Description	Used Network
Patients	Wearable devices (glucometer, fitness bands, heart rate monitoring cuffs, ingestible, and blood pressure), RFID tags, mobiles, and smart watches	WSN and RFID and MANET
Physicians	RFID tags, mobiles, sensors (monitoring and medical), clothes, cars, keys, sonar, surgical tools, laparoscopes, respiratory devices, emergency devices, etc.	WSN and RFID and MANET
Inventories	RFID tags, sensors (weight, temperature, motion, monitoring, and humidity), cargo, lamps, workers, books, offices, etc.	WSN and RFID
Pharmacy	RFID tags, sensors (temperature, touch, motion, monitoring and humidity), mobile applications, refractometer, thermometer, microscope, vacuum oven, etc.	WSN and RFID and MANET
Insurance Company	RFID tags, sensors (temperature, monitoring, and touch), and selected insurance company devices	WSN and RFID

Table 3. Security simulation parameters.

Part	Description
Hash	Secure Hash Algorithm (SHA)-256
Block size	1 MB
Number of clusters	Random (10 to 100)
Cluster size	Random (50 to 100)
Total number of miners	Random (10,000 to 200,000)
Number of selected miners	Random (10 to 50)
Number of blocks	Random (144 to 288)
Importance of block	Random (1/2 H: 1/4 M: 1/4 L)
Number of digital signatures	Random (1 to 10)
Total number of nodes	Random (20,000 to 40,000)

4.2. Results and Discussion

The performance metrics are processing time, the number of miners, average energy consumption, average throughput, average end-to-end delay, packet loss ratio, the access time of healthcare data records, and rate of change between data blocks with different levels of importance. The simulation results of LBSS are compared with the Leila's model and the Bitcoin model [19,31]. The Bitcoin model was chosen to compare its results with the results of the proposed security scheme because it is one of the most important models that uses the blockchain technology. In addition, the Leila's model was chosen because it is the closest related work to our proposed security scheme.

The processing time performance metric can be measured using a consumption time to validate the transactions, which are represented by blocks in the blockchain system. Figure 9 shows the processing time results for the security scheme, the Leila's model, and the Bitcoin model. The x-axis represents the number of blocks (transactions) and the y-axis represents the processing time (seconds). Notably, LBSS has the lowest processing time values. The Leila's model and the Bitcoin model rank after LBSS. This is explained by the classification of healthcare data into many levels of importance, which decreases the data processing requirements and leads to reduced time consumption.

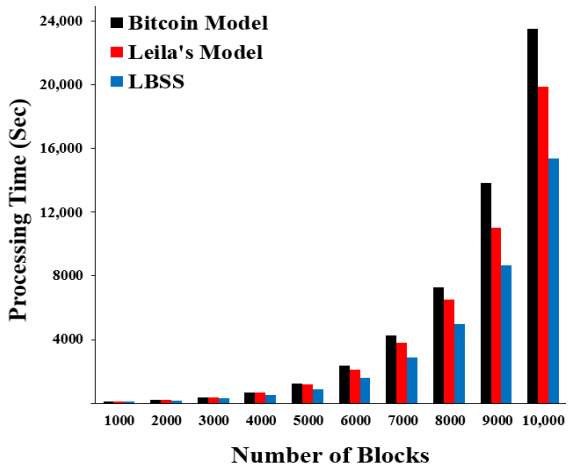


Figure 9. Processing time for transaction integrity.

The number of miners performance metric is measured for LBSS and the Bitcoin model. This is because the number of miners metric for the Leila's model has the same behavior as the Bitcoin model. This performance metric is measured using the calculation of the average number of miners, which are used to validate the data transactions. Figure 10 shows the result of the changing miner performance metric. The x-axis represents the simulation time in minutes divided by ten and the y-axis represents the number of miners divided by 10^4. The number of miners in the proposed security scheme is less than that of the Bitcoin model. This is because the data classification minimizes the number of miners in case there are less important data transactions.

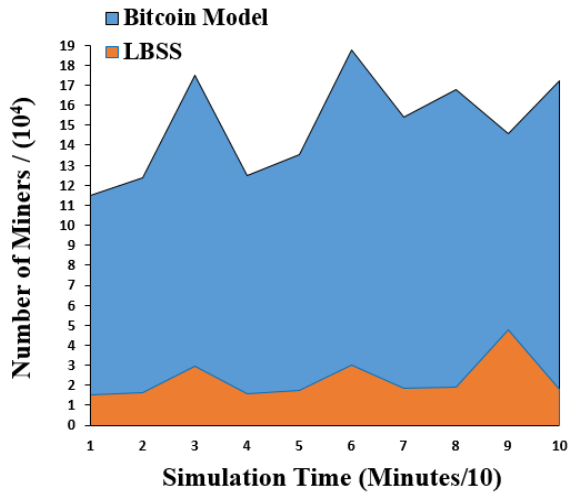


Figure 10. Changing the number of miners over a time.

The energy consumption performance metric is measured by the average of the energy consumption values for the energy-based healthcare things in the IoT environment. This performance metric determines the effect of the proposed scheme on the energy-based nodes. Figure 11 shows the results of the energy consumption. The x-axis represents the simulation time in minutes divided by ten and the y-axis represents the average of the energy consumption in "Joules". The plot of LBSS has the lowest values for energy consumption within the simulation time. The Leila's model and the Bitcoin model come after the proposed security scheme, respectively. This is explained by the availability of LBSS to decrease the overhead computations, which lower the energy consumption rates.

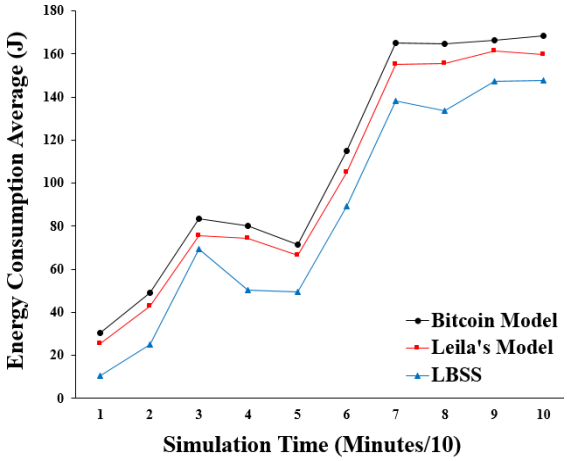


Figure 11. Energy consumption average.

The throughput performance metric is measured by calculating the size of the data, which is transmitted and received correctly. This performance metric also reflects the effect of the proposed security scheme on the efficiency of the IoT environment because, if the proposed scheme causes a computation overload on the healthcare system, the first metric that will be affected is the size of the correct transmitted data. Figure 12 shows the results of the throughput. The x-axis represents the simulation time in minutes and the y-axis represents the average throughput in "kb/s." divided by 10^7. Notably, the throughput plot of LBSS has the highest values compared with that of the Leila's model and the Bitcoin model. This is explained by the ability of the proposed security scheme to reduce the number of computations when there is an occurrence of bottlenecks or collisions. Additionally, both the clustering idea and the number of miners affect the throughput performance metric. The clustering idea, which is applied to LBSS and the Leila's model, reduces their complexity and increases their throughput. However, in LBSS, reducing the number of miners leads to a reduction in the number of transmitted messages, including messages related to the security system. It also leads to a decrease in the negative impact of hash functions' usage that contributes to an additional increase in the throughput, which was not present in other models. Furthermore, classifying healthcare data into several levels of importance is considered the main factor in determining the behavior of LBSS and making it more flexible.

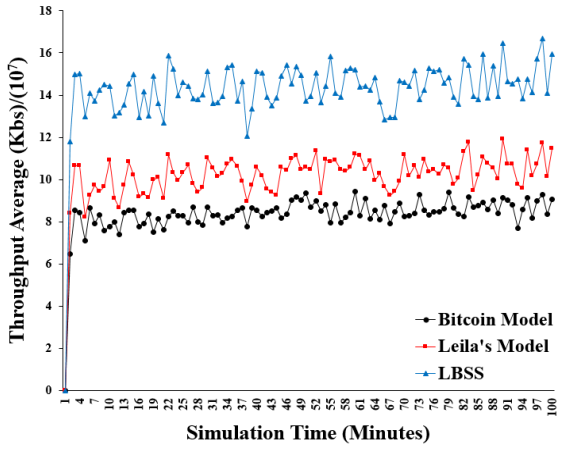


Figure 12. Throughput average.

End-to-end delay is an important performance metric to make sure that the proposed security model does not negatively affect the entire IoT system efficiency. This metric is measured by the calculation of the average of queuing, processing, and transmission delays. Figure 13 shows the end-to-end delay results. The x-axis represents the simulation

time, and the *y*-axis represents average end-to-end delay. Notably, the end-to-end delay values for the proposed security scheme are less than both the Bitcoin and Leila's models. In addition, the Bitcoin model has the largest end-to-end delay. This is explained by the flexibility of the proposed scheme to decrease the number of security messages in case of network starvation. However, the complexity of the Bitcoin model is so high that it has negatively affected the IoT-based healthcare environment and increased the average end-to-end delay.

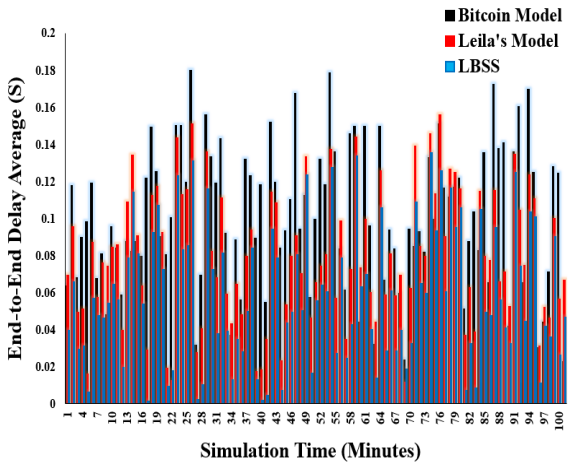


Figure 13. End-to-end delay average.

Packet loss is also a very important performance metric to measure the efficiency of the IoT-based healthcare system. This metric is measured by the ratio of packets that are lost during the transmission process to the total number of sent packets. Figure 14 shows the packet loss ratio results. The *x*-axis represents the simulation time in minutes divided by ten. The *y*-axis represents the packet loss ratio values. Notably, the packet loss ratio for the proposed security scheme is less than that of both the Leila's and Bitcoin models. This also reflects the efficiency of the proposed security scheme to dynamically change its behavior depending on the network status.

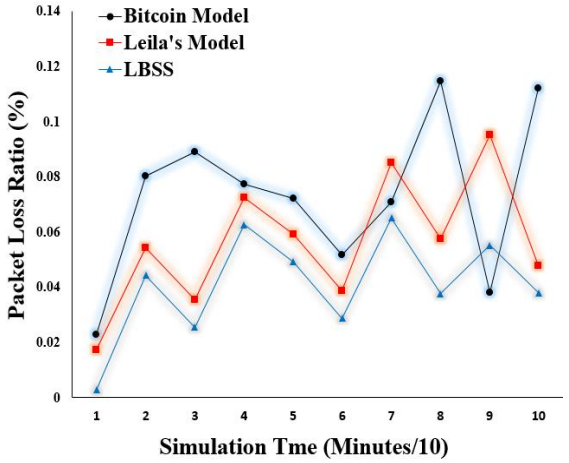


Figure 14. Packet loss ratio.

The access time performance metric equals the average consumption time that is required to access healthcare data. This metric measures the performance of the data access mechanism, which is proposed in LBSS. Therefore, it is measured for LBSS and compared to the Leila's model. Figure 15 shows the results of the access time performance metric. The number of data blocks is ranged from 1000 to 10,000 and the access time is ranged from zero to 9000 "ms". The access time for the proposed security scheme is less than that of the

Leila's model. This is because the variety of security actions that are executed depends on the level of data importance and type of things.

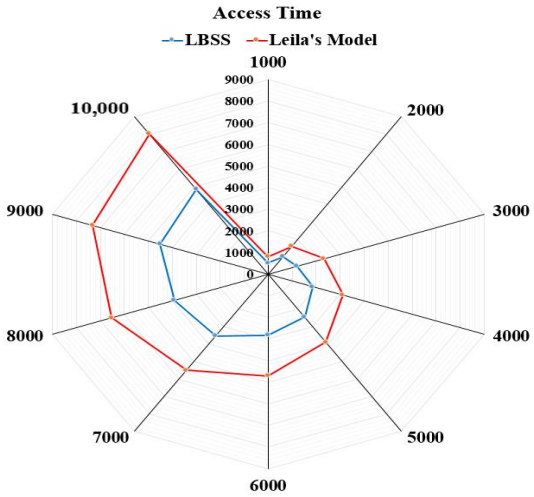


Figure 15. Average consumption time that is required to access healthcare data.

For the transactions with data performance metrics that have different importance levels, they are measured by the number of transactions which occurred for different levels of data importance: high, medium, and low. This is measured to ensure that the changes between the level of data importance work effectively. Figure 16 shows the results of this performance metric. The *x*-axis represents the simulation time in minutes divided by ten and the *y*-axis represents the number of transaction blocks.

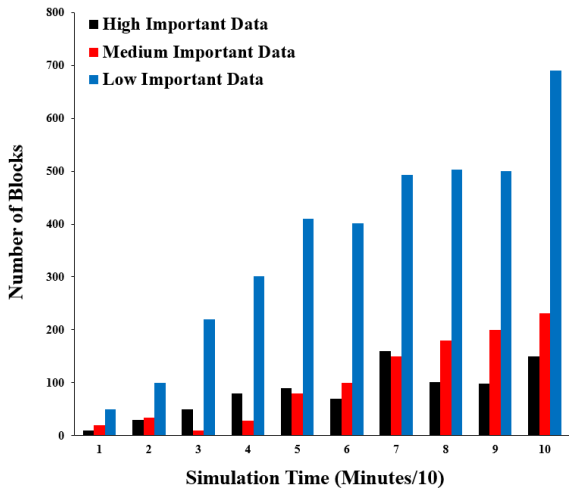


Figure 16. Number of transactions with different levels of importance.

The importance levels are distributed between high, medium, and low. Additionally, the number of transaction blocks is mostly arranged in ascending order: low, medium, and high. In the few simulation time points, the high importance level increases the medium importance level, which reflects the real nature of the healthcare environment and comprises occasionally important data.

As shown in Table 4, the simulation results proved that the proposed security scheme, LBSS, outperformed the performance of the related models, the Bitcoin model and the Leila's model.

Table 4. Conclusion of LBSS enhancements compared to both of the Leila's and Bitcoin models.

Performance Metric	Enhancement
The average processing time for transaction integrity	Decreased by ≈ 22.727% ↓—Leila's model. Decreased by ≈ 34.349% ↓—Bitcoin model
The changing rate of miners	Decreased by ≈ 84.821% ↓—Bitcoin model.
The energy consumption average	Decreased by ≈ 15.752% ↓—Leila's model. Decreased by ≈ 21.367% ↓—Bitcoin model.
The average throughput	Increased by ≈ 28.643% ↑—Leila's model. Increased by ≈ 41.347% ↑—Bitcoin model.
The end-to-end delay	Decreased by ≈ 25.865% ↓—Leila's model. Decreased by ≈ 42.171% ↓—Bitcoin model.
The packet loss ratio	Decreased by ≈ 27.404% ↓—Leila's model. Decreased by ≈ 43.880% ↓—Bitcoin model.
The access time for the healthcare data blocks	Decreased by ≈ 39.189% ↓—Leila's model.

5. Conclusions

In this paper, a security scheme, LBSS, was proposed for the IoT-enabled healthcare environment. The proposed security scheme deployed blockchain technology to enhance integrity, confidentiality, and availability. Therefore, the healthcare data found in the blockchain was difficult (if not impossible) to access, change, and store without notification and consensus from the all the miners using simple and complex hash functions. Additionally, the proposed scheme was lightweight because its complexity was decreased or increased depending on the data importance level. Moreover, the performance of LBSS was evaluated using an IoT-enabled healthcare simulation environment, and all of its characteristics were precisely generated using the NS3 package. Furthermore, the metrics were chosen to measure the performance of LBSS in addition to evaluating its impact on the entire IoT system. Moreover, the simulation results proved that LBSS outperformed both the Bitcoin model and the Leila's model. Finally, the recommended areas for future work are deeper analysis of the healthcare data to determine its sensitivity, construction of additional simulation experiments to include other network types such as cellular, applying LBSS to other IoT fields such as the military and agriculture, and comparing LBSS with more complicated systems such as Ethereum.

Funding: The work was supported by the Taif University Researchers Supporting Project number (TURSP-2020/60), Taif University, Taif, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used in this study is created by the simulation package (NS_3).

Acknowledgments: The author extends their appreciation to the Taif University Researchers Supporting Project number (TURSP-2020/60), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Xu, C.; Qu, Y.; Luan, T.H.; Eklund, P.W.; Xiang, Y.; Gao, L. A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 4371–4384. [CrossRef]
2. Liqiong, H.; Yuanyuan, W. Congestion Control of Multipath Parallel Transmission of Data for Blockchain Applications. *IETE J. Res.* **2022**, 1–10. [CrossRef]
3. Mirani, A.A.; Velasco-Hernandez, G.; Awasthi, A.; Walsh, J. Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review. *Sensors* **2022**, *22*, 5836. [CrossRef] [PubMed]
4. Azamuddin, W.M.H.; Aman, A.H.M.; Hassan, R.; Mansor, N. Comparison of Named Data Networking Mobility Methodology in a Merged Cloud Internet of Things and Artificial Intelligence Environment. *Sensors* **2022**, *22*, 6668. [CrossRef] [PubMed]

5. Lavaur, T.; Lacan, J.; Chanel, C.P.C. Enabling Blockchain Services for IoE with Zk-Rollups. *Sensors* **2022**, *22*, 6493. [CrossRef]
6. Wang, X.; Cai, S. Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud. *Futur. Gener. Comput. Syst.* **2020**, *112*, 320–329. [CrossRef]
7. Fotouhi, M.; Bayat, M.; Das, A.K.; Far, H.A.N.; Pournaghi, S.M.; Doostari, M. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Comput. Netw.* **2020**, *177*, 107333. [CrossRef]
8. Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F.-Y. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 942–950. [CrossRef]
9. Ismail, L.; Materwala, H.; Zeadally, S. Lightweight Blockchain for Healthcare. *IEEE Access* **2019**, *7*, 149935–149951. [CrossRef]
10. Haghparast, M.B.; Berehlia, S.; Akbari, M.; Sayadi, A. Developing and evaluating a proposed health security framework in IoT using fuzzy analytic network process method. *J. Ambient Intell. Humaniz. Comput.* **2020**, *12*, 3121–3138. [CrossRef]
11. Gupta, P.K.; Maharaj, B.T.; Malekian, R. A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres. *Multimedia Tools Appl.* **2016**, *76*, 18489–18512. [CrossRef]
12. Ning, Z.; Sun, S.; Wang, X.; Guo, L.; Guo, S.; Hu, X.; Hu, B.; Kwok, R. Blockchain-enabled Intelligent Transportation Systems: A Distributed Crowdsensing Framework. *IEEE Trans. Mob. Comput.* **2021**. [CrossRef]
13. Lakhan, A.; Mohammed, M.A.; Nedoma, J.; Martinek, R.; Tiwari, P.; Vidyarthi, A.; Alkhayyat, A.; Wang, W. Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare. *IEEE J. Biomed. Health Inform.* **2022**. [CrossRef] [PubMed]
14. Manoharan, H.; Selvarajan, S.; Yafoz, A.; Alterazi, H.A.; Uddin, M.; Chen, C.L.; Wu, C.M. Deep Conviction Systems for Biomedical Applications Using Intuiting Procedures with Cross Point Approach. *Front. Public Health* **2022**, *10*, 909628. [CrossRef]
15. Selvarajan, S.; Manoharan, H.; Hasanin, T.; Alsini, R.; Uddin, M.; Shorfuzzaman, M.; Alsufyani, A. Biomedical Signals for Healthcare Using Hadoop Infrastructure with Artificial Intelligence and Fuzzy Logic Interpretation. *Appl. Sci.* **2022**, *12*, 5097. [CrossRef]
16. Anitha, S.; Jayanthi, P.; Chandrasekaran, V. An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks. *Measurement* **2020**, *167*, 108272. [CrossRef]
17. Benil, T.; Jasper, J. Cloud based security on outsourcing using blockchain in E-health systems. *Comput. Netw.* **2020**, *178*, 107344. [CrossRef]
18. Kong, F.; Zhou, Y.; Xia, B.; Pan, L.; Zhu, L. A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment. *IEEE Access* **2019**, *7*, 161822–161830. [CrossRef]
19. Wang, L.; Ali, Y.; Nazir, S.; Niazi, M. ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods. *IEEE Access* **2020**, *8*, 152316–152332. [CrossRef]
20. Abou-Nassar, E.M.; Iliyasu, A.M.; El-Kafrawy, P.M.; Song, O.-Y.; Bashir, A.K.; Abd El-Latif, A.A. DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access* **2020**, *8*, 111223–111238. [CrossRef]
21. Kavitha, S.; Alphonse, P.; Reddy, Y. An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System. *J. Med. Syst.* **2019**, *43*, 260. [CrossRef] [PubMed]
22. Tai, W.; Chang, Y.; Lo, Y. An Anonymity, Availability and Security-Ensured Authentication Model of the IoT Control System for Reliable and Anonymous eHealth Services. *J. Med. Biol. Eng.* **2019**, *39*, 443–455. [CrossRef]
23. Pawar, P.; Parolia, N.; Shinde, S.; Edoh, T.O.; Singh, M. eHealthChain—A blockchain-based personal health information management system. *Ann. Telecommun.* **2021**, *77*, 33–45. [CrossRef] [PubMed]
24. Hasanova, H.; Tufail, M.; Baek, U.-J.; Park, J.-T.; Kim, M.-S. A novel blockchain-enabled heart disease prediction mechanism using machine learning. *Comput. Electr. Eng.* **2022**, *101*, 108086. [CrossRef]
25. Marwan, M.; Kartit, A.; Ouahmane, H. Security Enhancement in Healthcare Cloud using Machine Learning. *Procedia Comput. Sci.* **2018**, *127*, 388–397. [CrossRef]
26. Ding, R.; Zhong, H.; Ma, J.; Liu, X.; Ning, J. Lightweight Privacy-Preserving Identity-Based Verifiable IoT-Based Health Storage System. *IEEE Internet Things J.* **2019**, *6*, 8393–8405. [CrossRef]
27. Li, P.; Xu, C.; Jin, H.; Hu, C.; Luo, Y.; Cao, Y.; Mathew, J.; Ma, Y. ChainSDI: A Software-Defined Infrastructure for Regulation-Compliant Home-Based Healthcare Services Secured by Blockchains. *IEEE Syst. J.* **2020**, *14*, 2042–2053. [CrossRef]
28. Vedaraj, M.; Ezhumalai, P. HERDE-MSNB: A predictive security architecture for IoT health cloud system. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 7333–7342. [CrossRef]
29. Wang, X.; Ning, Z.; Guo, S.; Wen, M.; Poor, H.V. Minimizing the Age-of-Critical-Information: An Imitation Learning-Based Scheduling Approach under Partial Observations. *IEEE Trans. Mob. Comput.* **2021**, *21*, 3225–3238. [CrossRef]
30. Ning, Z.; Yang, Y.; Wang, X.; Guo, L.; Gao, X.; Guo, S.; Wang, G. Dynamic Computation Offloading and Server Deployment for UAV-Enabled Multi-Access Edge Computing. *IEEE Trans. Mob. Comput.* **2021**. [CrossRef]
31. Zarour, M.; Ansari, T.J.; Alenezi, M.; Sarkar, A.K.; Faizan, M.; Agrawal, A.; Kumar, R.; Khan, R.A. Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records. *IEEE Access* **2020**, *8*, 157959–157973. [CrossRef]
32. Sharma, H.; Kumar, A.; Pant, S.; Ram, M. 3 Role of Artificial Intelligence, IoT and Blockchain in Smart Healthcare. In *Artificial Intelligence, Blockchain and IoT for Smart Healthcare*; River Publishers: Aalborg, Denmark, 2022; pp. 25–36.
33. Xiao, J.; Tian, Y.; Xie, L.; Jiang, X.; Huang, J. A Hybrid Classification Framework Based on Clustering. *IEEE Trans. Ind. Inform.* **2019**, *16*, 2177–2188. [CrossRef]

34. Katarahweire, M.; Bainomugisha, E.; Mughal, K.A. Data Classification for Secure Mobile Health Data Collection Systems. *Dev. Eng.* **2020**, *5*, 100054. [CrossRef]
35. Bera, B.; Chattaraj, D.; Das, A.K. Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. *Comput. Commun.* **2020**, *153*, 229–249. [CrossRef]
36. Grunspan, C.; Marco, R. The mathematics of Bitcoin. *Eur. Math. Soc. Mag.* **2020**, *115*, 31–37. [CrossRef]
37. Said, O.; Tolba, A. DORS: A data overhead reduction scheme for hybrid networks in smart cities. *Int. J. Commun. Syst.* **2020**, *33*, e4435. [CrossRef]
38. Roquero, P.; Aracil, J. On Performance and Scalability of Cost-Effective SNMP Managers for Large-Scale Polling. *IEEE Access* **2021**, *9*, 7374–7383. [CrossRef]
39. Badea, A.; Croitoru, V.; Gheorghică, D. Computer networks security based on the detection of user's behavior. In Proceedings of the 9th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, Romania, 7–9 May 2015; pp. 55–60. [CrossRef]
40. How to Represent a Blockchain through a Mathematical Model? Study Carried Out by the Data Science Practice. Available online: https://canopee-group.com/wp-content/uploads/2020/05/Blockchain-Coperneec.pdf (accessed on 15 October 2022).
41. Said, O.; Tolba, A. Design and performance evaluation of mixed multicast architecture for internet of things environment. *Supercomput. J.* **2018**, *74*, 3295–3328. [CrossRef]
42. Forjan, M.; David, V.; Wagner, M.; Dolesch, L.; Lechner, M.; Sauermann, S. Conceptualization of an ICU Infrastructure for Simulation Based Education in Medical Engineering & eHealth. In Proceedings of the 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Berlin, Germany, 23–27 July 2019; pp. 4186–4189. [CrossRef]
43. Kim, H.H.; Bruce, N.; Park, S.; Jo, J.; Lee, H.J. Modeling and Simulation of Identification Protocol for Wireless Medical Devices in Healthcare System Communication. In *Information Science and Applications; Lecture Notes in Electrical Engineering*; Kim, K., Ed.; Springer: Berlin/Heidelberg, Germany, 2015; p. 339. [CrossRef]
44. Avventuroso, G.; Silvestri, M.; Frazzon, E. Additive Manufacturing Plant for Large Scale Production of Medical Devices: A Simulation Study. *IFAC-PapersOnLine* **2018**, *51*, 1442–1447. [CrossRef]