electronics

MDPI

Article

Blockchain-Based Security Mechanism for the Medical Data at Fog Computing Architecture of Internet of Things

Desire Ngabo [1,2,†], Dong Wang [1,*,†], Celestine Iwendi [3,4,†], Joseph Henry Anajemba [5,†], Lukman Adewale Ajao [6,†] and Cresantus Biamba [7,*,†]

1 Department of Computer Science and Electronics Engineering, Hunan University, Changsha 410082, China; dngabo@hnu.edu.cn
2 African Center of Excellence in the Internet of Things, University of Rwanda, Kigali P.O. Box 3900, Rwanda
3 School of Creative Technologies, University of Bolton, Bolton BL3 5AB, UK; celestine.iwendi@ieee.org
4 Department of Mathematics and Computer Science, Coal City University Enugu, Enugu 400231, Nigeria
5 Department of Communication Engineering, College of Internet of Things, Hohai University, Changzhou 230001, China; herinopallazo@ieee.org
6 Department of Computer Engineering, Federal University of Technology, Minna 92011, Nigeria; ajao.wale@futminna.edu.ng
7 Faculty of Education and Business Studies, University of Gävle, 80176 Gävle, Sweden
* Correspondence: wangd@hnu.edu.cn (D.W.); cresantus.biamba@hig.se (C.B.)
† These authors contributed equally to this work.

Abstract: The recent developments in fog computing architecture and cloud of things (CoT) technology includes data mining management and artificial intelligence operations. However, one of the major challenges of this model is vulnerability to security threats and cyber-attacks against the fog computing layers. In such a scenario, each of the layers are susceptible to different intimidations, including the sensed data (edge layer), computing and processing of data (fog (layer), and storage and management for public users (cloud). The conventional data storage and security mechanisms that are currently in use appear to not be suitable for such a huge amount of generated data in the fog computing architecture. Thus, the major focus of this research is to provide security countermeasures against medical data mining threats, which are generated from the sensing layer (a human wearable device) and storage of data in the cloud database of internet of things (IoT). Therefore, we propose a public-permissioned blockchain security mechanism using elliptic curve crypto (ECC) digital signature that that supports a distributed ledger database (server) to provide an immutable security solution, transaction transparency and prevent the patient records tampering at the IoTs fog layer. The blockchain technology approach also helps to mitigate these issues of latency, centralization, and scalability in the fog model.

Keywords: blockchain; cloud of things; fog layer; medical data; security mechanism; privacy; elliptic curve cryptography; distributed ledger; fog and edge computing

Citation: Ngabo, D.; Wang, D.; Iwendi, C.; Anajemba, J.H.; Ajao, L.A.; Biamba, C. Blockchain-Based Security Mechanism for the Medical Data at Fog Computing Architecture of Internet of Things. *Electronics* **2021**, *10*, 2110. https://doi.org/10.3390/electronics10172110

Academic Editor: Priyadarsi Nanda

Received: 15 June 2021
Accepted: 24 August 2021
Published: 30 August 2021

1. Introduction

Recently, data mining has become an emerging area in the Internet of Things (IoT) and many other technological applications. Data mining utilizes data for driving the digital economy in business model services and industries [1]. These data can be generated from different areas of smart technology applications, such as healthcare, smart cities, and smart agriculture. However, the privacy and security management of data mining records is an important research area. IoT-based smart healthcare is being developed for monitoring patient health vitals using wearable sensors/devices [2].

On the other hand, the objective of the study of [3] was to offer a solution for security and intrusion issues. To realize this goal, they proposed a model based on the blockchain-Internet of things model, which is equipped with a bio-sensor that estimates and gathers real time data regarding a patient's medical status and stores these data in the blockchain.

Their bio-sensor equipped technique is capable of reporting and tamper proofing storage of data in a more accurate and shorter time frame. These sensors generate highly sensitive and personal information that is vulnerable to privacy and security breaches. In a conventional smart health ecosystem, the data is analyzed and stored in clouds [4]. However, the cloud database has latency bottleneck and does not provide location awareness.

In addition, it provides centralized solutions for storing/analyzing this data. If a physician wants to access the data or in case of urgent response and action, this delay is not acceptable in delay-sensitive scenarios, such as in the case of a heart attack or hypertensive situation where immediate action is required [5]. The research of [6] recommended a new simulation-driven framework referred to as the Edge-Based Assisted Living Platform for Home-care (E-ALPHA). This technique implements computation using both edge and cloud models to establish innovative Ambient Assisted Living (AAL) services in scenarios of different health care scales.

On the other hand, the research of [7] presents a framework for IoT that utilizes an edge computing layer of Fog nodes measured and achieved by an SDN network to realize great consistency and convenience for latency-sensitive IoT devices. They implemented blockchain to guarantee devolution in a trustful method.

In all these techniques, the data acquired from the edge layer are processed and transmitted to the cloud computing database through the fog layer of IoT architecture using internet network services. Both the internet and cloud computing database are exposed to security threats on the data sensed from the sensor (edge layer) or stored in the cloud layer [8,9]. The conventional data storage and security mechanisms are also not suitable for such a massive amount of generated data.

Therefore, to mitigate these issues (latency, security, centralization, and scalability), we propose a blockchain-based security mechanism for providing an immutable security solution for such data at the fog layer as illustrated in Figure 1. In this research, the proposed blockchain technology is implemented as a security mechanism for medical data. The fog computing can be described as the notion of outer edges in the network layer, managing the flows of data created from the sensing layer to the cloud database where data is stored at the data center of the IoT model.

The motivation of this paper is due to the vulnerability, security threats, and cyber-attacks against the fog computing layers. This is a situation where each of the layers is susceptible to different intimidations: the sensed data (edge layer), computing and processing of data (fog (layer), and storage and management for public users (cloud). This fog model was developed for securing medical data by dividing into three layers (including the sensing, fog, and cloud layers).

The sensed data is stored on a fog-enabled blockchain ledger, and a copy of this blockchain will be available on the cloud database as multiple fogs. This is to enable and ensure the data security, and latency issues are resolved through fog layers. The scalability and centralized storage issues are mitigated using public-permissioned blockchain technology that utilizes a decentralized ledger in the record management. This also provides transparency and prevents patient record tampering using a digital signature type called elliptical curve cryptography. The physicians can access data from these blockchains, which are distributively installed on different fog layers using the key generation. This paper's contributions include:

- We propose and develop a permissioned-based public blockchain technology for securing data packet transmitted/received at the fog layer of IoT.
- The adoption of elliptical curve cryptography digital signature algorithm (ECCDSA) for hashing certificate is developed and used as an immutable security for fog layer.
- A distributed ledger database (server) was used to provide immutable security solution and transaction transparency and to prevent patient record tampering at the fog layer of the IoT.
- We implemented blockchain technology to mitigate the issues of latency, centralization, and scalability in the fog model.

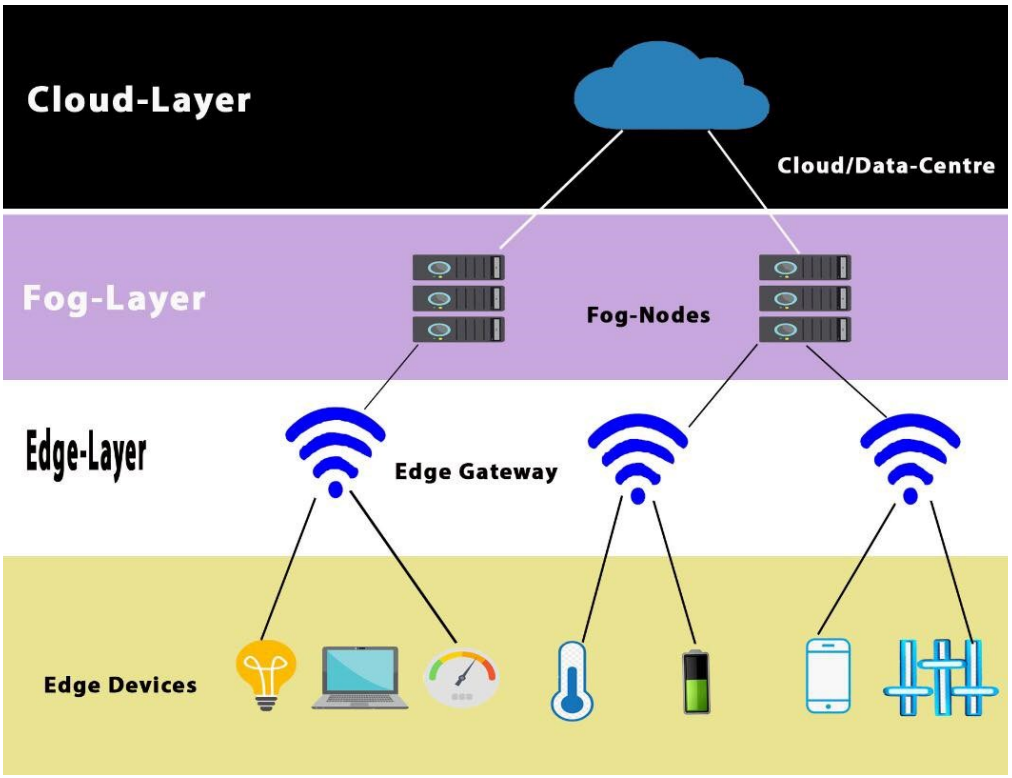


Figure 1. Fog computing architecture-based IoT.

Research Organization

The remaining part of this research is structured as follows: In Section 2, several related literature works are collected, reviewed, and analyzed in comparison to the current study. The proposed models coupled with the selected dataset are analyzed and established in Section 3. Several numerical experiments to prove the performance of the proposed model are performed and discussed in Section 4. The results of the performances are also extensively analyzed in this section. Finally, our conclusions and findings are outlined in Section 5.

2. Literature Review

Cloud computing can be seen as assets or services that are offered through the use of the internet. The authors of [10] attempted to pinpoint the most endangered security concerns in cloud computing, which will aid vendors, researchers, and users in knowing the key threats, what to watch out for, and the various frameworks proposed to solve these concerns. A framework for the detection of Distributed Denial of Service (DDoS) attacks was proposed in [11–13], which can cause a large amount of network traffic and is a threat to Internet Service Providers. The results from the experiment prove that the suggested framework has an increased detection performance when likened to the other techniques.

To address the threats to cloud computing, a security model that accurately calculates the empirical capacity of a contender authentication framework for securing the transmission of data in cloud computing architecture was proposed in [14]. The results from the experiment carried out show that the suggested framework was more efficient than the existing ones.

The authors of [15–17] presented a mechanism that is based on an I-AES, along with a database design that is private. It also makes a provision for a theoretical basis when regarding the large amount of 5G gadgets that can be applied in the IoT. The results from the experiment carried out proved that the suggested algorithm outperformed the current ones regarding the execution duration and throughput.

An efficient energy management algorithm for support of an IoT network and its architecture has been proposed in [18–20]. It selects safe and reliable shortcuts for the transmission of data packets to its destination, based on key management architecture using ant colony optimization. A spider-monkey synchronization method for vehicular networks is also used to reduce the time it takes for data packet delivery and without consuming too much energy. The experimental results illustrate that the suggested algorithm performs better in energy efficiency, transmission of data packets, and over long distance transmission.

In [21], the authors addressed the issue of protection of data and performance by proposing a model for trust translation, introducing an access control for fog nodes and coming up with a service for the management of alterations in users and their locations. The authors of [22] discussed an Artificial Intelligence algorithm whose goal is to decrease the time it takes to respond and network traffic, by assigning various tasks to the cloud and fog servers. Experimental results showed that this technique significantly decreases the time for response when compared to existing approaches.

The authors of [23] attempted to explain how a fog computing framework could subjugate the security issues of the customary IoT cloud framework and how it could be improved in the future by inventing an application for the monitoring of the system with the proposed framework at the center. In [24,25], the authors discussed the storage of data; the accessibility, integrity, and quality of service; and how their proposed architecture could affect fog computing, the cloud framework, and mobile edge computing.

The authors of [26] proposed a mechanism based on blockchain to resolve the issue of leakage of data in the management of security. Their proposed model contained nodes and power terminals, which aid in data collection. In [27], the authors proposed a security management model based on blockchain, which generates, releases, receives, and stores data intelligently in the blockchain. The authors of [28,29] proposed a protection of privacy scheme based on blockchain for surveillance cameras. Its job is to secure the privacy of people in surveillance with the feature of blurring while still keeping a close eye on them.

In [30,31], the authors proposed a sharing protocol based on blockchain in order to aid in the easy transmission of the health records of patients. The proposed protocol was experimented on in the Ethereum platform, and researchers discovered that its computational efficacy was quite high. The authors of [32] discussed more on the use of blockchain in the healthcare sector and suggested a framework to execute blockchain-based technology for electronic health records.

A crypto hash algorithm-based blockchain technology was developed by [33,34] to manage and secure the decentralized distributed ledger of oil and gas product distribution across the country. The secure hash algorithm-1 (SHA-1) technique was used in the database security against any alteration from chain participants and to render assistance of immutability and transparency in the chain.

The evaluations of the system proved efficient in security measures against a distributed database, which is easy to maintain as it does not authorize any individual for record tampering but supports agreement of about 75% of the participants in the chain to make any changes to the database recross. Thus far, none of these discussed papers have highlighted the need for blockchain security in the way that our paper will showcase how these medical data can be securely protected.

Finally, for every IoT-related system like ours, there are always surrounding risk factors. Generally, risk denotes the latent potential for some event to occur, be it positive or negative. Regarding the IoT cyber risk, the researchers of [35–37] designed and implemented a framework of quality estimation for commercial cyber insurance. Unlike our study, which focuses on providing an efficient technique with respect to data retrieval size and key generation management, the authors modeled a prospective electronic intrusion with a steady state not considering time factors and data retrieval mechanism.

Our proposed technique employs a decentralized and distributed ledger blockchain record management system paradigm for mitigating all the system scalability and centralized issues. This provides transparency and prevents tampering of the patient records by

intruders. However, authorized medical personnel can access data from these blockchains that are distributively installed on different fog layers.

3. Proposed Methodology

The proposed medical data security at the fog layer of IoT-based cloud computing model is illustrated in Figure 2 using public permissioned blockchain technology with an ECC digital signature as a security solution in the model. The secure hashing algorithm 256 (SHA-256) is adopted using elliptical curve cryptography digital signature Algorithm (ECDSA) for the certificate hashing. This is popularly used in securing messaging apps and is the main basis for bitcoin security.

The blockchain technique was used due to shortcomings in the existing security countermeasure of WSN-IoT, which resulted in computation complexity, memory inconvenience, processor power consumption, latency, vulnerability to social attacks, and other problems. The ECDSA approach was to use a hash algorithm in the blockchain for security purposes, immutability and transparency among the participants in the chain. This elliptic curve cryptography hashing is very short in computation, efficient and stronger by 10,000 times compare to the RSA with the key size of 256 bits equivalent to 2048 and 3072 bits of RSA. Particularly, the avalanche effect is stronger over the random number generation for hashing.

The sensed data are kept in a fog-enabled blockchain ledger with a copy sent to the cloud as multiple fogs through the fog layer. This model will help to secure the data (immutability) and resolve latency issues through the decentralized records at the fog layers. The scalability and centralized storage issues are mitigated using blockchain technology with an elliptic curve cryptography hash algorithm.

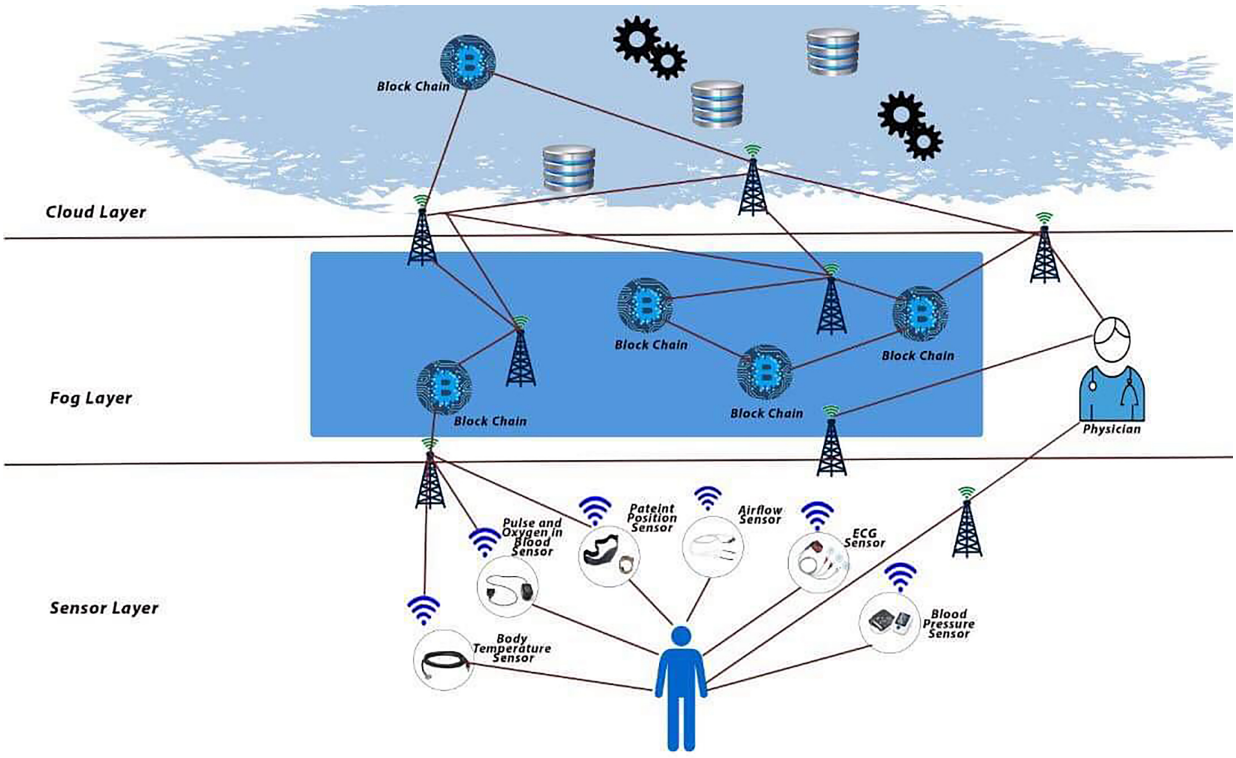


Figure 2. Blockchain-based security model for medical data at the fog layer.

However, physicians can be permitted to access the encrypted distributed ledger records with a crypto hash-based blockchain using a generated private key that is distributively installed on the fog layers. A copy of this transaction is well-kept on the cloud layer for permanent storage and is accessible. The overall flow process and the transaction of the internal process for the proposed model are presented in Figures 3 and 4. The medical data security-based fog layer algorithm is presented in Table 1.

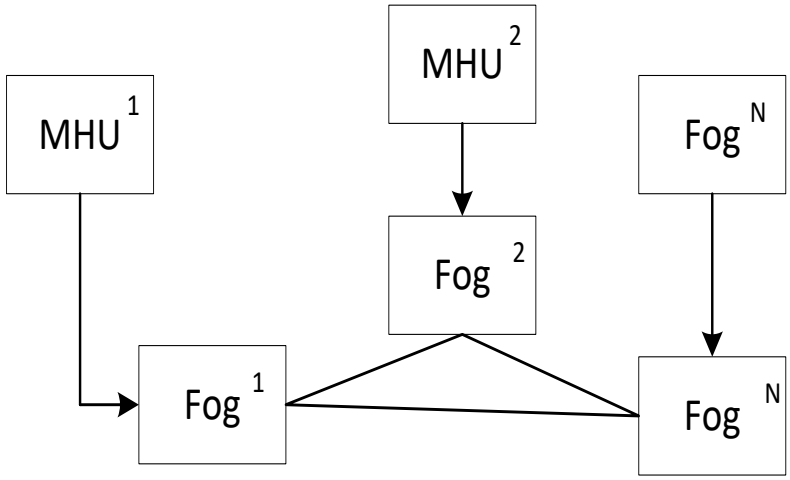


Figure 3. The overall flow of the proposed model.

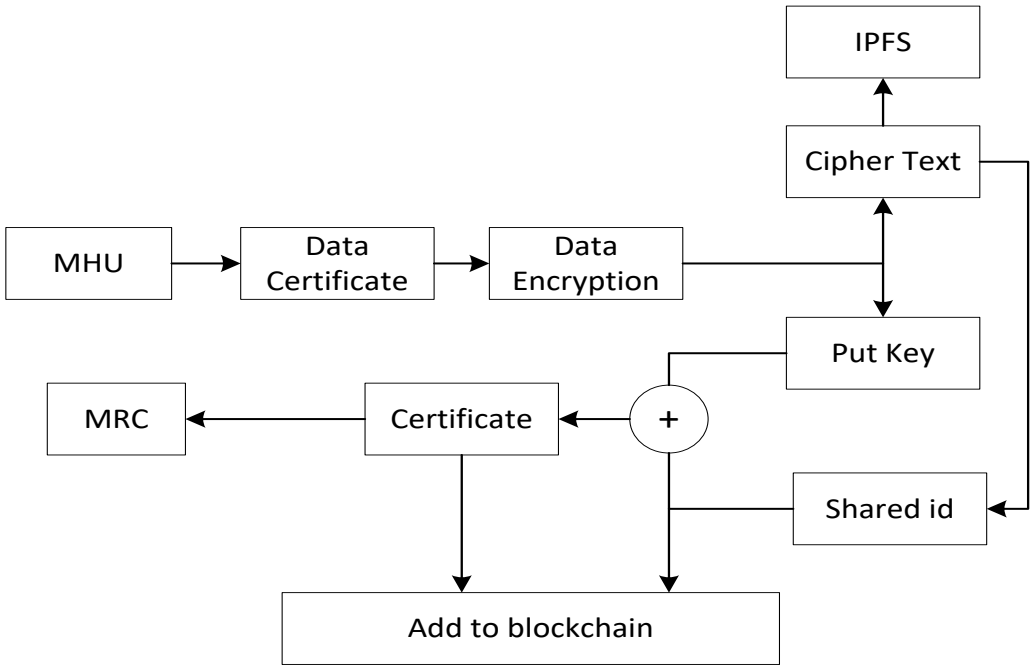


Figure 4. Internal process flow of the medical data security at the fog layer.

Table 1. Workflow of the proposed model for ensuring medical data security at the fog layer.

S/N	Medical Data Security Algorithm
1	All the operations were performed by the Fog servers rather than the mobile phones or other device
2	Data is first encrypted with the private (pvt) key, and then stored in the IPFS system (peer-to-peer application for data sharing in blockchain-based systems).
3	A unique hash file is obtained under control of the user owner
4	The hash file and shared link is encrypted by providing a certificate for the user only
5	Once the certificate is opened, the private (pvt) key share link is obtained by the request for the download of the cipher text using pvt for document accessibility
6	At any time, the user can remove access by revoking the certificate. That is, by changing the share link and pvt key of the data, and deleting all the mappings stored in the blockchain
7	Any time that data can be re-shared to the user, these actions are performed on the same smart contract using a single blockchain technology.
8	The dedicated fog servers, further reducing the computation and communication costs for medical health units and users.

3.1. Application of Public-Permissioned Blockchain at Fog Layer

The blockchain application for the fog computing model of IoT is a recent innovation that renders the advantage of immutability and prevent records tampering in the process of transactions or exchange of information in a secure network. The elliptic curve crypto hash function approach has a special feature with various properties that make it suitable for public permissioned blockchain applications. It is deterministic (gives the same results whenever you parse an input through a hash function) with quick computation, pre-image resistance, collision resistance, and avalanche effects.

A public-permissioned blockchain technology was also used to allow the information to be transmitted within the network of decentralized records, with limited authorized monitoring of nodes and restriction to any unauthorized administrator. Every block (node) in this network at fog layer functions on a peer-to-peer network architecture as given in Figure 5 where the blockchain consists of nodes in a cluster model. Each sensor node in the cluster network will have a copy of the exchange information (the shared ledger), which is updated frequently and then verifies the transactions from initialized or received transactions to create blocks.

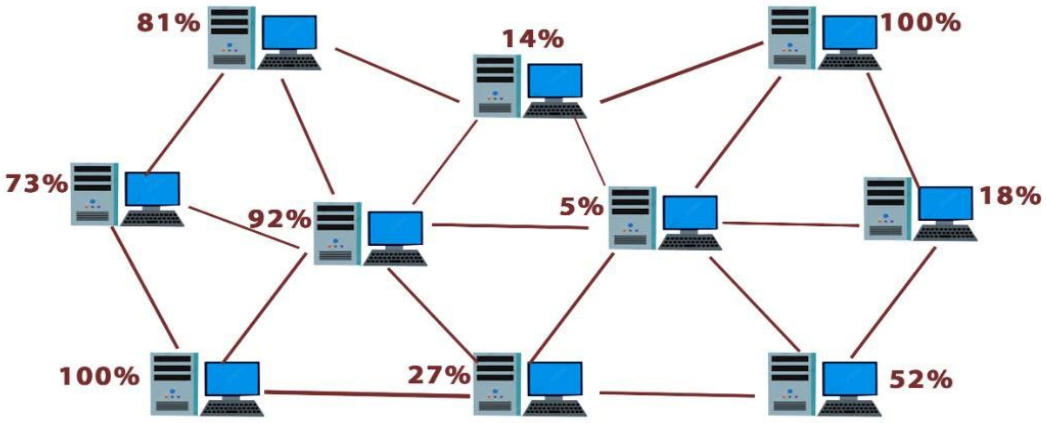


Figure 5. Decentralized node connections in peer-to-peer architecture.

3.2. The Transaction Process of Secured Decentralized Records

The transaction process of this distributed sensor node required peer-to-peer connections in a cluster for the initialization. The data (block) are then hashed for security purposes (that is, sensed devices, body parameters, and wireless transmission to the fog layer). The transaction process of this model consists of the body parameters acquired (source), a third party (transaction), and the agent (destination) at the fog layer. The initialization of this hashing transaction is generated based on the previous transaction using SHA-256 for providing a public and private key as illustrated in Figure 6.

The distributed wireless body area sensor is referred to as the source in this model, the transaction, a copy of transference of assets (body parameter) is called the third-party, which utilizes wireless technology to transmit the acquired patient health parameters but is not trusted in the chain, and the agent/destination in this model is known as the fog layer. The flowchart of this proposed methodology is illustrated in Figure 7.

3.3. Blockchain Transaction Sequence Model for the Fog Layer

The public permissioned blockchain adopted in this model functions on the two principles of open ledger belief (OLB) and decentralized ledger cryptogram (DLC) system. The open ledger belief (OLB) is a system that cares for every participant that is involved in the transaction over the network/chain and validates the content of teh hashing blockchain using a mining algorithm (public key) as computed in Equation (1).

$$\forall = \frac{\sum_{i=0}^{32} \omega * \frac{N.10^8}{2^i}}{10^8} \quad (1)$$

where $\forall$ is the mining computation, ω is the hash rate in mega hashes per second (MH/s), and N is the number of bitcoins.

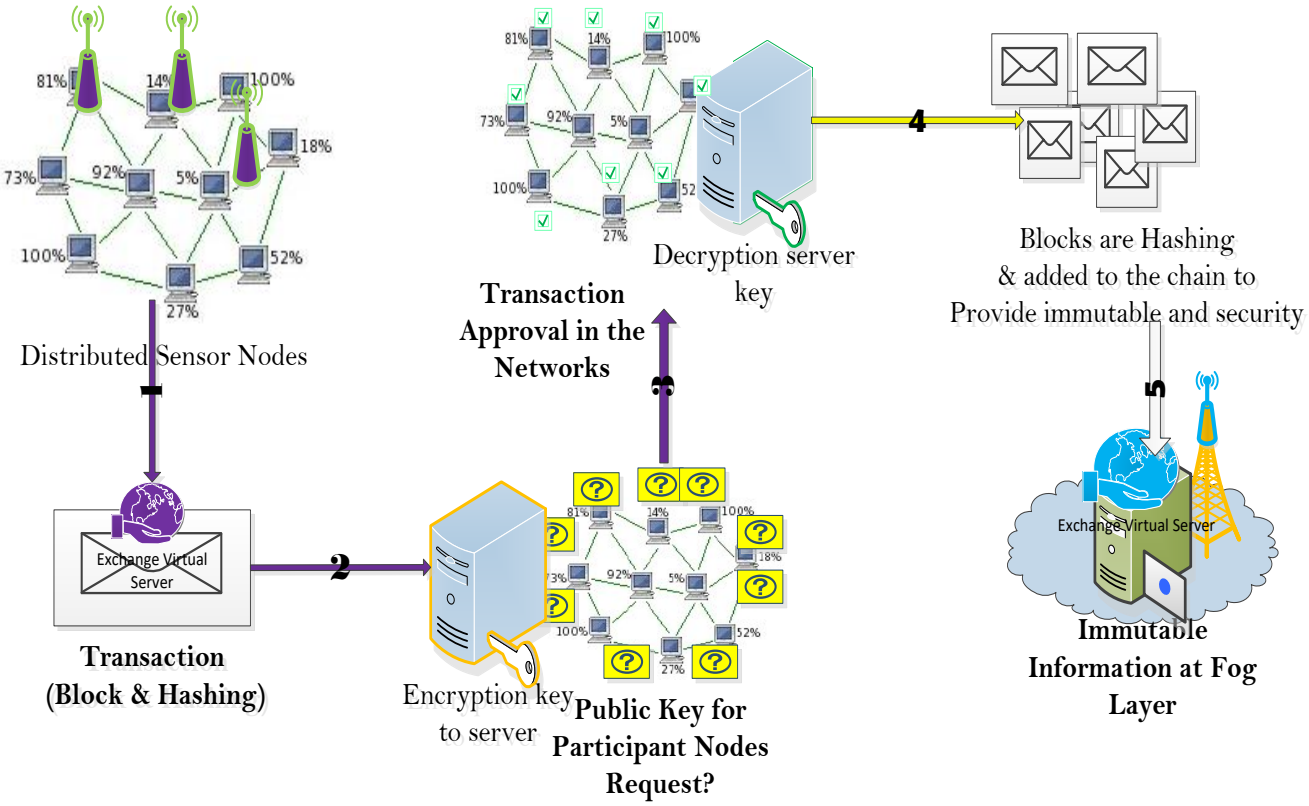


Figure 6. Blockchain transaction model of the distributer WSN.

The decentralized ledger protocol (DLC) is a developed database that helps to administer the transaction through the network chain with consensus agreement on the record updates without permission of a central authority or third-party negotiation. This DLC-database provides a timestamp with a unique credential signature to make the transaction history in the chain immutable. A sequence diagram of a proposed medical data security model at the fog layer is shown in Figure 8, and the procedure is discussed as follows.

1. The acquisition of the body area parameters from the sensed environment are transmitted through the third party (wireless technology).
2. The third-party (wireless technology) is not trusted with transactions with the acquisition of body parameters. Therefore, this transaction is encrypted using a public key and attached with a link.
3. All these transactions in the network/chain are validated using a public key for every node participant agreement in the network.
4. Then, the copy of broadcasting transactions is published through the networks.
5. The transaction copy then synchronises to ensure quick and safe delivery to all participant nodes in the chain/network.
6. The mining algorithm is used to validate the data transaction using computation of a hash number random generation of a special or private key used by all the participants in the network.

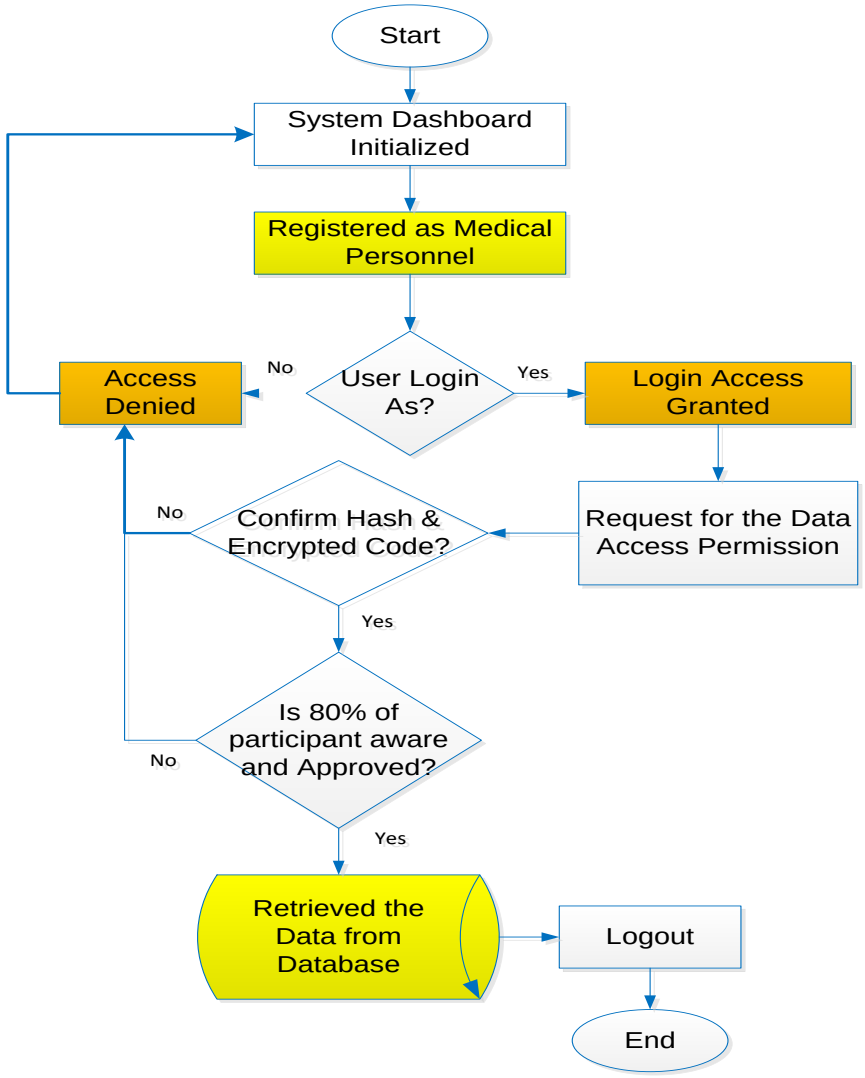


Figure 7. A secure public-permissioned blockchain database system for fog layer information.

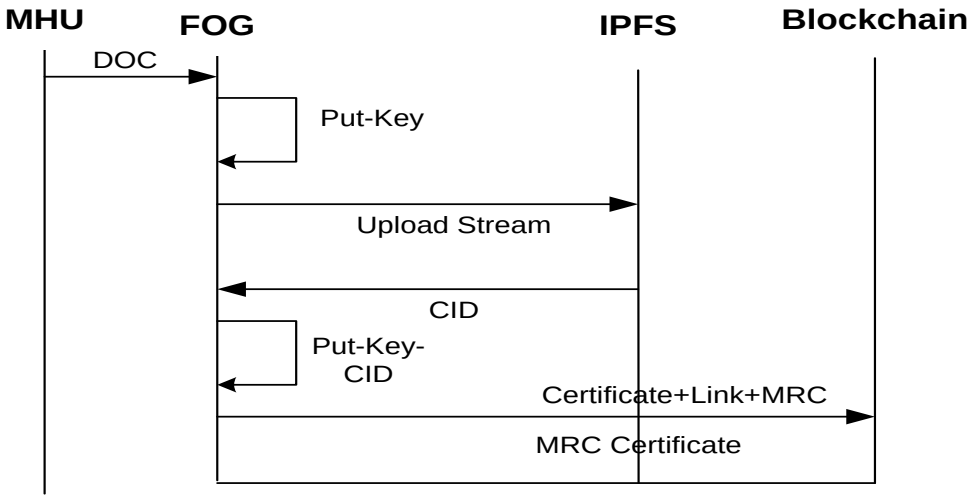


Figure 8. Sequence diagram of the proposed model.

3.4. Secure Hash Algorithm-256 (Sha-256)

This is a digest kind of signature for securing the data file, which generates a unique 32-byte (256-bit) signature for text called a secure crypto hash algorithm (SCHA-256). SHA-

256 is a suitable hash function with no known vulnerabilities. It is also a building block for other cryptographic constructs. Other advantages include the formulation of the hash table with avalanche effects, handshake authentication (HA), integrity verification (IV), digital signature (DS), and anti-tamper (no data loss transmission). The SHA-256 architecture is shown in Figure 9. This comprises additional modulo 2^{32} and a bitwise rotation operation that uses different constants (ch, $\sum 1$, Ma, and $\sum 0$). The development of SHA-256 involves several phases, as discussed here.

1. The preprocessing stage: The block is first divided into 32-bits of 16 words each.
2. The initial hash value computation (H^0): The initial hash value is computed from the 32-bits length, 8-words of remaining blocks, and premeditated from the first eight primes, which is the square root in modulo 1 before multiplied by 16^8 and rounded to the nearest integer value as expressed in Equation (2). Where the initial hash values ($\rho = 2, 3, 5, 7, 11, 13, 17, 19$).

$$\text{int}\left(\sqrt{\rho \bmod 1}\right) * 16^8 \tag{2}$$

3. The hash computation: Addition 48-words are computed from the preprocessing data of over-all 64 numbers to achieve four blocks using the expression in Equation (3).

$$\omega_t = \tau_{left}(\sigma_1(\omega_{t-2}) + \omega_{t-7} + \sigma_1(\omega_{t-15}) + \omega_{t-16}) \tag{3}$$

$$\sigma_0(x) = \tau^7_{right}(x) \otimes \tau^{18}_{right}(x) \otimes \xi^3_{right}(x) \tag{4}$$

$$\sigma_1(x) = \tau^{17}_{right}(x) \otimes \tau^{19}_{right}(x) \otimes \xi^{10}_{right}(x), t = 16 \tag{5}$$

4. where $x = \omega_{t-15} = \omega_1, x = \omega_{t-2} = \omega_{14}, \tau_{left}$ is rotated left, τ^7_{right} is rotated right seven times and so on, $\otimes$ is exclusive OR takes two binary digits and returns a value. For $t = 0$ to 63:
   $\{$
   $\zeta_1 = h + \sum_1^{\{256\}}(e) + ch(e, f, g) + K_t^{\{256\}} + \omega_t$
   $\zeta_0 = \sum_0^{\{256\}}(a) + \psi(a, b, c)$
   $h = g$
   $g = f$
   $f = e$
   $e = d + \zeta_1$
   $d = c$
   $c = b$
   $b = a$
   $a = \zeta_1 + \zeta_2$
   $\}$
5. The final hash message computation: the final hash value can be computed as given in (6). The Table 2 shows the initial value (input) and the final message (hash value) with time.

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} \tag{6}$$

Table 2. The computation of the input message and hash result with time.

Input Data	Hash Value	Time (ms)
Henry Joe	cb7c172128f26436e028fd6dcb35d1abe6c96a8328aec4342c1c5e969d48119b	0.90
Joe Henry	94e98eb1503b872e577e1d61c4a34e84524b6b040539f140dd350daa75739fea	1.00
Desire Ngabo	15065cdfb1a150464c4f1420ed8f63be941b64f46a0fb77c80ec514798a453d1	0.89
Ngabo Desire	307c7a5c575a1c08edbb06f2081091a4cb36c1cb8ea27fa695e4cdd880f2c3db	0.90

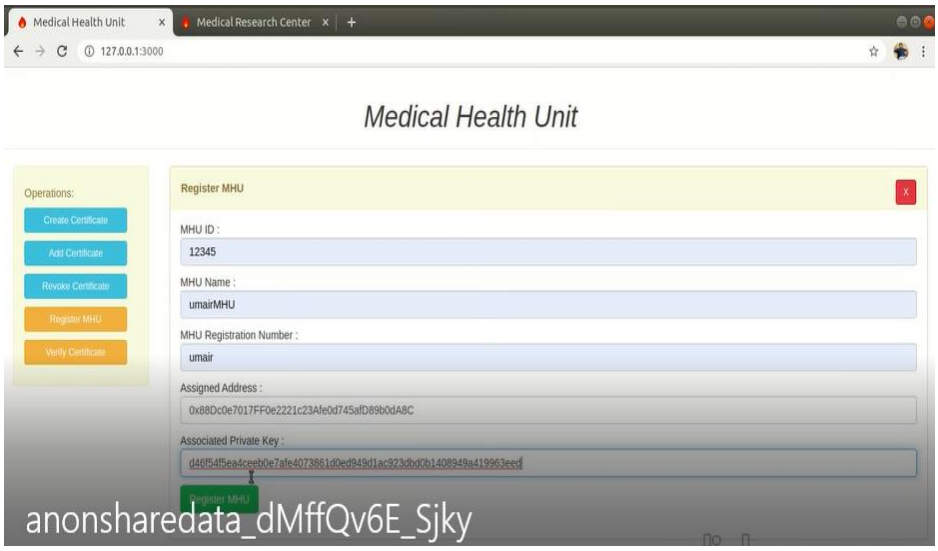


Figure 9. Blockchain-powered secured dashboard for the medical research center in order to preserve the records' privacy with/using SHA-256.

3.5. The Elliptic Curve Cryptography (Ecc) for Sha-256 Key Generation and Verification Process

The key generation and verification process as used in the blockchain based fog layer security is discussed using elliptic curve crypto digital signature Algorithm (ECDSA). The ECC is an asymmetric type of cryptography that utilizes a key agreement, digital signatures, and pseudo-random generators for the hash technique from the algebraic structure of elliptic curves over finite fields. The ECC algorithm adopts Bitcoin to ensure that any transactions within the blockchain are secure and immutable. This algorithm uses a private key, public key, and signature to ensure the security capability.

1. Key generation algorithm (KGA): the process of generating both private key (pvk) and public key (pbk) through the elliptic curve point is given $pbk = pvk * G$. G is the generator point. The pvk is generated from a random integer that range from $0 \ldots n-1$, and the pbk is achieved from an elliptic curve with point x, y.
   - i Calculate the input hash message using SHA-256: $h = hash(M)$
   - ii Generate a random number of k within the range of $[1 \ldots n-1]$, which is secure using HMAC derivation $h + pvk$
   - iii Calculate the random elliptic curve point where $R = k * G$ and calculate its x-coordinate: $r = R.x$
   - iv Calculate the signature proof: $s = k - 1 * (h + r * privKey)(\mathrm{mod}\, n)$
   - v The modular inverse $k - 1(\mathrm{mod}\, n)$ is an integer, such that $k * k - 1 = 1(\mathrm{mod}\, n)$
   - vi Return the signature r, s.
2. Signature verification algorithm (SVA): This algorithm is computed for the verification process of the adopted digital signature-based elliptic curve crypto. The input message (M) is accepted with the signature r, s from the algorithm to produce the output Boolean value of pbk that corresponds to the pvk signature (which is a valid or invalid signature). The notion of the verification signature is important to recover the ECC point R' through the generated pbk and cross-check the identical point R, through the random key generated during signing progression. The verification signature algorithm for the ECC is simplified as follows.
   - i Calculate the hashing message using the same hash function crypto during the signing: $h = hash(M)$
   - ii Calculate the modular inverse of the signature resistant: $s1 = s^{-1}(\mathrm{mod}\, n)$
   - iii Retrieve the random point of initial signing: $R' = (h * s1) * G + (r * s1) * pbk$
   - iv From R', retrieve the ECC x-coordinate: $r' = R'.x$

v Finally, calculate the validation signature result by comparing if $r' = r$. The verification signature can be transformed, and then substitute pbk with $pvk * G$ as expressed in (7)–(9).

$$R' = (h * s1) * G + (r * s1) * pbk \tag{7}$$

$$R' = (h * s1) * G + (r * s1) * pvk * G \tag{8}$$

$$R' = (h + r * pvk) * s1 * G \tag{9}$$

If the number $s = k^{-1} * (h + r * pvk) \bmod n$, then, the signing process can be $s1 = s^{-1} \bmod n$, as given in (10).

$$\begin{array}{l} s1 = s^{-1} \bmod n = \\ s1 = k^{-1} * (h + r * pvk) \bmod n = \\ s1 = k * (h + r * pvk)^{-1} \bmod n \end{array} \tag{10}$$

If we substitute $s1$ to the x-coordinate point of R', then the expression in (11) is realized as,

$$\begin{array}{l} R' = (h + r * pvk) * s1 * G = \\ R' = (h + r * pvk) * k * k * (h + r * pvk)^{-1} \bmod n * G = k * G \end{array} \tag{11}$$

4. Results and Discussion

The cloud computing model described in this paper was developed for securing remote patient medical data acquisition by dividing it into three layers (including the sensing, fog, and cloud layer) using the ECC digital signature for hashing key generation for the blockchain transactions. The sensed data was stored on a fog-enabled blockchain ledger, and a copy of this blockchain was made available on the cloud database as multiple fogs. This was to ensure the data security and to resolve the latency issues around the fog layers. The scalability and centralized storage issues were mitigated using blockchain technology that utilized a decentralized and distributed ledger in the record management.

This blockchain technique also provides transparency and prevents tampering of the patient records by intruders. The physicians can access data from these blockchains that are distributively installed on different fog layers. A copy is also kept on the cloud for permanent storage, which is also accessible. In summary, all the operations were performed by the fog servers rather than the mobile phones or other device. The data was first encrypted with the pvt key and then stored in IPFS system (peer to peer application for data sharing in blockchain-based systems).

We obtained a unique file hash that was under full control of the administrator of medical research center (MRC) as illustrated in Figure 9. The time taken digital certificate for the encryption and hashing against the retrieval time of data packet transmitted within the model is illustrated in Figure 10.

The performance evaluation of the blockchain technology using ECC digital signature was carried out based on the transaction's latency (the certification time, data retrieval time, and certificate size measured in milliseconds. The data retrieval size is measured and plotted against the digital certificate efficiency with respect to the time in milliseconds, as illustrated in Figure 11. The data retrieval latency, size, and certificate (key generation time) were compared and plotted as presented in Figure 12.

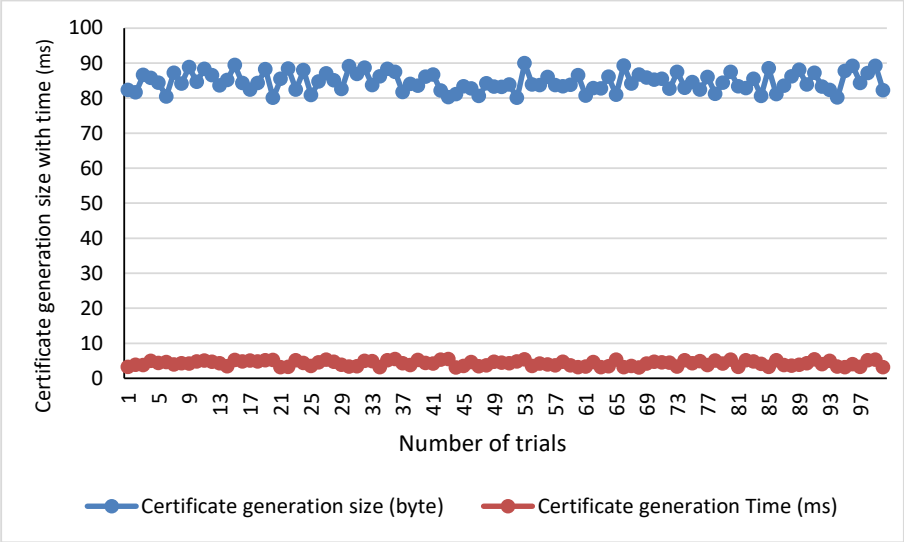


Figure 10. Certificate generation size (byte) with response time (ms) against the number of trials.

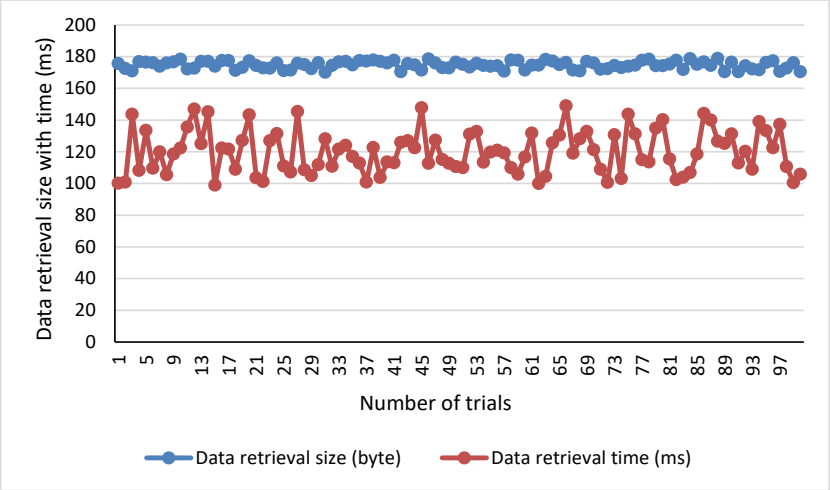


Figure 11. Data retrieval size (bytes) with time against the number of trials.

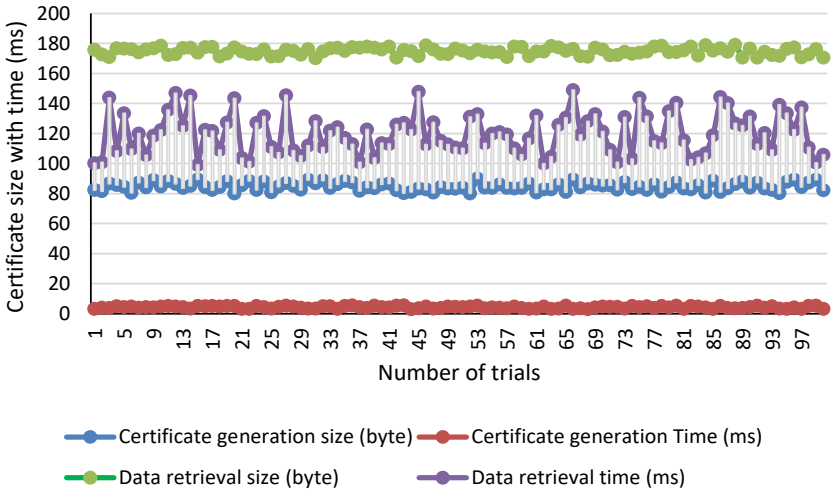
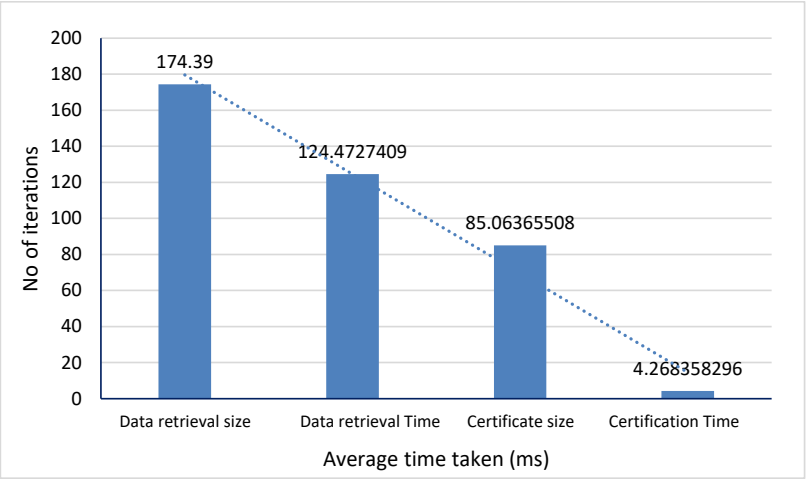


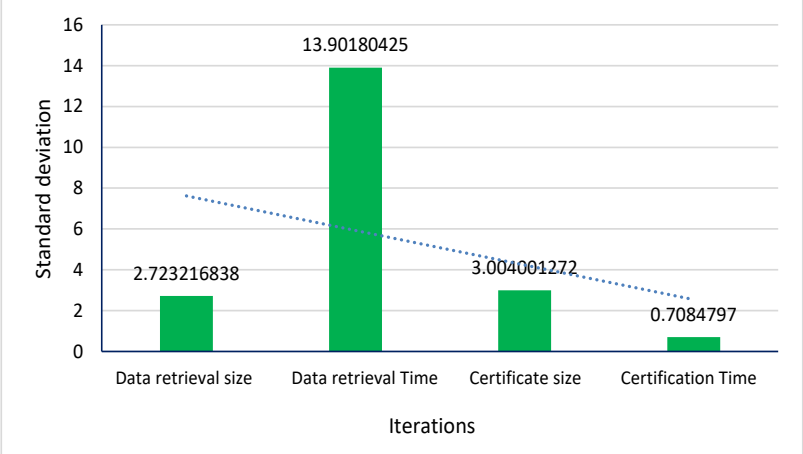
Figure 12. Comparison results of the certification latency, data retrieve latency, and data retrieval size.

The performance evaluation of the proposed digital certificate was performed using the average response time and the standard deviation as the metrics. Figure 13a. illustrates

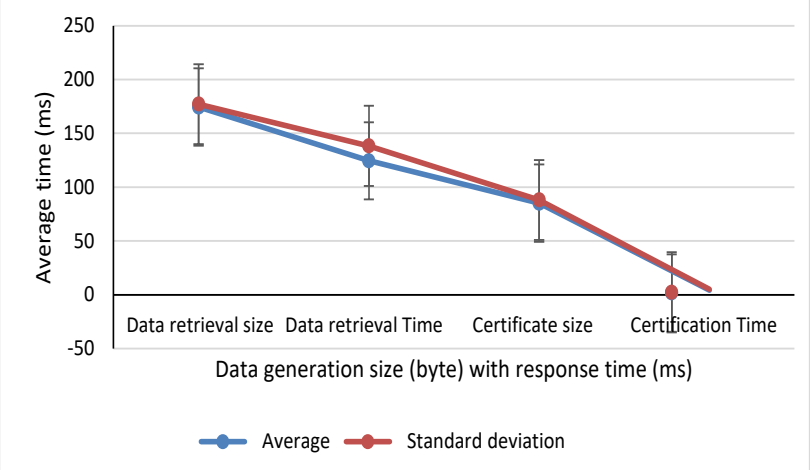
that the average response time (ms) of data retrieval size was 174 bytes, and the data retrieval time taken was 124 milliseconds. The certificate generation size to ensure the user privacy and the system confidentiality was 85 bytes, and the average time taken for the processes was 4 milliseconds.



(**a**) The average time taken measure in testing for the certificate generating.



(**b**) The standard deviation measure during the certificate generation trials.



(**c**) Comparison evaluation performance of the system response time and its scalability.

Figure 13. Performance evaluation of the proposed digital certificate model.

The standard deviation metrics were used to measure the differences or amount of deviation between the number of certificate data size generation and the time taken to complete the processes at random. The standard deviation of the certificate generation size obtained during 100 time trials was 3 bytes, and the time taken was 0.7 milliseconds. However, the deviation of the certificate data retrieval size was 2.7 bytes, which took about 13 milliseconds for the retrieval. Figure 13b illustrates the standard deviation between the certificate generation and the time taken to complete the process.

Figure 13c illustrates the comparison of the response time deviation between the certificate generation size and the time taken for 100 time trials. This result shows the response time of the proposed method with improvements in the latency issues of blockchain and its scalability. The application of our model is that when more participants join the chain, it does not affect the system response time and its performances.

5. Conclusions and Future Work

This research is focused on how to mitigate issues including the latency, security, centralization, and scalability of fog computing architecture. The public-permissioned blockchain using an ECC digital signature as a hashing technique was proposed. This security mechanism provides an immutable security solution for medical data at the fog layer of IoT. Meanwhile, in a scenario where anyone can request the files, the hash of the file with share link is encrypted, and then a certificate is provided that can only be opened by the intended requester.

Furthermore, a fog-enabled blockchain ledger was implemented for storing the sensed data, while a copy of the stored blockchain data was processed on the cloud database as multiple fogs. The essence of this performance is to establish and guarantee optimal security of user data as well as resolving the latency issues around the fog layers.

This research also employed a decentralized and distributed ledger blockchain record management system paradigm for mitigating all the system scalability and centralized issues, thus, providing transparency and preventing tampering of the patient records by intruders. However, authorized medical personnel can access data from these blockchains that are distributively installed on different fog layers. In general, the experimental performance of the proposed blockchain technology that utilizes an ECC digital signature was carried out based on the transaction's latency (the certification time, data retrieval time, and certificate size measured in milliseconds.

The measurement of the data retrieval size against the digital certificate efficiency with respect to the time in milliseconds indicates a minimized data minimized rate of about 180 milliseconds. Similarly, the data retrieval latency, size, and certificate (key generation time) was also tested and presented. The results of this experiment show that the proposed technique achieved a better time with respect to key generation.

Future work could be the development of special decentralized software that provides a facility with the ability to open and view health documents without pvt key provision. Instead, it will ask the user for the public key of the sender, and the software will then automatically find the associated pvt key from the system. Therefore, the misuse of the patient medical privacy data can be secured and prevented from access by a compromised user through the application of a crypto hash cipher text that will generate the pvt key.

Author Contributions: Conceptualization, C.I. and J.H.A.; methodology, J.H.A. and L.A.A.; software, J.H.A., D.W. and L.A.A.; validation, C.I., C.B. and J.H.A.; formal analysis, C.I., D.W. and L.A.A.; investigation, C.B. and L.A.A.; resources, C.B. and D.W.; data curation, D.W. and C.I.; writing—original draft preparation, C.I., D.N. and J.H.A.; writing—review and editing, D.N.; visualization, C.I., J.H.A. and L.A.A.; supervision, C.I.; project administration, J.H.A. and L.A.A.; funding acquisition, C.B. and D.W. All authors read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China (Grants Nos.61301148 and 61272061), Fundamental Research Funds for the Central Research Funds for the Doctoral Program of Higher Education of China (Nos. 201301-61110002 & 20120161120019), the Hunan Natural Science Foundation of China (No.14- JJ7023) and University of Gavle, Sweden.

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

References

1. Lee, G.; Jayasinghe, U. AI and Blockchain enabled Edge of Things with Privacy Preserving Computation. In Proceedings of the XIII International Scientific Conference PERSPECTIVE Technologies in the Information Transfer Means, Vladimir-Suzdal, Russia, 3–5 July 2019; pp. 39–43.
2. Ahmed, A.; Lukman, A.A.; James, A.; Mikail, O.O.; Umar, B.; Samuel, E. Human Vital Physiological Parameters Monitoring: A Wireless Body Area Technology Based Internet of Things. *J. Teknol. Dan Sist. Komput.* **2018**, *6*, 115–121. [CrossRef]
3. Dey, T.; Jaiswal, S.; Sunderkrishnan, S.; Katre, N. HealthSense: A medical use case of Internet of Things and blockchain. In Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 7–8 December 2017; pp. 486–491. [CrossRef]
4. Jibril, I.; Agajo, J.; Ajao, L.A.; Kolo, J.; Ogbole, C.I. Development of a Medical Expert System for Hypertensive Patients Diagnosis: A Knowledge-Based Rules. *Adv. Electr. Telecommun. Eng.* **2018**, *1*, 39–47
5. HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. *Future Gener. Comput. Syst.* **2020**, *104*, 187–200. [CrossRef]
6. Aloi, G.; Fortino, G.; Gravina, R.; Pace, P.; Savaglio, C. Simulation-Driven Platform for Edge-Based AAL Systems. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 446–462. [CrossRef]
7. Muthanna, A.; A. Ateya, A.; Khakimov, A.; Gudkova, I.; Abuarqoub, A.; Samouylov, K.; Koucheryavy, A. Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain. *J. Sens. Actuator Netw.* **2019**, *8*. [CrossRef]
8. Yi, S.; Li, C.; Li, Q. *A Survey of Fog Computing: Concepts, Applications and Issues*; Association for Computing Machinery: New York, NY, USA, 2015. [CrossRef]
9. Chen, Z.; Cui, H.; Wu, E.; Li, Y.; Xi, Y. Secure Distributed Data Management for Fog Computing in Large-Scale IoT Application: A Blockchain-Based Solution. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
10. Kajal, N.; Ikram, N.; Prachi, C. Security threats in cloud computing. In Proceedings of the International Conference on Computing, Communication Automation, Greater Noida, India, 15–16 May 2015; pp. 691–694. [CrossRef]
11. Erhan, D.; Anarim, E. Hybrid DDoS Detection Framework Using Matching Pursuit Algorithm. *IEEE Access* **2020**, *8*, 118912–118923. [CrossRef]
12. Mittal, M.; Iwendi, C.; Khan, S.; Rehman Javed, A. Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg-Marquardt neural network and gated recurrent unit for intrusion detection system. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e3997. [CrossRef]
13. Mittal, M.; Iwendi, C. A Survey on Energy-Aware Wireless Sensor Routing Protocols. *EAI Endorsed Trans. Energy Web* **2019**, *6*. [CrossRef]
14. Ahmed, A.A.; Wendy, K.; Kabir, M.N.; Sadiq, A.S. Dynamic Reciprocal Authentication Protocol for Mobile Cloud Computing. *IEEE Syst. J.* **2021**, *15*, 727–737. [CrossRef]
15. Wei, J.; Wang, X.; Li, N.; Yang, G.; Mu, Y. A Privacy-Preserving Fog Computing Framework for Vehicular Crowdsensing Networks. *IEEE Access* **2018**, *6*, 43776–43784. [CrossRef]
16. Camacho, J.; Maciá-Fernández, G.; Fuentes-García, N.M.; Saccenti, E. Semi-Supervised Multivariate Statistical Network Monitoring for Learning Security Threats. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2179–2189. [CrossRef]
17. Anajemba, J.H.; Iwendi, C.; Mittal, M.; Yue, T. Improved Advance Encryption Standard with a Privacy Database Structure for IoT Nodes. In Proceedings of the 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 10–12 April 2020; pp. 201–206. [CrossRef]
18. Iwendi, C.; Ansere, J.A.; Nkurunziza, P.; Anajemba, J.H.; Yixuan, Z. An ACO-KMT Energy Efficient Routing Scheme for Sensed-IoT Network. In Proceedings of the IECON 2018—44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018; pp. 3841–3846. [CrossRef]
19. Iwendi, C.; Uddin, M.; Ansere, J.A.; Nkurunziza, P.; Anajemba, J.H.; Bashir, A.K. On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique. *IEEE Access* **2018**, *6*, 47258–47267. [CrossRef]
20. Anajemba, J.H.; Yue, T.; Iwendi, C.; Chatterjee, P.; Ngabo, D.; Alnumay, W.S. A Secure Multi-user Privacy Technique for Wireless IoT Networks using Stochastic Privacy Optimization. *IEEE Internet Things J.* **2021**. [CrossRef]
21. Dang, T.D.; Hoang, D. A data protection model for fog computing. In Proceedings of the 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), Valencia, Spain, 8–11 May 2017; pp. 32–38. [CrossRef]
22. Abedi, M.; Pourkiani, M. Resource Allocation in Combined Fog-Cloud Scenarios by Using Artificial Intelligence. In Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, 20–23 April 2020; pp. 218–222. [CrossRef]
23. Winnie, Y.; Umamaheswari, E.; Ajay, D. Enhancing Data Security in IoT Healthcare Services Using Fog Computing. In Proceedings of the 2018 International Conference on Recent Trends in Advance Computing (ICRTAC), Chennai, India, 10–11 September 2018; pp. 200–205. [CrossRef]

24. Elie, E. Keynote speech 3: Intel Optane™ technology as differentiator for Internet of everything and fog computing. In Proceedings of the 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 23–26 April 2018; p. 3. [CrossRef]
25. Mittal, M.; Saraswat, L.K.; Iwendi, C.; Anajemba, J.H. A Neuro-Fuzzy Approach for Intrusion Detection in Energy Efficient Sensor Routing. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–5. [CrossRef]
26. Zhang, Z.; Wang, F.; Zhong, C.; Ma, H. Grid Terminal Data Security Management Mechanism Based On Master-Slave Blockchain. In Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15–18 May 2020; pp. 67–70. [CrossRef]
27. Fitwi, A.; Chen, Y.; Zhu, S. A Lightweight Blockchain-Based Privacy Protection for Smart Surveillance at the Edge. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 552–555. [CrossRef]
28. Wang, Y.; Zhang, A.; Zhang, P.; Wang, H. Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain. *IEEE Access* **2019**, *7*, 136704–136719. [CrossRef]
29. Shahnaz, A.; Qamar, U.; Khalid, A. Using Blockchain for Electronic Health Records. *IEEE Access* **2019**, *7*, 147782–147795. [CrossRef]
30. Ajao, L.A.; Agajo, J.; Adedokun, E.A.; Karngong, L. Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil and Gas Industry. *J* **2019**, *2*, 300–325. [CrossRef]
31. Ali, T.A.A.; Xiao, Z.; Sun, J.; Mirjalili, S.; Havyarimana, V.; Jiang, H. Optimal design of IIR wideband digital differentiators and integrators using salp swarm algorithm. *Knowl.-Based Syst.* **2019**, *182*, 104834. [CrossRef]
32. Iwendi, C.; Anajemba, J.H.; Biamba, C.; Ngabo, D. Security of Things Intrusion Detection System for Smart Healthcare. *Electronics* **2021**, *10*, 1375. [CrossRef]
33. Iwendi, C.; Khan, S.; Anajemba, J.H.; Mittal, M.; Alenezi, M.; Alazab, M. The Use of Ensemble Models for Multiple Class and Binary Class Classification for Improving Intrusion Detection Systems. *Sensors* **2020**, *20*, 2559. [CrossRef] [PubMed]
34. Anajemba, J.H.; Tang, Y.; Iwendi, C.; Ohwoekevwo, A.; Srivastava, G.; Jo, O. Realizing Efficient Security and Privacy in IoT Networks. *Sensors* **2020**, *20*, 2609. [CrossRef] [PubMed]
35. Yang, Z.; Liu, Y.; Campbell, M.; Ten, C.W.; Rho, Y.; Wang, L.; Wei, W. Premium Calculation for Insurance Businesses Based on Cyber Risks in IP-Based Power Substations. *IEEE Access* **2020**, *8*, 78890–78900. [CrossRef]
36. Xiao, Z.; Li, F.; Jiang, H.; Bai, J.; Xu, J.; Zeng, F.; Liu, M. A joint information and energy cooperation framework for CR-enabled macro–femto heterogeneous networks. *IEEE Internet Things J.* **2019**, *7*, 2828–2839. [CrossRef]
37. Xiao, Z.; Dai, X.; Jiang, H.; Wang, D.; Chen, H.; Yang, L.; Zeng, F. Vehicular task offloading via heat-aware MEC cooperation using game-theoretic method. *IEEE Internet Things J.* **2019**, *7*, 2038–2052. [CrossRef]