Hindawi
Security and Communication Networks
Volume 2022, Article ID 3940849, 11 pages
https://doi.org/10.1155/2022/3940849

Research Article

Secure Model for IoT Healthcare System under Encrypted Blockchain Framework

Rubal Jeet,[1] **Sandeep Singh Kang**,[1] **Shah Md. Safiul Hoque**,[2] **and Betty Nokobi Dugbakie**[3]

[1]*Chandigarh University, Gharuan, Mohali, Punjab, India*
[2]*Sohar University, Sohar, Oman*
[3]*Department of Chemical Engineering, Kwame Nkrumah University of Science and Technology, KNUST, Ghana*

Correspondence should be addressed to Rubal Jeet; rubaljeet86@gmail.com and Betty Nokobi Dugbakie; bdnokobi@st.knust.edu.gh

Received 4 March 2022; Accepted 15 April 2022; Published 9 May 2022

Academic Editor: Mukesh Soni

With the advancements in the new technologies like IoT, the healthcare sector is also growing rapidly. The core concept of introducing IoT in the healthcare centers is to make it remotely accessible, so that communication between doctor and patient can be easy, and diagnosis of any disease can be remotely done through the Internet in case of emergency. The major objective of this study is to develop a security framework for the healthcare industry that can encrypt secret data on cloud servers using block-based data encoding. Since any information that is available on the Internet is vulnerable to various attacks, and the medical records of the patients carry sensitive information that must not be accessible to any unauthorized or unauthentic person, in this context, the concept of Blockchain (BC) technology was introduced in the healthcare systems. In the past few years, a number of BC based healthcare models were proposed in the system; however, these systems are decentralized in nature, which is a feature of Blockchain technology, but in certain applications, especially in healthcare, this feature gave rise to a problem termed as disease overlapping when the count of chains gets increased. To solve this issue, a BC based framework is used in this work that has a feature of creating a separate block in the chain every time whenever any alteration in information about patient's health, any allergies, new symptoms, medications, etc. is updated. In addition to this, securing the sensitive information of patients is taken into consideration by developing an improved and enhanced multilayer Blockchain based IoT data security approach that not only protects the data, but also builds the trust between patients/user and healthcare service providers. The main focused area of this research article is to propose a security framework for healthcare domain that can encrypt the confidential data over cloud server under block-based data encoding. In the proposed approach, 128-bit AES key is generated in order to support the SHA-256 hashing algorithm. Individual user's data is subdivided to blocks and encrypted to secure it from unauthorized access. An interface-based system is designed to present the real-world usage of the proposed model in healthcare application. Finally, the effectiveness of the proposed approach is validated in the MATLAB software in terms of MAE, RMSE, MSE, encryption time, and decryption time. The RSA and DSA are the most trending encryption algorithms. These algorithms are crucial components of Blockchain technology, implemented in the proposed work, and later on, their performances are also compared with each other to check their effectiveness. The simulation results demonstrated that the proposed encrypting algorithm surpasses the other encryption approaches such as RSA and DSA in all factors to prove its supremacy. The experimental results show that the encryption and decryption time are lowest in the proposed framework; therefore, its performance is more effective and robust. It is also more effective and resilient.

1. Introduction

In this 21st century, the medical field is still in its infancy and is growing exponentially in the developing nations. Significant attempts have been made by researchers in recent decades to incorporate information and communication technology (ICT) into healthcare practices. According to HIPAA security, data must establish means and processes to protect private data from unauthorized deletion or alteration. Moreover, a hashing algorithm may be employed to maintain data integrity. Implementing Blockchain network is one of the most successful methods since altering the

hashes of the information affects the whole chain. The technological developments are combined with medical information in E-healthcare, encompassing constant monitoring and transmission of health-related issues from the patient-centric environment to appropriate network operators [1]. Because of its incorporation in IoT (Internet of things), it is believed that, in the coming years, medical services and applications will produce hundreds of billions of dollars in revenue sector. The IoT devices play a crucial role in health care system. The use of Blockchain in the medical system is critical because it allows doctors to rapidly and effectively acquire medical information about patients and treat them accordingly. This entire procedure of quickly getting patients' information may well be incredibly advantageous since doctors can readily access patients' medical records when the patient is unconscious and hospitalized for emergency treatment. Moreover, as individuals interact with a significant number of healthcare experts throughout their lives, and each one of them saves data in their own platform, which results in a fragmented systems and distinct database [2], this issue is solved by the IoT, which makes the life quite easier by requiring minimum human intervention; however, it also raises several security issues. The key contribution of this research is that it provides a BC-based framework that has characteristics of creating a separate block in the chain every time whenever any alteration in information about patient's health. Multiple IoT systems are deployed in the healthcare sector. In a typical IoT system, the data like BP, chest pain, heart rate, oxygen level, etc. is captured from the patients and is stored in the cloud server. This data can be accessed anytime and anywhere by the healthcare experts to monitor patients' health. In addition to this, the doctors and physicians can also retrieve patients past medical records, which help them in diagnosing the disease properly. However, with the increase in the number of IoT devices, safety of patient's sensitive data is also becoming increasingly important. In the cloud, healthcare data may not be as secure as it appears. An intruder may manipulate patient records, exposing sensitive information about a patient. Health information is highly delicate, and an intruder can take full advantage of a person's vulnerabilities. For example, if a person is intolerant to a particular food, the attacker can take use of this [3]. Moreover, there are some other security and privacy issues in healthcare centers that are discussed in the following section.

1.1. Security Issues in Healthcare Systems. As we all understand, cloud technology does have its own set of security issues that come up at times as a result of inadequate security technology and a lack of safety adherence [4–7]. Some of them are discussed here.

1.1.1. Confidentiality. It can be defined as a technique or method that prevents unwanted exposure to healthcare data through external or internal customers. This unauthorized and unauthentic access is problematic because it can lead to data leaks and possibly major financial harm to enterprises. In the healthcare field, secrecy is critical since patients may be hesitant to provide personal information to physicians when they are not comfortable in the anonymity. It can be accomplished by restricting user access and employing encrypted mechanisms.

1.1.2. Data Integrity. It is a crucial aspect that ensures that patients' information is not altered or hindered at any point. As per the HIPAA security, the data must implement methods and procedures to secure confidential information from any improper deletion or modifications. Furthermore, a hashing technique may be used to ensure integrity of data. Adopting Blockchain applications is among the best and most effective techniques since changing the hashing of the information would affect the entire chain.

1.1.3. Lack of Security Technologies. The construction of adequate security framework to survive attacks is the most difficult problem throughout the move to cloud services. Consequently, numerous firms are still baffled by this approach. The companies believe that cloud migration is all about lifting and shifting process where data is moved from their current IT infrastructure and safety measures to the cloud servers; however, in reality, data is vulnerable to a variety of dangers. A lack of understanding of the shared security obligation is another factor.

1.1.4. Account Hijacking. It is an important characteristic that allows hackers to obtain administrative privileges and leverage dangerous or vulnerable permissions. Such credentials may be vulnerable to criminal attacks on sensitive information, cloud system breaches, or accessibility to intercepted signals.

As a result, considering the prevailing medical system's issues, it is critical to take advantage of Blockchain technology's possibilities in the healthcare sector [4]. However, by utilizing Blockchain technology, these issues are alleviated, and the consumer is given ultimate control over his information. Without his permission, the data can be exchanged with anybody [5].

The present article has been planned into various sections. Section 1 deals with introducing the concept and importance of IoT system in healthcare. Section sheds light on literature survey. Section 3 illustrates proposed framework of IoT Blockchain system. The proposed algorithm is described in Section 4. The experimental analyses are described in Section 5. Finally, Section 6 portrays the conclusion and possible future works based on the proposed framework.

1.2. Blockchain Technology and Its Architecture. An article entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" was published in 2008 by a person or group of people authoring underneath the name Satoshi Nakamoto. This study suggested a peer-to-peer digital money system, which allows Internet payments to be made straight from one person to the other without having to go through a banking institution. This concept was first realized in Bitcoin. In

contrast to schemes wherein payments are channeled through a trusted centralized body, the term cryptocurrency is now used to represent all platforms and means of exchange that use encryption to safeguard operations [6].

Blockchain technology can be defined as the distributed digital database that is used to secure ever-growing data lists and transactions on the Internet. In other words, it can be defined as the data structure that is cryptographically secure and irreversible and can be written once and retrieved anyplace. It is composed of blocks that are connected altogether via a nonmodifiable key referencing method. In conventional databases, the centralized authentication system governs access control, which makes it difficult for individuals to access data present in it at one time [7]. The blockchain technology allows information to be examined with minimum human interaction, reducing the chance of human error. Compared to traditional methods, research has demonstrated that adopting Blockchain protocols improves the security of sending and retrieving e-health information. The medical sector's rapid adoption of digitalization has led in the creation of huge computerized patient data. The advancement of Blockchain technology has opened up new possibilities for dealing with major privacy protection, authenticity, and security challenges in the healthcare industry. Additionally, Blockchain technology has been implemented in various areas, like energy resources, elections, and medical systems.

Generally, the details about the transactions are divided into blocks with encryption to form a chain, which can never be erased from it. A linked list of cryptographic operations, which employs a hashing instead of a pointer, secures the information in Blockchain. The hashish function is used to generate a hash value by encrypting the input data. It serves as an intermediary to the patient's medical record and lays the basis of a distributed medical service stage maintained by patients and providers [8, 9]. The architecture of the proposed of the Blockchain is shown in Figure 1.

A typical Blockchain network comprises Blockchain network, peer to peer network, and consensus and security mechanism. The important and sensitive information about the patient's health is maintained by the Blockchain network. The similar Blockchain data structure instances are present in the peer to peer network, while the consensus method ensures that Blockchain's synchronized development and the security method protect the immutability of stored data on the Blockchain network.

1.3. Application of Blockchain in Health Sectors. As discussed earlier, the concept of the Blockchain can be integrated in a number of fields. Among the all areas, implementation of the Blockchain in medical system is crucial because, through this, the doctors can obtain the medical information of patients quickly and effectively and treat accordingly. This whole process of swiftly obtaining patients information could be very beneficial as doctors can retrieve patient's medical information easily whilst the patient is unconscious and hospitalized for emergency treatment. This would improve the treatment's efficiency and boost the chances of a satisfactory result. This would improve the treatment's efficiency and boost the chances of a satisfactory result. In comparison to traditional approaches, investigations have shown that using Blockchain protocols enhances safety for exchanging and retrieving e-health records.

Blockchain also enables information to be analyzed with minimal human intervention, lowering the risk of human mistake. The proposed model of blockchain is more secure than previous blockchain models. The previous blockchain is decentralized in nature, which is a characteristic of Blockchain technology, but in some applications, particularly in healthcare, this feature gave rise to a problem termed as disease overlapping when the count of chains gets increased. The suggested framework is effective and efficient because it incorporates an additional data security level, which increases patient trust. Another way blockchain technology could be used in healthcare is in combination with wearing smart technologies. With so many individuals wearing wearable gadgets, creating a safe mechanism to communicate this information can help physicians and other healthcare practitioners treat and track their patients better. Doctors may be able to let their patient's live normal lifestyles even though they are at a higher risk for health problems by tracking their data remotely. This technique might also improve clinical studies by providing a new tool for patients and clinicians to monitor their development. Individuals may be readier to engage in studies or experimental treatments if they do not have to go to the physician that often [10]. Even though there are number of advantages of the Blockchain technology, still there exist a number of unresolved challenges related to the confidentiality and privacy of patient's data such as information security, confidentiality, transaction mutability, and reliability, to name a few [11, 12]. Different encryption techniques can be used to mitigate these issues. A significant number of modern encrypting algorithms such as RSA, AES, Triple DES, Two-fish, and others act as the key components in Blockchain technology, hence bringing attention to Blockchain cryptography. The guarantee of consumer data and transactional data protection is a must for blockchain's attractiveness to grow [13].

2. Literature Survey

Over the years, a huge number of researchers used various encryption algorithms to offer the data security and data integrity. Some of the recently proposed approaches are discussed here; Bhutta et al. [14] suggested an effective and secured disease prediction model in fog computing that was based on Blockchain. Diabetes and cardiovascular illnesses were taken into account while making predictions. The authors obtained the patient data through fog nodes, which was later on stored in Blockchain. The patient medical files were firstly clustered using the innovative rule-based clustering method and after that, feature selection based adaptive neuro-fuzzy inference system (FS-ANFIS) was employed for forecast diabetes and cardiovascular illnesses. The test findings revealed that when compared to existing

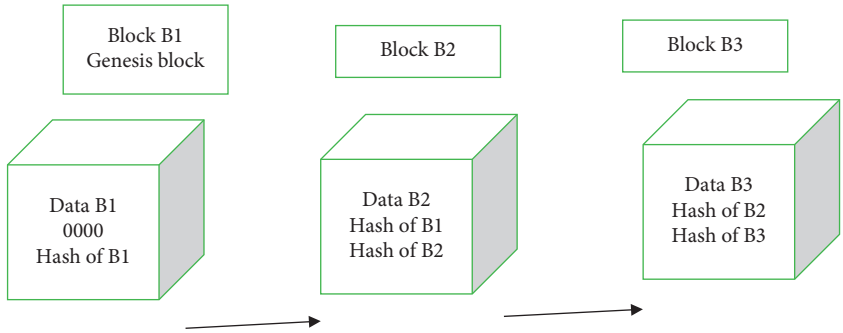

Figure 1: Blockchain architecture.

NN techniques, the suggested approach achieves an accuracy rate of over 81 percent. Kumar et al. [4] suggested a new model for Blockchain encryption in which the MD5 was used as the encryption algorithm. The main benefit of the suggested scheme was that modifying or updating data was very difficult with authorization and hence incorporated the Blockchain with the distributed approach. Mahoreet al. [15] suggested a paradigm that focused on supplying academics with the medical information while maintaining the privacy and confidentiality of the users for static analysis. The authors also combined the tailored access control mechanism with the asymmetric cryptography for enhancing the security of the system. In addition to this, the information was exchanged from one point to another by using proxy reencryption method. In Shynu et al. [16], a dual Blockchain strategy for the health industry was suggested. The idea was to connect the medical institution Blockchain with patient personal Blockchain so that a secure authorization monitoring protocol can be created that improves records and authorization consistency while increasing security and privacy. The recommended paradigm and its potential implementation were explored in relation to Alberta's healthcare privacy regulations. Sehgal et al. [17] incorporated the Blockchain technique with the IoT security that relied on remotely monitoring patient's health. The study discussed various advantages and drawbacks of Blockchain-based security techniques in IoT-based remote patient monitoring. In addition to this, the study assessed and evaluated a number of cryptographic methods that could be useful in IoT deployments. Sosu et al. [18] developed, constructed, and launched an architecture in which they attempted to leverage Public Key Infrastructure (PKI) and Hyperledger fabric to replicate healthcare process whilst assuring that patients' health files are under the absolute control of the patient exclusively. Moreover, the proxy reencryption was also used for providing access to others with the consent of patients. Mahore et al. [19], in order to ensure data security and integrity, proposed BiiMED approach that improved data interoperability and integrity in HER sharing. Moreover, an access management system permitting the transmission of EHRs among multiple health personnel and a decentralized Trusted Third Party Auditor (TTPA) for assuring data integrity are among the recommended techniques. Goel et al. [20] presented a Blockchain based distributed solution for providing security to patients data when viewed. The current system comprised three parts: the first is authentication, which was done through quantum cryptography, the second part was encryption that was done via AES, and finally for retrieving data, SHA algorithm was used. Ghozali et al. [21] examined the importance of Blockchain in healthcare systems to develop a more effective way as well as how the emergence of this revolutionary system can result in more effectual and adaptable facilities for managing records while maintaining the confidentiality and ensuring privacy to sensitive data. Srivastava et al. [22] proposed a Blockchain based system for storing and maintaining the records of patients. By doing so, the sensitive information of patients was accessed by the patients, doctors, and other information centers while protecting patients privacy.

After analyzing the literature survey, it was observed that, over the years, a significant number of Blockchain based methods were proposed to ensure data security and integrity. However, the major problem in these systems was that while sending the data over the cloud, it was susceptible to many attacks. This causes a sense of insecurity among the patients, and hence, they are not comfortable in sharing their details. However, this problem could be eliminated by encrypting the data through various encryption algorithms. However, after reviewing the literature, we observed that not much work has been done with encryption algorithms. Only few researchers have utilized encryption algorithms, but even those methods had high complexity and are less thorough. Moreover, the high encrypting and decrypting time of such algorithms also became a problem. Therefore, in order to protect any unauthorized and unauthentic access to patient's data, an improved Blockchain based IoT framework for health care systems will be proposed in this paper.

3. Proposed Framework of IoT Blockchain System

The introduction of IoT in the medical and healthcare centers was done in order to make the patient data remotely accessible anywhere and anytime. Since the Internet is susceptible to many attacks that are carried out by hackers/attackers, the patients are not comfortable in sharing their data over the network. The concept of blockchain technology is defined as the distributed digital database that is used to secure ever-growing data lists and transactions on the

Internet. It is made up of blocks that are linked together using a nonmodifiable key referencing system. The limitation of blockchain technology in healthcare is that, in certain applications, especially in healthcare, this feature gave rise to a problem termed as disease overlapping when the count of chains gets increased. The patients fear that their sensitive and confidential medical information can be accessed by some unauthorized and unauthentic persons, which can later be used against them. In order to give a sense of relief to patients, the concept of Blockchain technology is introduced in the healthcare systems. Over the years, a significant number of Blockchain based healthcare systems have been proposed for enhancing the reliability and accessibility of the data. But the problem with these systems was that they were too time-consuming and were different for individual medical institution/hospital. This means that when the patient moves to any other hospital for treating the any disease, the earlier medical records cannot be accessed because of the different BCs, and the new information about patients' allergies, symptoms, and medications cannot be added to the records. This causes disease overlapping problem, which leads to discrepancies that hinder the treatment process. In order to address this issue, a Blockchain based approach is considered in this framework, in which whenever any change is observed in the patient's records, a separate block is created that depicts the changes like allergies, new symptoms, change in medications, etc. and adds it to the existing chain without taking any particular permissions or details from the hospitals. By doing so, the patients' data is updated continuously without overlapping the existing data, and hence, treatment is done accordingly by the doctor through accessing data from the records. The detailed information about our BC based framework to handle disease overlapping can be studied in [23]. Securing the sensitive medical information over the network is achieved by proposing a security framework in this paper that will enhance the security by storing the patient information in the encrypted form. The main motive of the proposed Blockchain based IoT framework is to develop an effective and robust security procedure by using encryption algorithm and public Blockchain [24]. As data security is one of the major issues in IoT healthcare systems that cannot be overheard, therefore, the main focus of proposed work is to develop an IoT Blockchain system in which the patient's data will be more secure and scalable.

By doing so, the patients will feel free to share their sensitive medical information with doctors and information centers, which in return will make the entire process more reliable and trustworthy [25]. Keeping these objectives in mind, this research aims to provide a framework contributing to manage the healthcare system with security to sensitive information for IoT cloud-based data servers using Blockchain technology. Figure 2 represents the architectural diagram of the proposed Blockchain based IoT healthcare system. Generally, in any IoT based Blockchain system, the data is transmitted from real world to the cloud server through three layers. At the lower layer, the information is collected through sensors or actuators. This information is then directly passed to the second layer where it is divided into a number of blocks and finally sent to the cloud server in the third layer. Since the patient's data contains sensitive information, which cannot be accessed or revealed to any unauthorized person, therefore, securing this data in the IoT framework is very crucial [26]. In order to secure this data from any unauthorized and unauthentic access, in this research, modifications are done in the second layer of the IoT system, as depicted in Figure 2. By adding the extra data security mechanism in the second layer, the reliability and trust among patients and information centers are boosted. In the proposed framework, information is acquired through the patients, doctors, and even hospitals. In order to avoid complexity and dimensionality issues, a real time dataset has been used that is taken from Kaggle.com. This dataset contains information of confidential information of patients like age, sex, Chest pain, BP, S.C, H.R.A, P.E, thal, etc. Table 1 illustrates an example of the patient's data obtained from the real world.

As mentioned earlier, the data collected at the prior level is sensitive and confidential and must be secured. In order to provide that additional security, the patient's data is encrypted by using the encryption algorithm. However, as there are a number of encryption algorithms available, it is difficult to select one algorithm and implement it. Therefore, the three most trending encryption algorithms, that is, RSA, DSA, and AES, are implemented in the proposed work, and later on, their performances are also compared with each other to check their effectiveness [27]. In the proposed work, the AES encryption algorithm used has become its key expansion ability. By encrypting the patient's data, not only the sensitive medical information of patients is secured from any unauthorized access, but it also builds the trust among patients and information center like hospitals. Thus, it provides an extra layer of security to the current IoT systems. Once the data is encrypted, it is broken down into a number of heterogeneous blocks. After this, hashing algorithm is then applied to these blocks, thus providing a double layer security to the patient's data. In the third and final layer of the proposed model, the encrypted and secured data of patient is moved to the cloud layer where it is stored and can be accessed whenever needed. On the basis of these enumerated layers of the suggested IoT architecture, the given goals must be accomplished [28].

(i) Authentication: the users must be authenticated and authorized for accessing the model and for this public Blockchain used.

(ii) Privacy protection: the privacy of the users must be maintained and to do so, our model used the multilayer security system (encryption and Blockchain).

(iii) Trust: the proposed IoT framework must be able to build trust between different IoT members.

3.1. Interface of the Proposed Blockchain Based IoT Healthcare System. Now, the question is how the proposed Blockchain based IOT system for healthcare works to

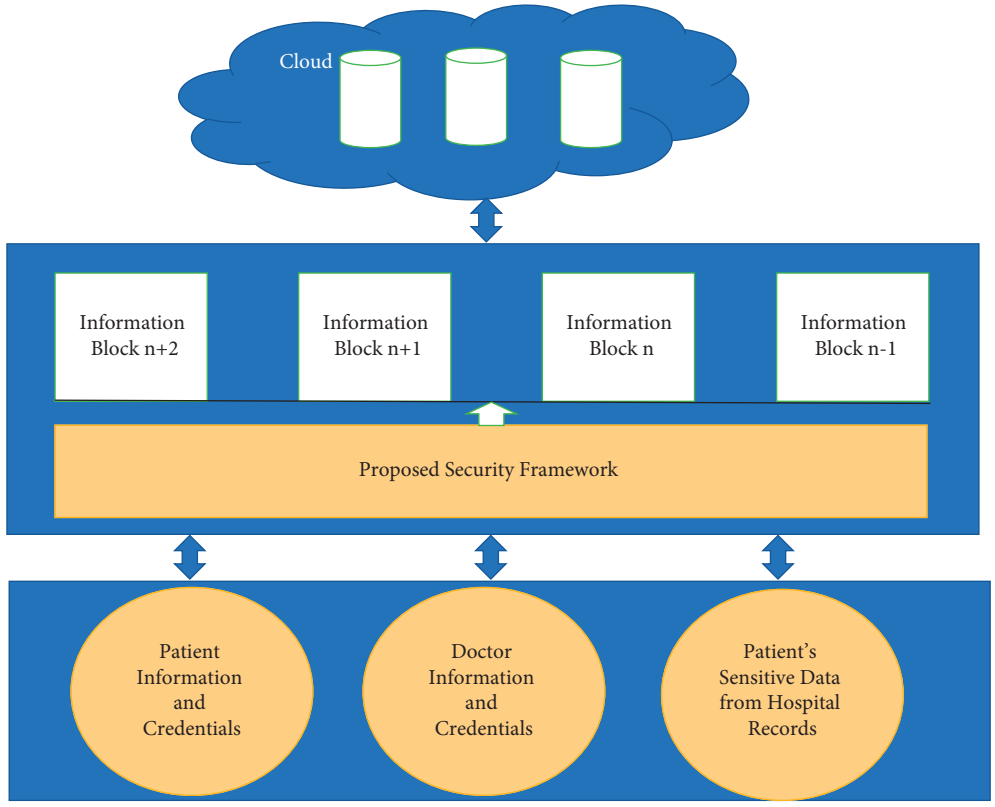

Figure 2: Proposed frameworks for IoT Blockchain system.

Table 1: Patient's information dataset.

Age	Sex	Chest pain	B.P	S.C	H.R.A	P.E	N.M.V	Thal
70	1	4	130	322	109	2	3	3
67	0	3	115	564	160	2	0	7
57	1	2	124	261	141	1	0	7
64	1	4	128	263	105	2	1	7
74	0	2	120	269	121	1	1	3

achieve above-mentioned objectives. For this, an application-oriented model is developed where users can register themselves by entering their credentials. Figure 3 illustrates the interface of the proposed IoT-blockchain approach for healthcare systems.

The suggested Blockchain based IoT healthcare system includes different sections, which include registration unit, login unit, authentication form, and data center. Here, we will be explaining each component very briefly in a step by step manner.

(i) Registration: to access the system, the first step is to register the user, which can be a doctor or a patient. During this process, critical information like username, contact number, user id, password, user type, and image is recorded and stored. The user type depicts whether the registering person is a doctor or a patient. Moreover, the image is uploaded in the database so that it can be used for verification in the latter process. Once the user submits all the necessary information, it is stored at the cloud.

(ii) Authentication: once the users are registered, they can easily login into the system by simply entering their login credentials. The person enters his or her user id and password along with the user type and hits the login button to access the proposed IoT system. As soon as the user hits login button, a request is sent by the login module to the cloud storage, which matches the entered credentials with the registered ones. If the credentials entered matched with the any of the registered users, it sends a response back to the login module and allows the user to access the system and denies the access request when the credentials do not match with anyone in the cloud, thereby giving access only to the authorized and authentic persons. As mentioned earlier, the user can be either doctor or a patient. Both parties can view and enter different information.

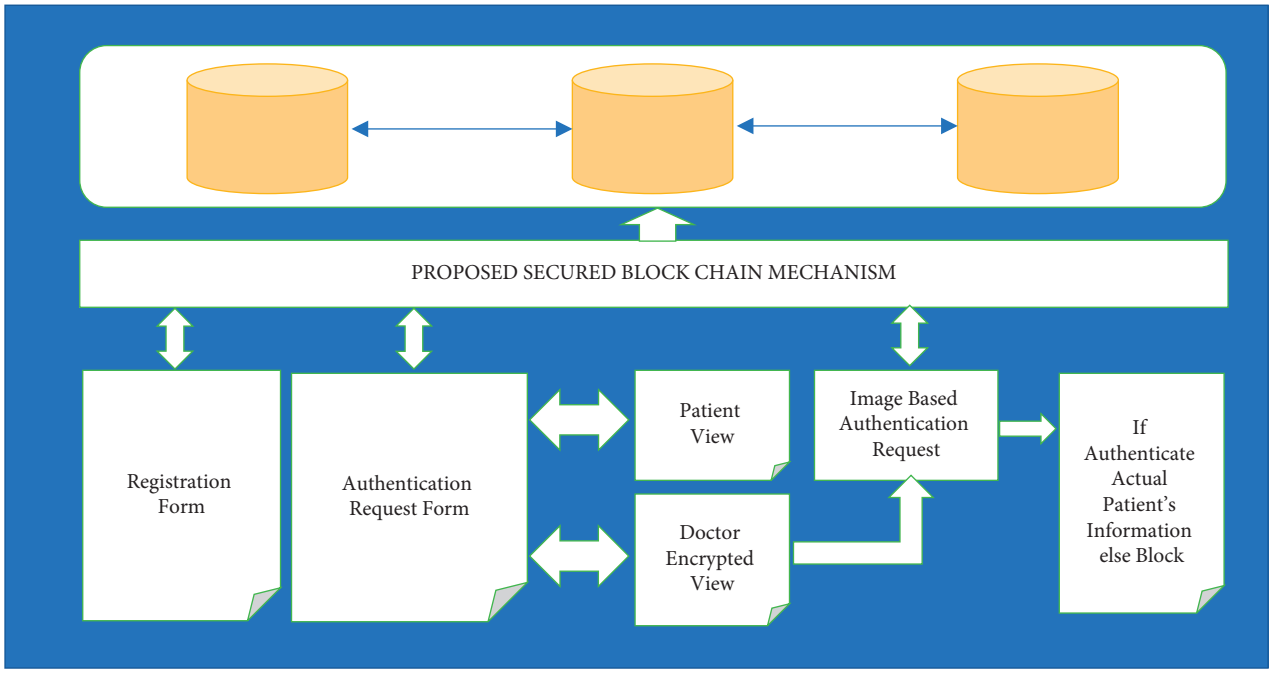

Figure 3: Interface of proposed IoT approach.

(iii) Patient view: when the user is a patient, the information to be entered or viewed is his/her name, contact number, age, and sex. Moreover, their medical records, which include BP, SC, HRA, PENMV, and the doctor assigned to the patient is also displayed.

(iv) Doctor view: on the other hand, when the doctor is using the systems by entering his credentials, a screen appears where the doctor can see and examine the health of the patient by selecting his name. However, as the information obtained earlier is encrypted, so the doctor will not be able to see the patients' records easily.

(v) Image based authentication: in order to view the sensitive information of patient, the doctor needs to submit the decoding credentials where his picture is uploaded. The system again checks and tries to authenticate the request with the cloud storage to validate the decoding credentials; if it matches, the medical information of patient is decoded and can be accessed by the assigned doctor; otherwise, the request to access the data is denied, thus providing a multiple layer of security.

4. Proposed Algorithm

The proposed algorithm will undergo a number of steps to attain the desired results. As mentioned in the previous section, the patient data (user id, password, contact number, age, and medical information) is collected and encrypted before storing it in the cloud database in order to maintain the privacy and security of data. This sensitive data is stored at multiple locations, so that information can be retrieved anytime anywhere even if one server is down due to some reasons. Similarly, all the necessary information about the doctor, which includes name, user id, password, contact number, and photograph, is collected and stored in the local server without encryption. Once all the information is attained, the main process of encryption begins. In this section, our major focus will be on how encryption and decryption of the data are done in the proposed framework. The algorithm of the proposed encryption process is given as follows:

Pseudocode for encryption

(1) # Parameters
(2) Pinfo = Patient's Confidential Information
(3) Dkey = Doctor's authentication key
(4) Key_Size = 128
(5) Split_Size = 32
(6) GnBlk = Genrel Block
(7) ##
######
(8) # Encryption Algorithm
(9) ##
######
(10) Begin
(11) Key = AESKeyGeneration (Key_Size)
(12) Len = length (Key)
(13) SplittedKeys [K1, K2, K3, K4] =
[Key [1 : Split_Size: Len]]
(14) GnBlk = join (K1 ⊕ K2, K3 ⊕ K4)
(15) # Information scalling

(16) If rem (len (Pinfo)/SplitSize) = = Null: DataP = Pinfo
(17) Else: DataP = Join (Pinfo, zeros (rem (len (Pinfo)/SplitSize)))
(18) BlockData = DataP (1 : 32 : length(DataP))
(19) # Encryption Started
(20) BlkCount = len (1 : 32 : length(DataP))
(21) YData = Block ⊕ GnBlk;
(22) Fori = 2: BlkCount
(23) Block = BlockData (*i*);
(24) Ydata(*i*) = Block ⊕ GnBlk (*i* − 1);
(25) GnBlk(*i*) = SHA256HashCompute (Ydata(*i*));
(26) End

4.1. Encryption Process. In order to add the extra layer of security to the patient's data, it needs to be encrypted by some sort of strong encryption algorithm. In the proposed work, AES algorithm is be employed for data encryption because of its key expansion ability where the first key is utilized to generate a succession of new keys known as round keys in order to provide that extra level of security. These round keys are created through a series of modifications, each of which makes it more difficult to decrypt the data. The process of encryption begins with the key generation whose length is 128 bits after key generation data blocks are formed.

4.2. Block Formation and Information Scaling. Once the key of 128 bits is generated, blocks are formed by dividing the data packet into four blocks, with each block having a size of 32 bits. A block can be defined as the fundamental piece that stores information about transactions. It basically consists of two parts: one is called the header, and the other is called the body. Information like block number, hash code, previous block hash, metadata, and timestamp is stored in the block header, while information like transaction and transaction counters is stored in the block body. Each and every block in the system is cryptographically connected to the other system, making the data withdrawal easier. Moreover, while forming the blocks, their size is checked and adjusted if it is less than 32 bits by filling up the clank spaces with zeros, which is also called zero padding.

4.3. AES Key Division. Now, when the size of blocks is adjusted to 32 bits, the next step is to use the AES encryption key. To do so, we divided the key into 4 groups, each with size of 32 bits. After this, two groups of K1, K2 and K3, K4 are formed, and XOR operation is applied to them. The output of the two groups is the genesis block, which is helpful for encrypting data. To form a chain, SHA-256 hashing algorithm is used.

4.4. SHA-256 Hashing Algorithm. To encrypt the data, a 32-bit data block is received, which is then combined with the genesis block, and XOR operation is applied to form a new block and create a chain. The first block in the chain formation will be the AES key itself, and to form the new block, the SHA hasher updates the block every time on the basis of the encrypted data in the prior block and encrypts data in the next block. This process is repeated until all the data is encrypted successfully. Once it is encrypted, the data is sent to the cloud so that it is securely stored.

4.5. Decryption Process. As the information available on the data is now encrypted, so as soon as the doctor enters his credentials to access the patient's data, he receives the information in the encrypted form. To decrypt this data, the doctor must confirm his identity. To do so, the doctor uploads his picture, which is then validated by matching it with the doctor database in the local server. If it matches it, the information is decrypted; otherwise, the authentication request is denied/rejected. The process of decryption is just the reverse procedure of the encryption algorithm. The pseudocode of for the decryption is given below. In the decryption process, the first data block is retrieved from the generated key itself, and then, the SHA256hashcompute is applied to the next block. After this, the XOR operation is performed on the 32-bit data block and genesis block to get the original and decrypted data. The process is repeated continuously till all the information is decrypted successfully.

Pseudocode for decryption process
(1) ##
######
(2) # Decryption Algorithm
(3) ##
######
(4) Key = AESKeyGeneration (Key_Size);
(5) Len = length (Key);
(6) SplittedKeys [K1, K2, K3, K4] = [Key [1: Split_Size: Len]];
(7) GnBlk = join (K1 ⊕ K2, K3 ⊕ K4);
(8) DecryptMes = zeros;
(9) DataP = [];
(10) *k* = 1;
(11) Fori = 1: BlkCount
(12) GnBlk (*k* + 1) = SHA256HashCompute (BlockData (*i*));
(13) DecryptMes (*i*) = Block ⊕ GnBlk (*k*);
(14) *k*++;
(15) DataP = DataP.join (DecryptMes (*i*));
(16) End
(17) DecryptedData = DataP;

4.6. Implementing Proposed IoT Network Architecture. In order to ensure the robustness and steadfastness of the proposed Blockchain based IoT health care system, it must satisfy all the security compatibility requirements. The core

safety, compatibility goals, and prerequisites for our suggested scheme are highlighted in this section.

(a) Scalability: it refers to the capability of the system that ensures that the size of the model does not hinder its performance. In the suggested scheme, a peer to peer network can accommodate two communication types: one is associated and the other is aggregated requests. While the first utilizes a public Blockchain to handle association queries, the other employs a health-edge to allow for regulated interaction on aggregate requests between members across zones.

(b) Authentication and authorization: a blockchain-based authentication mechanism is employed in the proposed framework, through which the credentials of the IoT members are validated. This mechanism safeguards the model from spoofing. Also, by validating the credentials, only the authorized person can access the data stored in the cloud database.

(c) Trustworthiness: in classical IoT based healthcare systems, the reliability of the system was evaluated by using the hashing and signed exchanged messages. In our proposed model, we enhance the security level by encrypting the user data before uploading it on the cloud. This encrypted data can be decrypted by the authorized persons only, thereby boosting the trust among different IoT members.

(d) Data integrity: data integrity ensures the authenticity of the data stored in the system. In other words, it can also be defined as the policy that ensures that no exchanged communications can be altered or updated from one user to another during their entire life cycle. The changes can only be made by the authentic and authorized person therefore, safeguarding the system.

In addition to the above-mentioned critical parameters, the efficacy of the suggested Blockchain based IoT healthcare system is examined in the MATLAB environment in terms of mean absolute error (MAE), Root mean square error (RMSE), and mean squared error (MSE). The value of all the three parameters should be high in order to prove its effectiveness. The detailed version of how the proposed encryption model performs is given in the following section of this paper.

5. Experimental Analysis

The analysis of the proposed IoT model is firstly analyzed and compared with the MAE results obtained in the traditional RSA and DSA encryption algorithms, and the graph obtained from the same is given in Figure 4. The blue and orange bars depict the performance of traditional RSA and DSA algorithms, respectively, while the yellow colored bar depicts the performance of proposed system. After examining the graph closely, it was observed that the value of MAE delineated in traditional RSA and DSA techniques was 45.22305 and 59.11055, respectively, whereas the value

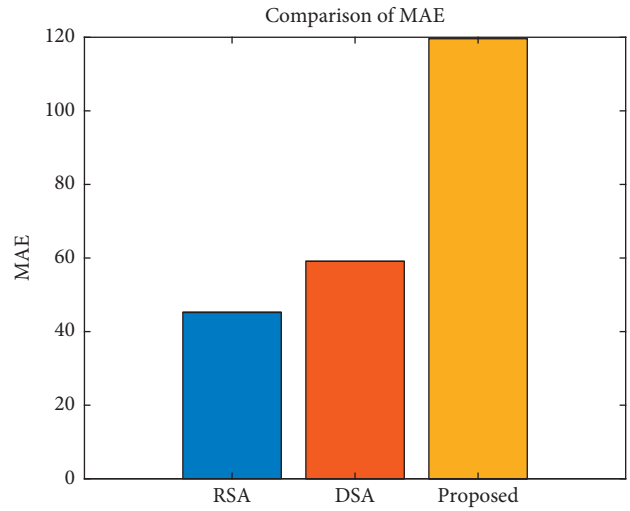

Figure 4: Comparisons for mean absolute error.

attained for MAE in the proposed IoT model came out to be incredibly high at 119.6063, marking its efficacy and effectiveness.

Likewise, the performance of the suggested scheme was analyzed and observed in terms of the RMSE (see Figure 5). The simulating results obtained were also compared with the traditional RSA and DSA encryption algorithm to prove the supremacy of the suggested approach. From the graph, it is observed that the value of the root mean square error in traditional RSA model came out to be 53.70382, followed by the DSA with 60.17446, whereas the RMSE attained in the proposed model is quite higher with a value of 140.339. This increased value of RMSE showcased that proposed model is more effective and resilient.

In addition to this, the effectiveness of the suggested model is delineated and later on compared with the standard RSA and DSA system in terms of Mean Squared Error (MSE). Figure 5 depicts the comparison graph obtained for the same.

Figure 6 illustrates the comparison graph of the proposed framework and conventional RSA, DSA frameworks in terms of MSE. The x-axis and the y-axis of the graph calibrate to the different algorithms and their respective values. After thoroughly examining the graph, it was found that the MSE value came out to be maximizing in the proposed model with 19695.03 making it supreme and effective, while the value of MSE came out to be minimum in standard RSA method with just 2884.1 values followed by the standard DSA model with 3620.966. These low values in MSE make these models less effective and less efficient and, therefore, are not recommended in the real-world scenario.

5.1. Time Oriented Evaluation. Additionally, the performance of the proposed framework is also depicted and contrasted with the standard RSA and DSA algorithms in terms of their encryption and decryption time. The encryption time of the system depicts the total time taken by the algorithm to generate cipher or encrypted text from the plain text. It also determines the throughput of algorithm

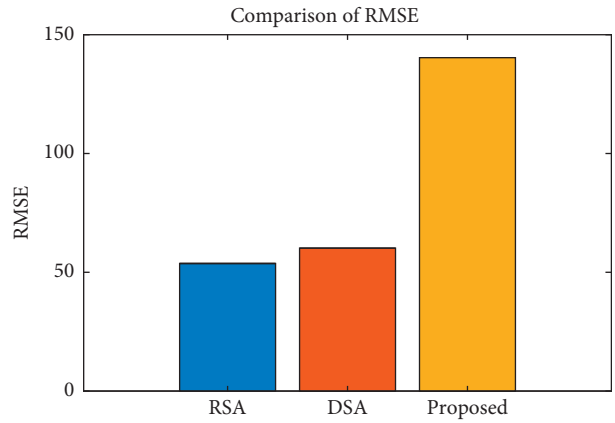

Figure 5: Comparisons for root mean square error.

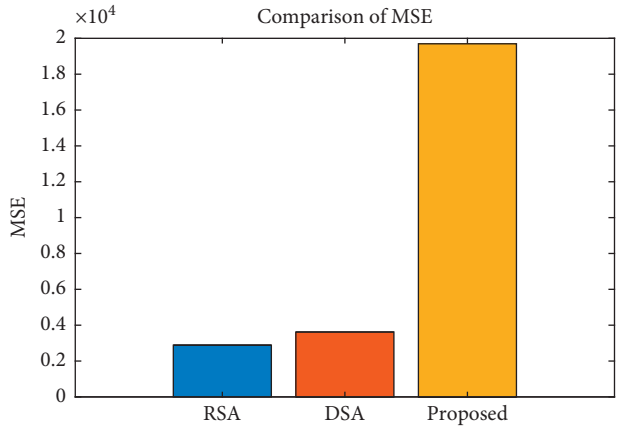

Figure 6: Comparison for mean squared error (MSE).

that is computed by dividing the total encrypted plaintext (MB or bytes) by the encryption time (MS). The throughput of any encryption algorithm determined the speed of its encryption, which means that if we want a high throughput, the encrypting time must be as minimum as possible. As the output of an encryption technology increases, the power consumption of that approach decreases due to the reduction in time spent encrypting and decrypting data. The encryption time came out to be minimizing in the proposed framework with just 0.032955 encryption time, while it came out to be maximizing in DSA algorithm with 11.1202 followed by RSA with 0.253194. The decryption time can be defined as just the reverse of the encryption time, that is, the time taken by the algorithm to obtain plain text from the encrypted text. The decryption time also indicates the throughput of the algorithm. The shorter the decryption time, the better the performance of the algorithm. In the proposed work, least decryption time is attained by the proposed algorithm, that is, just 0.024304 ms, while it is higher in DSA with 10.8254 ms and 0.254536 ms in RSA algorithm. As the encryption and decryption time are lowest in the proposed framework, therefore, its performance is more effective and robust. Table 2 shows the precise values obtained in each system.

Table 2: Exact values of parameters obtained in traditional RSA, DSA, and proposed model.

Parameters	RSA	DSA	Proposed
MAE	45.22305	59.11055	119.6063
RMSE	53.70382	60.17446	140.339
MSE	2884.1	3620.966	19695.03
Enc time	0.253194	11.1202	0.032955
Dec time	0.254536	10.8254	0.024304

6. Conclusion

Blockchain technology offers a solid foundation for securing and improving the efficiency of IoT systems used in healthcare systems. In this paper, a multilayer security blockchain based IoT health care system is proposed. The data of the patients is secured and protected by using the AES key generation property for encryption and SHA256 for chain formation. The proposed framework is effective and efficient as it includes the extra data security level, which in return boosts the trust of patients. The efficacy of the suggested framework is analyzed in the MATLAB software under different encrypting parameters like mean absolute error (MAE), Root Mean Square Error (RMSE), and Mean squared error (MSE), encryption time, and decryption time. Upon analyzing the results, it was found that MAE is highest in the proposed approach with 119.6063, while it was just 59.11055 in DSA and 45.22305 in RSA encryption algorithms. Moreover, the RMSE and MSE values obtained by the proposed approach came out to be 140.339 and 19695.03, respectively, while their values in the standard RSA and DSA were just 53.70382, 2884.1 and 60.17446, 3620.966, respectively. In addition to this, the efficiency of the encryption algorithm is depicted by its encrypting and decrypting time that calibrated to the 0.032955 and 0.024304 in the proposed model. The encryption and decryption time came out to be highest in DSA algorithm with 11.1202 and 10.8254, while they were 0.253194 and 0.254536 in the standard RSA algorithm. These values are enough to prove the supremacy of the proposed framework with highest MAE, RMSE, and MSE values and lowest encryption and decryption time.

Data Availability

The data shall be made available upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. Churi, A. Pawar, and A. J. Moreno-Guerrero, "A comprehensive survey on data utility and privacy: taking Indian healthcare system as a potential case study," *Inventions*, vol. 6, no. 3, p. 45, 2021.

[2] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-based approach for e-health data access management with privacy protection," in *Proceedings of the 2019 IEEE 24th International Workshop on Computer Aided Modelling and*

Design of Communication Links and Networks (CAMAD), pp. 1–7, Limassol, Cyprus, September 2019.

[3] A. Jangid, P. K. Dubey, and B. R. Chandavarkar, "Security issues and challenges in healthcare automated devices," in *Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 19–23, Bangalore, India, January 2020.

[4] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain Utilization in Healthcare: Key Requirements and Challenges," in *Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–7, Ostrava, Czech Republic, September 2018.

[5] A. Banotra, J. S. Sharma, S. Gupta, S. K. Gupta, D. Sachin, and M. Rashid, "Use of blockchain and internet of things for securing data in healthcare systems," *Multimedia Security*, pp. 255–267, 2021.

[6] R. Bharti, A. Khamparia, M. Shabaz, G. Dhiman, S. Pande, and P. Singh, "Prediction of heart disease using a combination of machine learning and deep learning," *Computational Intelligence and Neuroscience*, vol. 2021, pp. 1–11, Article ID 8387680, 2021.

[7] M. Crosby, P. P. Nachiappan, S. Verma, and V. Kalyanaraman, "BlockChain Technology beyond Bitcoin," Technical Report, 2015, Sutardja Center for Entrepreneurship & Technology, Berkeley, California, 2015.

[8] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: a state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, 2019.

[9] S. Gandhi and M. Shabaz, "Evichain: evaluating and scrutinizing crime using block chain," *International Journal of Recent Technology and Engineering*, vol. 8, no. 3, pp. 3992–3994, 2019.

[10] W. Alshahrani and R. Alshahrani, "Assessment of blockchain technology application in the improvement of pharmaceutical industry," in *Proceedings of the 2021 International Conference of Women in Data Science at Taif University (WiDSTaif)*, pp. 1–5, TU, Saudi Arabia, March 2021.

[11] S. Jain, A. Anand, A. Gupta, K. Awasthi, S. Gujrati, and J. Channegowda, "Blockchain and Machine Learning in Health Care and Management," in *Proceedings of the 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI)*, pp. 1–5, February 2020.

[12] K. Wilber, S. Vayansky, N. Costello, D. Berdik, and Y. Jararweh, "A Survey on Blockchain for Healthcare Informatics and Applications," in *Proceedings of the 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 1–9, Paris, France, December 2020.

[13] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of Blockchain and Internet of Things in healthcare and medical sector: applications, challenges, and future perspectives," *Journal of Food Quality*, vol. 2021, pp. 1–20, Article ID 7608296, 2021.

[14] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem et al., "A survey on blockchain technology: evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021.

[15] G. Iredale, "10 Blockchains," 2021, https://101blockchains.com/blockchain-cryptography.

[16] P. G. Shynu, V. G. Menon, R. L. Kumar, S. Kadry, and Y. Nam, "Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing," *IEEE Access*, vol. 9, pp. 45706–45720, 2021.

[17] P. Sehgal, B. Kumar, M. Sharma, A. A. Salameh, S. Kumar, and P. Asha, "Role of IoT in transformation of marketing: a quantitative study of opportunities and challenges," *Webology*, vol. 18, no. 3, pp. 1–11, 2022.

[18] R. N. A. Sosu, K. Quist-Aphetsi, and L. Nana, "A decentralized cryptographic blockchain approach for health information system," in *Proceedings of the 2019 International Conference on Computing, Computational Modelling and Applications (ICCMA)*, pp. 120–1204, Cape Coast, Ghana, March 2019.

[19] V. Mahore, P. Aggarwal, N. Andola, and S. Venkatesan, "Secure and Privacy Focused Electronic Health Record Management System Using Permissioned Blockchain," in *Proceedings of the 2019 IEEE Conference on Information and Communication Technology*, pp. 1–6, Allahabad, India, December 2019.

[20] U. Goel, R. Ruhl, and P. Zavarsky, "Using healthcare authority and patient blockchains to develop a tamper-proof record tracking system," in *Proceedings of the 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pp. 25–30, Washington, DC, USA, May 2019.

[21] M. Ghozali, S. Satibi, Z. Ikawati, and L. Lazuardi, "Asthma self-management app for Indonesian asthmatics: a patient-centered design," *Computer Methods and Programs in Biomedicine*, vol. 211, no. 106392, p. 106392, 2021.

[22] G. Srivastava, J. Crichigno, and S. Dhar, "A Light and Secure Healthcare Blockchain for IoT Medical Devices," in *Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, pp. 1–5, Edmonton, AB, Canada, May 2019.

[23] D. K. Meena, R. Dwivedi, and S. Shukla, "Preserving patient's privacy using proxy Re-encryption in permissioned blockchain," in *Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 450–457, Granada, Spain, October 2019.

[24] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: enhancing shared electronic health record interoperability and integrity," in *Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pp. 310–317, Doha, Qatar, February 2020.

[25] M. S. Christo, P. Sarathy, and C. Priyanka, "An efficient data security in medical report using block chain technology," in *Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP)*, pp. 0606–0610, Chennai, India, April 2019.

[26] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Blockchain vehicles for efficient Medical Record management," *NPJ Digital Medicine*, vol. 3, p. 1, 2020.

[27] J. Vora, A. Nayyar, S. Tanwar et al., "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," in *Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, Abu Dhabi, United Arab Emirates, December 2018.

[28] R. Jeet and S. S. Kang, "E-biomedical: a positive prospect to monitor human healthcare system using blockchain technology," *World Journal of Engineering*, vol. 19, no. 1, pp. 13–20, 2020.