



## Article

# Blockchain-Based Healthcare Information Preservation Using Extended Chaotic Maps for HIPAA Privacy/Security Regulations

Tian-Fu Lee <sup>1</sup>, I-Pin Chang <sup>2,\*</sup> and Ting-Shun Kung <sup>1</sup><sup>1</sup> Department of Medical Informatics and Institute of Medical Sciences, Tzu Chi University, Hualien 97004, Taiwan; jackytflee@mail.tcu.edu.tw (T.-F.L.); 107325109@gms.tcu.edu.tw (T.-S.K.)<sup>2</sup> Department of Industrial Management, National Taiwan University of Science and Technology, Taipei 106335, Taiwan

\* Correspondence: ipin@mail.ntust.edu.tw; Tel.: +886-2-2737-6731

**Abstract:** A healthcare information system allows patients and other users to remotely login to medical services to access health data through the Internet. To protect the privacy of patients and security over the public network, secure communication is required. Therefore, the security of data in transmission has been attracting increasing attention. In recent years, blockchain technology has also attracted more attention. Relevant research has been published at a high rate. Most methods of satisfying relevant security-related regulations use modular and exponential calculation. This study proposes a medical care information preservation mechanism that considers the entire process of data storage in devices from wearable devices to mobile devices to medical center servers. The entire process is protected and complies with HIPAA privacy and security regulations. The proposed scheme uses extended chaotic map technology to develop ID-based key negotiation for wearable devices, and thereby reduces the amount of computing that must be carried out by wearable devices and achieve lightness quantify. It also uses the non-tamperability of the blockchain to ensure that the data have not been tampered with, improving data security. The proposed mechanism can resist a variety of attacks and is computationally lighter than the elliptic curve point multiplication that has been used elsewhere, while retaining its security characteristics.

**Keywords:** blockchain; chaotic maps; HIPAA; access control; healthcare information; information security; patient privacy



**Citation:** Lee, T.-F.; Chang, I.-P.; Kung, T.-S. Blockchain-Based Healthcare Information Preservation Using Extended Chaotic Maps for HIPAA Privacy/Security Regulations. *Appl. Sci.* **2021**, *11*, 10576. <https://doi.org/10.3390/app112210576>

Academic Editors: Subhas Mukhopadhyay, Shantanu Pal and Nagender Kumar Suryadevara

Received: 6 September 2021

Accepted: 8 November 2021

Published: 10 November 2021

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



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

A healthcare information system allows patients and other users to login remotely to medical services to access health data through the Internet. To protect the privacy of patients and ensure security over the public network, secure communication is necessary.

Rapid technological development has made access to information part of our daily life, along with health care. In the field of personal health care, data sharing has become an important topic. The security of data in transmission is attracting increasing attention. In recent years, blockchain technology has also been attracting more attention. Relevant research has been published at a high rate [1–4]. It draws on many fields, including medicine, leasehold, energy, and others. However, with respect to personal information privacy, most attempts to satisfy security-related regulations use modular and exponential calculation.

To improve the security of the healthcare system, many studies have proposed the use of blockchain technology. In 2016, Azaria et al. [1] proposed a method of using blockchain technology to decentralize the management of large-scale data in electronic medical records (EMR), and enable patients to access them. The use of blockchain technology makes the records immutable and prevents malicious tampering with user cases, which violates the rights of patients.

In the same year, Peterson et al. [5] proposed a scheme in which blockchain technology is used to share data among hospitals. Using the concept of a distributed ledger and fast

healthcare interoperability resources (FHIR), they established standards for the integration of patient data with different specifications at different hospitals. They used Merkle tree architecture to integrate each user's medical records, facilitating verification of the data. In 2018, Jiang et al. [6] proposed BloCHIE, a blockchain-based platform for healthcare information exchange, which uses two loosely coupled blockchains to handle different kinds of healthcare data: the EMR-Chain handles electronic medical records while the PHD-Chain handles personal healthcare data. Implementation and evaluation revealed the practicability and effectiveness of BloCHIE. In 2018, Li et al. [7] proposed a medical information preservation system that is based on blockchain. The system splits each private file into many parts and uses elliptic curve cryptography to generate a key to encrypt the file for access by the patient. The file is then stored in different storage spaces in the system, and the file storage location index value is encrypted. However, this method was inconsistent with blockchain's decentralization.

Also in 2018, Kaur et al. [8] proposed an architecture of blockchain that ensures decentralization all healthcare data on centralized servers. They proposed a blockchain-based platform that can store and manage huge healthcare datasets with ease and security. In the same year, Esposito et al. [9] observed a significant shift of healthcare data to cloud services, but the mechanisms of this shift may not ensure data security and privacy. High et al. [10] proposed a unique blockchain-based method for accessing patient information that cannot be communicated but can be stored securely on wearable devices using blockchain. The patient's information is stored using an encrypted private key and a public key. The private key can be decrypted only using the patient's biometric signature. The combination of the public and private keys ensures that the critical records of the patient can be accessed only in emergency situations.

As seen above, a lot of research on healthcare information systems that use blockchain technology has been published [11–20]. However, to achieve the mutual authentication, the confidentiality and non-repudiation of data, and other security specifications, most research relies on computationally heavy modular exponential operations or elliptic curve point multiplication operations. The structures of these operations are very complex, and the number of involved calculations is huge, and the problem of efficiency remains to be solved. Therefore, this investigation will attempt to use light-weight operations, such as the hash function and chaotic mapping technique, to increase computational efficiency. Extended chaotic mapping technique will be used to develop a blockchain-based medical data protection mechanism that complies with Health Insurance Portability and Accountability Act (HIPAA) security regulations. The proposed mechanism does not use time-consuming modular exponential calculations or elliptic curve point multiplication calculations, reducing the computational complexity of the operations that are carried out in wearable devices and improving computational efficiency.

The contributions of this paper are as follows:

- This research attempt to use light-weight operations such as hash function and chaotic mapping technology to improve computing efficiency;
- This research uses extended chaotic mapping technology to develop a blockchain medical data protection mechanism and complies with Health Insurance Portability and Accountability Act (HIPAA) security regulations;
- The proposed mechanism does not need to use time-consuming modular exponential calculations and elliptic curve point multiplication calculations, so it can reduce the computational complexity of the wearable device and improve computational efficiency.

The remainder of this paper is structured as follows. Section 2 discusses the main existing research in the healthcare information system. Section 3 introduces background knowledge relevant to the paper, such as HIPAA privacy/security, blockchain, and chaotic maps. Section 4 presents the proposed scheme in detail. Section 5 the result of the paper which evaluates the proposed scheme, and Section 6 introduces the discussion. Finally, Section 7 draws conclusions and future work.

## 2. Related Work

This section will discuss the main existing research in the healthcare information system where blockchain technology has been used to improve the security. Table 1 summarizes related work in this paper according to their main contributions and goals.

In 2019, Vazirani et al. [13] studied blockchain as a way to manage healthcare information efficiently the study was discussing potential benefits and limitations of blockchain technology for healthcare and the paper concluded the discussion on how blockchain could be a better fit for managing health care records on the cloud system, while maintaining security and privacy of data.

In 2020, Khatoon [14] presented a healthcare smart contract system for different medical workflow and to streamline complex medical procedures. He also indicated the potential use of blockchain in healthcare and to show blockchain research's challenges and possible directions.

In 2020, Tripathi et al. [15] proposed a blockchain-based smart healthcare system (SHS) framework in order to provide a secured and privacy-preserved healthcare system. The paper explores the technological and social barriers in adoption of SHS by analyzing state-of-the-art expert views and user's perception.

In 2020, Khan et al. [16] presented a state-of-the-art network for blockchain healthcare applications with a mobile app model called HDG for the automation of medical records without compromising privacy, and discussed security challenges on a smart grid and its application for sustainable development in healthcare.

In 2019, Han et al. [17] proposed a blockchain-based health information sharing prototype to protect the patient's medical record includes personal information. Han et al. [17] used digital signatures to protect the record against forgery and unauthorized access and concluded that blockchain technology has a great potential for healthcare systems, providing data integrity and medical data sharing traceability. However, some security issues such as availability, scalability, and privacy were not evaluated.

In 2020, Jabbar et al. [18] proposed BiiMED: a blockchain-based framework method which use Ethereum. The framework is used to manage and validate shared data between medical providers who register health data in the cloud and share Electronic Health Records (EHR) of patients. This method presented the Trusted Third-Party Auditor (TTPA) based on blockchain technology. The proposed solution ensures data interoperability and integrity while sharing health data and according to the evaluation of the solution was conducted by testing the following properties: Turing-complete operations, scalability across large populations of patients, user identification and authentication, structural interoperability at the minimum, and cost-effectiveness.

In 2021, Shakor and Surameery [19] proposed a hybrid cryptosystem in a cloud framework using a built-in encrypted cloud storage system to make the proposed system strong against vulnerabilities. The framework combines the Advanced Encryption Standard (AES) and the Cryptographic Curve Cryptography (ECC). The paper shows that the impact of this built-in approach is more important than the other secure algorithms. In addition, it also showed that the availability of security and speed in this system makes it most suitable for storing sensitive data for the COVID-19 pandemic in health institutions.

In 2021, Zaabar et al. [20] proposed a system, HealthBlock, which is based on an architecture that leverages both blockchain and IoT technologies to ensure a secure healthcare management system including Remote Patient Monitoring (RPM) and Electronic Health Record (EHR) sharing. The HealthBlock system allows patients to manage their healthcare data securely on their own and its performance evaluation results proves that the performance of our proposed system is far better than the prominent existing ones, as it reduces the mining cost, the latency, and provides a considerable increase in overall throughput.

**Table 1.** Summary of related works.

Reference	Contribution/Goal
Khatoon [14]	Design and implementation of different medical workflows
Tripathi et al. [15]	Design and implementation of health data
Khan et al. [16]	Improvement in throughput of the blockchain network and a mobile app
Han et al. [17]	Health Data Sharing
Jabbar et al. [18]	Shared EHR of patients with a decentralized Trusted Third-Party Auditor (TTPA)
Shakor and Surameery [19]	COVID-19 Data Sharing
Zaabar et al. [20]	Design and implementation of RPM and EHR sharing

### 3. Preliminaries

This section describes the underlying primitives that are used in this paper. They are HIPAA privacy/security, blockchain, and chaotic maps.

#### 3.1. HIPAA Privacy Guidelines

Privacy guidelines define terms that are related to the limits of patients' privacy and rights to understand and control the use/disclosure of protected health information (PHI), which (comprises OR consists of TRY includes) the patient's name, address, contact number and medical records. The privacy guidelines of HIPAA [21–23], use the following seven main terms.

- (1) Patients' understanding: Patients have the right to understand how their health information will be stored and used and kept by care providers;
- (2) Confidentiality: Various software safeguards such as encryption, decryption, and authentication protect health data during storage and transmission. The health data of patients must not be undisclosed to any party who has no right to access the data;
- (3) Patients' control: Patients must be able to control who can access and use their health data;
- (4) Data integrity: Patients' electronic health information should be protected from improper alteration or destruction;
- (5) Consent exception: In limited circumstances (life-saving and other exceptional situations), health information can be disclosed and used without a patient's individual authorization;
- (6) Non-repudiation: To ensure that authorities meet their responsibilities in relation to patients' information, any related activity must be provable with evidence;
- (7) Auditing: To ensure that patients' health information is protected, that information and logs of related activity must be frequently monitored and assurance must be provided to patients regarding the security of their health information.

#### 3.2. Blockchain

Blockchain is an open and distributed ledger that is based on peer-to-peer networks and consensus algorithms. It refers to a chain of blocks that are linked and secured using cryptography [4]. The most obvious and outstanding benefit of blockchain is the fact that it removes the need for a centralized trusted third party in distributed applications. By enabling two or more parties to carry out transactions in a distributed environment without a centralized authority, blockchain overcomes the problem of the single point of failure that a central authority otherwise introduces. Blockchain is now considered to be a general proposed technology that has found applications in different industries and has various use cases, such as identity management, dispute resolution, contract management, supply chain management, insurance, and healthcare [24,25].

The benefits of blockchain for healthcare systems are as follows [25].

- (1) Decentralization: Blockchain provides a decentralized health data management backbone, meaning that all users (doctors, patients, and others) can access the same health records;
- (2) Improved data security and privacy: The immutability of blockchain can improve the security of health data, which, once saved to the blockchain, cannot be corrupted or altered;
- (3) Ownership of health data: Blockchain helps patients to own their health data and control how their data are used through strong cryptographic protocols and well-defined smart contracts;
- (4) Availability/robustness: The availability of patients' health data that are stored on blockchain is resilient against data losses, data corruption, and some security attacks;
- (5) Transparency and trust: Blockchain, being open and transparent, establishes a sense of trust in distributed healthcare systems;
- (6) Data verifiability: Even without accessing the plaintext of records that are stored on blockchain, the integrity and validity of those records can be verified.

### 3.3. Chaotic Maps

A chaotic map is a non-linear dynamical system that exhibits statistical properties, such as responsiveness to parameters, pseudo-random generator, and a large selection of points. The definition of the chaotic map is based on a Chebyshev polynomial. The Chebyshev chaotic map has special features, such as a semigroup structure and the commutative property. Recent research shows that cryptographic systems that use chaotic mapping are more efficient than those that use exponential and scalar multiplication on elliptic curves. Additionally, enhanced Chebyshev polynomials exhibit the semi-group property and the commutative property, and they are subject to the discrete logarithm problem and the Diffie-Hellman problem [26–28], which are described as follows.

#### 3.3.1. Chebyshev Chaotic Maps

The Chebyshev polynomial  $T_n(x)$  is a polynomial with  $x$  of degree  $n$ . The Chebyshev polynomial [20]  $T_n(x): [-1, 1] \rightarrow [-1, 1]$  is defined as  $T_n(x) = \cos(ncos^{-1}(x))$ . The Chebyshev polynomial is defined by the following recurrence relation.

$$\begin{cases} T_0(x) = 1; \\ T_1(x) = x; \text{ and} \\ T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), \text{ for } n \geq 2, \end{cases}$$

where  $r, s \in N$ ,  $x \in [-1, 1]$ . The Chebyshev polynomials satisfy the semi-group property and are commutative under composition. Then,

$$T_r(T_s(x)) \equiv T_{r \cdot s}(x) \equiv T_s(T_r(x)),$$

holds.

#### 3.3.2. Enhanced Chebyshev Maps

The cryptographic system, which is based on chaotic maps, has proven to be more efficient than traditional cryptographic systems that use modular exponential operations and point multiplication operations on elliptic curves [26–31]. Enhanced Chebyshev polynomials have semi-group and commutative properties and suffer from the discrete logarithm problem, the Diffie-Hellmann problem, and the inverse assumption.

After the security problems of the Chebyshev polynomial were raised by Bergamo et al. [27], Zhang [31] proposed an improved Chebyshev polynomial and proved that if that Chebyshev polynomial is defined not in the interval  $[-1, 1]$  but in  $(-\infty, +\infty)$ , then the security issue can be solved, and the characteristics are maintained. The definition and characteristics of the Chebyshev polynomials and their enhancement are described as follows.

$$\begin{cases} T_0(x) = 1; \\ T_1(x) = x; \text{ and} \\ T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \bmod p, \text{ for } n \geq 2, \end{cases}$$

when  $x \in (-\infty, +\infty)$  and  $p$  is a large prime number. Chebyshev polynomial satisfies the Semi-Group characteristics (closure and associativity) and the commutative rate.

$$T_r(T_s(x)) \equiv T_{r \cdot s}(x) \equiv T_s(T_r(x)) \bmod p.$$

(1) Extended Chaotic Map-Based Discrete Logarithm Problem

The variable  $y$  is the result of the operation of Chebyshev polynomial degree as  $r$ . When  $x$ ,  $y$ , and  $p$  are known, it's difficult to find an integer  $r$  to satisfy the following formula:

$$T_r(x) \equiv y \pmod{p}$$

(2) Extended Chaotic Map-Based Diffie-Hellman Problem:

Knowing that  $T_u(x)$ ,  $T_v(x)$ ,  $T(\cdot)$ ,  $x$  and  $p$ , when  $u, v \geq 2$  and  $x \in (-\infty, +\infty)$ ,  $p$  is a large prime number, it is difficult to find the following formula:

$$T_{u \cdot v}(x) \equiv T_u(T_v(x)) \equiv T_v(T_u(x)) \bmod p.$$

(3) Extended Chaotic Map-Based Inverse Assumption:

Since the Chebyshev polynomial satisfies the semi-group (closure and associativity), it is known that  $u, v, T(\cdot)$ ,  $x$  and  $p$ ;  $u, v \geq 2$ ;  $x \in (-\infty, +\infty)$ , and  $p$  is a large prime number, it is difficult to find an integer  $u^{-1}$  that satisfies the following formula:

$$T_{u^{-1}}(T_{u \cdot v}(x)) \equiv T_{u^{-1} \cdot u \cdot v}(x) \equiv T_v(x) \bmod p.$$

### 3.4. Review of the Novel Blockchain-Based Data Preservation System of Li et al.

Li et al. [7] proposed a novel blockchain-based data preservation system (DPS) for medical data. Their scheme comprises preservation submission (PS) and primitiveness verification (PV), as follows.

(1) Preservation submission (PS):

In the PS phase, the user uploads text or files that need to be preserved. After confirmation that the uploaded content is correct, this content is stored officially in the DPS and cannot be changed. The three steps in this process are as follows.

Step 1: Receiving and processing the as-yet unpreserved health data that have been uploaded by the user.

The DPS can accept health data in two formats—as a file or as text. If the preserved data is of the file type, then the system will process the file, store it in randomly generated folders, and calculate the hashr of the file using the SHA-256 algorithm. If the preserved data are text files, then they will be stored temporarily in the database, and the hashr of the text files will be calculated using the SHA-256 algorithm. Finally, a pair of asymmetrical keys is generated by the ECC algorithm.

Step 2: Protecting the processed data by encryption

This function is invoked when a user verifies the validity of the data to be preserved. If the user confirms the preservation, then the DPS uses the AES algorithm to encrypt the as-of-yet unpreserved data using a symmetric key  $K_{sym}$ . Next,  $K_{sym}$  is encrypted using the public key  $pubKey$ , which is the asymmetric key that was generated in step 1. Finally, the encrypted data are returned. The stored files in the random folder or text in the database will be deleted.

Step 3: Storing data to be preserved in the blockchain.

First, the identity of the user is checked to determine whether she/he is legal, based on the user's registration information and past preserve operations. If the user is legal,



then the preserved data will be stored in the blockchain, and the DPS will then return the transaction hash  $Tx$ .

## (2) Primitiveness verification (PV).

The PV module implements three main steps.

Step 4: Viewing the preserved health data that are stored in the blockchain.

First, the DPS retrieves the stored and encrypted data from the blockchain by using  $Tx$ . Then, the private key  $priKey$  is used to decrypt the data  $C$ . Second, the consistency with the stored hashr, which hash is extracted from the original data, with hashc, which is the calculated hash of content  $M$ , is checked. If they are consistent, then the preserved information is decrypted and returned. Otherwise, null is returned.

Step 5: Verifying consistency with original data.

The data that are uploaded by users must be verified by the DPS, which calculates hashc using the SHA-256 algorithm and hashr from the original data. If they are consistent, then the health data to be verified are deemed identical to the preserved data.

Step 6: Extracting health data from the blockchain.

The DPS obtains all information using the transaction hash  $Tx$  and extracts the health data that were previously preserved.

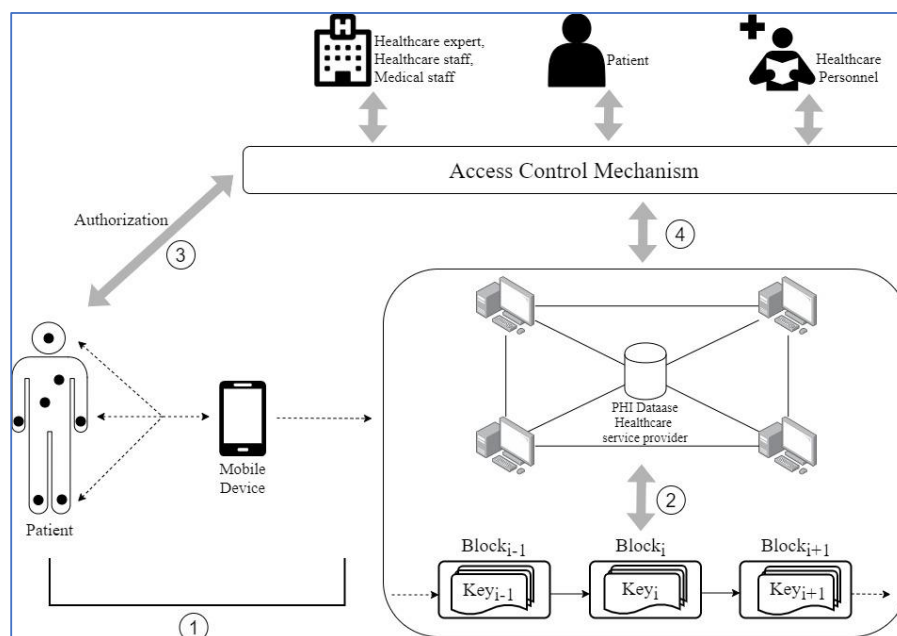
Li et al. [7] used a cryptographic mechanism to securely and reliably share a patient's data, but if the user stores many files, he or she will need to record the private key and  $Tx$  of each file separately. As the number of patients increases daily, this fact makes the management of patients' key pairs a huge challenge in their system.

## 4. Method

This section concerns blockchain-based healthcare information preservation using extended chaotic maps to satisfy HIPAA privacy/security regulations.

### 4.1. The Simple Structure of the Medical Care Information System

Figure 1 shows the authorization and access control of the proposed medical care information system. Patients' health data may be held by various medical organizations, such as hospitals and clinics. All users, which may include patients, healthcare experts, healthcare staff, and medical staff, must be able to request patients' health records within the medical care information system. Patients' health data are stored in the PHI database of the healthcare service provider, which exploits the non-tampering feature of the blockchain, as follows.



**Figure 1.** The proposed authorization and access control of the medical care information system.

- (a) Medical Sensor,  $S$ : A sensor is worn by the patient. It collects physiological data, which are verified and transmitted by a mobile device;
- (b) Mobile Device,  $M$ : A mobile device is carried by the patient. It integrates the data that are measured by each sensor and transmits them to the server at a medical center. The mobile device may be a smartphone or a tablet;
- (c) Medical Center Server,  $MCS$ : The Medical Center Server stores the data that are received from the user's mobile device in a database. It uploads a summary of the data to the blockchain to verify the integrity of the data;
- (d) Registration Center,  $RC$ : The registration center allows network entities to register their identity and obtain corresponding private keys. After registration, the registration center publishes the identity.

#### 4.2. The Proposed Scheme Uses Extended Chaotic Maps

The mechanism that is described in this paper has three phases, which are the parameter initialization phase, the registration phase, and the key generation phase. Table 2 presents the symbols that will be used hereafter.

**Table 2.** Symbol of the scheme.

$E$	Entities on the network. Can be wearable devices, mobile devices, and medical center servers
$S$	Wearable devices
$M$	Mobile devices
$MCS$	Medical center server
$ID_e, ID_S, ID_M, ID_{MCS}$	Identity of network entity, wearable devices, mobile devices, and medical center servers
$SK_e, SK_S, SK_M$	Private key of network entity, wearable devices, and mobile devices
$Mk$	Private key of registration center (RC)
$x, r_1, r_2$	Random number $[-\infty, \infty]$
$T(\cdot)$	Chaotic map function
$H(\cdot)$	One way hash function
$P$	Big large prime number
$K$	key
$Key$	Communication key
$P$	Origin data
$C_1, C_2$	Encrypted data
$V$	Verification data

##### 4.2.1. Parameter Initialization Phase

The registration center prepares the necessary parameters, which are the chaotic map function  $T(\cdot)$ , the hash function  $h(\cdot)$ , a random number  $x$ , a prime number  $p$ , and publishes  $x, p, T(\cdot), h(\cdot)$ .

##### 4.2.2. Registration Phase

In this phase, the entity ( $e$ ) registers its identity ( $ID$ ) with the registration center ( $RC$ ) and generates the corresponding private key ( $SK$ ). This  $SK$  is then sent back through a secure channel to the entity ( $e$ ), whose identity ( $ID$ ) is published. Figure 2 schematically depicts the registration phase.

Step 1: Network entity( $e$ ) send  $ID_e$  to the registration center ( $RC$ ).

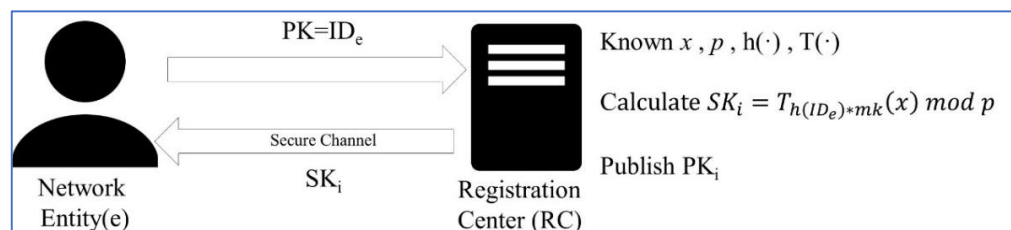
Step 2: Registration center ( $RC$ ) has known  $x, p, T(\cdot), h(\cdot)$ . After the registration center ( $RC$ ) receiving the  $ID_e$  from the network entity( $e$ ), the registration center ( $RC$ ) calculates its corresponding privacy key  $SK_i$ .



$$SK_i = T_{h(ID_e)*mk}(x) \bmod p.$$

After calculating the private key  $SK_e$ , send it back to the network entity (e) through the secure channel.

Step 3: After the registration center (RC) sends back the private key  $SK_e$  and publishes the identity  $ID_e$  of the network entity.



**Figure 2.** Network entity registration illustration diagram.

#### 4.2.3. Key Generation Phase

This phase comprises two parts. The first part is the protocol that governs the sending of data by the wearable device sensor to the database for storage through the mobile node. It can be subdivided into the sensor data collection stage and the social network information transmission stage, separated by dotted lines in Figure 2. The second part concerns the agreement for medical staff under which they access data; in this part, a data summary is uploaded to the blockchain for subsequent verification and to increase its confidentiality. The second part manifests the main contribution of this paper.

Step 1: Mobile devices  $M$  connect to sensor  $S$ , and send  $ID_M$  and random number  $x$  to the sensor

Step 2: The sensor  $S$  calculates the key by using the identity  $ID_M$  of the mobile devices  $M$

$$K_{MS} = T_{h(ID_M)}(SK_S) \bmod p.$$

Then, calculate the encryption key by using the random number  $r_1$  and key  $K_{MS}$ .

$$key_{MS} = T_{r_1}(K_{MS}) \bmod p.$$

After calculating the encryption key  $key_{MS}$ , encrypt the origin data  $P$  by  $key_{MS}$ .

$$C_1 = P \oplus key_{MS}.$$

The sensor  $S$  sends its identity  $ID_S$  and encrypted data  $C_1$  back to the mobile devices  $M$  after encrypting the origin data  $P$ .

Step 3: The mobile devices  $M$  calculates the key by using the identity  $ID_S$  of the Sensor  $S$

$$K_{MS} = T_{h(ID_S)}(SK_M) \bmod p.$$

Then, calculate the encryption key by using the random number  $r_1$  and key  $K_{MS}$ .

$$Key_{MS} = T_{r_1}(K_{MS}) \bmod p.$$

After calculating the encryption key  $key_{MS}$ , decrypt the encrypted data  $C_1$  by  $key_{MS}$

$$P = C_1 \oplus key_{MS}.$$

After obtaining the original data  $P$ , send the identity of mobile device  $ID_M$  to the medical center server MCS.

Step 4: Medical center server MCS returned its identity  $ID_{MCS}$  and random number  $r_2$  to the mobile device  $M$ .

Step 5: The mobile devices  $M$  calculates the key by using the identity of the medical center server IDMSC.

$$K_{MMCS} = T_{h(ID_{MCS})}(SK_M) \bmod p.$$

Then, using the random number  $r_2$  and key  $K_{MMCS}$  to calculate the encryption key  $key_{MMCS}$ .

$$key_{MMCS} = T_{r_2}(K_{MMCS}) \bmod p.$$

After calculating the encryption key  $key_{MMCS}$ , encrypt the origin data  $P$  by  $key_{MMCS}$ .

$$C_2 = P \oplus key_{MMCS}.$$

When the data is encrypted, send the encrypted data  $C_2$  to the medical center server MCS.

Step 6: The medical center server MCS calculates the message summary  $v$  by using the encrypted data  $C_2$  and random number  $r_2$ . After calculating the message summary  $v$ , it uploads it to the blockchain.

Step 7: The medical center server stores the encrypted data  $C_2$ , random number  $r_2$ , and messages the summary  $v$  to the database.

When the data have been stored by the medical center server MCS, when they need to be authorized, an authorization action is performed. When the MCS confirms that the requester has a right to access the data, it decrypts those data and uses its private key and the public key of the requester to generate a new key, which is used to encrypt the data for sending back to the data requester. The data requester can use his or her private key and the public key of the MCS to calculate the encryption and decryption keys to decrypt the data. Having received the file, the data requester can verify the message summary against the message summary that is stored on the blockchain. Figure 3 presents the key agreement in the proposed scheme.

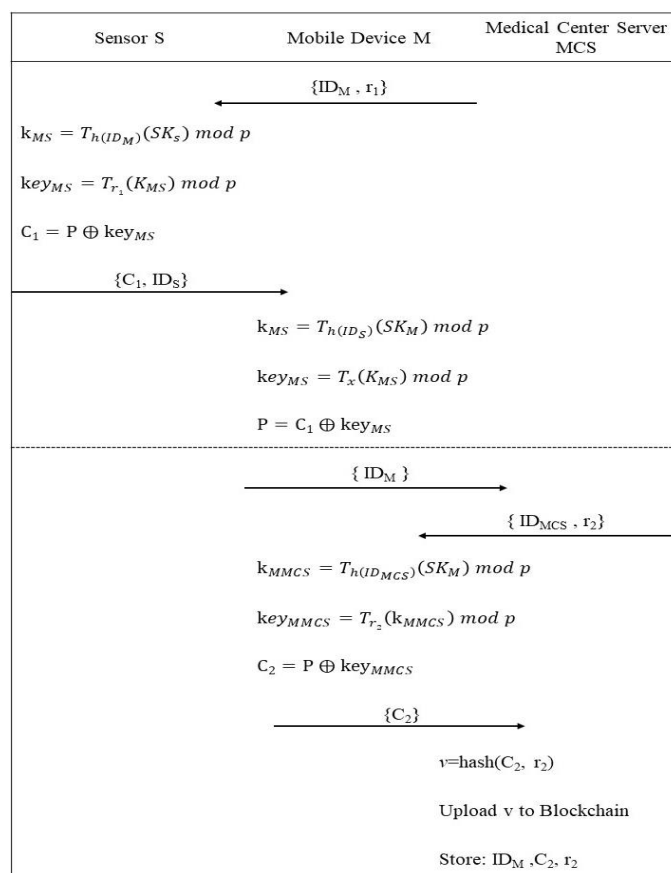


Figure 3. The key agreement of proposed scheme.

## 5. Results

This section will analyze the security and performance of the proposed scheme.

### 5.1. Security Analysis

Analysis of the security of the proposed scheme will be divided into a sensor data collection phase, a social network information transmission phase, and a HIPAA security regulation analysis phase for the purposes of discussion.

#### 5.1.1. Sensor Data Collection Phase

1. **Mutual Authentication:** All devices register their ID with the RC and obtain their own private keys  $SK$ . When device B encrypts data, it uses device A's IDA and its private key  $SK_B$  to calculate the encryption key and encrypt the data. Device A uses device B's IDB and its private key  $SK_A$  to calculate the decryption key and decrypt the encrypted data. Based on the assumption that A can correctly decrypt the encrypted data, the mutual authentication of devices A and B is successful;
2. **Impersonation Attack:** Attackers, including internal legal users, cannot obtain the private key  $mk$  of the RC, the private key  $SK_S$  and  $SK_M$  of the wearable device and the mobile device, respectively, or the communication key  $key_{MS}$  between the wearable device and the mobile device. Therefore, such attackers cannot impersonate other wearable devices or mobile devices to send out messages;
3. **Known Key Security:** If the communication key  $key = T_x(k) \bmod p$  of both parties is unfortunately leaked, then the other communication key will not have been leaked because each communication generates a new random number  $x$ , where  $k$  is  $key_{MS}$  or  $K_{MMCS}$ ;
4. **Forward Secrecy:** As in known key security, even if any communication key is disclosed, the attacker cannot calculate a previous communication key;
5. **Node Capture Attack:** If an attacker captures any legal node, only the private key that is obtained during registration and its ID are stored in the node. Other revealed information is composed of random numbers and an exchanged message. The attacker wants to use known information to calculate the private key of the RC, and so faces the Extended Chaotic Map-Based Discrete Logarithm Problem (DLP). Therefore, the proposed scheme is secure against node capture attacks.
6. **Replay Attack:** The mobile device generates a new random number  $x$  in every new session and so can use  $x$  to ensure that the data that are received in each round are up to date. The challenge-response principle is applied to verify the freshness of the messages. The random number  $x$  that is generated in each round is a challenge. If the mobile device receives data from the sensor and can use  $x$  to decrypt those data correctly, then the challenge is successful. When data are being collected, the random number  $x$  in the round differs from those in the previous round. The correct information cannot be decrypted, and the challenge fails.
7. **Man-in-the-middle Attack:** Since the mutual authentication of the devices and the attacker cannot yield the private key of the wearable device, the encryption and decryption key cannot be calculated. Furthermore, the original data cannot be calculated by the attacker, which cannot use its private for encryption. Therefore, the proposed mechanism resists the man-in-middle attack.
8. **Modification Attack:** As in the man-in-middle attack, the attacker cannot obtain the private key of the wearable device and therefore cannot calculate the encryption and decryption keys and then modify the transmitted data. Therefore, this attack is ineffective.

### 5.1.2. Social Network Information Transmission Phase

1. Impersonation Attack: Attackers, including internal legal users, cannot obtain the private key  $mk$ ,  $SK_{SM}$ ,  $SK_{MSC}$  of the RC, mobile devices  $M$ , MCS or the communication key  $key_{MMCS}$  between the mobile devices and the medical center server. Therefore, they cannot pretend to be mobile devices or the MCS from which a message can be sent;
2. Sending Data Error: Since the transmitted data are all encrypted, if a problem with the data occurs during the transmission process, then the correct data will not be able to be decrypted successfully. Restated, if the correct data can be decrypted, no problem can have occurred during data transmission;
3. Data Tampering: After the MCS receives the encrypted data that are sent by the mobile device, it uses these data and the random number  $x$  to calculate a message summary  $v$ , which it uploads to the blockchain for storage. When the user accesses data in the database, the message summary  $v'$  is calculated and compared with the message summary  $v$  on the blockchain. If the data have been tampered with, this tampering will be identified immediately when the data are accessed. In this study, the MCS performs only data upload actions and does not directly interact with miners' computers. Tampering with data on the blockchain requires control of more than 51% of the computers. Therefore, data on the blockchain is prevented from being tampered with and the accuracy of the verification data is ensured.

### 5.1.3. HIPAA Security Regulation Analysis Phase

Since this study only studies the data transmission to the server for storage and does not authorize the data. Therefore, there is no safety analysis of Patient's Control and Consent Exception.

1. Patient's Understanding: The patient signs a consent form at the registration stage, which clearly states how the medical center server will use and store medical record data;
2. Confidentiality: During the data upload stage, the mobile device and medical center server do the Chaotic Map-based Diffie Hellman Key Exchange to generate key  $k_{MS} = T_{h(ID_M)}(SK_S) \bmod p$ ,  $key_{MS} = T_{r_1}(k_{MS}) \bmod p$ ,  $k_{MMCS} = T_{h(ID_{MCS})}(SK_M) \bmod p$ , and  $key_{MMCS} = T_{r_2}(k_{MMCS}) \bmod p$ . In the process of data transmission, the data transmitted are all encrypted data  $C_1 = P \oplus key_{MS}$ , and  $C_2 = P \oplus key_{MMCS}$  to ensure the confidentiality of patient data;
3. Data Integrity: In the process of data transmission, the data transmitted are encrypted data  $C_1 = P \oplus key_{MS}$  and  $C_2 = P \oplus key_{MMCS}$ , which can ensure the integrity of patient data.

### 5.2. Performance Analysis

The method that is proposed herein is compared with those proposed by Li et al. [7] and Zhang et al. [32] in terms of computational complexity and response time. For a detailed analysis, refer to Table 3 below. The simulation environment and test results are listed in Table 4 below. The mechanism that is proposed herein uses only light-weight computing techniques such as chaotic mapping and the hash function. The required time and computational complexity in the sensor data transmission stage are less than those of the elliptic-curve point multiplication that is used by Zhang et al. [32]. Figure 4 displays simulation results concerning the response time in the sensor data transmission stage in the scheme of Zhang et al. [32] and proposed scheme for  $n = 1, 10, 50, 100, 200$ , and 500. In the social network information transmission stage, the data encryption and decryption are more efficient than those associated with the symmetrical formula of Li et al. [7]. Figure 5 displays simulation results for the reaction time of social network information transmission stage of Li et al. [7] and proposed scheme for  $n = 1, 10, 50, 100, 200$ , and 500.

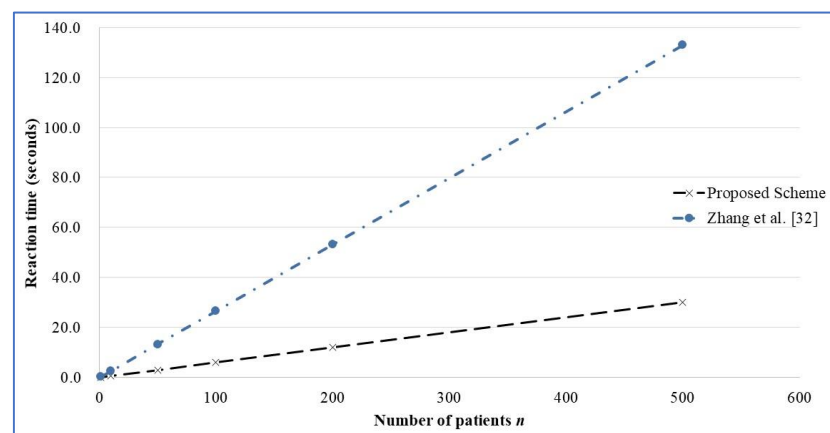
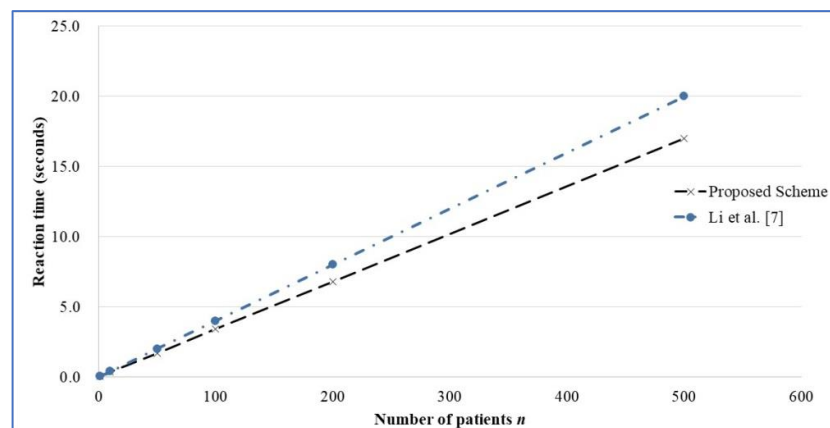
**Table 3.** Comparison table of calculation amount.

	Li et al. [7]	Zhang et al. [32]	Proposed Scheme
Registration stage Reaction time	X	X	$1T_h + 1T_{chao}$ $\approx 0.017$ s
Sensor data transmission stage Reaction time	X	$3T_h + 2T_e$ $\approx 0.266$ s	$2T_h + 4T_{chao}$ $\approx 0.06$ s
Social network information transmission stage Reaction time	$2T_s + 1T_h$ $\approx 0.04$ s	X	$2T_h + 2T_{chao}$ $\approx 0.034$ s

$T_h$ : Time required for one-way hash function calculation,  $T_e$ : Time required for one elliptic curve point multiplication calculation,  $T_{chao}$ : Time required for a chaotic mapping function calculation,  $T_s$ : Time required for a symmetric encryption and decryption calculation.

**Table 4.** Real machine efficiency simulation time.

Experiment Environment	Operation System: Windows 10 build 2004 CPU: Intel(R) Core (TM) i7-3770 CPU @ 3.40 GHz Development program: C++ Memory: 20 G Enter bit: 256 bits	
	Average operation time	
Used Software	SHA256 one-way hash function	0.004 s
	ECC elliptic curve point multiplication	0.127 s
	AES symmetric encryption and decryption	0.018 s
	Chaotic Maps	0.013 s

**Figure 4.** The reaction time of the sensor data transmission stage of Zhang et al. and proposed one.**Figure 5.** The reaction time of social network information transmission stage of Li et al. and proposed one.

## 6. Discussion

To improve the security of the healthcare system most of the research is still relying on computationally heavy modular exponential operations or elliptic curve point multiplication operations. The structures of these operations are very complicated and the amount of calculations are huge. The proposed authentication and key agreement Scheme using extended Chaotic Maps has a number of advantages compared to previous health data system. The first is that it can reduce the amount of computing on wearable devices to achieve lightness to quantify the effect of the operation. The password system based on identity authentication can reduce the information that the device needs to store. It only needs to save the private key of the device, which it obtains from the registration server. After the mobile device collects the physiological data of the wearable device, it is uploaded to the database of the medical center server for storage. The second advantage is the data is calculated for the message summary and uploaded to the blockchain for storage. Using the non-tampering feature of the blockchain, the data in the medical center server can be compared with the message summary on the blockchain to ensure that the data has not been tampered with and improve data security. In terms of security, the proposed mechanism can resist a variety of attacks to reduce to possibility of privacy disclosure.

However, the current scheme still needs to be improved. There are some limitations to the proposed scheme. The first is about the structure of the data stored in the blockchain. It is difficult to query data within a blockchain, limiting the statistical and research uses of data. A better data structure could be setup to write a large number of different health data in the blockchain for more efficiency and to implement high concurrency. The second limitation is the scalability issue for healthcare big data, due to blockchain using a decentralized architecture. If millions of users, including private clinics, healthcare centers, patients, and IoT startups etc., were to use different block chain infrastructures and blockchain technologies, a higher computation power would be required, which not every user would be able to provide.

## 7. Conclusions and Future Work

Advancements in science and technology have led to new research on telemedicine. Data about a user that are measured by a wearable device can enable doctors more accurately to determine the physical condition of the user. This study proposes a mechanism for preserving medical information that considers the entire process of data from data generation through transmission by wearable devices to mobile devices and then to a medical center server. When the data that are generated by a wearable device on the user are transmitted to a hospital to be viewed by medical staff, this process is protected in a manner that complies with HIPAA privacy and security regulations. This goal of this work is to improve the security and privacy of users' physiological data in transmission, and to provide a secure data transmission channel for telemedicine, supporting further developments in the medical industry. As part of future work, the scalability issue for healthcare big data must be taken care of seriously in order to make blockchain popular and to integrate artificial intelligence features in the process of analyzing collected health data and healthcare diagnosis decisions.

**Author Contributions:** Conceptualization, T.-F.L., I.-P.C. and T.-S.K.; methodology, T.-F.L. and T.-S.K.; writing—original draft preparation, T.-F.L., I.-P.C. and T.-S.K.; Writing—review and editing, T.-F.L. and I.-P.C. All authors have read and agreed to the published version of the manuscript.

**Funding:** Supported in part by grants from the Ministry of Science and Technology of the Republic of China (Grant No. MOST110-2221E320-005-MY2).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Acknowledgments:** Ted Knoy is appreciated for his editorial.

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



## References

1. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [\[CrossRef\]](#)
2. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-Based Packing of Industrial IoT Data in Permissioned Blockchains. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7639–7649. [\[CrossRef\]](#)
3. Zhang, L.; Zhu, S.; Tang, S. Privacy Protection for Telecare Medicine Information Systems Using a Chaotic Map-Based Three-Factor Authenticated Key Agreement Scheme. *IEEE J. Biomed. Health Inform.* **2017**, *21*, 465–475. [\[CrossRef\]](#) [\[PubMed\]](#)
4. Li, X.; Wu, F.; Khan, M.K.; Xu, L.; Shen, J.; Jo, M. A secure chaotic map-based remote authentication scheme for telecare medicine information systems. *Future Gener. Comput. Syst.* **2018**, *84*, 149–159. [\[CrossRef\]](#)
5. Peterson, K.; Deeduvanu, R.; Kanjamala, P.; Boles, K. A blockchain-based approach to health information exchange networks. In Proceedings of the NIST Workshop Blockchain Healthcare, Gaithersburg, MD, USA, 26–27 September 2016; Volume 1, pp. 1–10.
6. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.D.; He, J. BlochIE: A BLOCKchain-Based Platform for Healthcare Information Exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 49–56. [\[CrossRef\]](#)
7. Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-Based Data Preservation System for Medical Data. *J. Med. Syst.* **2018**, *42*, 141. [\[CrossRef\]](#) [\[PubMed\]](#)
8. Kaur, H.; Alam, A.; Jameel, R.; Mourya, A.K.; Chang, V. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *J. Med. Syst.* **2018**, *42*, 156. [\[CrossRef\]](#) [\[PubMed\]](#)
9. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [\[CrossRef\]](#)
10. High, D.R.; Wilkinson, B.W.; Mattingly, T.; Cantrell, R.; O'Brien, V.J.J.; McHale, B.G.; Jurich, J., Jr. Obtaining a Medical Record Stored on a Blockchain from a Wearable Device. U.S. Patent 15/840,589, 14 June 2018.
11. Jiang, S.; Cao, J.; McCann, J.A.; Yang, Y.; Liu, Y.; Wang, X.; Deng, Y. Privacy-Preserving and Efficient Multi-Keyword Search over Encrypted Data on Blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 405–410. [\[CrossRef\]](#)
12. Wang, H.; Song, Y. Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. *J. Med. Syst.* **2018**, *42*, 152. [\[CrossRef\]](#)
13. Vazirani, A.; O'Donoghue, O.; Brindley, D.; Meinert, E. Implementing Blockchains for Efficient Health Care: Systematic Review. *J. Med. Internet Res.* **2019**, *21*, e12439. [\[CrossRef\]](#)
14. Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics* **2020**, *9*, 94. [\[CrossRef\]](#)
15. Tripathi, G.; Ahad, M.A.; Paiva, S. S2HS- A blockchain based approach for smart healthcare system. *Healthcare* **2020**, *8*, 100391. [\[CrossRef\]](#)
16. Khan, F.A.; Asif, M.; Ahmad, A.; Alharbi, M.; Aljuaid, H. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustain. Cities Soc.* **2020**, *55*, 102018. [\[CrossRef\]](#)
17. Han, S.H.; Kim, J.H.; Song, W.S.; Gim, G.Y. An empirical analysis on medical information sharing model based on blockchain. *Int. J. Adv. Comput. Res.* **2019**, *9*, 20–27. [\[CrossRef\]](#)
18. Jabbar, R.; Fetais, N.; Krichen, M.; Barkaoui, K. 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), Doha, Qatar, 2–5 February 2020; pp. 310–317.
19. Shakor, M.Y.; Surameery, N.M.S. Built-in Encrypted Health Cloud Environment for Sharing COVID-19 Data. In Proceedings of the 3rd International Conference on Computer Communication and the Internet (ICCCI), Nagoya, Japan, 25–27 June 2021; pp. 96–101.
20. Zaabar, B.; Cheikhrouhou, O.; Jamil, F.; Ammi, M.; Abid, M. HealthBlock: A secure blockchain-based healthcare data management system. *Comput. Netw.* **2021**, *200*, 108500. [\[CrossRef\]](#)
21. Act, A. Health insurance portability and accountability act of 1996. *Public Law* **1996**, *104*, 191.
22. Ray, S.; Biswas, G. A Certificate Authority (CA)-based cryptographic solution for HIPAA privacy/security regulations. *Comput. Inf. Sci.* **2014**, *26*, 170–180. [\[CrossRef\]](#)
23. Pussewalage, H.S.G.; Oleshchuk, V.A. Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *Int. J. Inf. Manag.* **2016**, *36*, 1161–1173. [\[CrossRef\]](#)
24. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [\[CrossRef\]](#)
25. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [\[CrossRef\]](#)
26. Kocarev, L.; Tasev, Z. Public-key encryption based on Chebyshev maps. In Proceedings of the 2003 International Symposium on Circuits and Systems, Bangkok, Thailand, 25–28 May 2003; pp. 28–31.
27. Bergamo, P.; Darco, P.; De Santis, A.; Kocarev, L. Security of public-key cryptosystems based on Chebyshev polynomials. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2005**, *52*, 1382–1393. [\[CrossRef\]](#)

- 
28. Sun, Y.; Zhu, H.; Feng, X. A novel and concise multi-receiver protocol based on chaotic maps with privacy protection. *Int. J. Netw. Secur.* **2017**, *19*, 371–382.
  29. Mason, J.C.; Handscomb, D.C. *Chebyshev Polynomials*; Chapman & Hall/CRC: Boca Raton, FL, USA, 2003.
  30. Kocarev, L.; Sterjev, M.; Fekete, A.; Vattay, G. Public-key encryption with chaos. *Chaos Interdiscip. J. Nonlinear Sci.* **2004**, *14*, 1078–1082. [[CrossRef](#)] [[PubMed](#)]
  31. Zhang, L. Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos Solitons Fractals* **2008**, *37*, 669–674. [[CrossRef](#)]
  32. Zhang, J.; Xue, N.; Huang, X. A Secure System for Pervasive Social Network-Based Healthcare. *IEEE Access* **2016**, *4*, 9239–9250. [[CrossRef](#)]