IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 7, 2020, accepted September 19, 2020, date of publication September 22, 2020,
date of current version October 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3025898

A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System

CHUN-TA LI[1], (Member, IEEE), DONG-HER SHIH[2], CHUN-CHENG WANG[2], CHIN-LING CHEN[3,4,5], AND CHENG-CHI LEE[6,7]

[1]Department of Information Management, Tainan University of Technology, Tainan City 71002, Taiwan, R.O.C.
[2]Department of Information Management, National Yunlin University of Science and Technology, Douliu 64002, Taiwan, R.O.C.
[3]Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung City 41307, Taiwan, R.O.C.
[4]School of Information Engineering, Changchun University of Science and Technology, Changchun 130012, China
[5]School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China
[6]Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei City 24205, Taiwan, R.O.C.
[7]Department of Photonics and Communication Engineering, Asia University, Taichung City 41354, Taiwan, R.O.C.

Corresponding authors: Chin-Ling Chen (clc@mail.cyut.edu.tw) and Cheng-Chi Lee (cclee@mail.fju.edu.tw)

This work was supported in part by the Ministry of Science and Technology, Taiwan, R.O.C., under Contract MOST 108-2410-H-165-004 and Contract MOST 109-2410-H-165-001.

ABSTRACT In recent years, due to the rapid development of information techniques and network technologies, more and more medical documents have been replaced by electronic files for sharing and transmitting in real time. However, medical data transmitted over public communication channels may suffer from security attacks and privacy threats. Blockchain technology has been gotten many attentions in different areas due to its unique properties such as anonymity, verifiability, immutability and decentralization. In order to secure patient privacy and provide more personal healthcare services, in this paper, we propose a data aggregation scheme based on Blockchain technology for medical environments. Moreover, in order to implement remote medical monitoring, we design a group authentication mechanism for multiple authorized users (such as patient, doctors, caregivers, family and friends) to freely access patient's personal health records. The authorized group members in a group will agree on a group session key and use it to protect patient's sensitive information. In case of a new member joins the medical group or an old member leaves the medical group, the group session key needs to be updated at any time. Finally, the electronic medical system will become more secure, reliable and useful by our proposed scheme.

INDEX TERMS Electronic medical record, data aggregation, blockchain technology, group authentication, electronic medical system.

I. INTRODUCTION

In current medical fields, there are three main types of medical-related electronic documents are widely used for implementing medical diagnostics and real-time telemedicine, including: electronic medical records (EMR), electronic health records (EHR) and personal health records (PHR), where electronic medical records and electronic health records are medical records stored in medical institutions, while personal health records are collected by personal health sensing device and stored in personal mobile device.

The associate editor coordinating the review of this manuscript and approving it for publication was Yanjiao Chen.

Both EMR and EHR are medical records stored in computers, with the purpose of enabling doctors to improve medical quality and control medical costs. More and more countries, including Europe and the United States, have begun to use electronic medical records. The integration of EMR, EHR, and PHR can make the medical care environment more personalized and meet the needs of patients. EMR is a file flowing in the internal organization, and EHR is defined as inter-organization transmission. PHR is an online system operated and used by patients, and its aim is to make patients' physiological information transparent, so that the patients can be better understand and participate in the treatment process. The integration of these three types of electronic

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

records can help doctors understand the basic physiological information of patients before making a diagnosis, including allergic drugs, past medical history, and major operations, so it not only can make the medical diagnosis process more rapid, but also reduce the occurrence of medical accidents caused by misdiagnosis in the treatment process. In addition, the sharing, preservation and protection of medical electronic files can be carried out safely, thus making the medical process more transparent, realizing telemedicine service, and enabling statistical analysis of medical related research [3].

When the United States was hit by Hurricane Katrina in 2005, the importance of EMR attracted new attention to the demand for EMR, because many medical records have been destroyed or missed due to the hurricane attack. Therefore, if medical records can be stored electronically or in the cloud, even if the hospital is damaged, the patients' EMR will not disappear because of the hospital's damage, but can be acquired remotely at any time and any place along with a patient [29]. Although EMR has considerable advantages, in addition to the methods of collection, storage and data analysis for the storage of electronic medical data, it is more important to ensure that users' privacy is not violated throughout the operation of the whole medical system, which is an important research topic. Internet of Things is going to create a world where physical things can be seamlessly integrated into communication networks in order to provide autonomous and intelligent services for improving human beings' life. In general, an IoT system involves three components, a sensing unit contains a large number of sensors, actuators, and mobile terminals to sense physical environments; a network layer includes all network techniques with heterogeneous network configurations for data transmission; an intelligent computing offers expected services or applications to IoT end users by mining and analyzing at data processors. However, there have some security threats when IoT users transmit data via public channel. Therefore, it is important to provide a secure IoT services [7], [10], [27]. On the other hand, most new technologies rely on the futuristic characteristics of the Internet. Electronic files are widely used and transmitted through the network. However, in public channels, files are vulnerable to malicious attacks resulting in information security concerns [19]–[22], [30], [35]. Blockchain can withstand most of the information security attacks, because Blockchain is composed of a data block with a decentralized architecture, each of which may point to another block in Blockchain to form a complete chain, which makes it difficult for hackers to carry out data security attacks [9], [11], [16], [23], [25], [31].

At present, due to the aging and fewer children in the social structure, when all the children go to work or school, the elderly may often be left alone at home. In addition, the number of patients with chronic diseases has increased in recent years, which results in a significant increase in the death rate of people due to chronic diseases [33]. In the current medical environment, patients have to check their own physiological conditions regularly by using sphygmomanometer and blood glucose meter themselves, so as to ensure their physiological conditions. However, during the non-checkup period, or if a patient is unable to check himself, accident may occur, and the patient may miss the prime time for treatment, because there is no one around and the patient has lost the ability to ask for help. Nowadays, remote care has become a trend in the medical field. If the above three medical records can be integrated, the vision of telemedicine will be realized, and especially the patients living in remote areas or suffering from chronic diseases can receive professional and accurate medical advice without having to go to the hospital. Therefore, this paper aims to design a group authentication mechanism, which can protect the privacy of patients and system users, and enable members of the medical group to conduct remote care and medical monitoring according to patients' physiological conditions in real time.

Because the electronic files are transmitted through the network, and the information transmitted through the Internet has the problem of information security during transmission, there are many mechanisms to protect the data from being intercepted, eavesdropped and tampered in the process of transmission. In order to effectively solve the problems related to information security, many researchers are trying to apply Blockchain technology to various professional fields, so as to achieve the purpose of protecting user privacy security by using the unique characteristics of Blockchain technology, including anonymity, non-repudiation, traceability, data not being tampered, node data synchronization, and decentralization. As the data in traditional medical databases will be large, complex, heterogeneous and time varying and medical industry is moving towards patient-centric models, all the components are being framed to benefit the patient. Using Blockchain technology for electronic medical data can provide high quality services at a relatively low cost. In order to realize the remote monitoring and diagnosis of patients, this study aims to design a sharing mechanism that allows patients' EMR to be accessed by authorized group members. Therefore, in this paper, Internet of Things (IoT) and Blockchain technology are combined to enable the medical users to use mobile devices and sensors for data collection, report generation and remote monitoring services, and these three types of electronic records can be aggregated automatically to help medical institutions to provide more personal health care for patients. In order to protect the patient's personal health privacy and make the statistical analysis of medical disease trends more effective, all electronic records will be transformed and encrypted before being uploaded to the medical Blockchain network for storage and sharing. Finally, with group authentication mechanism, the medical group members are authenticated interactively and jointly calculate the group session key, so that the authenticated authorized group members can decrypt to review the patient data.

The remainder of the paper is organized as follows. In Section 2, we review the related works on electronic medical systems and Blockchain technology. Then, in Section 3, we present the details of our new data aggregation and group

TABLE 1. The items of electronic medical records.

	EHR	EMR	PHR
1	Patient's profile	Patient's profile	Patient's profile
2	Medical history	Medical histories	Medications
3	Laboratory and test	Laboratory and test	Allergies
4	Medications	Allergies	List and dates of illnesses and surgeries
5	Treatment plans	Vital signs	Chronic health problems
6	Immunization dates	Administrative and billing data	Living will or advance directives
7	Allergies	Diagnoses	Family history
8	Radiology images	Medications	Immunization history
9	Diagnoses	Immunization dates	Blood pressure
10		Progress notes	Exercise and dietary habits
11		Radiology images	Health goals

authentication scheme for electronic medical system using Blockchain. Section 4 offers the results of some analyses on the proposed scheme including security discussions and functionality comparisons among related schemes. Finally, we make some conclusions in Section 5.

II. LITERATURE REVIEW

In the traditional medical model, patients go to the hospital to receive medical services in person. The process of going back and forth to the hospital is extremely inconvenient for patients, especially those who live far away. In addition, patients may experience repeated examinations when seeking medical services in different hospitals, which consumes medical resources and is time-consuming [12], [26], [34]. Nowadays, many scholars have begun to study TMIS in combination with EMR to provide medical expertise and knowledge online, which can help patients and medical institutions access EMR or health reports faster. However, the transmission of EMR may have privacy problems. For example, the administrator of medical records may disclose the patients' privacy information intentionally or unintentionally. Furthermore, in Telecare Medical Information System (TMIS), the whole system is based on the Internet, so it may also suffer from data security attacks in the process of data transmission. The three types of electronic records have different needs and uses respectively, and the contents of the records in which are also different [1], [2], [17]. EHR is mainly about the examination results of patients in the general direction; EMR is the diagnosis content of patients' physical health for the current condition; and the content of PHR is relatively flexible, and may also add items and health objectives that patients need to record, besides the physical information of general patients, as shown in Table 1.

Blockchain is a distributed electronic database that can set up a way to update this information and store any information, such as records, events and transactions. Blockchain may increase continuously with the increase of block price, and use hash function to point to the previous block to form the concept of chain [6]. The schematic diagram of Bitcoin Blockchain is shown in Figure 1. The hash value in the block is generated by calculating the content of the block through cryptographic hash functions, such as secure hash and other algorithms. An ideal hash function is easy to output to a value

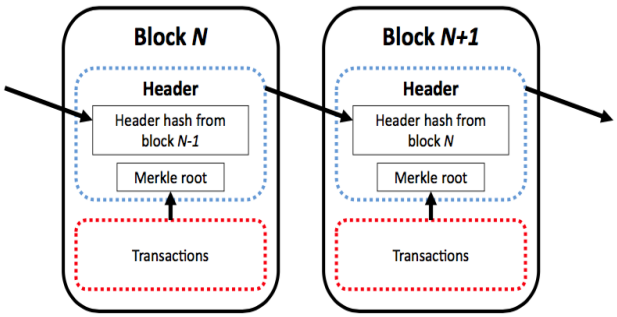

FIGURE 1. The schematic diagram of Bitcoin Blockchain.

of a fixed length, but hard to invert back to the input value. In addition, any change of the original input value results in a radically different output. In the Blockchain, all blocks are linked in chronological order, namely, the current block contains the hash value and timestamp of the previous block. Unless a malicious attacker can modify all blocks after the current block, it is unable to change all information content in the entire Blockchain.

In this study, in order to protect the privacy security of users in the process of information transmission and the non-repudiation of data generation, this study uses the security protocol method of Blockchain to sign and encrypt with the user's personal public and private keys, which has reached the sensitive information security, anonymity and non-repudiation. Because Blockchain uses a distributed storage architecture, and the blocks uploaded to the Blockchain cannot be changed or removed, the electronic records of patients will not be lost due to the damage of a medical institution, and the medical data of the past years can be preserved completely, so that patients or doctors can review the past data at any time. In addition, a large number of historical medical records can also be used for data analysis and exploration, from which we can find out the current trend of citizens' health or understand the impact of new viruses and diseases on human body and the possible symptoms of patients, so as to achieve more accurate diagnosis and prevent people's casualties caused by the spread of epidemic diseases.

Data aggregation technology has been extensively studied. Because most sensor nodes are used to monitor remote areas

TABLE 2. Functionality comparisons of related literature.

Schemes → / Functions ↓	Xu et al. (2014)	Chen et al. (2014)	Deng et al. (2017)	Pham et al. (2018)
Electronic medical records	√	√	√	√
Remote medical monitoring	√	√	√	χ
Internet of things	χ	χ	√	√
Medical record aggregation	χ	χ	χ	√
Blockchain technology	χ	χ	χ	χ
Group authentication	χ	χ	χ	χ

√: It indicates that the function can be achieved.
χ: It indicates that the function cannot be achieved.

that are not easily managed, it is difficult to continuously maintain and replace batteries. The service life of sensor nodes depends on the communication between the nodes. Therefore, the overall consumption of wireless sensor networks can be reduced through information aggregation. Data aggregation is often used for data collection in wireless sensor networks, and the corresponding data is sent to the collection center or base station for further aggregation processing. Aggregation process and energy conservation have been discussed in many studies to meet specific needs. Aggregation is defined as the process of aggregating data from multiple sensors to reduce the number of transmissions. In general, the factors that can be used for aggregation include planning to collect important information from sensors and transmitting the information to the receiving device with minimum delay and computation cost. The security of aggregation process is also concerned. For example, in an unattended environment, the attacker can hack into the sensor nodes to modify or delete part of the aggregated data.

In recent years, in order to enable patients to have more perfect and more convenient and safe medical services, many researchers focus on the research related to medical development, among which TMIS has gained considerable attention. Xu *et al.* (2014) [32] used ECC encryption technology to improve the authentication and key protocol of TMIS, and services such as EMR and remote monitoring were provided. Chen *et al.* (2014) [4] proposed the transmission mode of EMR and made medical resources more convenient. Zhu (2016) [36] developed a group key authentication mechanism to reduce the computation cost and ensure the transmission safety for transmitting data to multiple people. Wu *et al.* (2012) proposed a TMIS authentication scheme [30], which can withstand various types of information security attacks, including replay attack, password guessing attack, impersonation attack and authentication theft attack, and provided comprehensive information security measures, such as session key security and perfect forward secrecy. However, He *et al.* (2012) [13] found that this scheme could not withstand the impersonation attack and internal attack, and proposed a scheme to improve this defect. In the same year, Wei *et al.* (2012) [28] suggested that this improvement scheme could not defend against offline password guessing attack, and further proposed an improvement scheme to solve this problem of information security. Jiang *et al.* (2013) [14] argued that the approach proposed by Wei *et al.* still could not withstand password guessing attack, and then proposed a scheme of enhanced authentication. Kumari *et al.* (2013) [18] pointed out that the enhanced scheme proposed by Jiang *et al.* could not defend against theft authentication attack, online password guessing attack and impersonation attack. In the following year, Jiang *et al.* (2014) proposed a key agreement scheme based on chaotic mapping with strong anonymity [15]. Deng *et al.* (2017) [8] proposed to achieve telemedicine service with readers, and form a lightweight Body Area Network with readers held by patients and medical service providers and sensors on patients. This scheme combined IoT and used electronic records for transmission to realize telemedicine. Pham *et al.* (2018) [24] used Internet connection devices to provide comprehensive nursing staff information, including health data. This scheme designed a CoSHE system to integrate home service robot, environmental sensor, non-intrusive wearable sensor and cloud-based infrastructure. In view of the relevant literature listed above, this study collates and compares the functions provided by the literature, as shown in Table 2.

III. THE PROPOSED SCHEME

The main participants in this study are Healthcare Center (HC), Doctor (D), Patient (P), Group Member (GM) and Blockchain Transformation System (BT). HC generates the patient's EHR after the patient receives a physical health examination. The doctor generates EMR after the patient receives a physical diagnosis from the doctor. Finally, the patient himself/herself uses the body sensor network on him/her and uses IoT mechanism to allow the sensor automatically collect the physiological information of the patient, generate the PHR and upload it by a mobile device. Finally, P aggregates previous electronic health records and finally generates Aggregation Personal Health Record (APHR). After the healthcare center, the doctor and the patient generate EMR, the information will be sent to a workstation which will calculate and generate blocks which are finally uploaded to Blockchain network. When P collects three electronic medical related documents, P can decrypt and aggregate the privacy information in the blocks and then transmit it to the workstation for calculation to generate block APHR and upload it to the Blockchain network. After the steps in this phase are completed, the group member may retrieve the

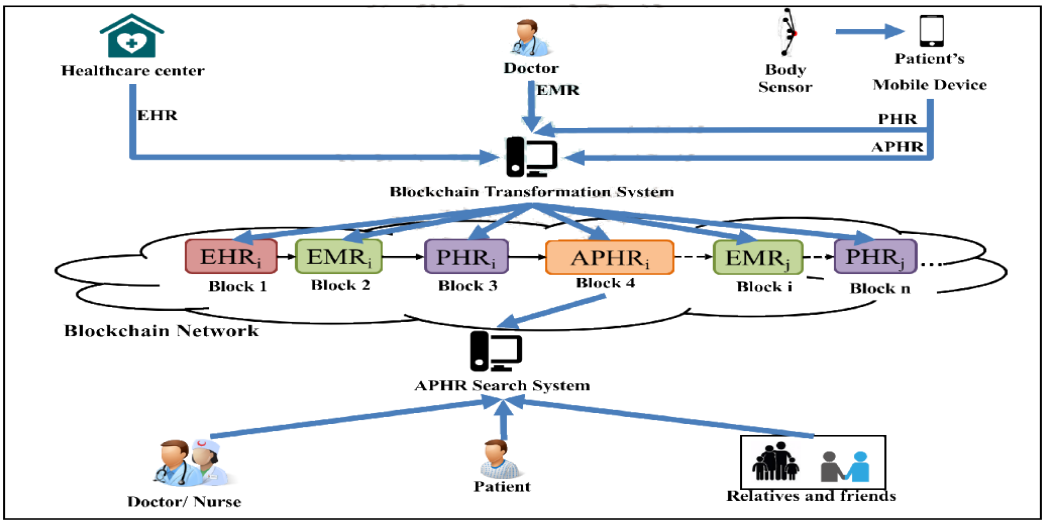

FIGURE 2. The architecture of Blockchain-based data aggregation and group authentication scheme in electronic medical system.

aggregate records of the patient through an APHR search system. The detailed research architecture is shown in Figure 2.

The medical records aggregation mechanism proposed in this study subdivides the upload phase into EHR upload phase, EMR upload phase, PHR upload phase and APHR upload phase. In the upload phase, HC, D and P upload their electronic records to the Blockchain network, and then the patient aggregates and uploads three types of medical records. Group setting will be introduced in Section 3.2.2, including mutual authentication of group members and addition and removal of group members. In the group setting phase, all group members need to perform mutual authentication, and finally, a group session key is jointly agreed and then is used to decrypt the APHR uploaded by the patient. Finally, the retrieval method of group members will be described in Section 3.2.3.

A. THE CONTENTS OF A BLOCK

The contents of a block include block number, block ID, previous block ID, Nonce, receiver public key, record generation timestamp, block generation timestamp, block brief information and sensitive information. The detailed contents of a block are shown in Figure 3.

The block ID is stored in the header, which is the value generated by the hash of previous block ID, previous block content and nonce, and the block ID is to guide all blocks forward to form the Blockchain. The most important part of block generation is the calculation of block ID, and the calculation result must meet the difficulty limit. The first few numbers must be kept as a number of zeros, and the nonce value is used to achieve this result. The receiver public key is equivalent to the concept of the receiver's address when sending a letter, so when the block stores the public key, the receiver can use his/her public key to retrieve his/her own block in the Blockchain. The block timestamp is the time

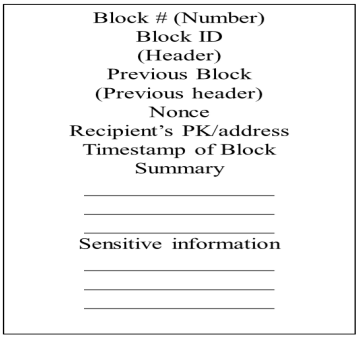

FIGURE 3. The contents of a block.

when the block is generated, and its purpose is to identify the sequence of block generation. The block brief information is public information, the public information content in this paper has different storage information contents for three different electronic records, and the information contents are the patient's physiological data, physiological condition and medical advice. The sensitive information is the personal information related to the patient's personal privacy, the content of this block will be encrypted by the receiver's public key or group session key, only the owner of the key can decrypt the cipher text into plain text for viewing, and a random number is added into the privacy content to avoid certain information security attacks. The detailed block storage content is shown in Figures Figure 4 and 5, and the block content simulation is shown in Figure 6.

B. THE AGGREGATION OF MEDICAL REPORT

This section will first introduce the signature, encryption and decryption to be calculated by HC, D and P when uploading EHR, EMR, PHR and APHR, and the introduce the process and operation mode in detail. Then it explains the

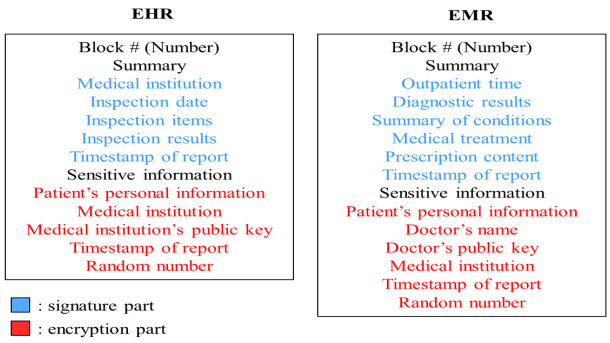

FIGURE 4. The contents of EHR and EMR.

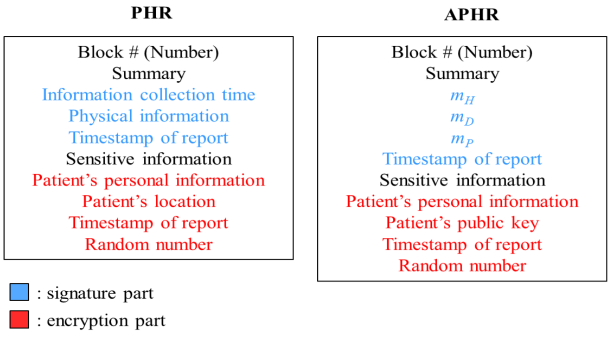

FIGURE 5. The contents of PHR and APHR.

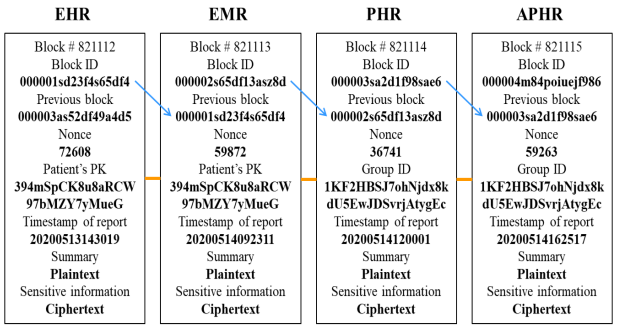

FIGURE 6. The simulation of block content.

group members including doctors, patients, relatives, friends and care providers, the verification and calculation to be performed in the group setting phase, and the final joint agreement on a session key. Finally, it introduces how group members obtain the aggregate records APHR of the patient. The notations used in this paper are shown in Table 3.

C. UPLOAD PHASE

This section will describes the upload phase which is divided into EHR, EMR, PHR and APHR, and HC and D generate electronic records (EHR and EMR) and use the patient public key to encrypt and upload such electronic records to the Blockchain network. The patient generates PHR and APHR, then encrypts the records by key_w obtained during the first examination at HC, and uploads them to the Blockchain network. The detailed process is as follows.

1) EHR UPLOAD PHASE

The healthcare center selects a random number r_H and stores it into SI_H. The content of EHR includes examination information m_H and sensitive information SI_H. HC uses P's public key PK_P and the random number r_H to encrypt the sensitive information and generates $s_H = E_{PK_P}(SI_H, H(r_H))$. Then, the public information m_H and encrypted sensitive information s_H are signed with HC's own private key to generate Sig_H. Finally, all information is signed with the private key of HC, $C_1 = S_{SK_H}(m_H, Sig_H, s_H, T_H^1, H(r_H))$ indicates that the information is generated by HC, C_1 and the public key PK_H are sent to Blockchain Transformation (BT), and here T_H^1 represents the time when HC sends this information. After receiving C_1, BT decrypts it by using the public key PK_H of HC to obtain $(m_H, Sig_H, s_H, T_H^1, H(r_H)) = D_{PK_H}(C_1)$, and verifies whether the information transmission is within the legal time by calculating $T_{BT}^1 - T_H^1 \leq \Delta T$. If it is correct, BT will find the header of the last block in current Blockchain and guess the nonce value to make the header of this block less than or equal to the difficulty value. Finally, BT uploads the calculated block to the block network and transmits $header_H$ to HC. After receiving $header_H$ from BT, HC goes to the Blockchain network to check whether a block in the Blockchain network has $header_H$ and confirms whether the sent information has been uploaded to the Blockchain network. The details of EHR upload phase are shown in Figure 7.

2) EMR UPLOAD PHASE

The doctor selects a random number r_D and stores it into SI_D when electronic health report (EMR) is generated. The content of EMR includes diagnostic information m_D and sensitive information SI_D. D uses P's public key PK_P and the random number r_D to encrypt the sensitive information and generates $s_D = E_{PK_P}(SI_D, H(r_D))$. Then, the public information m_D and encrypted sensitive information s_D are signed with D's private key to generate Sig_D. Finally, all information is encrypted with the private key of D, $C_2 = S_{SK_D}(m_D, Sig_D, s_D, T_D^1, H(r_D))$ indicates that the information is generated by D, C_1 and the public key PK_H are sent to Blockchain Transformation, and here T_D^1 represents the time when D sends this information. After receiving C_2, BT decrypts it by using the public key of D_{PK_D} to obtain $(m_D, Sig_D, s_D, T_D^1,) = D_{PK_D}(C_2)$, and verifies whether the information transmission is within the legal time by calculating $T_{BT}^2 - T_D^1 \leq \Delta T$. If it is correct, BT will find the header of the last block in current Blockchain and guess the nonce value to make the header of this block less than or equal to the difficulty value. Finally, BT uploads the calculated block to the block network and transmits $header_D$ to D. After receiving $header_D$ from BT, D goes to the Blockchain network to check whether a block in the Blockchain network has $header_D$ and confirms whether the sent information has been uploaded to the Blockchain network. The details of EMR upload phase are shown in Figure 8.

TABLE 3. Notations.

Notation	Description
SI_H	Patient sensitive information generated by HC
SI_D	Patient sensitive information generated by D
SI_P	Patient sensitive information generated by P
s_i	s_H, s_D and s_P are the sensitive information encrypted by P's public key, s_G is the sensitive information encrypted by group session key
m_i	Physiological information generated by user i
r_i	Random number selected by user i
T_i	Timestamp generated by user i
key_w	APHR encryption key obtained by P on his/her first visit to the HC
$E_k(m)/D_k(m)$	Use key k to encrypt/decrypt message m
$S_k(m)/V_k(m)$	Use key k to sign/verify message m
$\|\|$	Connect two adjacent messages
$H(\cdot)$	One-way hash function based on Chebyshev chaotic maps
$x, T_{s_i}(x)$	Public key of user i based on Chebyshev chaotic maps
s_i	Private key of user i based on Chebyshev chaotic maps

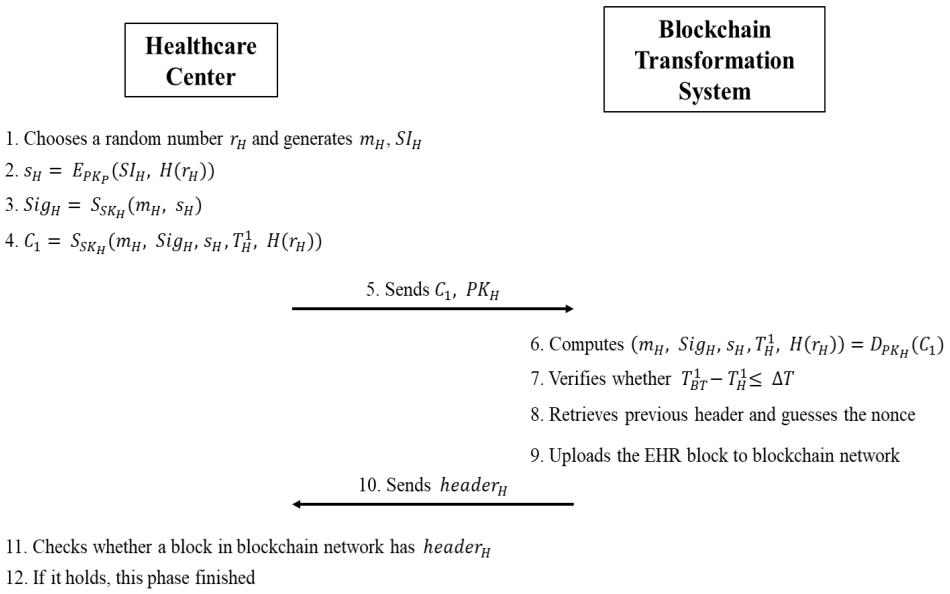

FIGURE 7. EHR upload phase.

3) PHR UPLOAD PHASE

The patient selects a random number r_P and stores it into SI_P when electronic health report (PHR) is generated. The content of PHR includes patient's physiological information m_P and sensitive information SI_P. P uses his/her own public key PK_P and the random number r_P to encrypt the sensitive information and generates $s_P = E_{PK_P}(SI_P, H(r_P))$. Then, the public information m_P and encrypted sensitive information s_P are signed with P's private key to generate Sig_P. In this phase, the public key of P which was originally stored in m_P will be replaced by ID_G which is the public temporary information composed of the identity of group members and random numbers, which aims to protect the protocol from known key attacks. Finally, all information is encrypted with the private key of P, $C_3 = S_{SK_P}(m_P, Sig_P, s_P, T_P^1, H(r_P))$ indicates that the information is generated by P, C_3 and the key PK_P are sent to Blockchain Transformation, and here T_P^1 represents the time when P sends this information. After receiving C_3, BT decrypts it by using the public key of P to obtain $(m_P, Sig_P, s_P, T_P^1, H(r_P)) = D_{PK_P}(C_3)$, and verifies whether the information transmission is within the legal time by calculating $T_{BT}^3 - T_P^1 \leq \Delta T$. If it is correct, BT will find the header of the last block in current Blockchain and guess the nonce value to make the header of this block less than or equal to the difficulty value. Finally, BT uploads the calculated block to the block network and transmits $header_P$ to P. After receiving $header_P$ from BT, P goes to the Blockchain network to check whether a block in the Blockchain network has $header_P$ and confirms whether the sent information has been uploaded to the Blockchain network. The details of PHR upload phase are shown in Figure 9.

4) APHR UPLOAD PHASE

In this phase, the patient collects the last block of three electronic files, and decrypts the sensitive information $D_{SK_P}(S_H) = (SI_H, H(r_H))$ and $D_{SK_P}(S_D) = (SI_D, H(r_D))$ and verifies whether its content is correct by calculating $V_{PK_H}(Sig_H) = (m_H, s_H)$ and $V_{PK_D}(Sig_D) = (m_D, s_D)$.

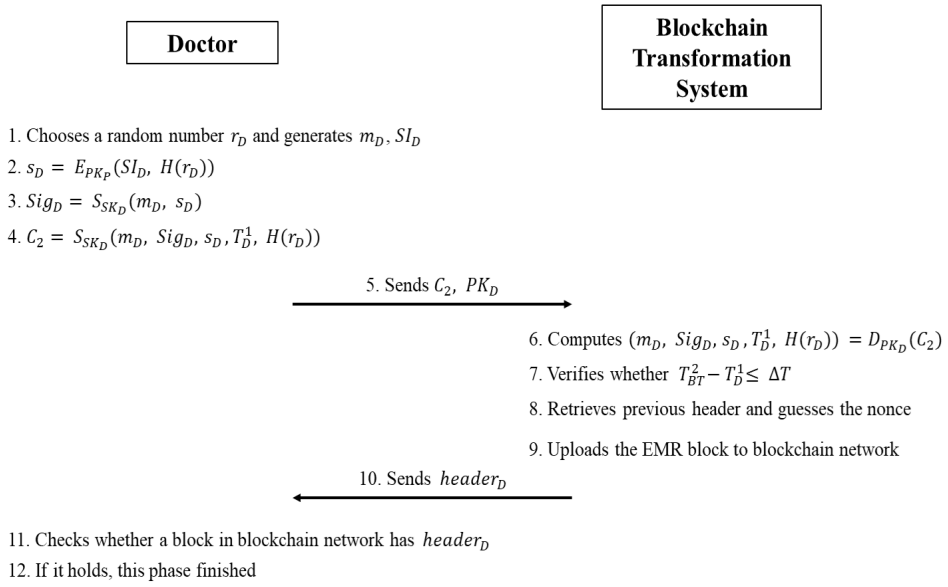

FIGURE 8. EMR upload phase.

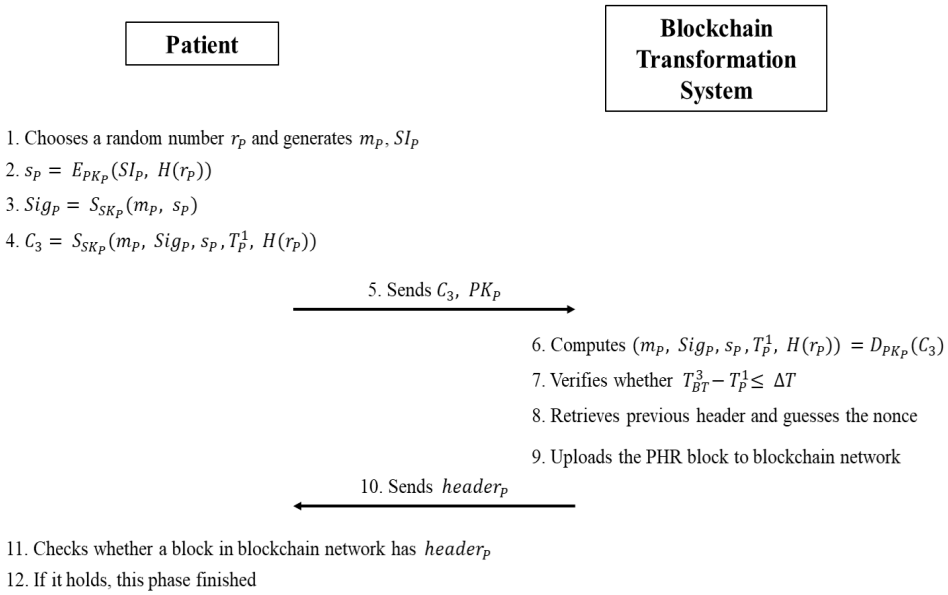

FIGURE 9. PHR upload phase.

If it holds, P selects a random number r_G and stores it into SI_G when electronic health report APHR is generated. The content of APHR includes the aggregation of patient's physiological information m_G and sensitive information SI_G. P uses a group session key GSK and $H(r_G)$ to encrypt the sensitive information and generates $s_G = E_{GSK}(SI_G, Sig_H, Sig_D, Sig_P)$. Then the public information m_G and encrypted sensitive information s_G are signed with P's private key to generate Sig_G. Finally, all information is encrypted with the private key of P, $C_4 = E_{SK_P}(m_G, Sig_G, s_G, T_P^2, H(r_G))$ indicates that the information is generated by P, C_4 and the key PK_P are sent to Blockchain Transformation, and here T_P^2 represents the time when P sends this information. After receiving C_4, BT decrypts it by using the public key of P to obtain $(m_G, Sig_G, s_G, T_P^2, H(r_G)) = D_{PK_P}(C_4)$, and verifies whether the information transmission is within the legal time by calculating $T_{BT}^4 - T_P^2 \leq \Delta T$. If it is correct, BT will find the header of the last block in current Blockchain and guess the nonce value to make the header of this block less than or equal to the difficulty value. Finally, BT uploads the calculated block to the block network and transmits $header_G$ to P. After receiving

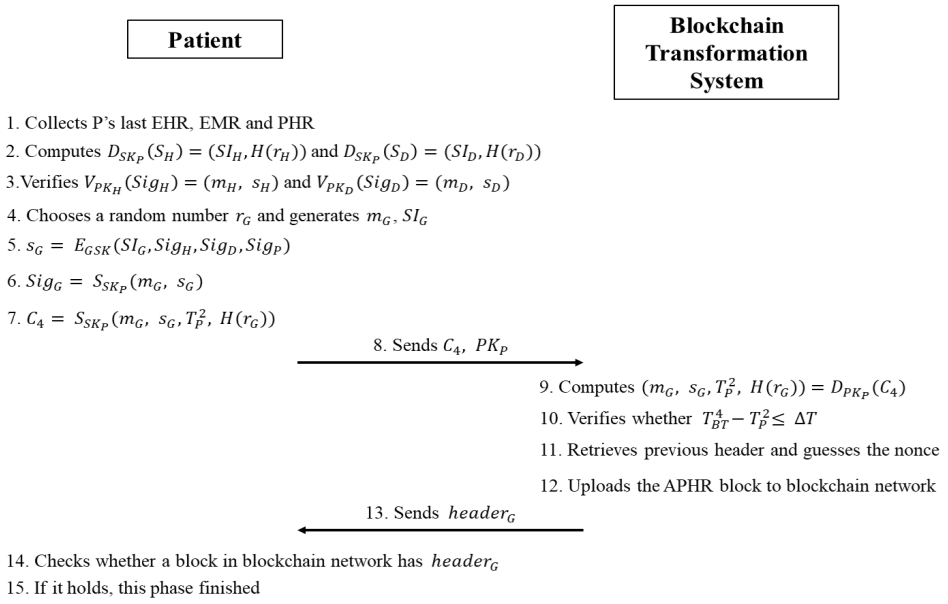

FIGURE 10. APHR upload phase.

$header_G$ from BT, P goes to the Blockchain network to check whether a block in the Blockchain network has $header_G$ and confirms whether the sent information has been uploaded to the Blockchain network. The details of APHR upload phase are shown in Figure 10.

D. GROUP SETUP PHASE

The main purpose of this phase is to construct a group environment. The group members including patients, doctors, relatives, friends and medical care providers conduct mutual authentication and jointly agree on a group session key, so that in the phase of final group member retrieval, the group members can use this key to view the encrypted privacy information.

1) MUTUAL AUTHENTICATION AND TWO-PARTY AGREEMENT PHASE

In this phase, we assume that n group members $U_1, U_2, , U_n$ are organized in an ordered chain and U_{i+1} is the successor of U_i. Moreover, all ID information and their corresponding public keys have been arranged and all members in a group perform the following steps:

Step 1: U_i selects a random number r_i and computes $K_{i,i+1} = T_{r_i}T_{s_{i+1}}(x)$, $C_i = E_{K_{i,i+1}}(ID_i||ID_{i+1}||T_{r_i}(x))$ and $MAC_{i,i+1} = H(ID_i||ID_{i+1}||C_i||H(T_{s_i}T_{s_{i+1}}(x))||T_{r_i}(x))$. Then, U_i sends $C_1, T_{r_i}(x), MAC_{i,i+1}$ to its successor U_{i+1}.

Step 2: After receiving the message from U_i, U_{i+1} uses his/her private key s_{i+1} and $T_{r_i}(x)$ to compute $K'_{i,i+1} = T_{s_{i+1}}T_{r_i}(x)$. Then U_{i+1} reveals $(ID_i||ID_{i+1}||T_{r_1}(x))$ by computing $D_{K'_{i,i+1}}(C_i)$ and checks whether $H(ID_i||ID_{i+1}||C_i||H(T_{s_{i+1}}T_{s_i}(x))||T_{r_i}(x))$ is equal to $MAC_{i,i+1}$ or not. If it holds, U_{i+1} selects a random number r_{i+1} and computes $K_{i+1,i} = T_{r_{i+1}}T_{s_i}(x)$, $SK = T_{r_{i+1}}T_{r_i}(x)$, $C_{i+1} = E_{K_{i+1,i}}(ID_i||ID_{i+1}||T_{r_{i+1}}(x))$ and $MAC_{i+1,i} = H(ID_i||ID_{i+1}||C_{i+1}||T_{r_{i+1}}(x)||H(T_{s_{i+1}}T_{s_i}(x))||SK)$. Then U_{i+1} sends C_{i+1}, $T_{r_{i+1}}(x)$, $MAC_{i+1,i}$ to its predecessor U_i.

Step 3: After receiving the message from U_{i+1}, U_i uses his/her private key s_i and $T_{r_{i+1}}(x)$ to compute $K'_{i+1,i} = T_{s_i}T_{r_{i+1}}(x)$. Then U_i reveals $(ID_i||ID_{i+1}||T_{r_{i+1}}(x))$ by computing $D_{K'_{i+1,i}}(C_{i+1})$ and checks whether $H(ID_i||ID_{i+1}||C_{i+1}||T_{r_{i+1}}(x)||H(T_{s_i}T_{s_{i+1}}(x))||SK')$ is equal to $MAC_{i+1,i}$ or not, where $SK' = T_{r_i}T_{r_{i+1}}(x)$. If it holds, U_{i+1} is authenticated by U_i. Then U_i computes $MAC'_{i,i+1} = H(ID_i||ID_{i+1}||H(T_{s_i}T_{s_{i+1}}(x))||SK_{i,i+1})$ and sends the acknowledgement message $MAC'_{i,i+1}$ to U_{i+1}, where $SK_{i,i+1} = H(ID_i||ID_{i+1}||T_{r_i}T_{r_{i+1}}(x))$ is the session key shared between U_i and U_{i+1}.

Step 4: After receiving $MAC'_{i,i+1}$ from U_i, U_{i+1} computes the session key $SK_{i+1,i} = H(ID_i||ID_{i+1}||T_{r_{i+1}}T_{r_i}(x))$ and checks whether $H(ID_i||ID_{i+1}||H(T_{s_{i+1}}T_{s_i}(x))||SK_{i+1,i}$ is equal to $MAC'_{i,i+1}$ or not. If it is not valid, the authentication is failed and the session is terminated. Otherwise, U_i is authenticated by U_{i+1} and end this phase.

2) GROUP SESSION KEY AGREEMENT PHASE

In this phase, each group member U_i uses its group identity GID_i to compute B_{i-1} and B_i, where $B_{i-1} = H(SK_{i-1,i} \oplus T_{S_i}T_{S_{i-1}}(x) \oplus GID_i)$ and $B_i = H(SK_{i,i+1} \oplus T_{S_i}T_{S_{i+1}}(x) \oplus GID_i)$. Next U_i computes $X_i = B_{i-1} \oplus B_i$ and broadcasts X_i to

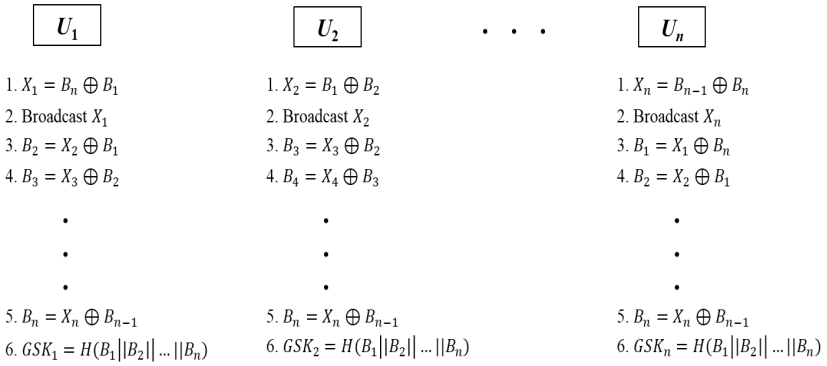

FIGURE 11. Group key agreement phase.

the group. After collecting all X_i from $n-1$ members, each U_i checks whether $X_1 \oplus X_2 \oplus \ldots \oplus X_{n-1} \oplus X_n$ is equal to 0 or not. If not, U_i terminated this phase. Otherwise, U_i can use B_i and X_{i+1} to derive all B_j by using continuous XOR operation, where $j = 1, \ldots, n$. For example, U_1 uses his/her B_1 to derive U_2's B_2 by computing $X_2 \oplus B_1$, where $X_2 = B_1 \oplus B_2$. After deriving B_2, U_1 can further use it to get U_3's B_3 by computing $X_3 \oplus B_2$. To sum it up, the values of B_i and X_i are shown in Table 4 and 5. Finally, after deriving all B_j, all group members can compute the common group session key GSK_i by computing $GSK_i = H(B_1||B_2|| \ldots ||B_n)$, where $GSK_1 = GSK_2 = \ldots = GSK_n$. The details of this phase are shown in Figure 11.

TABLE 4. The values of B_i.

Parameter	Value
B_1	$H(SK_{1,2} \oplus T_{S_1} T_{S_2}(x) \oplus GID_i)$
B_2	$H(SK_{2,3} \oplus T_{S_2} T_{S_3}(x) \oplus GID_i)$
$\vdots$	$\vdots$
B_n	$H(SK_{n,1} \oplus T_{S_n} T_{S_1}(x) \oplus GID_i)$

TABLE 5. The values of X_i.

Parameter	Value
X_1	$B_n \oplus B_1$
X_2	$B_1 \oplus B_2$
$\vdots$	$\vdots$
X_n	$B_{n-1} \oplus B_n$

3) MEMBER JOIN PHASE

In case of a new member is authorized to join the group of which size is n, the new member U_{n+1} becomes the successor of member U_n and the member U_1 becomes the successor of member U_{n+1}. Firstly, U_n sends $C_n, T_{r_n}(x), MAC_{n,n+1}$ to its new successor U_{n+1} while U_{n+1} sends $C_{n+1}, T_{r_{n+1}}(x), MAC_{n+1}$ to its new successor U_1. Next, U_{n+1} checks the validity of messages $C_n, T_{r_n}(x), MAC_{n,n+1}$ and computes new secret $SK_{n,n+1}$ shared between U_{n+1} and its new predecessor U_n. In the same way, the member U_1 updates its new secret with $SK_{n+1,1}$. Finally, all the $(n+1)$ members in the group can derive a new group session key by recomputing the protocol of group key agreement phase.

4) MEMBER LEAVE PHASE

In case of a member U_k leaves the group and the group size changes into $(n-1)$, in order to protect patient privacy, all remaining members must update group session key and prevent the leaving U_k to derive the updated group session key. Firstly, U_{k-1} and U_{k+1} remove the shared secrets $SK_{k-1,k}$ and $SK_{k,k+1}$ with U_k. U_{k+1} becomes the new successor of U_{k-1} and U_{k-1} needs to send $C_{k-1}, T_{r_{k-1}}(x), MAC_{k-1}$ to its new successor U_{k+1}. After receiving messages from U_{k-1}, U_{k+1} checks the validity of messages $C_{k-1}, T_{r_{k-1}}(x), MAC_{k-1}$ and derives the new secret $SK_{k-1,k+1}$ shared between U_{k+1} and U_{k-1}. Similarly, U_{k+1} sends $C_{k+1}, T_{r_{k+1}}(x), MAC_{k+1}$ to its new predecessor U_{k-1} and U_{k-1} checks the validity of messages $C_{k+1}, T_{r_{k+1}}(x), MAC_{k+1}$. If it holds, U_{k-1} derives new secret $SK_{k-1,k+1}$ shared between U_{k-1} and U_{k+1}. Finally, each member U_j that follows U_k changes its index to $(j-1)$ and all the existing $(n-1)$ members can derive a new group session key by recomputing the protocol of group key agreement phase.

E. GROUP MEMBER RETRIEVAL PHASE

In this phase, the valid group members can retrieve APHR through the APHR search system. The member first transmits the group identity GID_i and retrieves it in the Blockchain network. After receiving the request from the member, the search system retrieves and displays all the blocks conforming to GID_i. The group members who want to view its information content, decrypt the sensitive information $D_{GSK}(S_G) = (SI_G, Sig_H, Sig_D, Sig_P)$ through GSK, verify its content $V_{PK_H}(Sig_H) = (m_H, s_H)$, $V_{PK_D}(Sig_D) = (m_D, s_D)$ and $V_{PK_P}(Sig_P) = (m_P, s_P)$, and if correct, retrieve it and end this phase.

IV. ANALYSES OF THE PROPOSED SCHEME

The common security problems in group authentication include user anonymity, replay attack, known key security,

internal attack and off-line password guessing attack. In the proposed scheme, security and function analysis will be performed in this section to show that our suggested mechanism can withstand the following common security attacks and meet the security functional requirements, as detailed in the following sections.

A. PATIENT ANONYMITY

In the proposed scheme, all messages are encrypted and signed with the public and private keys of the user, the patient's identity is transmitted without disclosing publicly, and the identity and the encryption and decryption of messages are verified by the calculation through public and private keys. In the APHR upload phase, the patient aggregates all electronic records, then uses the group session key GSK to encrypt the sensitive information and uploads it to BT, and finally calculates it into the Blockchain network. In the group member retrieval phase, the group member transmits GID_i to the APHR search system which uses such identification code to index, and finally all matching blocks are displayed. To view the contents, the authorized group member must use the group session key GSK to decrypt and confirm the patient's information and physiological condition. Because the patient's personal identity has not been transmitted in plain text over the public channel during the whole process, the attacker cannot track the patient's identity and collect the physiological information of a specific patient.

B. NON-REPUDIATION

In this study, the producers of all generated health records need to use their own private keys to sign all their data including m_i, Sig_i, s_i, T_i before uploading. Before being calculated into a block, they must decrypt the signature. At this time, they need to use the public key of the signer. Only the owner of the private key can sign the data. Therefore, when a block is generated, it also means that the content of the block has been confirmed to be generated by the uploader. In order to achieve data correctness in the proposed scheme, each generated record must be authenticated by the signature of the producer $Sig_i = S_{SK_i}(m_i, s_i)$ as proof of generating data.

C. PREVENTION OF KNOWN KEY ATTACK

In the phase of mutual authentication and two-party agreement, the generation of $SK = T_{r_{i+1}} T_{r_i}(x)$ depends on random numbers r_i and r_{i+1}, and each key generation is independent. Therefore, even if a member accidentally leaks the key to the attacker, the attacker cannot calculate the past and future keys. In the phase of group session key agreement, the generation mode of group session key is $GSK_i = H(B_1||B_2||\ldots||B_n)$, the required parameters are calculated on the basis of the random numbers selected by all group members. Therefore, the attacker cannot use this key to calculate any past or future group session key.

D. PREVENTION OF INSIDER ATTACK

After being transmitted by the patient, the message is transformed into a block conforming to the format through the block transformation system and then uploaded to the Blockchain network. After the block transformation system receives the message, the sensitive information containing the patient's identity is still cipher text. The content containing the patient's personal sensitive information includes s_H, s_D, s_P, and s_G, wherein, s_H, s_D and s_P are encrypted with the patient's public key $s_P = E_{PK_P}(SI_P, H(r_P))$, s_G is encrypted with the group session key $s_G = E_{GSK}(SI_G, Sig_H, Sig_D, Sig_P)$, and the content can be decrypted only by the patient P using his/her own private key or by the group member using the group session key, without using personal identification password during the whole process. Therefore, the insider cannot use his/her own authorized identity to steal the patient's sensitive information or the user identification password for other service server login attempts.

E. PREVENTION OF REPLAY ATTACK

Replay attack is the most common attack in the process of authentication. The common countermeasures are timestamp and random number. In the record upload process proposed in this paper, each message contains a timestamp, and it verifies for each receipt whether the transmission period conforms to a standard interval. In the phase of mutual authentication and two-party agreement. Since the random number r_i selected by the group member is the latest in each session, if the attacker captures the message and sends $T_{r_i}(x)$ again, the session request will be rejected when U_{i+1} finds that the message has appeared or is currently being processed, which makes the replay attack initiated by the attacker invalid. In addition, if the attacker wants to successfully launch a replay attack, it must be calculated and modified C_i and $T_{r_i}(x)$, correctly, but this is impossible.

F. SECURITY AND FUNCTIONALITY COMPARISONS

In terms of security comparison with TMIS-related literature, the scheme proposed by He *et al.* (2012) [13] was found by Wei *et al.* (2012) [28] that this improvement scheme was unable to withstand off-line password guessing attack. Jiang *et al.* (2013) [14] found that the approach proposed by Wei *et al.* was still unable to withstand password guessing attack. It was found that the approach of Xu *et al.* (2014) [32] was unable to resist replay attack. Furthermore, the scheme of Chen *et al.* [4] was found by Chiou *et al.* [5] to be unable to achieve user anonymity and resist off-line password guessing attack, and most of the schemes do not provide group authentication mechanism. In this paper, the common security threats mentioned above can be avoided, and the arrangement is shown in Table 6.

On the other hand, in terms of functionality comparison with related literature, this study combines Blockchain and IoT technologies and provides the group authentication

TABLE 6. Security comparisons among the proposed scheme and other related schemes.

Schemes → / Security ↓	He et al. (2012)	Wei et al. (2012)	Xu et al. (2014)	Chen et al. (2014)	Our scheme
Patient anonymity	√	√	√	χ	√
Known key attack resistance	√	√	√	√	√
Insider attack resistance	√	√	√	√	√
Password guessing attack resistance	χ	χ	√	χ	√
Replay attack resistance	√	√	χ	√	√

√: It indicates that the function can be achieved.
χ: It indicates that the function cannot be achieved.

TABLE 7. Functionality comparisons among the proposed scheme and other related schemes.

Schemes → / Security ↓	Xu et al. (2014)	Chen et al. (2014)	Deng et al. (2017)	Pham et al. (2018)	Our scheme
Remote medical monitoring	√	√	√	χ	√
Non-repudiation	√	√	√	√	√
Group authentication	χ	χ	χ	χ	√
Medical data aggregation	χ	χ	χ	√	√
Blockchain technology	χ	χ	χ	χ	√

√: It indicates that the function can be achieved.
χ: It indicates that the function cannot be achieved.

mechanism, which enables authorized group members to view patients' aggregated medical records, and enables doctors to conduct remote monitoring and provide medical advice. The detailed functionality comparison with related literature is shown in Table 7.

V. CONCLUSION

With the rapid development of science and technology and network, more and more paper-based documents have been replaced by electronic files. In addition to being more environmentally friendly than paper-based documents, digital data can be transmitted and shared in real time. Wherein, electronic medical information can bring a lot of convenience, including telemedicine, data retrieval, medical data collection and statistics and analysis of epidemic trends in recent years. Wherein, the three types of common medical records (EHR, EMR and PHR) all belong to the patients' extremely private medical records. If they are transmitted through the network, there may be doubts about information security. Therefore, many researchers have proposed many information security protection mechanisms to protect the patients' private medical records from improper access.

Blockchain has become a very important technology in information security of the day. Its application scope is not limited to financial flow related fields, but also includes other fields, such as smart home, smart grid, food safety application and other fields. This study combines the security, storage, anonymity, non-repudiation and other features of Blockchain with the remote, real-time, automation and other features of IoT, and proposes a security mechanism that can aggregate three types of medical records. The purpose of this mechanism is not only to solve the problems of medical record storage, accelerating the medical process, and reducing medical errors, but also to provide more personalized medical services for patients. In this study, the healthcare center, the doctor and the patient may encrypt and sign the privacy information for the generated electronic records (EHR, EMR, PHR) and send it to the Blockchain transformation system to be calculated into blocks and uploaded to the Blockchain network. After that, the patient can obtain his/her own EHR, EMR and PHR through the Blockchain network and aggregate these three files to generate APHR which is then uploaded to the block network through the Blockchain transformation system. On the other hand, in this study, a group authentication mechanism is designed to enable authorized group members, such as doctors, medical service providers, relatives and friends, to view the medical information of the patient and monitor the physiological information of the patient anytime and anywhere. The group identity and group session key agreed by the group member co-authentication enable the patient to use the group session key to encrypt and protect personal physiological information. If other authorized group members want to view and monitor the current physiological health data of the patient, they can also use this group session key to decrypt, so as to realize the real-time remote medical monitoring function.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

[1] R. Ballweg, D. Brown, D. Vetrosky, and T. Ritsema, *Physician Assistant: A Guide to Clinical Practice*. Amsterdam, The Netherlands: Elsevier, 2017.
[2] S. Blecker, K. Goldfeld, N. Park, D. Shine, J. S. Austrian, R. S. Braithwaite, M. J. Radford, and M. N. Gourevitch, "Electronic health record use, intensity of hospital care, and patient outcomes," *Amer. J. Med.*, vol. 127, no. 3, pp. 216–221, Mar. 2014.
[3] D. Blumenthal and M. Tavenner, "The 'meaningful use' regulation for electronic health records," *New England J. Med.*, vol. 363, no. 6, pp. 501–504, 2010.

[4] C.-L. Chen, T.-T. Yang, M.-L. Chiang, and T.-F. Shih, "A privacy authentication scheme based on cloud for medical environment," *J. Med. Syst.*, vol. 38, no. 11, p. 143, Nov. 2014.
[5] S.-Y. Chiou, Z. Ying, and J. Liu, "Improvement of a privacy authentication scheme based on cloud for medical environment," *J. Med. Syst.*, vol. 40, no. 4, p. 101, Apr. 2016.
[6] J. Condos, W. H. Sorrell, and S. L. Donegan. (2016). *Blockchain Technology: Opportunities and Risks*. [Online]. Available: http://https://tpc-management.ro/en/blockchain-technologies-opportunities-and-chances/
[7] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125, Dec. 2018.
[8] Y.-Y. Deng, C.-L. Chen, W.-J. Tsaur, Y.-W. Tang, and J.-H. Chen, "Internet of Things (IoT) based design of a secure and lightweight body area network (BAN) healthcare system," *Sensors*, vol. 17, no. 12, pp. 1–18, Dec. 2017.
[9] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.
[10] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M. A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," *Comput. Netw.*, vol. 177, Aug. 2020, Art. no. 107333.
[11] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, "BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for Internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.
[12] C. He, X. Jin, Z. Zhao, and T. Xiang, "A cloud computing solution for hospital information system," in *Proc. IEEE Int. Conf. Intell. Comput. Intell. Syst.*, vol. 2, Oct. 2010, pp. 517–520.
[13] H. Debiao, C. Jianhua, and Z. Rui, "A more secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1989–1995, Jun. 2012.
[14] Q. Jiang, J. Ma, Z. Ma, and G. Li, "A privacy enhanced authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 37, no. 1, p. 9897, Feb. 2013.
[15] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 2, p. 12, Feb. 2014.
[16] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *J. Med. Syst.*, vol. 42, no. 8, p. 156, Aug. 2018.
[17] A. S. Kazley, A. N. Simpson, K. N. Simpson, and R. Teufel, "Association of electronic health records with cost savings in a national sample," *Amer. J. Managed Care*, vol. 20, no. 6, pp. 183–190, 2014.
[18] S. Kumari, M. K. Khan, and R. Kumar, "Cryptanalysis and improvement of 'a privacy enhanced scheme for telecare medical information systems,'" *J. Med. Syst.*, vol. 37, no. 4, p. 9952, Aug. 2013.
[19] C.-T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," *Sensors*, vol. 17, no. 7, p. 1482, Jun. 2017.
[20] C.-T. Li, T.-Y. Wu, and C.-M. Chen, "A provably secure group key agreement scheme with privacy preservation for online social networks using extended chaotic maps," *IEEE Access*, vol. 6, pp. 66742–66753, 2018.
[21] C.-T. Li, D.-H. Shih, and C.-C. Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems," *Comput. Methods Programs Biomed.*, vol. 157, pp. 191–203, Apr. 2018.
[22] D. Mishra, "Understanding security failures of two authentication and key agreement schemes for telecare medicine information systems," *J. Med. Syst.*, vol. 39, no. 3, pp. 1–8, Mar. 2015.
[23] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://bitcoin.org/bitcoin.pdf
[24] M. Pham, Y. Mengistu, H. Do, and W. Sheng, "Delivering home healthcare through a cloud-based smart home environment (CoSHE)," *Future Gener. Comput. Syst.*, vol. 81, pp. 129–140, Apr. 2018.
[25] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl. Energy*, vol. 195, pp. 234–246, Jun. 2017.
[26] K. Toyoda, "Standardization and security for the EMR," *Int. J. Med. Informat.*, vol. 48, nos. 1–3, pp. 57–60, Feb. 1998.
[27] M. Wazid, A. K. Das, V. K. Bhat, and A. V. Vasilakos, "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," *J. Netw. Comput. Appl.*, vol. 150, Jan. 2020, Art. no. 102496.
[28] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3597–3604, Dec. 2012.
[29] F. Williams and S. Boren, "The role of the electronic medical record (EMR) in care delivery development in developing countries: A systematic review," *J. Innov. Health Informat.*, vol. 16, no. 2, pp. 139–145, Jul. 2008.
[30] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1529–1535, Jun. 2012.
[31] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.
[32] X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, and L. He, "A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 1, p. 9994, Jan. 2014.
[33] D. Yach, C. Hawkes, C. L. Gould, and K. J. Hofman, "The global burden of chronic diseases: Overcoming impediments to prevention and control," *J. Amer. Med. Assoc.*, vol. 291, no. 21, pp. 2522–2616, 2004.
[34] K. Yeo, K. Lee, J. M. Kim, T. H. Kim, Y. H. Choi, W. J. Jeong, H. Hwang, R. M. Baek, and S. Yoo, "Pitfalls and security measures for the mobile EMR system in medical facilities," *Healthcare Informat. Res.*, vol. 18, no. 2, pp. 125–135, 2012.
[35] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, Oct. 2016.
[36] H. Zhu, "Secure chaotic maps-based group key agreement scheme with privacy preserving," *Int. J. Netw. Secur.*, vol. 18, no. 6, pp. 1001–1009, Nov. 2016.

CHUN-TA LI (Member, IEEE) received the Ph.D. degree in computer science and engineering from National Chung Hsing University, Taiwan, in 2008. He is currently an Associate Professor with the Department of Information Management, Tainan University of Technology, Taiwan. His research interests include information security, wireless sensor networks, mobile computing, and security protocols for IoTs and ad hoc networks. He had published more than 100 international journal and international conference papers on the above research fields.

DONG-HER SHIH received the Ph.D. degree in electrical engineering from National Cheng Kung University, Tainan City, Taiwan, in 1986. He is currently a Senior Professor with the Department of Information Management, National Yunlin University of Science and Technology, Taiwan. His current research interests include intrusion prevention systems (IPSs), machine learning, data mining, security, ontology, and wireless networks.

CHUN-CHENG WANG received the master's degree in information management from the National Yunlin University of Science and Technology, Taiwan. His research interests include network security and security protocols for telemedicine information systems.

CHIN-LING CHEN received the Ph.D. degree from National Chung Hsing University, Taiwan, in 2005. From 1979 to 2005, he was a Senior Engineer with Chunghwa Telecom Company Ltd. He is currently a Professor. He has published over 100 articles in SCI/SSCI international journals. His research interests include cryptography, network security, and electronic commerce.

CHENG-CHI LEE received the Ph.D. degree in computer science from National Chung Hsing University (NCHU), Taiwan, in 2007. He is currently a Distinguished Professor with the Department of Library and Information Science, Fu Jen Catholic University. He is also as an editorial board member of some journals. He has also served as a reviewer in many SCI-index journals, other journals, and other conferences. His current research interests include data security, cryptography, network security, mobile communications and computing, and wireless communications. He had published more than 200 articles on the above research fields in international journals.