Contents lists available at ScienceDirect

Computer Methods and Programs in Biomedicine

journal homepage: www.elsevier.com/locate/cmpb

Article

SEMRES - A Triple Security Protected Blockchain Based Medical Record Exchange Structure

Yen-Liang Lee[a,b], Hsiu-An Lee[c,d,e,*], Chien-Yeh Hsu[d,e,f,*], Hsin-Hua Kung[d,e], Hung-Wen Chiu[a,g,*]

[a] Graduate Institute of Biomedical Informatics, Taipei Medical University, Taipei, Taiwan
[b] Internet of Things Laboratory, Chunghwa Telecom Laboratories, Tao Yuen, Taiwan
[c] National Institute of Cancer Research, National Health Research Institutes, Tainan, Taiwan
[d] Standards and Interoperability Lab, Smart Healthcare Center of Excellence, Taipei, Taiwan
[e] Department of Information Management, National Taipei University of Nursing and Health Sciences, Taipei, Taiwan
[f] Master Program in Global Health and Development, Taipei Medical University, Taipei, Taiwan
[g] Clinical Big Data Research Center, Taipei Medical University Hospital, Taipei City, Taiwan

ARTICLE INFO

Article history:
Received 17 July 2021
Revised 12 December 2021
Accepted 17 December 2021

Keywords:
Blockchain
Security
EMR Protection
Encryption
Data exchange

ABSTRACT

Background and Objective: COVID-19, a serious infectious disease outbreak started in the end of 2019, has caused a strong impact on the overall medical system, which reflects the gap in the volume and capacity of medical services and highlights the importance of clinical data ex-change and application. The most important concerns of medical records in the medical field include data privacy, data correctness, and data security. By realizing these three goals, medical records can be made available to different hospital information systems to achieve the most complete medical care services. The privacy and protection of health data require detailed specification and usage requirements, which is particularly important for cross-agency data exchange.
Methods: This research is composed of three main modules. "Combined Encryption and Decryption Architecture", which includes the hybrid double encryption mechanism of AES and RSA, and encrypts medical records to produce "Secured Encrypted Medical Record". "Decentralize EMR Repository", which includes data decryption and an exchange mechanism. After a data transmission is completed, the content verification and data decryption process will be launched to confirm the correctness of the data and obtain the data. A blockchain architecture is used to store the hash value of the encrypted EMR, and completes the correctness verification of the EMR after transmission through the hash value.
Results: The results of this study provide an efficient triple encryption mechanism for electronic medical records. SEMRES ensures the correctness of data through the non-repudiation feature of a blockchain open ledger, and complete integrated information security protection and data verification architecture, in order that medical data can be exchanged, verified, and applied in different locations. After the patient receives medical services, the medical record is re-encrypted and verified and stored in the patient's medical record. The blockchain architecture is used to ensure the verification of non-repudiation of medical service, and finally to complete the payment for medical services.
Conclusions: The main aim of this study was to complete a security architecture for medical data, and develop a triple encryption authentication architecture to help data owners easily and securely share personal medical records with medical service personnel.

1. Introduction

With the increasing demand for medical care services, diversified medical services have been offered to accommodate the changes in working environment, climate, and social environment. COVID-19, a serious infectious disease outbreak started in the end of 2019, has caused a strong impact on the overall medical system, which reflects the gap in the volume and capacity of medical ser-

* Corresponding authors.
E-mail addresses: d610101008@tmu.edu.tw (Y.-L. Lee), billy72325@gmail.com (H.-A. Lee), cyhsu@ntunhs.edu.tw (C.-Y. Hsu), hsinhuakung@gmail.com (H.-H. Kung), hwchiu@tmu.edu.tw (H.-W. Chiu).

https://doi.org/10.1016/j.cmpb.2021.106595
0169-2607/© 2021 Elsevier B.V. All rights reserved.

vices and highlights the importance of clinical data exchange and application.

Information technology has continuously advanced and has been integrated with medical technology to produce superb medical technology. As different technologies depend on the exchange and application of data, the most important concerns of medical records in the medical field include data privacy, data correctness, and data security. By realizing these three goals, medical records can be made available to other system applications to achieve the most complete medical care services.

The concerns regarding data privacy can be traced back to the Health Insurance Portability and Accountability Act (HIPAA) of the United States in 1996. HIPAA was enacted to modernize the information flow of health care, and specifically, to protect the personal identity information maintained by the health care and medical insurance industry from fraud and theft, and address limitations on medical insurance coverage. The first complete version was formulated in 2003. As a complete specification for the protection and disclosure of private patient data, it consists of national regulations and involves the use and disclosure of protected health information (PHI) of protected entities in health care treatment, payment, and institutional operation. According to the regulations, HHS extended the HIPAA privacy rules to include the independent contractors of covered entities, meaning it is applicable to the definition of "business partner". PHI includes all the information held by a covered entity regarding the health status, the provided health care, and health care payments that can be linked to any individual. In terms of insurance applications, in order to facilitate treatment, payment, and health care operations, an underwriting entity may disclose PHI to certain parties without the explicit written authorization of the patient. Any other disclosure of PHI requires the protected entity to obtain written authorization for disclosure from the individual. In general, when a covered entity discloses any PHI, it must make reasonable efforts to disclose only the minimum necessary information to achieve its purpose.

The privacy and protection of health data require detailed specification and usage requirements, which is particularly important for cross-agency data exchange. In addition, there is a strong demand for medical correctness in insurance payments, and the corresponding costs must be paid according to the correct information; otherwise, it may result in many crimes related to health care, as well as civil and criminal penalties due to illegal acts. Data correctness is also critical in medical services and clinical care. The information contained in medical records enables health care providers to determine the history of patients and provide informed care, thus, medical records in medical services have the effect of supporting clinicians in making decisions. Medical records can be used as a central database for planning patient care, and record communications between patients, medical service providers, and professionals who contribute to patient care.

An electronic personal health record is a complete record that integrates information about a person's surgeries, medications, diagnoses, tests, allergies, etc., which enables patients to share medical records between providers and health care systems through effective data exchange. A variety of medical service models have been proposed with the development of science and technology; for example, physiological data are measured through IoT physiological sensing devices in daily life for long-term tracking [1–4]. There is a large demand for data exchange and integration in different forms of remote care services [[5–7]], various personal health management applications, health insurance payment applications, and data applications between medical institutions. While it is convenient and efficient to transmit data through information communication technology, it is critical to protect the privacy and correctness of the data.

The purpose of this study is to construct an efficient triple encryption mechanism for electronic medical records, which will ensure the correctness of data through the non-repudiation feature of a blockchain open ledger, and complete an integrated information security protection and data verification architecture, in order that medical data can be exchanged, verified, and applied in different locations.

2. Literature review

PHR is a digital file that brings many privacy and security issues while facilitating people's daily life [8]. When discussing the use of medical data, according to developments based on data privacy protection and security management, data owners should generally encrypt sensitive data before sending it to third parties. While the encryption of data can guarantee the confidentiality of data to some extent, as only the holder of the decryption key can decrypt the encrypted data to obtain the correct data, it brings new challenges to research. Encrypted data loses the flexibility and operability of the original data, and users cannot obtain the expected data through the conventional keyword retrieval method. Research on encrypted data search [9] has been a goal continuously explored in the field of information security. In recent years, people have paid more and more attention to the application and management technology of encrypted medical data.

With the emergence of cloud storage technology, an increasing number of issues regarding data protection and management have been raised. Once medical records are uploaded to the cloud, patients will lose physical control of their data [10], thus, one of the biggest concerns for patients is to ensure the integrity of data stored in untrusted cloud storage; for example, even if the data is wrong, cloud storage technology may still claim that the data is complete. Moreover, cloud storage technology may deliberately delete un-accessed or rarely accessed EMR data to save storage space [11–13], and deleting EMR data can make it difficult to recover corrupted data. Different from conventional data management, cloud storage space provides users with a guarantee of audit integrity for outsourced EMR data, and ensures the recoverability of damaged data. Traditionally, if it fails to validate the data integrity, it usually means that the outsourced data has been corrupted, thus, storing only one copy may result in permanent loss of EMR data.

Blockchain, as derived from Bitcoin and launched in 2008, is a transaction architecture based on P2P network technology, encryption technology, and timestamp records. After the establishment of a blockchain, there will be a growing list of records called record blocks, which are linked together by cryptography. Each block contains the encrypted hash value, timestamp, and transaction data of the previous block. A blockchain consists of data structures that represent financial ledger entries or transaction records, and each transaction is digitally signed to ensure its authenticity, and cannot be tampered with, thus, the ledger itself, and the existing transactions in it, are considered to be of high integrity. The basic advantages of blockchain technology include decentralization, peer-to-peer networks, immutability, security, and transparency. If data is re-entered into the record, the original data will not be deleted, but updated. Each block in the blockchain has a permanent timestamp indicating authentication and verification. The abovementioned show that the blockchain structure can effectively solve the problem of EMR content verification and ensure that the data content will not be tampered with.

Akshay et al. [14] proposed a hybrid framework called MediTrust for the encryption management of electronic medical records. The proposed MediTrust framework combines role-based access control with attribute-based encryption, and works on a semantic database to ensure the accessibility of patient data for different access controls. Before the data is outsourced to the cloud server, the patient data should be encrypted by the provider, downloaded from the cloud server, and then, decrypted on the client side. General patient information collected as PHR is stored in a separate cloud server, while medical reports are stored in another cloud server. However, under this structure, multiple cloud storage spaces are required for decentralized management, and the data must be separately decrypted after being retrieved, which reduces the overall application efficiency and cannot verify the correctness of the data content. Xu et al. [15] proposed an asymmetric pairing searchable encryption method for case retrieval, which is available on the public platform, and assists patients and doctors by providing private data search and encryption functions. The system uses an extended public key encryption system with a keyword search function, and the server can determine whether the file stored in the platform contains keywords without releasing any information from the encrypted file. Thus, while this platform solves the problem of data privacy disclosure, it lacks the ability to retrieve complete medical records. Moreover, due to the time required for encryption and decryption, the efficiency of real-time application is reduced, and the correctness of the data cannot be verified.

While there are many encryption methods for traditional data files, they have different advantages and disadvantages, and the application of encryption to medical data depends on the situation. The Advanced Encryption Standard (AES) is a kind of encryption algorithm proposed by the National Bureau of Standards and Technology of the United States [16], which is commonly used to protect data transmission and storage. This encryption mechanism is a symmetric encryption algorithm, which has the advantages of very fast encryption speed and very large encrypted content files. However, since there is only one key to encrypt and decrypt data, it is usually used in conjunction with the RSA (Rivest, Shamir, and Adleman) encryption algorithm, which was officially used publicly in 1997 [17]. This encryption mechanism was proposed by Rivest, Shamir, and Adleman of the Massachusetts Institute of Technology in the United States, and RSA is the combination of the first letters of their surnames. The RSA encryption algorithm is an asymmetric encryption algorithm that uses two different prime numbers as two keys in the encryption mechanism, which are known as the public key and the private key for data encryption or data decryption, respectively. The operation is that, when one key is used to encrypt, the decryption must be done by the other key; if the public key is used to encrypt the data, the private key is needed to decrypt the data. This encryption mechanism is often used for data transmission in electronic commerce to ensure the security of data. While RSA can indeed ensure the security of data, it cannot encrypt very large files and the encryption speed is very slow.

Therefore, this study used the advantages of AES and RSA encryption technologies to design a dual encryption method, verified the actual data with a blockchain to ensure the correctness of medical data, and proposed SEMRES (Secured Encrypted Medical Record Exchange Structure), which is a Triple-protected blockchain based medical record exchange structure, and serves as an application framework for data security and verification in the cloud of medical records. Finally, the triple encryption structure with the non-repudiation feature of third layer verification was completed through the blockchain open ledger architecture. After the EMR content is verified, exchanged, and provided to the authorizer for medical services, the authorizer can add new clinical data content to the patient's EMR. When the block is verified, the medical service is completed, and the blockchain architecture add payment information to the block information to complete the payment process for telemedicine services.

3. Materials and methods

SEMRES is composed of three main modules. The first module is CEDA (Combined Encryption and Decryption Architecture), which includes the hybrid double encryption mechanism of AES and RSA, and encrypts medical records to produce SMeR (Secured Encrypted Medical Record). The second module is DERy (Decentralize EMR Repository), which includes data decryption and an exchange mechanism. After a data transmission is completed, the content verification and data decryption process will be launched to confirm the correctness of the data and obtain the data. The third module is a blockchain architecture for data validation. A blockchain is used to store the hash value of the encrypted EMR, and completes the correctness verification of the EMR after transmission through the hash value. There are three main parts in this research framework; the EMR owner is first, the authorized person is second, and the system is third. Figs. 1–3

3.1. CEDA (Combined encryption and decryption architecture)

Before a medical record is stored or transmitted, the medical record first encrypts the data through CEDA with a random number of AES keys generated by CEDA, and then, encrypts the data with the RSA public key of the authorized person. These two encrypted files are merged and named SMeR (Secured Encrypted Medical Record) and sent to the DERy.

The detailed double encryption process is defined, as follows:

1 Import original medical records
2 CEDA randomly generates AES keys
3 AES symmetric encryption of original medical records through the AES key
4 Create encrypted medical records
5 Perform asymmetric cryptography with the AES key through the RSA public key of the authorized person.
6 Create an encrypted AES key
7 Combine the encrypted AES key and encrypted medical records to create SMeR.

The encryption process and decryption process as follows:

AES is based on a design principle called a permutation network, which is effective in both software and hardware. AES is a variant of Rijndael with a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. AES operates on a 4 × 4 column-major sequence byte array called state. In our design, AES calculations are conducted in a specific finite field.

The process of AES encryption is conducted according to the following steps:

Step 1. KeyExpansion

The round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128-bit round key for each round plus one more.

Step 2. Initial round key addition:

AddRoundKey

Combine each byte of the state with a byte of the round key using bitwise xor.

Step 3. 9 main rounds:

SubBytes

Non-linear replacement step, in which each byte is replaced by another byte according to a lookup table.

1 ShiftRows

Transposition step, in which the last three lines of the state are cyclically shifted by a certain number of steps.

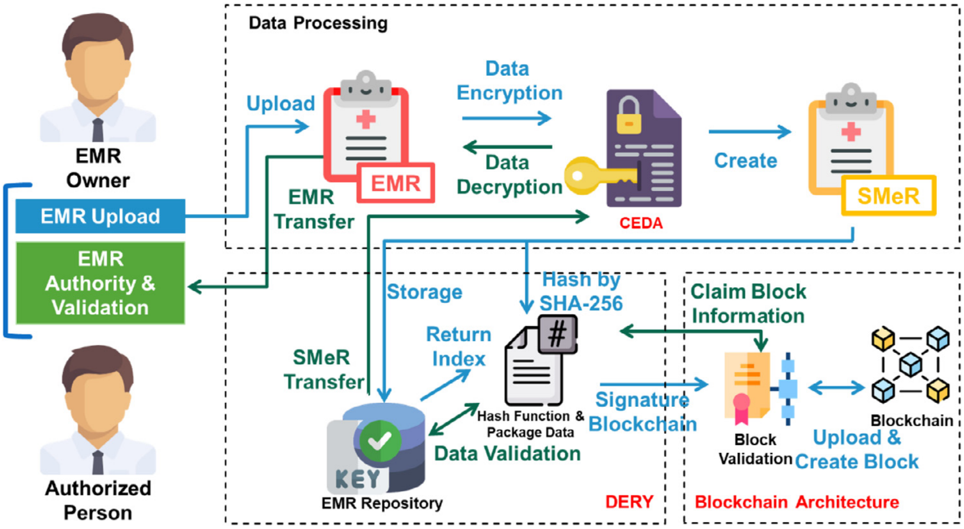


Fig. 1. SEMRES module architecture.

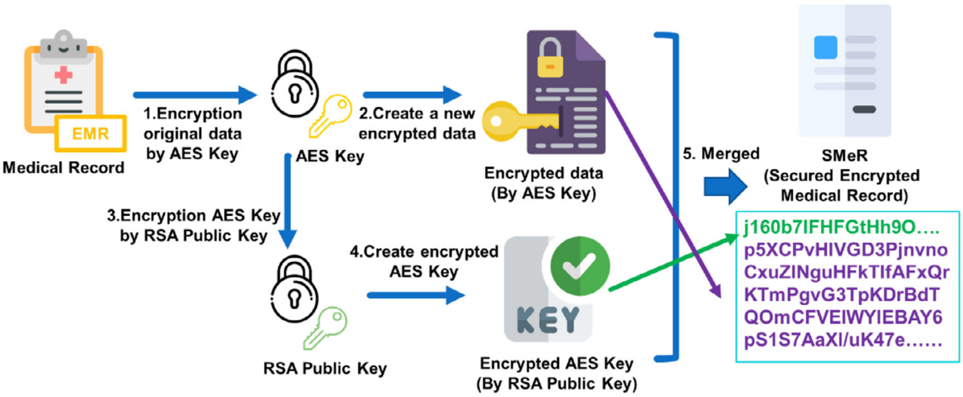

EMR
Medical Record
1.Encryption original data by AES Key
AES Key
2.Create a new encrypted data
Encrypted data (By AES Key)
3.Encryption AES Key by RSA Public Key
RSA Public Key
4.Create encrypted AES Key
KEY
Encrypted AES Key (By RSA Public Key)
5. Merged
SMeR (Secured Encrypted Medical Record)
j160b7IFHFGtHh9O….
p5XCPvHIVGD3Pjnvno
CxuZINguHFkTIfAFxQr
KTmPgvG3TpKDrBdT
QOmCFVEIWYIEBAY6
pS1S7AaXI/uK47e……

Fig. 2. CEDA - Original EMR Encryption Process.

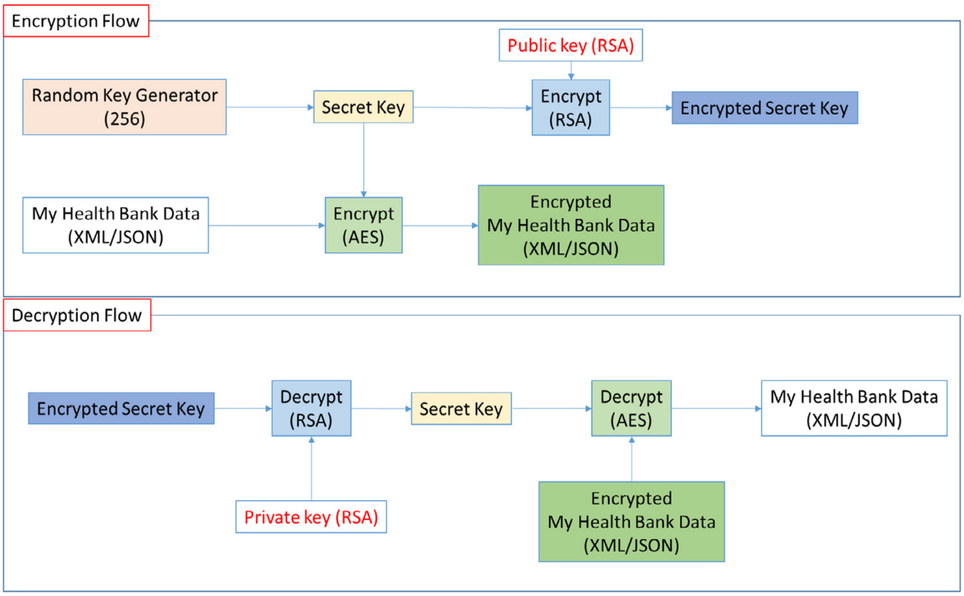


Fig. 3. The encryption process and decryption process of CEDA.

1 MixColumns

Linear mixing operation, operates on the columns of states, and combines the four bytes in each column.

1 AddRoundKey

Step 4. Final round (making 10 rounds in total):

1 SubBytes
2 ShiftRows
3 AddRoundKey

In this study, the 128-bit key size is used to encrypt the original medical record. Then, the AES key is encrypted by the authorized person RSA public key. RSA creates a public key based on two large prime numbers and an auxiliary value. While anyone can encrypt a message with a public key, prime numbers are kept secret, thus, only those who know the prime number can decode the message. The security of RSA depends on the actual difficulty of decomposing the product of two large prime numbers, that is, the "decomposition problem". If a key with enough bits is used, there is no public method to invalidate the system; however, as RSA is a relatively slow algorithm, it is not usually used to directly encrypt user data. This study used RSA to transmit the shared key of symmetric key cryptography.

RSA for Generation of public key and private key

When an authorized person wants to receive an EMR from the EMR owner through our architecture, CEDA will generate a public key and a private key in the following manner to encrypt the AES key:

1 Choose two larges prime numbers p and q, where p is not equal to q, and calculate $N = pq$.
2 According to Euler's function, the number of integers not greater than N and relatively prime to N is (p −1) (q −1)
3 Choose an integer e that is relatively prime to (p −1) *(q −1), and e is less than (p −1) *(q −1)
4 Calculate d with the following formula: d*e ≡ 1 (mod (p −1) (q −1))
5 Then, the p and q records are destroyed.

(N,e) is the public key; (N,d) is the private key; (N,d) is secret. An authorized person passes the public key (N, e) to the EMR owner, and hides the private key (N, d).

Encrypted EMR

When the EMR owner wants to share an EMR m with an authorized person, the EMR owner knows the N and e values generated by the authorized person. Then, the EMR owner uses the format, as agreed with the authorized person, to convert the AES key of the encrypted EMR m into an integer n less than N; for example, the EMR owner can convert each word into the Unicode code of the word, and then, concatenate these numbers together to form a number. If this message is very long, the EMR owner can divide the message into several paragraphs, and then, convert each paragraph to n. Thus, n can be encrypted into c with the following formula:

$$n^e \equiv c(mod\ N)$$

Calculating c is not complicated; after the EMR owner calculates c, the EMR owner can pass it to the authorized person.

Decrypted EMR

After the authorized person receives the EMR owner's message c, they can use the d key to decode the message. The authorized person can use the following formula to convert c to n:

$$c^d \equiv n(mod\ N)$$

After receiving n, the authorized person can restore the original information through m.

The principle of decoding is

$$c^d \equiv n^{e-d}(mod\ N)$$

where ed ≡ 1 (mod p −1) and ed ≡ 1 (mod q −1), and can be proved by Fermat's theorem (because p and q are prime numbers)

$$c^{e-d} \equiv n(mod\ p) \text{ with } c^{e-d} \equiv n(mod\ q)$$

This shows (because p and q are different prime numbers, p and q are relatively prime)

$$n^{e-d} \equiv n(mod\ pq)$$

3.2. SMeR (Secured encrypted medical record)

SMeR content mainly includes 1. encrypted AES key, which is encrypted by the RSA public key, and 2. the encrypted medical record, which is encrypted by the AES key. The entire document will be stored in DERy, and indexed and verified by the blockchain structure.

3.3. DERy (Decentralize emr repository)

The Hash function, which uses SHA256, is applied in DERy to generate the Hash value of SMeR, and can be used to map data with arbitrary size into 256-bit values. Then, integrate the index of SMeR in DERy, the Hash of SMeR, and Authority status, and the integrated data will be signed by the data owner with the private key of the block. This signature is intended to prove that the content of the block data is authorized by the data owner for data transmission. Finally, DERy stores the hash value, the SMeR index, the authorization status, and the signature value in the content of the block. The blockchain architecture uses the verification structure of the blockchain to confirm whether the block is authorized by the data owner. After verification, the block is created and synchronized to each node of the blockchain to complete the data encryption process. The process of block creation encryption is shown in Fig. 4.

3.4. Blockchain architecture

The blockchain architecture was developed using the open source foundation of Ethereum to establish a private chain. There are three common consensus mechanisms in the blockchain system, including Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA).

PoW is the consensus mechanism originally used in the blockchain system [18–20]. The reason why it is called proof of work is that miners must spend computer resources (time, power, and computing power) to establish a new block, which must be completed by solving complex calculation problems. In order to stabilize the time and security required for blockchain establishment, the difficulty of block establishment will increase over time.

The PoS method is to solve the problem of excessive energy consumption by PoW [19]. The PoS consensus mechanism is designed according to the concept of equity, meaning the person with the highest equity has the power to verify (establish) the block and use their own currency as collateral; if it is found that the block creation is fake, all the currency of the person who created the block will be confiscated. However, this equity is calculated based on the amount of currency of the user and the number of days of ownership. After each successful verification of a block, the equity is reset to zero and recalculated, and rewards based on equity will be given. This mechanism is intended to allow nodes with a large amount of currency to jointly maintain the security of the blockchain, and reduce the time and resource consumption of

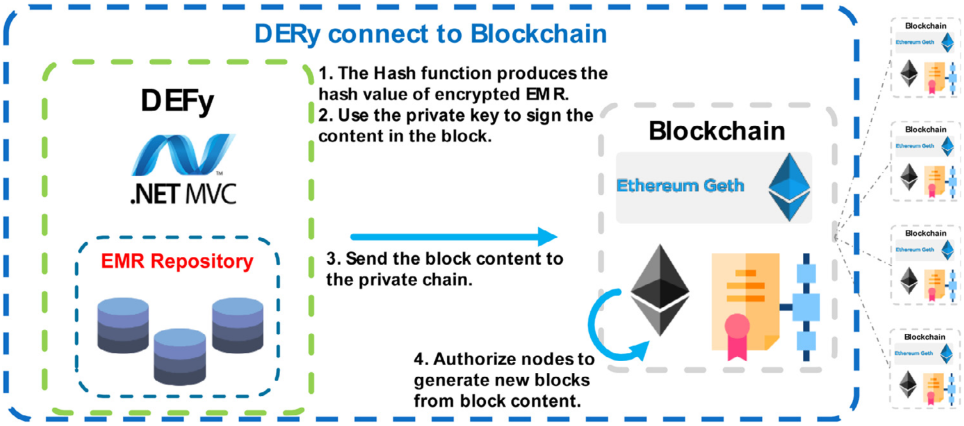

DERy connect to Blockchain
DEFy
.NET MVC
EMR Repository
1. The Hash function produces the hash value of encrypted EMR.
2. Use the private key to sign the content in the block.
3. Send the block content to the private chain.
4. Authorize nodes to generate new blocks from block content.
Blockchain
Ethereum Geth
Blockchain
Ethereum Geth
Blockchain
Ethereum Geth
Blockchain
Ethereum Geth
Blockchain
Ethereum Geth

Fig. 4. Block creation encryption process.

Table 1.
Evaluation of the different consensus mechanism.

Consensus Mechanism	Transaction speed	Resource consumption	Blockchain stability	Data privacy
PoW	Slow	High	High	Low
PoS	Normal	Normal	Normal	Normal
PoA	Fast	Low	Normal	High

building blocks. However, this consensus mechanism makes nodes with more currencies have higher probability and currency. Compared with fewer nodes, building blocks is more difficult, which is also a limitation of PoS.

PoA was proposed by Ethereum co-founder Gacin Wood in 2017. The purpose of this consensus algorithm is to establish an authorized node for the person who built the block (block verifier), and is a centralized consensus mechanism compared to PoS. PoA is collateralized by reputation to build the block. All blocks will be built by the selected authorized nodes, which reduces the amount of time required to build blocks and addresses data consistency issues. PoA is more commonly used in private blockchains, which are used in different fields, including insurance, banks, and logistics companies. PoA processes a large amount of transaction data faster than PoS and PoA. Table 1

This research considers the user’s EMR privacy and the need to process a large number of medical records, thus, the blockchain adopts a private chain architecture and uses PoA (fast transaction speed and high privacy) as the consensus mechanism on the blockchain.

PoA ensures that the nodes that authenticate blocks are authorized nodes. In addition, as the speed of PoA building blocks is higher than other consensus mechanisms, it can effectively improve the speed of data reading and exchange when applied to medical information exchange.

When the authorized person reads the EMR, the system will look for the block that belongs to the record in the blockchain, and send the block content to DERy to verify whether the data is correct. The first step is to obtain the index of the SMeR in the depository.

The second step is to identify the SMeR and generate the Hash value of the SMeR content through the Hash function. The third step is to determine whether the Hash value of the SMeR in the block is consistent, thus, when the Hash value generated by the HASH function is the same, DERy can verify that the data content is correct.

After the above process, the authorized person can read the SMeR content through DERy, unlock the first part of the SMeR data with their RSA private key, and then, obtain the AES key. The AES key is used to decrypt the second part of the EMR, in order to obtain the complete medical record. The process of an authorized person obtaining the EMR is shown in Fig. 5.

The consensus structure of the blockchain is used to verify the correctness of the content, including "block number", "Pre-Hash", "Hash", "Time", "EMR Owner", "Authority person", "Data index", "Hash of SMeR", "Authority status", "Signature", and “Payment”, and the detailed descriptions are shown in Fig. 6. The two information "the hash of SMeR" and "Signature" are used to prove that the authorized person is qualified to access the medical record and that the content of the medical record has not been tampered with.

4. Results

4.1. The process of SEMRES

This research completes the SEMRES system to achieve the verifiability and security protection of the EMR, while the triple encryption mechanism ensures privacy, meaning the correctness and safety of the EMR. During the CEDA implementation, the ASP.NET function AES, RSACryptoServiceProvider, SHA256CryptoServiceProvider are used for system development.

"My Health Bank (MHB)" as launched by the Ministry of Health and Welfare, Taiwan. MHB is an online health information query system, which provides Taiwan citizen that can conveniently query personal health information anytime and anywhere. It can also provide physicians for reference when seeking medical treatment, helping physicians quickly grasp personal health conditions, and improve the safety and quality of medical care. The data in MHB including "Western, Chinese, and dental clinics, medication data, laboratory data, imaging or pathological examination data", Hospitalization and surgery information", "Allergy Information", "Summary of discharged medical records", "Donation or peace to ease medical willingness", "Adult preventive health care results", and "Vaccination information". MHB is used to demonstrate the EMR exchange in this study. The MHB file is shown in Fig. 7.

In the CEDA module, EMR is encrypted through the AES and RSA mechanisms. The AES key is automatically generated by CEDA based on the timestamp. An example of an AES key is shown in

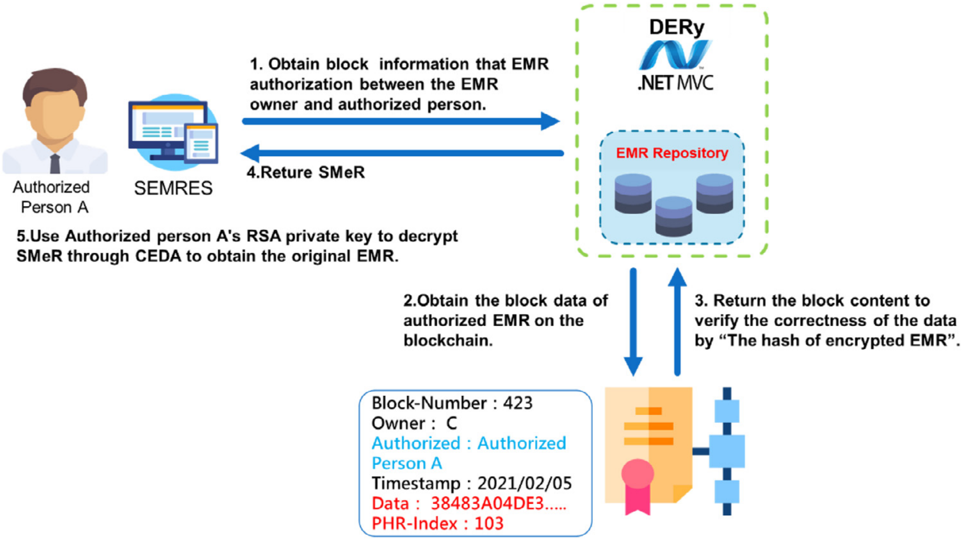
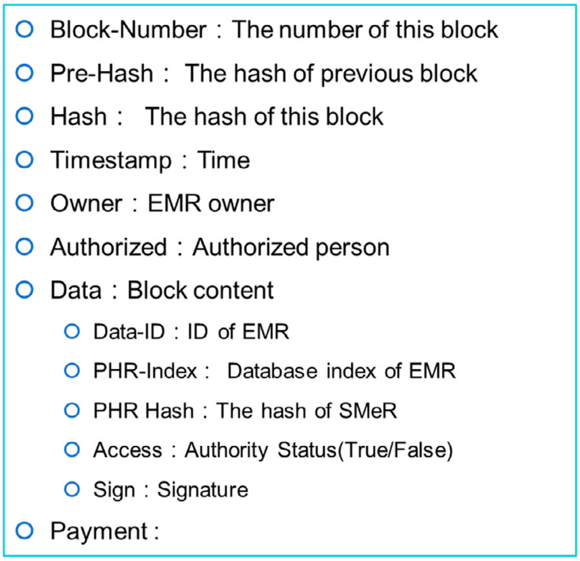
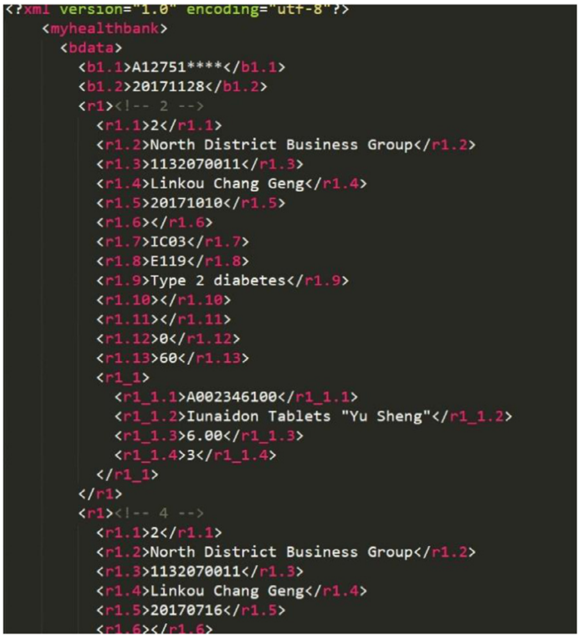

Authorized Person A
SEMRES
1. Obtain block information that EMR authorization between the EMR owner and authorized person.
4.Reture SMeR
5.Use Authorized person A's RSA private key to decrypt SMeR through CEDA to obtain the original EMR.
DERy
.NET MVC
EMR Repository
2.Obtain the block data of authorized EMR on the blockchain.
3. Return the block content to verify the correctness of the data by "The hash of encrypted EMR".
Block-Number : 423
Owner : C
Authorized : Authorized Person A
Timestamp : 2021/02/05
Data : 38483A04DE3.....
PHR-Index : 103

Fig. 5. The process of authorized person obtaining the EMR.



- ○ Block-Number : The number of this block
- ○ Pre-Hash : The hash of previous block
- ○ Hash : The hash of this block
- ○ Timestamp : Time
- ○ Owner : EMR owner
- ○ Authorized : Authorized person
- ○ Data : Block content
    - ○ Data-ID : ID of EMR
    - ○ PHR-Index : Database index of EMR
    - ○ PHR Hash : The hash of SMeR
    - ○ Access : Authority Status(True/False)
    - ○ Sign : Signature
- ○ Payment :

Fig. 6. Block content in SEMRES.



```
<?xml version="1.0" encoding="utf-8"?>
    <myhealthbank>
      <bdata>
        <b1.1>A12751****</b1.1>
        <b1.2>20171128</b1.2>
        <r1><!-- 2 -->
          <r1.1>2</r1.1>
          <r1.2>North District Business Group</r1.2>
          <r1.3>1132070011</r1.3>
          <r1.4>Linkou Chang Geng</r1.4>
          <r1.5>20171010</r1.5>
          <r1.6></r1.6>
          <r1.7>IC03</r1.7>
          <r1.8>E119</r1.8>
          <r1.9>Type 2 diabetes</r1.9>
          <r1.10></r1.10>
          <r1.11></r1.11>
          <r1.12>0</r1.12>
          <r1.13>60</r1.13>
          <r1_1>
            <r1_1.1>A002346100</r1_1.1>
            <r1_1.2>Iunaidon Tablets "Yu Sheng"</r1_1.2>
            <r1_1.3>6.00</r1_1.3>
            <r1_1.4>3</r1_1.4>
          </r1_1>
        </r1>
        <r1><!-- 4 -->
          <r1.1>2</r1.1>
          <r1.2>North District Business Group</r1.2>
          <r1.3>1132070011</r1.3>
          <r1.4>Linkou Chang Geng</r1.4>
          <r1.5>20170716</r1.5>
          <r1.6></r1.6>
```

Fig. 7. The MHB file.

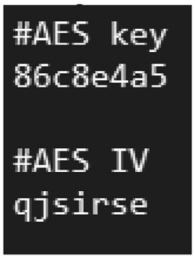
Fig. 8. The timestamp and IV (initialization vector) parameter are used to avoid generating the same AES key.

The original medical records are converted into encrypted data after being encrypted by the AES key. An encrypted EMR example is shown in Fig. 9.

CEDA will also generate the RSA public key and private key of the authorized person. The RSA public key is announced on the platform, and is used by CEDA to encrypt the AES key used to encrypt the original EMR. Examples of RSA public and private keys are shown in Fig. 10. The RSA private key includes the public key, DP (d mod p – 1), DQ (d mod q – 1), and Inverse Q (q– 1 mod p).

After EMR encryption, the AES key is encrypted by the RSA public key, which creates new encrypted data. The encrypted AES key is shown in Fig. 11.

SMeR is created after the encryption process. The SMeR content includes the encrypted AES key, which is encrypted by the RSA public key, and the encrypted medical record, which is encrypted by the AES key. The SMeR example is shown in Fig. 12.

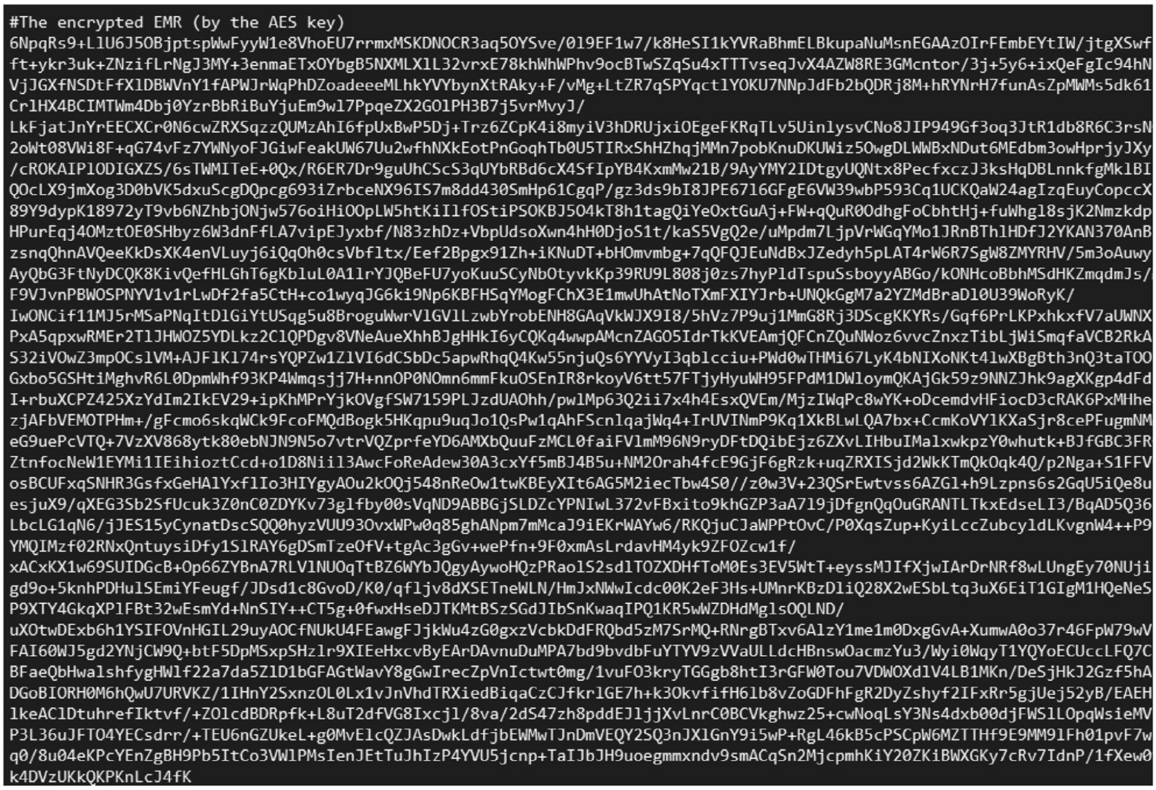


```
#AES key
86c8e4a5

#AES IV
qjsirse
```

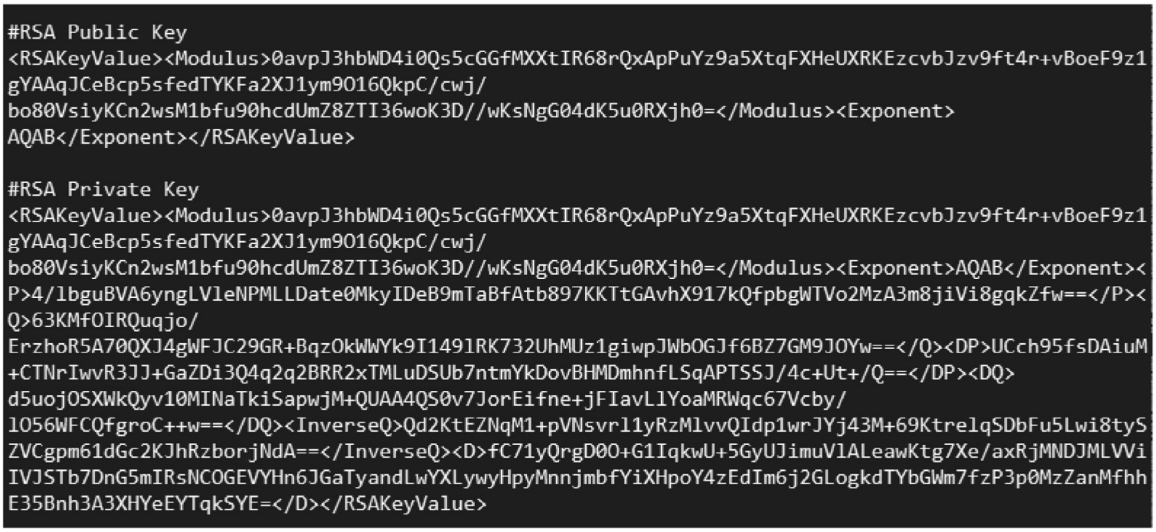
Fig. 8. Example of AES key.

Finally, the SMeR will be transferred to DEFy for storage and hash calculation through SHA-256, and then, stored in the open ledger of the blockchain. The block content is shown in Fig. 13.



```
#The encrypted EMR (by the AES key)
6NpqRs9+LlU6J5OBjptspWwFyyW1e8VhoEU7rrmxMSKDNOCR3aq5OYSve/0l9EF1w7/k8HeSI1kYVRaBhmELBkupaNuMsnEGAAzOIrFEmbEYtIW/jtgXSwf
ft+ykr3uk+ZNzifLrNgJ3MY+3enmaETxOYbgB5NXMLX1L32vrxE78khWhWPhv9ocBTwSZqSu4xTTTvseqJvX4AZW8RE3GMcntor/3j+5y6+ixQeFgIc94hN
VjJGXfNSDtFfX1DBWVnY1fAPWJrWqPhDZoadeeeMLhkYVYbynXtRAky+F/vMg+LtZR7qSPYqctlYOKU7NNpJdFb2bQDRj8M+hRYNrH7funAsZpMWMs5dk61
CrlHX4BCIMTWm4Dbj0YzrBbRiBuYjuEm9wl7PpqeZX2GOlPH3B7j5vrMvyJ/
LkFjatJnYrEECXCr0N6cwZRXSqzzQUMzAhI6fpUxBwP5Dj+Trz6ZCpK4i8myiV3hDRUjxiOEgeFKRqTLv5UinlysvCNo8JIP949Gf3oq3JtR1db8R6C3rsN
2oWt08VWi8F+qG74vFz7YWNyoFJGiwFeakUW67Uu2wfhNXkEotPnGoqhTb0U5TIRxShHZhqjMMn7pobKnuDKUWiz5OwgDLWWBxNDut6MEdbm3owHprjyJXy
/cROKAIPlODIGXZS/6sTWMITeE+0Qx/R6ER7Dr9guUhCScS3qUYbRBd6cX4SfIpYB4KxmMw21B/9AyYMY2IDtgyUQNtx8PecfxczJ3ksHqDBLnnkfgMklBI
QOcLX9jmXog3D0bVK5dxuScgDQpcg693iZrbceNX96IS7m8dd430SmHp61CgqP/gz3ds9bI8JPE67l6GFgE6VW39wbP593Cq1UCKQaW24agIzqEuyCopccX
89Y9dypK18972yT9vb6NZhbjONjw576oiHiOOpLW5htKiIlfOStiPSOKBJ5O4kT8h1tagQiYeOxtGuAj+FW+qQuR0OdhgFoCbhtHj+fuWhgl8sjK2Nmzkdp
HPurEqj4OMztOE0SHbyz6W3dnFfLA7vipEJyxbf/N83zhDz+VbpUdsoXwn4hH0DjoS1t/kaS5VgQ2e/uMpdm7LjpVrWGqYMo1JRnBThlHDfJ2YKAN370AnB
zsnqQhnAVQeeKkDsXK4enVLuyj6iQqOh0csVbfltx/Eef2Bpgx91Zh+iKNuDT+bHOmvmbg+7qQFQJEuNdBxJZedyh5pLAT4rW6R7SgW8ZMYRHV/5m3oAuwy
AyQbG3FtNyDCQK8KivQefHLGhT6gKbluL0A1lrYJQBeFU7yoKuuSCyNbOtyvkKp39RU9L808j0zs7hyPldTspuSsboyyABGo/kONHcoBbhMSdHKZmqdmJs/
F9VJvnPBWOSPNYV1v1rLwDf2fa5CtH+co1wyqJG6ki9Np6KBFHSqYMogFChX3E1mwUhAtNoTXmFXIYJrb+UNQkGgM7a2YZMdBraDl0U39WoRyK/
IwONCif11MJ5rMSaPNqItDlGiYtUSqg5u8BroguWwrVlGVlLzwbYrobENH8GAqVkWJX9I8/5hVz7P9uj1MmG8Rj3DScgKKYRs/Gqf6PrLKPxhkxfV7aUWNX
PxA5qpxwRMEr2TlJHWOZ5YDLkz2ClQPDgv8VNeAueXhhBJgHHkI6yCQKq4wwpAMcnZAGO5IdrTkKVEAmjQFCnZQuNWoz6vvcZnxzTibLjWiSmqfaVCB2RkA
S32iVOwZ3mpOCslVM+AJFlKl74rsYQPZw1ZlVI6dCSbDc5apwRhqQ4Kw55njuQs6YYVyI3qblcciu+PWd0wTHMi67LyK4bNIXoNKt4lwXBgBth3nQ3taTOO
Gxbo5GSHtiMghvR6L0DpmWhf93KP4Wmqsjj7H+nnOP0NOmn6mmFkuOSEnIR8rkoyV6tt57FTjyHyuWH95FPdM1DWloymQKAjGk59z9NNZJhk9agXKgp4dFd
I+rbuXCPZ425XzYdIm2IkEV29+ipKhMPrYjkOVgfSW7159PLJzdUAOhh/pwlMp63Q2ii7x4h4EsxQVEm/MjzIWqPc8wYK+oDcemdvHFiocD3cRAK6PxMHhe
zjAFbVEMOTPHm+/gFcmo6skqWCk9FcoFMQdBogk5HKqpu9uqJo1QsPw1qAhFScnlqajWq4+IrUVINmP9Kq1XkBLwLQA7bx+CcmKoVYlKXaSjr8cePFugmNM
eG9uePcVTQ+7VzXV868ytk80ebNJN9N5o7vtrVQZprfeYD6AMXbQuuFzMCL0faiFVlmM96N9ryDFtDQibEjz6ZXvLIHbuIMalxwkpzY0whutk+BJfGBC3FR
ZtnfocNeW1EYMi1IEihioztCcd+o1D8Niil3AwcFoReAdew30A3cxYf5mBJ4B5u+NM2Orah4fcE9GjF6gRzk+uqZRXISjd2WkKTmQkOqk4Q/p2Nga+S1FFV
osBCUFxqSNHR3GsfxGeHAlYxflIo3HIYgyAOu2kOQj548nReOw1twKBEyXIt6AG5M2iecTbw4S0//z0w3V+23QSrEwtvss6AZGl+h9Lzpns6s2GqU5iQe8u
esjuX9/qXEG3Sb2SfUcuk3Z0nC0ZDYKv73glfby00sVqND9ABBGjSLDZcYPNIwL372vFBxito9khGZP3aA7l9jDfgnQqOuGRANTLTkxEdseLI3/BqAD5Q36
LbcLG1qN6/jJES15yCynatDscSQQ0hyzVUU93OvxWPw0q85ghANpm7mMcaJ9iEKrWAYw6/RKQjuCJaWPPtOvC/P0XqsZup+KyiLccZubcyldLKvgnW4++P9
YMQIMzf02RNxQntuysiDfy1SlRAY6gDSmTzeOfV+tgAc3gGv+wePfn+9F0xmAsLrdavHM4yk9ZFOZcw1f/
xACxKX1w69SUIDGcB+Op66ZYBnA7RLV1NUOqTtBZ6WYbJQgyAywoHQzPRaolS2sdlTOZXDHfToM0Es3EV5WtT+eyssMJIfXjwIArDrNRf8wLUngEy70NUji
gd9o+5knhPDHulSEmiYFeugf/JDsd1c8GvoD/K0/qfljv8dXSETneWLN/HmJxNWwIcdc00K2eF3Hs+UMnrKBzDliQ28X2wESbLtq3uX6EiT1GIgM1HQeNeS
P9XTY4GkqXPlFBt32wEsmYd+NnSIY++CT5g+0fwxHseDJTKMtBSzSGdJIbSnKwaqIPQ1KR5wWZDHdMglsOQLND/
uXOtwDExb6h1YSIFOVnHGIL29uyAOCfNUkU4FEawgFJjkWu4zG0gxzVcbkDdFRQbd5zM7SrMQ+RNrgBTxv6AlzY1me1m0DxgGvA+XumwA0o37r46FpW79wV
FAI60WJ5gd2YNjCW9Q+btF5DpMSxpSHzlr9XIEeHxcvByEArDAvnuDuMPA7bd9bvdbFuYTYV9zVVaULLdcHBnswOacmzYu3/Wyi0WqyT1YQYoECUccLFQ7C
BFaeQbHwalshfygHWlf22a7da5ZlD1bGFAGtWavY8gGwIrecZpVnIctwt0mg/1vuFO3kryTGGgb8htI3rGFW0Tou7VDWOXdlV4LB1MKn/DeSjHkJ2Gzf5hA
DGoBIORH0M6hQwU7URVKZ/1IHnY2SxnzOL0Lx1vJnVhdTRXiedBiqaCzCJfkrlGE7h+k3OkvfifH6lb8vZoGDFhFgR2DyZshyf2IFxRr5gjUej52yB/EAEH
lkeACl DtuhrefIktvf/+ZOlcdBDRpfk+L8uT2dfVG8Ixcjl/8va/2dS47zh8pddEJljjXvLnrC0BCVkghwz25+cwNoqLsY3Ns4dxb00djFWSlLOpqWsieMV
P3L36uJFTO4YECsdrr/+TEU6nGZUkeL+g0MvElcQZJAsDwkLdfjbEWMwTJnDmVEQY2SQ3nJXlGnY9i5wP+RgL46kB5cPSCpW6MZTTHf9E9MM9lFh01pvF7w
q0/8u04eKPcYEnZgBH9Pb5ItCo3VWlPMsIenJEtTuJhIzP4YVU5jcnp+TaIJbJH9uoegmmxndv9smACqSn2MjcpmhKiY20ZKiBWXGKy7cRv7IdnP/1fXew0
k4DVzUKkQKPKnLcJ4fK
```

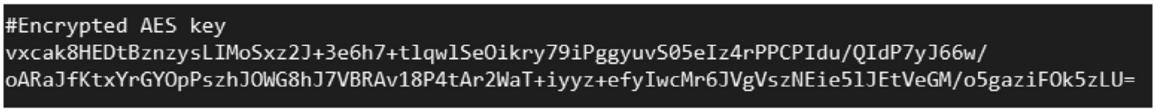
Fig. 9. The encrypted EMR example.



```
#RSA Public Key
<RSAKeyValue><Modulus>0avpJ3hbWD4i0Qs5cGGfMXXtIR68rQxApPuYz9a5XtqFXHeUXRKEzcvbJzv9ft4r+vBoeF9z1
gYAAqJCeBcp5sfedTYKFa2XJ1ym9O16QkpC/cwj/
bo80VsiyKCn2wsM1bfu90hcdUmZ8ZTI36woK3D//wKsNgG04dK5u0RXjh0=</Modulus><Exponent>
AQAB</Exponent></RSAKeyValue>

#RSA Private Key
<RSAKeyValue><Modulus>0avpJ3hbWD4i0Qs5cGGfMXXtIR68rQxApPuYz9a5XtqFXHeUXRKEzcvbJzv9ft4r+vBoeF9z1
gYAAqJCeBcp5sfedTYKFa2XJ1ym9O16QkpC/cwj/
bo80VsiyKCn2wsM1bfu90hcdUmZ8ZTI36woK3D//wKsNgG04dK5u0RXjh0=</Modulus><Exponent>AQAB</Exponent><
P>4/lbguBVA6yngLVleNPMLLDate0MkyIDeB9mTaBfAtb897KKTtGAvhX917kQfpbgWTVo2MzA3m8jiVi8gqkZfw==</P><
Q>63KMfOIRQuqjo/
ErzhoR5A70QXJ4gWFJC29GR+BqzOkWWYk9I149lRK732UhMUz1giwpJWbOGJf6BZ7GM9JOYw==</Q><DP>UCch95fsDAiuM
+CTNrIwvR3JJ+GaZDi3Q4q2q2BRR2xTMLuDSUb7ntmYkDovBHMDmhnfLSqAPTSSJ/4c+Ut+/Q==</DP><DQ>
d5uojOSXWkQyv10MINaTkiSapwjM+QUAA4QS0v7JorEifne+jFIavLlYoaMRWqc67Vcby/
lO56WFCQfgroC++w==</DQ><InverseQ>Qd2KtEZNqM1+pVNsvrl1yRzMlvvQIdp1wrJYj43M+69KtrelqSDbFu5Lwi8tyS
ZVCgpm61dGc2KJhRzborjNdA==</InverseQ><D>fC71yQrgD0O+G1IqkwU+5GyUJimuVlALeawKtg7Xe/axRjMNDJMLVVi
IVJSTb7DnG5mIRsNCOGEVYHn6JGaTyandLwYXLywyHpyMnnjmbfYiXHpoY4zEdIm6j2GLogkdTYbGWm7fzP3p0MzZanMfhh
E35Bnh3A3XHYeEYTqkSYE=</D></RSAKeyValue>
```

Fig. 10. The example of RSA private key.

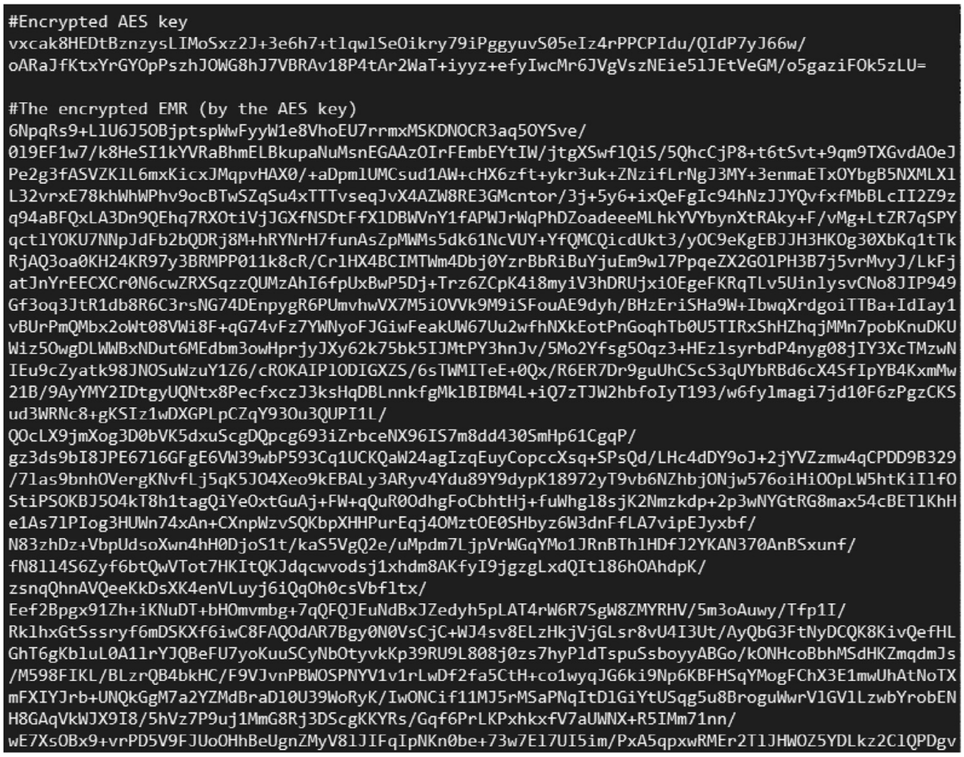


```
#Encrypted AES key
vxcak8HEDtBznzysLIMoSxz2J+3e6h7+tlqwlSeOikry79iPggyuvS05eIz4rPPCPIdu/QIdP7yJ66w/
oARaJfKtxYrGYOpPszhJOWG8hJ7VBRAv18P4tAr2WaT+iyyz+efyIwcMr6JVgVszNEie5lJEtVeGM/o5gaziFOk5zLU=
```

Fig. 11. The encrypted AES key.

4.2. The verification and security of SEMRES

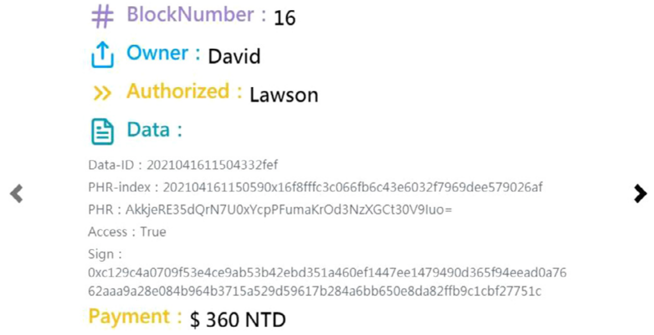
In the data verification process, when the authorized person wants to read the encrypted medical record, DERy will first enter the blockchain to search the block ledger. After the authorization of the authorized person to view the data is verified, it will locate the SMeR through the block information: meaning the index of SMeR and the hash of SMeR. After obtaining SMeR, the data is calculated again through the SHA-256 hash function to confirm that the hash value of the SMeR is the same as the authenticated data in the block before decryption. The decryption process is shown in Fig. 14. CEDA will obtain the RSA private key of the authorized



```
#Encrypted AES key
vxcak8HEDtBznzysLIMoSxz2J+3e6h7+tlqwlSeOikry79iPggyuvS05eIz4rPPCPIdu/QIdP7yJ66w/
oARaJfKtxYrGYOpPszhJOWG8hJ7VBRAv18P4tAr2WaT+iyyz+efyIwcMr6JVgVszNEie5lJEtVeGM/o5gaziFOk5zLU=

#The encrypted EMR (by the AES key)
6NpqRs9+L1U6J5OBjptspWwFyyW1e8VhoEU7rrmxMSKDNOCR3aq5OYSve/
0l9EF1w7/k8HeSI1kYVRaBhmELBkupaNuMsnEGAAzOIrFEmbEYtIW/jtgXSwflQiS/5QhcCjP8+t6tSvt+9qm9TXGvdAOeJ
Pe2g3fASVZKlL6mxKicxJMqpvHAX0/+aDpmlUMCsud1AW+cHX6zft+ykr3uk+ZNzifLrNgJ3MY+3enmaETxOYbgB5NXMLXl
L32vrxE78khWhWPhv9ocBTwSZqSu4xTTTvseqJvX4AZW8RE3GMcntor/3j+5y6+ixQeFgIc94hNzJJYQvfxfMbBLcII2Z9z
q94aBFQxLA3Dn9QEhq7RXOtiVjJGXfNSDtFfX1DBWVnY1fAPWJrWqPhDZoadeeeMLhkYVYbynXtRAky+F/vMg+LtZR7qSPY
qctlYOKU7NNpJdFb2bQDRj8M+hRYNrH7funAsZpMWMs5dk61NcVUY+YfQMCQicdUkt3/yOC9eKgEBJJH3HKOg30XbKq1tTk
RjAQ3oa0KH24KR97y3BRMPP011k8cR/CrlHX4BCIMTWm4Dbj0YzrBbRiBuYjuEm9wl7PpqeZX2GOlPH3B7j5vrMvyJ/LkFj
atJnYrEECXCr0N6cwZRXSqzzQUMzAhI6fpUxBwP5Dj+Trz6ZCpK4i8myiV3hDRUjxiOEgeFKRqTLv5UinlysvCNo8JIP949
Gf3oq3JtR1db8R6C3rsNG74DEnpygR6PUmvhwVX7M5iOVVk9M9iSFouAE9dyh/BHzEriSHa9W+IbwqXrdgoiTTBa+IdIay1
vBUrPmQMbx2oWt08VWi8F+qG74vFz7YWNyoFJGiwFeakUW67Uu2wfhNXkEotPnGoqhTb0U5TIRxShHZhqjMMn7pobKnuDKU
Wiz5OwgDLWWBxNDut6MEdbm3owHprjyJXy62k75bk5IJMtPY3hnJv/5Mo2Yfsg5Oqz3+HEzlsyrbdP4nyg08jIY3XcTMzwN
IEu9cZyatk98JNOSuWzuY1Z6/cROKAIPlODIGXZS/6sTWMITeE+0Qx/R6ER7Dr9guUhCScS3qUYbRBd6cX4SfIpYB4KxmMw
21B/9AyYMY2IDtgyUQNtx8PecfxczJ3ksHqDBLnnkfgMklBIBM4L+iQ7zTJW2hbfoIyT193/w6fylmagi7jd10F6zPgzCKS
ud3WRNc8+gKSIz1wDXGPLpCZqY93Ou3QUPI1L/
QOcLX9jmXog3D0bVK5dxuScgDQpcg693iZrbceNX96IS7m8dd430SmHp61CgqP/
gz3ds9bI8JPE67l6GFgE6VW39wbP593Cq1UCKQaW24agIzqEuyCopccXsq+SPsQd/LHc4dDY9oJ+2jYVZzmw4qCPDD9B329
/7las9bnhOVergKNvfLj5qK5JO4Xeo9kEBALy3ARyv4Ydu89Y9dypK18972yT9vb6NZhbjONjw576oiHiOOpLW5htKiIlfO
StiPSOKBJ5O4kT8h1tagQiYeOxtGuAj+FW+qQuR0OdhgFoCbhtHj+fuWhgl8sjK2Nmzkdp+2p3wNYGtRG8max54cBETlKhH
e1As7lPIog3HUWn74xAn+CXnpWzvSQKbpXHHPurEqj4OMztOE0SHbyz6W3dnFfLA7vipEJyxbf/
N83zhDz+VbpUdsoXwn4hH0DjoS1t/kaS5VgQ2e/uMpdm7LjpVrWGqYMo1JRnBThlHDfJ2YKAN370AnBSxunf/
fN8ll4S6Zyf6btQwVTot7HKItQKJdqcwvodsj1xhdm8AKfyI9jgzgLxdQItl86hOAhdpK/
zsnqQhnAVQeeKkDsXK4enVLuyj6iQqOh0csVbfltx/
Eef2Bpgx91Zh+iKNuDT+bHOmvmbg+7qQFQJEuNdBxJZedyh5pLAT4rW6R7SgW8ZMYRHV/5m3oAuwy/Tfp1I/
RklhxGtSssryf6mDSKXf6iwC8FAQOdAR7Bgy0N0VsCjC+WJ4sv8ELzHkjVjGLsr8vU4I3Ut/AyQbG3FtNyDCQK8KivQefHL
GhT6gKbluL0A1lrYJQBeFU7yoKuuSCyNbOtyvkKp39RU9L808j0zs7hyPldTspuSsboyyABGo/kONHcoBbhMSdHKZmqdmJs
/M598FIKL/BLzrQB4bkHC/F9VJvnPBWOSPNYV1v1rLwDf2fa5CtH+co1wyqJG6ki9Np6KBFHSqYMogFChX3E1mwUhAtNoTX
mFXIYJrb+UNQkGgM7a2YZMdBraDl0U39WoRyK/IwONCif11MJ5rMSaPNqItDlGiYtUSqg5u8BroguWwrVlGVlLzwbYrobEN
H8GAqVkWJX9I8/5hVz7P9uj1MmG8Rj3DScgKKYRs/Gqf6PrLKPxhkxfV7aUWNX+R5IMm71nn/
wE7XsOBx9+vrPD5V9FJUoOHhBeUgnZMyV8lJIFqIpNKn0be+73w7El7UI5im/PxA5qpxwRMEr2TlJHWOZ5YDLkz2ClQPDgv
```

Fig. 12. The example of SMeR.



BlockNumber : 16

Owner : David

Authorized : Lawson

Data :

Data-ID : 2021041611504332fef

PHR-index : 202104161150590x16f8fffc3c066fb6c43e6032f7969dee579026af

PHR : AkkjeRE35dQrN7U0xYcpPFumaKrOd3NzXGCt30V9Iuo=

Access : True

Sign :
0xc129c4a0709f53e4ce9ab53b42ebd351a460ef1447ee1479490d365f94eead0a76
62aaa9a28e084b964b3715a529d59617b284a6bb650e8da82ffb9c1cbf27751c

Payment : $ 360 NTD

Fig. 13. The example of block content.

person, and use the private key to decrypt the AES key, then, the medical record is decrypted through the AES key.

The authorized person can obtain the medical records, and these contents have been verified and have not been tampered with. The decrypted medical records are shown in Fig. 15. Information on the name of the medical institution, payment, medical order, and medication order is included in the EMR.

In this study, the original medical records were encrypted using AES, and the AES key was encrypted using RSA. The encrypted information is also hashed and stored in the blockchain. According to the characteristics of AES, the longer the key length, the more difficult it is to crack. At present, only the brute force method may be able to unlock the AES key, but taking the AES-128 algorithm as an example, on average, you need to try 2^127 ≈ 1.7 × 10^38 128bit random numbers as the key for encryption and decryption operations to find the correct key.

If the operation efficiency of AES is 2.564410^19 ≈ 2^64.4753 times/*sec*, the time required for 2^127 AES operations is: 2^127 / 2^64.4753 ≈ 2^62.5247 s ≈ 6.6345 10^18 s ≈ 1.8429 10^15 h ≈ 7.6789 10^13 days ≈ 2.104 * 10^11 years ≈ 210,400,000,000 years. The basic application of RSA is based on

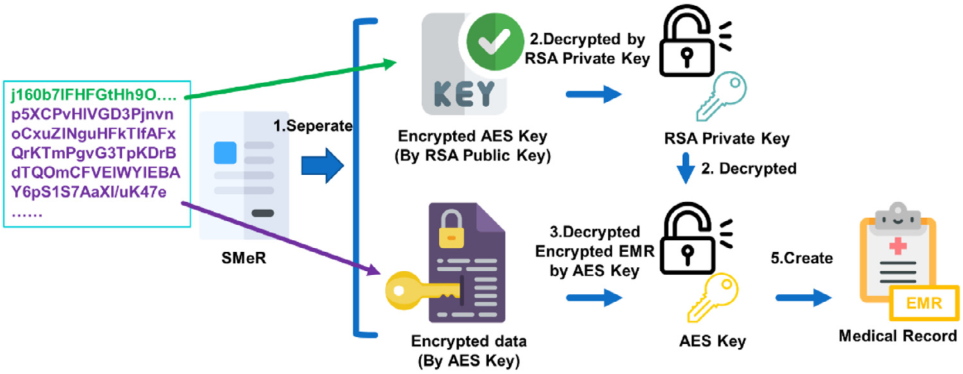
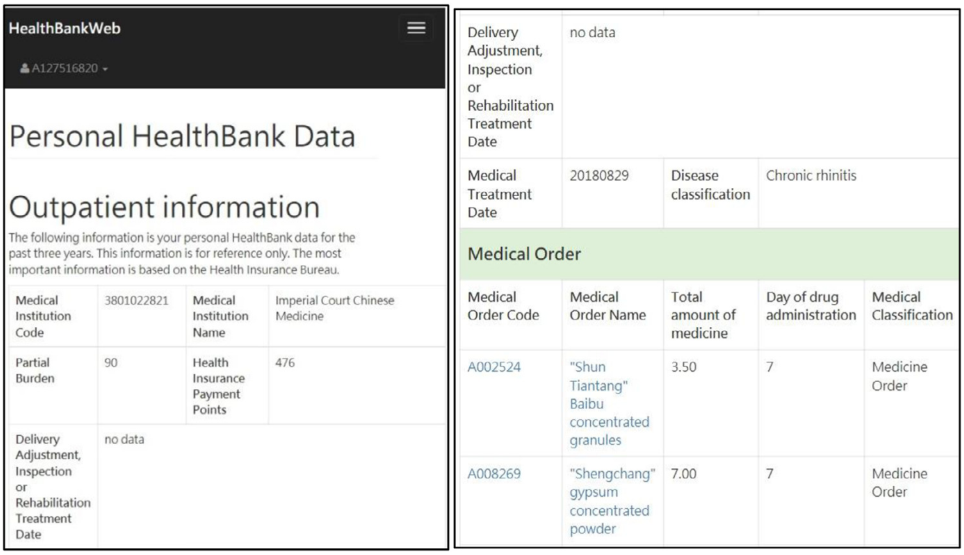


Fig. 14. The decryption process in CEDA.



Personal HealthBank Data

Outpatient information

The following information is your personal HealthBank data for the past three years. This information is for reference only. The most important information is based on the Health Insurance Bureau.

Medical Institution Code	3801022821	Medical Institution Name	Imperial Court Chinese Medicine
Partial Burden	90	Health Insurance Payment Points	476
Delivery Adjustment, Inspection or Rehabilitation Treatment Date	no data		

Delivery Adjustment, Inspection or Rehabilitation Treatment Date	no data		
Medical Treatment Date	20180829	Disease classification	Chronic rhinitis

Medical Order

Medical Order Code	Medical Order Name	Total amount of medicine	Day of drug administration	Medical Classification
A002524	"Shun Tiantang" Baibu concentrated granules	3.50	7	Medicine Order
A008269	"Shengchang" gypsum concentrated powder	7.00	7	Medicine Order

Fig. 15. An example of decrypted medical records.

a very large prime number. To decrypt the original medical record through the encrypted file, N (Prime number) must be factored, and if N is a very large Prime number, factorization is almost impossible, which guarantees the reliability of RSA encryption technology.

The verification mechanism for correct and complete medical records was implemented on blockchain. When the medical record is uploaded, the medical record with double encryption mechanism is calculated into a hash value through SHA-256. The hash value is generated in SHA-256 and stored in the block. When the medical records are exchanged, the system will perform a SHA-256 hash calculation on the retrieved encrypted medical records at one time, and compare the calculated hash value with the hash value on the blockchain. If the hash value is the same, the encrypted medical record is deemed correct.

5. Discussion and conclusion

The main aim of this study was to complete a security architecture for medical data, and develop a triple encryption authentication architecture to help data owners easily and securely share personal medical records with medical service personnel. The record transmission process is protected by a strict encryption mechanism through CEDA, and the correctness of records is verified by the hash value and blockchain, as based on the feature that blockchain information cannot be modified or deleted. The application of such triple protection can achieve the highest level of privacy and security for medical records.

The development of blockchain technology is very important for the application of precision medicine. Through the blockchain architecture, the data required by precision medicine can be integrated from different sources, and its correctness can be verified. In this study, in order to demonstrate the feasibility of MHB, medical data is ensured not to be leaked, and is strictly protected during transmission and exchange, which proves that the "SEMRES", as developed in this study, can be used to exchange and transmit EMR between different organizations and roles in an efficient and secure manner.

Hasselgren [21] pointed out the increased number studies conducted on the application of blockchains in the medical field, most of which explored how to use the blockchain architecture in health record systems (EHR and PHR), and how to use the characteristics of a blockchain to build a platform for sharing data between medical staff and researchers, in order to promote the continuity and interoperability of medical information between hospitals. Some studies focused on patients [22–25], and used a blockchain to establish a personal health record system, in order that patients can control their own rights to their personal health records, thus, promoting medical sharing between patients and doctors, and achieving continuous medical services.

In the previous developments of medical record exchange, the technical infrastructure of the medical system hindered secure and scalable data sharing across institutions [26]. In the face of such security and privacy issues, although it is necessary to share data, the identity and personal data of patients must still be protected [27]. If the network is used to exchange medical information, it may lead to the risk of clinical data leakage. Moreover, without a highly secure infrastructure, it may also lead to serious financial and legal problems [28]. However, the development and application of self-managed medical records has become more and more common in recent years. According to the definition by the American Health Information Management Association (AHIMA), each person has the right to manage their own health records, and the data of personal health records refers the records entered by medical service units and themselves. These data should be stored in a safe and private environment, and each person can decide who has the right to access [29].

However, to date, there are no good solutions regarding the specifications of data security or protection measures for the application environment, thus, most medical data is still stored in private servers, and use is limited.

Taiwan's first version of the My Health Bank was completed in September 2014. The purpose of My Health Bank is to return health data to the public, and let the public know and care about their health conditions through health data. In July 2016, My Health Bank was further improved in function, and called My Health Bank 2.0, which emphasizes the ability of data connection and linking. My Health Bank contains information about all medical services paid by health insurance and provides corresponding or related health management information; however, there are still concerns about the protection and verification of data. The Health Insurance Department allows individuals to download their medical record files, and once downloaded, there are no restrictions regarding the management, storage, or modification of the files, meaning people can modify the data content themselves, and the data content is not encrypted. If personal data is not managed properly, it may lead to privacy issues, which is still not effective for exchange and use.

The application of electronic medical records (EMR) has been developed all over the world. Kaiser Permanente, a non-profit medical insurance company in the United States, established the personal health record system of My Health Manager in 2007 [30], which is connected with electronic health record data, including vaccinations, examination records, medication prescriptions, allergy information, etc., and can also be used for clinical data exchange, as the system can be used to send e-mails to doctors to ask questions. In 2008, 2.4 million people signed up, and 62.1% visited the site more than twice within six months. In addition, on August 2, 2010, the U.S. government announced the Blue Button Initiative and started the Blue Button Program [29], which is a service mark registered on the website of the United States Department of Health and Human Services. Members of the public can see a clickable pattern of blue circles on the homepage of the website, and these Blue Buttons allow people to use the function of electronic health records, such as checking past and future appointments, problem lists, allergies, medications, laboratory results, life characteristics, and immunizations. By browsing the Blue Buttons, people can view, download, and print personal information and share their medical information with trusted people. At present, the Blue Button website page can receive patient user data, as provided by public and private organizations, such as the United States Department of Veterans Affairs (VA), the Department of Defense (DoD), and the Centers for Medicare & Medicaid Services (CMS), which have all joined the Blue Button Program. Moreover, hundreds of organizations have also agreed to participate in this program, and future developments include other personal health management systems based on Blue Button, such as My Military Health Records [30], which mainly allows soldiers to check their medical records and share data to save time during medical care.

According to Jae-woo Lee [[31], [32]], the My Health Bank personal health management system in South Korea was designed by the National Health Insurance Service (NHIS) for public use. This system provides a variety of health information, including the results of personal health examinations, questionnaires, medical and medication information, and health examination data. In addition, it provides the service of predicting public disease risks through health examination reports, and lifestyle and disease related questionnaires.

In 2009, the National Health and Hospital Reform Commission of Australia recommended that every Australian should have the ability to personally manage their electronic health records, in order to improve the quality, security, and efficiency of health care services [33–39]. The Australian Government developed the Personally Controlled Electronic Health Record (PCEHR) system, as based on HL7 CDA and IHE (Integrating the Healthcare Enterprise), and the XDS (Cross-Enterprise Document Sharing) standards of 2010, and began official operations of the personal health record (PCEHR) system in July 2012. All Australian citizens can apply to open an account in the system and completely control their health records. Medical service providers can also apply for accounts and use the system to provide better medical care for patients. The data exchanged in the system is divided into four areas, electronic inspection/examination report, electronic discharge medical record summary, electronic doctor referral, and electronic prescription management. Both the public and medical service providers can choose to join the PCEHR system. In addition, participating medical service providers can upload important health and medical information about patients, and with the authorization of the patient, can view the patients' information online. If citizens choose to join PCEHR, they can enter personal information, including prescription drugs, nutritional products, over-the-counter medicines, allergies, etc. Although the public cannot edit the information uploaded by medical service providers, they can choose which medical service providers can access their files and which information can be shared. However, the system has been on the market for nearly two years, and only 10% of Australians have registered to use it. Therefore, the Australian Government reviewed and examined the system again, and in 2015, the updated system was renamed "My Health Record". In addition, the Australian E-health Council was set up to replace the original National E-health Translation centre and operate the new system, which was officially launched in 2016. This new system claims to have strong protection measures to protect information, including encryption, a firewall, secure login, an authentication mechanism, and audit log records. When users complete the registration process, they can view their own health records, as well as their Medicare medical insurance records for the last two years.

At present, the security protection mechanism for exchanging electronic medical records is still based on information security protection. Each country has its own strict regulations, such as HIPPA in the United States, which requires data storage methods, database security protection, data transmission channels and encryption mechanisms, types of stored data, and places where the data can be used. The European Union's GDPR defines relevant regulations which including "Collection Limitation Principle", "Data Quality Principle", "Purpose Specification Principle", "Use Limitation Principle", "Security Safeguards Principle", "Openness Principle", "Individual Participation Principle", and "Accountability Principle". The electronic exchange center (EEC) in Taiwan is based on centralized architecture. EEC only record the index of medical record in different institution. The real medical record is deposited in institution, the completeness of medical records is relied on electronic signature.

While we can easily see that management systems, platforms, and data application functions have been widely developed for electronic medical records in various countries, the data are still stored in a central database and cannot be horizontally linked and concatenated. Thus, in the era of precision medicine, more priority should be given to the exchange and integration of data to provide a better infrastructure for the overall application of medical services. The SEMRES system, as proposed in this study, has good infrastructure, and this architecture can ensure the security and correctness of data and construct a transparent verification mechanism to protect personal privacy. At the same time, the payment process of telemedicine is completed through the mechanism of blockchain, which helps the overall telemedicine to create a good ecosystem.

In the field of medical care, patients, providers, and payers have formed a complex triangular relationship, and the interaction between them is often very redundant. And medical insurance rulings and payments involve a large number of reverse verifications and confirmations to verify compliance with contractual conditions and specifications, resulting in very complicated business processes.

As far as patients are concerned, from registering for medical treatment, applying for medical records to applying and writing off insurance premiums, the procedure is lengthy and full of uncertainty, which reduces the willingness to add insurance. For medical institutions, a large amount of manpower is invested in processing insurance reimbursements every year. The lengthy review and payment time is uncertain, which reduces financial stability and increases the risks of operation and management. For insurance companies, it spends a lot of cost input from contract signing, management, charging to claims acceptance, review and confirmation, but the delivery rate is still unsatisfactory.

McKinsey pointed out in the 2016 report [40] that blockchain technology is expected to provide new development potential for the insurance industry, including innovative insurance products and services, improving fraud detection and execution efficiency, and reducing management costs to achieve revenue growth . And believe that it is the best time for the entire insurance industry and individual insurance participants to further study blockchain technology and its potential.

In 2021 Taiwan a telecommunications company cooperates with the Life Insurance Business Association to apply blockchain technology to develop online insurance claims services, connect 14 insurance companies and 4 medical institutions, and obtain support and assistance from the capital city government. In a safe environment, transfer medical privacy information and quickly apply for insurance claims.

The blockchain has the characteristics of decentralization, openness, and information that cannot be tampered with. On a highly managed blockchain network, it can establish a trust mechanism across different institutions and industries, break the original barriers of data exchange and process interoperability, and develop innovation application to provide more efficient and convenient business services. Combining the results of this research will be able to develop patient-centered e-commerce medical services in a safer and more effective way, improve patient well-being and promote industrial innovation.

Author contributions

Conceptualization, Yen-Liang Lee, Hsiu-An Lee, and Chien-Yeh Hsu; methodology, Yen-Liang Lee, and Hsiu-An Lee; software, Yen-Liang Lee, and Hsin-Hua Kung; validation, Hsiu-An Lee; system structure design, Yen-Liang Lee, and Hsiu-An Lee; writing—original draft preparation, Hsiu-An Lee and Hsin-Hua Kung; writing—review and editing, Chien-Yeh Hsu and Hung-Wen Chiu; supervision, Hung-Wen Chiu; All authors have read and agreed to the published version of the manuscript.

Funding

This research has received funding from the Ministry of Education, Taiwan, under the project no. 107EH12-32.

Declaration of Competing Interest

The authors declare no conflict of interest.

Acknowledgments

This project has received funding from the Ministry of Education, Taiwan, under the project no. 107EH12–32 and Ministry of Science and Technology, under the project no. 109–2221-E-227 –003 -MY2.

References

[1] A.S. Manoj, M.A. Hussain, P.S. Teja, in: Patient Health Monitoring Using IOT, in Mobile Health Applications for Quality Healthcare Delivery, IGI Global, 2019, pp. 30–45.
[2] S. Misbahuddin, et al., IoT-based ambulatory vital signs data transfer system, J. Comput. Netw. Commun. 2018 (2018).
[3] F. Jamil, et al., Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals, Sensors 20 (8) (2020) 2195.
[4] K.N. Swaroop, et al., A health monitoring system for vital signs using IoT, Internet of Thing. 5 (2019) 116–129.
[5] Kathy J. MONTGOMERY, Development of a Tele-Healthcare Clinical Practice Guideline for Diabetic Patients, Walden University, 2019.
[6] W.E. Hills, K.T. Hills, Tele-health care and the use of virtual communication technologies in medical research and application: the future of telemedicine is now!, Med. Sci. Pulse 14 (3) (2020).
[7] R. Islam, et al., Portable Health Clinic: an Advanced Tele-Healthcare System for Unreached Communities, Stud. Health Technol. Inform. 264 (2019) 616–619.
[8] J. Benaloh, et al., Patient controlled encryption: ensuring privacy of electronic medical records, in: Proceedings of the 2009 ACM workshop on Cloud computing security, 2009.
[9] Chor, B., et al. Private Information Retrieval. IEEE.
[10] Z. Xia, et al., EPCBIR: an efficient and privacy-preserving content-based image retrieval scheme in cloud computing, Inf. Sci. (Ny) 387 (2017) 195–204.
[11] Giuseppe ATENIESE, et al., Provable data possession at untrusted stores, in: *Proceedings of the 14th ACM conference on Computer and communications security*, ACM Digital Library, 2007, pp. 598–609.
[12] Giuseppe ATENIESE, et al., in: Scalable and efficient provable data possession, ACM Digital Library, 2008, pp. 1–10.
[13] H. Wang, et al., Provable data possession with outsourced data transfer, IEEE Trans. Serv. Comput. (2019).
[14] A. Tembhare, et al., Role-based policy to maintain privacy of patient health records in cloud, J. Supercomput. 75 (9) (2019) 5866–5881.
[15] L. Xu, C. Xu, X. Zhang, A secure and efficient E-medical record system via searchable encryption in public platform, KSII Trans. Internet Inform. Syst. (TIIS) 11 (9) (2017) 4624–4640.
[16] J. Daemen, V. Rijmen, in: Announcing the Advanced Encryption Standard (aes), Federal Information Processing Standards Publication, 2001, p. 197.
[17] M. Calderbank, The Rsa cryptosystem: History, algorithm, Primes, math. uchicago. edu, Chicago, 2007.
[18] Satoshi. NAKAMOTOBitcoin, A peer-to-peer electronic cash system, Decentralized Business Review (2008) 21260.
[19] Pos pow and 12 other blockchain protocols you didn't know about, [online] Available: https://medium.corn/hackernoon/pos-pow-and-12-other-blockchain-protocols-you-didnt-know-about-3634b089d119/.
[20] Academy, B. Proof of Work Explained. 2019 30.12.2019; [online] Available: https://www.binance.vision/zt/blockchain/proof-of-work-explained.
[21] A. Hasselgren, et al., Blockchain in healthcare and health sciences—A scoping review, Int. J. Med. Inform. 134 (2020) 104040.
[22] X. Liang, et al., Integrating blockchain for data sharing and collaboration in mobile healthcare applications, 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, 2017.
[23] J. Zhang, N. Xue, X. Huang, in: A Secure System For Pervasive Social Network-Based Healthcare, 4, Ieee Access, 2016, pp. 9239–9250.
[24] X. Liang, et al., Towards decentralized accountability and self-sovereignty in healthcare systems, International Conference on Information and Communications Security, Springer, 2017.
[25] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain, J. Med. Syst. 42 (8) (2018) 140.
[26] P. Zhang, et al., FHIRChain: applying Blockchain to Securely and Scalably Share Clinical Data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.
[27] M. Terry, Medical identity theft and telemedicine security, Telemed. e-Health 15 (10) (2009) 928–933.
[28] A.S. Downey, S. Olson, Sharing Clinical Research data: Workshop Summary, National Academies Press, 2013.
[29] Group, A.e.-H.P.H.R.W.Defining the Personal Health Record. Defining the Personal Health Record/AHIMA, American Health Information Management Association, 2005.
[30] A.-.L. Silvestre, V.M. Sue, J.Y. Allen, If you build it, will they come? The Kaiser Permanente model of online health care, Health Affair, 28 (2) (2009) 334–344.
[31] J.-w. Lee, et al., The development and implementation of stroke risk prediction model in National Health Insurance Service's personal health record, Comput. Method. Program. Biomed. 153 (2018) 253–257.
[32] SHIN, Soon-Ae, et al. NHIS Big Data and Health Services-Consolidated Ageing Well Strategy in Korea. In: International Conference on Information and Communication Technologies for Ageing Well and e-Health. SCITEPRESS, 2015. p. 143-148.
[33] S. Duckett, S. Willcox, The Australian Health Care System, Oxford University Press, 2015.
[34] E. Lehnbom, J. Brien, A. McLachlan, Knowledge and attitudes regarding the personally controlled electronic health record: an Australian national survey, Intern. Med. J. 44 (4) (2014) 406–409.
[35] T.D. Gunter, N.P. Terry, The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions, J. Med. Internet Res. 7 (1) (2005) e3.
[36] L. Andrews, R. Gajanayake, T. Sahama, The Australian general public's perceptions of having a personally controlled electronic health record (PCEHR), Int J Med Inform 83 (12) (2014) 889–900.
[37] E. Lehnbom, H. Douglas, M. Makeham, Positive beliefs and privacy concerns shape the future for the Personally Controlled Electronic Health Record, Intern. Med. J. 46 (1) (2016) 108–111.
[38] L. Hanna, et al., Patient perspectives on a personally controlled electronic health record used in regional Australia: 'I can be like my own doctor', Health Inform. Manag. J. 46 (1) (2017) 42–48.
[39] C. Pearce, M. Bainbridge, A personally controlled electronic health record for Australia, J. Am. Med. Inform. Assoc. 21 (4) (2014) 707–713.
[40] J.-.T. Lorenz, et al., Blockchain in insurance-opportunity or threat, McKinsey & Company, 2016.