Hyperledger Fabric-based Reliable Personal Health Information Sharing Model

Jinsook Bong* and Uijin Jang

Soongsil University, Korea
E-mail: jsbong@ssu.ac.kr; neon7624@ssu.ac.kr
**Corresponding Author*

Received 27 April 2021; Accepted 26 January 2023;
Publication 29 April 2023

Abstract

To provide optimized individual-oriented medical service, an open eco system is required so that personal health information could be safely recorded, managed, shared and viewed.

However, the current health information is being separately collected, stored, managed by various management institutions, so data linkage is not guaranteed. The data ownership for personal health information belongs to management entities not an individual and also health information is electronically recorded and managed, so it's vulnerable to forgery and leakage like other electronic data.

This paper proposes a personal health information sharing platform applying the Hyperledger fabric. The proposed platform was designed based on blockchain to provide user-oriented health information management and access rights. Therefore, it is possible to create, manage and share reliable medical data.

Keywords: Hyperledger fabric, blockchain, health information, secure sharing.

Journal of Mobile Multimedia, Vol. 19_4, 1009–1020.
doi: 10.13052/jmm1550-4646.1944

1 Introduction

Due to the development of information and communication technology that leads the 4th industry, the individual-oriented precision medicine is possible. An open eco system is needed for optimized individual-oriented medical service that personal health information could be viewed, managed and distributed in anytime and anywhere [1].

A health information includes not only patient medical records, but also biometric information collected through smart devices and the information of personal medical examination stored in public institutions. Data linkage between them is not working well [2] because current personal health information is separately being collected and stored by various management institutions and reliability issues can be raised remain in the case of data collected from users [3].

In addition, there are the structural limitations in which the patients can't have access rights to their medical data.

To solve this problem, this paper proposes a reliable personal health information sharing model based on Hyperledger Fabric. The proposed personal health information sharing model is designed to use the authority of their medical data, and to enable data creation, management and sharing with a reliable user-oriented medical data.

2 Related Work

In related work, we summarize the current status of medical data sharing system and several technologies used in the proposed model.

2.1 Status of Medical Data Sharing System

Current sharing of medical data requires patients to obtain medical records from previous hospitals or institutions, and then deliver the records to the hospital they want to go. Therefore, lots of time and efforts are required for medical data sharing.

To solve this inconvenience, a medical data exchange project is being promoted under the initiative of the state. This project is kind of a method of automatically processing medical data exchange based on system between hospitals to reduce the inconvenience of the current system. However, this only focus on the inconvenience of medical data sharing and does not address the reliability of the transferred medical data (created by individuals or hospitals). And medical data is electronically recorded and managed, so it's

Table 1 The security threats of medical data

Data generation	Careless data measurement
	Collection of untrusted data
Data storage	Access to medical data by unauthorized persons
	Unjustified medical record change
	Forgery of data by hacking
	Data leakage by insiders and conspirators
Data sharing	Risk of personal information identification
	Medical data communication protocol attack

vulnerable to forgery and leakage like other electronic data [4]. Therefore, the reliability issue of shared medical data remains.

2.2 Security Threats and Requirements of Medical Data

Digitalization of medical data has promoted the convenience of using information, but it is necessary to protect it. According to VERIZON [5], data violations in the medical industry are caused by human error, misuse, physical theft, hacking, and malicious code. In addition, a number of documents [3, 6, 7] describe security threats in the medical field. The security threats of medical data in terms of data creation, storage, and sharing are as follows.

To prevent security threats described above, confidentiality, integrity and availability of medical data should be guaranteed. To protect privacy of the information subject, anonymity, dis-connectivity, access control, and authentication should be guaranteed as well [4].

2.3 Hyperledger Fabric

The proposed personal health information sharing platform handles medical data, which is sensitive information. Therefore, it is appropriate to use a permissioned blockchain that only authenticated users can participate in.

Hyperledger Fabric is a permissioned private blockchain. The only users registered in an authentication management system called Membership Service Provider (MSP) can participate in the network. Participants can build a blockchain platform properly for business purposes and select a block generation algorithm or transaction assurance policy for business systems.

In Hyperledger Fabric environment, there is smart contract called as chaincode and consensus process is configured by execution, ordering and validation.

Table 2 Security requirements for health information

Confidentiality	It must be encrypted and stored so that unauthorized persons cannot see the user's health information (medical record and health information).
Integrity	It should be confirmed that the stored and shared user's health information has not been illegally changed.
Availability	When an authorized person requests data retrieval or data sharing, it must be able to receive the retrieval or requested data within a reasonable time.
Anonymity	The elements that could indicate the identity of the data subject should not be identified.
Dis-connectivity	Unauthorized users should not be able to know the connection between medical data. In other words, it shouldn't be possible to know whether two medical pieces of information belong to the same data subject. This allows us to provide strong privacy by minimizing the ripple effect even if anonymity is violated.
Access Control	Unauthorized users should not be able to access personal health information.
Authentication	It is necessary to confirm whether the subject who intends to create, store, and share health information is legal or not.

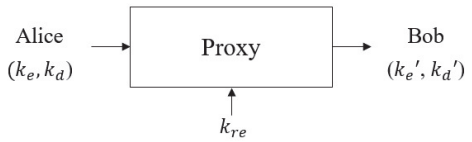

Figure 1 Proxy Re-encryption [9].

2.4 Proxy Re-encryption

Proxy Re-encryption [9, 10] is a kind of public key encryption technique that allows other users to get the decryption authority from original data owner. The proxy re-encryption technique has the advantage that plaintext is not exposed during data re-encryption. The user got the decryption authority can recover the encrypted data as shown in (Figure 1). The proxy re-encryption described in this paper referred to the content of [9].

3 Proposed Model

3.1 Composition of the Proposed Model

The proposed reliable personal health information sharing model is configured of each participant group and cloud storage as shown in (Figure 2). Each

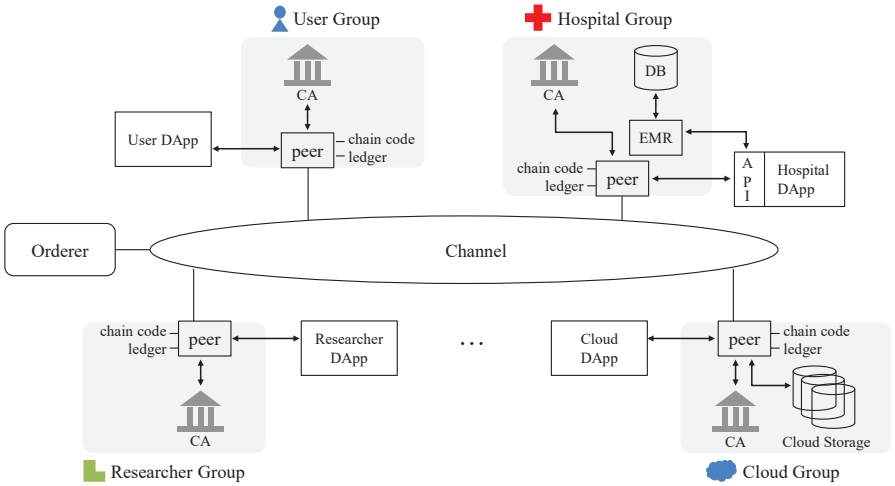

Figure 2 A proposed personal health information sharing platform.

group of participants is a node (peer) to maintain the blockchain network and manages the chaincode and distributed ledger. Cloud storage is used as a data storage for storing and sharing personal health information.

In the figure, only one node per group is shown, but there are actually a number of nodes. Depending on the role, it can be an endorsing node(endorser) or a commit node (committer).

3.2 Operation Procedure of the Proposed Sharing Platform

- User registration procedure

Hyperledger Fabric provides membership services itself using MSP. The proposed sharing platform has basic function of MSP, and additionally carries out the user registration process by adding identity verification and key exchange process.

– Each participant registers to group CA which they belong to.
– When registering, carry out user registration process by using mobile phone authentication if the user is legitimate.
– The group CA transmits the unique identifier, private key, public key and multi-vector values which will be used in the system to each participant.
– Initial data transmission between CA and participants is performed through a secure channel. The multi-vector value is hashed to the user's unique identifier, and generated output is used as a new identifier.

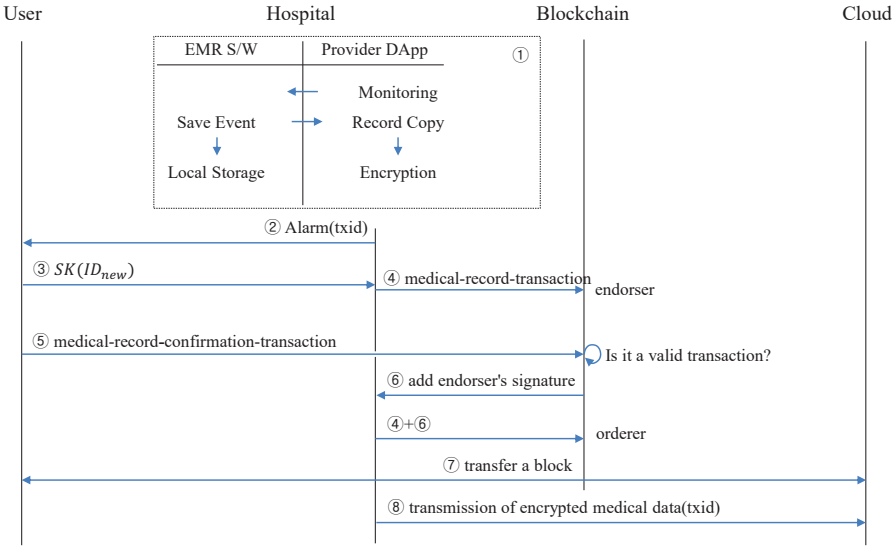

Figure 3 Procedure for creating and storing medical records.

- Transmission of medical data

Hospitals and users use the Diffie-Hellman algorithm to create a symmetric key(sk) to be used for encryption of medical records. Also, to use proxy re-encryption in the cloud, the cloud seed key (k_s), two constructors g_1, g_2 and functions f are publicly open in advance. Information to be transmitted to the cloud is encrypted with an encryption key ($k_e = {g_2}^{k_d}$) generated using a symmetric key.

- Hospital DApp monitors the hospital EMR system. In the occurrence of data storage, DApp encrypts with an encryption key(for cloud transmission) after the content is copied.
- Hospital DApp also sends an alarm including txid to user DApp to check his or her medical record.
- User DApp hashes the user's unique identifier with the multi-vector value received from the MSP to create a new identifier (ID_i, $i = 1, 2, \ldots, k$, k is the number of multi-vector), encrypts it with a symmetric key with the hospital, and sends it to the hospital.
- Hospital DApp creates a medical-record-transaction including a new identifier and transmits it to the blockchain.
- User DApp checks his/her medical records and then transmits the medical-record–confirmation-transaction to the blockchain.

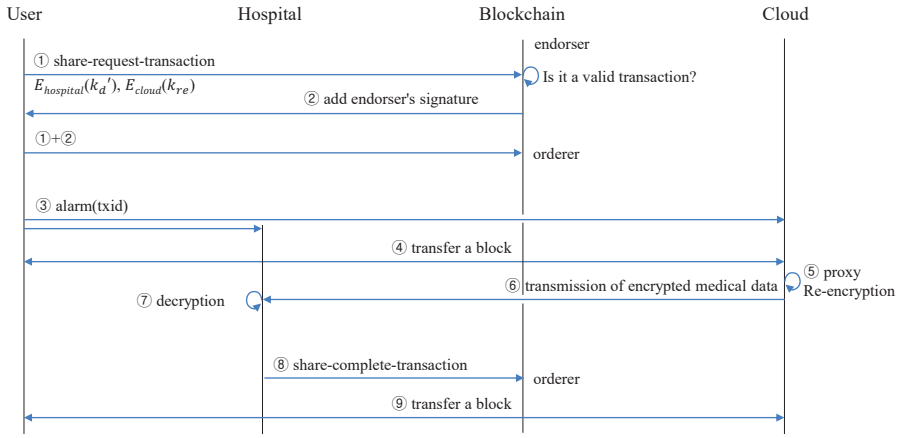

Figure 4 Procedures for sharing medical records.

– The endorser of the blockchain network checks the medical-record-transaction and the medical-record-confirmation-transaction, and if the two values match, it responds to hospital DApp by adding the result value and its own signature.
– After that, medical-record-transactions are recorded in the distributed ledger.
– Hospital DApp transmits encrypted medical data to cloud.

• Information sharing between hospitals

– When the user wants to transmit his/her medical record stored in the cloud to other hospital, the user transmits the share-request-transaction to the blockchain through user DApp, and also transmits the keys associated with the proxy re-encryption key.
Generation of Re-encryption key: The re-encryption key formula is as shown in (Equation 1).

$$k_{re} = \frac{k_e'}{k_e} \tag{1}$$

– The endorser of the blockchain checks whether the information of the shared item has been written before, and then if the shared item exists, it responds to user DApp by adding the result value and its own signature.
– User DApp receiving a response from endorsor transmits an alarm included txid to cloud and data receiving hospital.
– After that, the share-request-transactions are recorded in the distributed ledger.

– The cloud checks the transaction corresponding to the txid. And cloud decrypts the encrypted contents (1). The cloud re-encrypts the user's medical data by using the outcome (proxy re-encryption key) from decrypted process.
Re-encryption: Apply $C_i{}' = C_i \cdot e(Z, k_{re})$ to $i = 1, 2, \ldots l$ and re-encrypt as shown in (Equation (2)).

$$C_1{}'||C_2{}'||C_3{}'|| \cdots ||C_l{}'||Z \tag{2}$$

– Send re-encrypted data to the hospital.
– The hospital decrypts the data using the proxy decryption key encrypted with the hospital's public key included in the share-request-transaction and reads it.
Decryption: The message is decrypted as shown in (Equation (3)) using the decryption key transmitted by the user in step 1.

$$\begin{aligned} C' &= C \cdot e(Z, k_{re}) = M \cdot e(g_{1,}, k_e)^r \cdot e(Z, k_{re}) \\ &= M \cdot e(g_1, g_2)^{k_d r} \cdot e(g_1^r, g_2^{k_d{}' - k_d}) \\ &= M \cdot e(g_1, g_2)^{k_d r} \cdot e(g_1, g_2)^{r(k_d{}' - k_d)} \\ &= M \cdot e(g_1, g_2)^{k_d{}' r} = M \cdot e(g_1, k_e{}')^r \end{aligned} \tag{3}$$

– The hospital notifies that the data transfer is complete by sending the share-complete-transaction to the blockchain network.
– After that, the share-complete-transaction is recorded in the distributed ledger.

4 Performance Evaluation

4.1 Comparative Analysis

From a functional point of view, Table 3 compares the existing method in which users manually share their own medical data, a state-led medical information exchange project that handles online sharing requests and responding, and the proposed method that shares the personal health information using Hyperledger Fabric Blockchain. The medical information exchange project is meaningful in that, it allows information to be shared between hospitals online and it has created a Korean standard. However, users still cannot control his or her information, and even legitimate users cannot link and view all of his or her health records, and can only access shared information.

Table 3 Comparative analysis of currently used and proposed methods

Item	Existing Scheme	Exchange of Medical Information	Proposed Scheme
Self-information control	Impossible	Impossible	Possible
Data connectivity	Impossible	Limited to exchange information	Connect all data
Time and cost	Consuming a lot of time and money	Consuming less time and money	Consuming less time and money

Table 4 Techniques applied and added to meet security requirements

Item	Basic Suggestion	Additional Suggestions
Confidentiality	–	Proxy Re-encryption
Integrity	Hyperledger Fabric Blockchain	–
Availability	Hyperledger Fabric Blockchain	–
Anonymity	Hyperledger Fabric Blockchain	Use of multi-vector
Dis-connectivity	–	Use of multi-vector
Authentication	Hyperledger Fabric Blockchain	–

4.2 Security Analysis

The evaluation items of the security analysis are based on the security requirements written in the related research. Table 4 shows the blockchain techniques and additional proposed techniques used to meet the security requirements in this paper.

– Confidentiality: Personal health information is encrypted and stored in the cloud. Therefore, even a cloud administrator cannot decrypt personal medical data. In addition, when a user wants to share his or her medical data with other hospitals, since proxy re-encryption technique is used, the exposure of the key can be minimized and personal health information can be shared.

– Integrity: As all personal health information is generated electronically, it is vulnerable to forgery and leakage like other electronic data. In the proposed method, when the information is generated, the hash value of the original information is stored in the blockchain, so the integrity of the created medical record can be verified. Figure 5 shows the hash value of the original information contained in the blockchain.

– Availability: As all committer of the participating group have a distributed ledger, there is no single point of failure (SPoF) problem, and availability can be guaranteed when searching and managing personal health information history.

Figure 5 Hash value to check the data integrity.

– Anonymity: The proposed method uses the unique identifier provided by the MSP. Since user information is not used to create a unique identifier, personal identification using a unique identifier is not possible. In addition, the information included in the transaction satisfies the anonymity because only data irrelevant to personal information such as hash value and original URL are stored, not actual medical records or health records.

– Dis-connectivity: The proposed scheme satisfies the dis-connectivity by creating and using multiple identifiers by hashing the multi-vector value received from the MSP when the user registers with the user's unique identifier. Therefore, if k multi-vectors are used when one user has n medical data, even if the user's unique identifier is exposed, only n/k actual medical data is exposed, so the impact on exposure attacks can be reduced.

– Authentication: In Hyperledger Fabric, all network participants register with the MSP and sign the transaction using the key issued by the MSP. Therefore, verification of the identity of the participant can be performed using the MSP.

5 Conclusions

This paper proposes Hyperledger Fabric-based reliable personal health information sharing model. Since medical data is sensitive information, it is not easy to share medical information in particular. Although the medical data exchange project is being promoted under the initiative of the state, self-information control and data integrity are not covered yet.

In this paper, we proposed a personal health information sharing model that applies a blockchain which has advantages in terms of self-information control and data integrity to a medical domain. The proposed model enables self-information control by storing medical data with the consent of the patient. When storing transactions for medical records or health information, a hash value is included and used for checking data integrity if required. This

paper is meaningful as an effort to establish an open ecosystem for providing individual-oriented medical services.

Acknowledgement

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the National Program for Excellence in SW (2018-0-00209) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation).

References

[1] H. Han 'The use of blockchain technology in the medical field and policy suggestions', KHIDI Expert Report, May 2008.
[2] M. Kang, D. Park, 'The era of smart healthcare, prepare for the data war', Samjung KPMG Economic Research Institute, Nov. 2018.
[3] G. Ahn, 'System Requirements and Architecture for Judgment of Healthcare/Medical Data Trustworthiness', TTA Technical Report, Oct. 2016.
[4] H. Kwon, J. Kim, 'Connected Medical Device Security Trends and Issues' Weekly Technology Trends, No. 1911, pp. 14–26, Aug. 2019.
[5] calyptix, 'Top 5 Causes of Data Breaches in Healthcare'. 2018
[6] S. Baek, 'A study on patient anonymity preserving framework in the healthcare information sharing environment', Ph.D. thesis, May 2018.
[7] IoT Security Alliance, 'Cyber Security Guide for Smart Medical Service', May 2018.
[8] Y. Song, K. Park, 'Security/privacy requirements for medical data sharing and utilization services', REVIEW OF KIISC vol. 20, no. 3, pp. 90–96, June 2010.
[9] Y. Park, S. Seo, 'Method of Changing Password for Secure Cloud Storage based on Proxy Re-encryption Scheme', Journal of The Institute of Electronic and Information Engineers, vol. 53, no. 3, pp. 29–36, March 2016.
[10] Y. Song, K. Park, H. Kim, J. Do, D. Lee, 'A study on the secret sharing scheme for managing a large quantity of data including individual information', Korea Internet & Security Agency, Sep. 2009.

Biographies

Jinsook Bong received the master's degree in computer engineering from Soongsil University in 2005, and the philosophy of doctorate degree in computer engineering from Soongsil University in 2019, respectively. She is currently working as a Lecturer at Spartan Software Education Institute, Soongsil University. Her research areas are information security, IoT and blockchain technology.

Uijin Jang received the bachelor's degree in computer engineering from Soongsil University in 1999, the master's degree in computer engineering from Soongsil University in 2002, and the philosophy of doctorate degree in computer engineering from Soongsil University in 2011, respectively. She is currently working as an Assistant Professor at Spartan Software Education Institute, Soongsil University. Her research areas include information security and blockchain technology.