ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

A Trusted Sharing Model for Patient Records based on Permissioned Blockchain☆

Kyoung-jin Kim[1] Seng-phil Hong[1*]

ABSTRACT

As there has been growing interests in PHR-based personalized health management project, various institutions recently explore safe methods of recording personal medical and health information. In particular, innovative medical solution can be realized when medical researchers and medical service institutes can generally get access to patient data. As EMR data is extremely sensitive, there has been no progress in clinical information exchange. Moreover, patients cannot get access to their own health data and exchange it with researchers or service institutions. It can be operated in terms of technology, yet policy environment are affected by state laws as well as Privacy and Security Policy. Blockchain technology—independent, in transaction, and under test—is introduced in the medical industry in order to settle these problems. In other words, medical organizations can grant preliminary approval on patient information exchange by using the safely encrypted and distributed Blockchain ledger and can be managed independently and completely by individuals. More apparently, medical researchers can gain access to information, thereby contributing to the scientific advance in rare diseases or minor groups in the world.

In this paper, we focused on how to manage personal medical information and its protective use and proposes medical treatment exchange system for patients based on a permissioned Blockchain network for the safe PHR operation. Trusted Model for Sharing Medical Data (TMSMD), that is proposed model, is based on exchanging information as patients rely on hospitals as well as among hospitals. And introduce medical treatment exchange system for patients based on a permissioned Blockchain network. This system is a model that encrypts and records patients' medical information by using this permissioned Blockchain and further enhances the security due to its restricted counterfeit. This provides service to share medical information uploaded on the permissioned Blockchain to approved users through role-based access control. In addition, this paper presents methods with smart contracts if medical institutions request patient information complying with domestic laws by using the distributed Blockchain ledger and eventually granting preliminary approval for sharing information. This service will provide an independent information transaction and the Blockchain technology under test will be adopted in the medical industry.

☞ keyword : Permissioned blockchain, Role-based access control, Medical data

1. Introduction

As there has been growing interests in PHR (Personal Health Record)-based personalized health management project, various institutions recently explore safe methods of recording personal medical and health information. PHR[1] herein refers to data associated with information on medical treatment, activity, and life environment. A project provides personalized medical service. Affiliated hospitals integrated with medical treatment and information communication technology collect health information from customers, analyze it, and offer personalized health management service.

Health-related data was distributed in each hospital and complicated to use since measurement was impossible in previous days. Medical treatment records of patients are only stored in hospitals and it was impossible to collect activity information as there was no sensor or wearable device. However, the advance of the current technology enables us to measure activity data such as exercise amounts and blood pressure of patients (customers) created in daily life. As medical treatment records in hospitals are digitized, collected data can be analyzed in groups. This data centralization may trigger problems.

In 2013, Korea Pharmaceutical Information Center

1 Dept. of Convergence Security Engineering, Sungshin Women's University, Seoul, 02844, Korea.
* Corresponding author (philhong@sungshin.ac.kr)
[Received 29 August 2017, Reviewed 6 September 2017(R2 17 October 2017), Accepted 25 October 2017]
☆ This work was supported by the Sungshin University Research Grant of 2017.
☆ A preliminary version of this paper was presented at ICONI 2016 and was selected as an outstanding paper.

disclosed medical treatment information of patients without authorization by using PM 2000 pharmacy claim program[2,3]; what is called, a disclosure accident by Korea Pharmaceutical Information Center. Multiple businesses were indicted for collecting and dealing with nearly 4.7 billion cases of personal medical information amounting to about 4.4 million people without consent. Specifically they were convicted for selling medical treatment records or prescriptions collected by medical management software installed in medical institutions including hospitals and drugstores and overseas companies reprocessed this information and resold it to Korean pharmaceutical companies. The Korea Joint Investigation Team for Personal Information Crimes announced to indict them for an illegal collection of medical treatment and prescription from patients on August 2015.

Despite these problems, various IT technologies start to give constant influences over a medical field[4]. Personal medical information is particularly created as online database and personal medical information are exchanged for various purposes. If PHR is introduced, this exchange will be augmented by its multi-purposes.

This paper focuses on how to manage personal medical information and its protective use and proposes medical treatment exchange system for patients based on Blockchain network for the safe PHR operation.

2. Background and Related Works

2.1 Trend of Blockchain

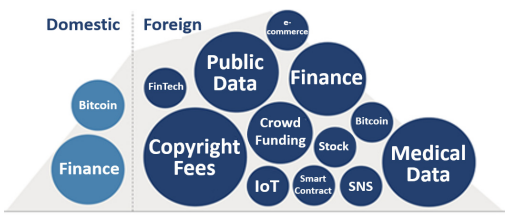
The world health system faces a complicated problem on how medical staff share medical documents for various purposes and personal information are secured and data integration. Medical documents among institutions have traditionally complied with three models[5]: Push, Pull, and View (See 2.3). Blockchain provides the fourth model and many researchers concentrate on Blockchain technology that offers effortless and safe data exchange protection as the fourth model.

The let us flip through the definition of Blockchain[6,7]. It gains attention as a trust-based transaction technology. Since each node in chains preserves photocopies written by hospital presidents and signs with an encrypted hash key, it is operated by P2P computer network that can trust mutual photocopies.

This technology has the following merits.

- **Transparency,** Distribute account books to all network participants and store them
- **Safety,** Intensified security measures with distributed data storage, safe and accurate recording transactions with encrypted access
- **Immediacy,** Approve immediately without mediation as the system is safe and grants an autonomous authority
- **Cost reduction,** As network participants equally distribute and store service, additional service is unnecessary (Low cost)

In addition to these features, transparent and safe direct transactions are available as there is no the third party's intervention. If this technology is applied into blood, organ management, and medical data exchange, it will boost up reliability. Foreign countries had already introduced this Blockchain area earlier than South Korea (See Figure. 1[8]) and the United States started to research on applying the Blockchain technology into EMR (Emergency Medical Responder) and data exchange launched by FDA (Food and Drug Administration).



(Figure 1) The Difference of Blockchain Technology Applied Areas Between Korea and Foreign Countries

This encrypted Blockchain access grants an authority to offer positions, manages dangerous elements surrounding identifications, and enables us to record data or get access to it. Moreover, this cannot revise all transactions and can be equipped with tracking function. Although the current technology operated in medical treatment can adopt this, this

Blockchain features provide more reliability.

2.2 Domestic Law, Blockchain in Terms of Institution

Personal medical information is the most sensitive one compared to any other personal information since it includes broad and private information such as physical features, the history of disease, and the history of drug administration. If this private information is leaked, it will definitely cause serious harms to patients' social prestige as well as economic lives. In particular, the disclosure of personal medical information works irreparable harms to patients. If the disclosure of resident identification number or credit card information is detected earlier, it could take immediate measures such as the change of resident identification number or the card suspension according to Korean regulations. In contrast, personal medical information remains permanent until they die. Therefore, disclosure causes tremendous harms and even is unable to prevent it[2].

According to the Act on the Protection of Personal Information[9], "health" related information and "genetic information" are classified into sensitive information and process is fundamentally prohibited. Therefore, it shall not be processed in terms of the efficiency of providing medical service, development and utilization of medical technology. Institution must be considered as well. Medical institutions can officially collect medical treatment records and personal information if patients give informed consent according to medical laws or inevitable reasons for executing medical treatment contracts (Collection Limitation Principle). In addition to these details, we examine domestic acts in terms of utilizing personal medical information in Table 1.

In addition, those who provide or receive personal information to the third person in violation of Article 23 without consents from information subjects (patients) shall be punished by imprisonment for not more than five years or a fine not exceeding fifty million won in accordance with Act on the Protection of Personal Information (Article 71) (Accountability Principle).

In order to process sensitive information pertained to medical information in compliance with these legal acts as exception:

(Table 1) Domestic acts in terms of utilizing personal medical information

Law	Article	Content	Principle for Protecting Personal Information
Framework Act on Health and Medical Services	Article 13 (Confidentiality Agreement)	Regarding health and medical treatment, individual physical and health secret and the secret of privacy are not interfered.	The Right to Privacy
Medical Law	Article 21 (Access to Records) Section1, Section 2	**Principally prohibited from disclosing** patient medical information **to other people save for patients** (Allow exceptions legally).	Use Limitation Principle
	Article 21 (Access to Records) Section 3	Stipulate a condition that medical staff shall send medical treatment records to other medical staff on condition of **patients' consents**	Use Limitation Principle, Individual Participation Principle
	Article 23 (Electric Medical Record) Section 3	**Forbidden to disclose, modify, or ruin personal information** stored in electronic medical records.	Security Safeguards Principle
	Article 18 (Prescription Writing and Delivery)	**Forbidden to detect, disclose, modify, or ruin personal information** stored in electronic prescriptions.	Security Safeguards Principle
Act on the Protection of Personal Information	Article 23 (Control on Processing Sensitive Information) - Presidential Decree Article 18	"**Sensitive Information**" includinghealth, sex life, and genes; **principally, process is prohibited.**	Use Limitation Principle

i) In Case of Special Consent from Information Subject, In case that information subjects recognize the process of sensitive information and clearly express personal opinion separated with the process of other personal information
ii) In case of explicitly requesting or permitting sensitive information process in other laws, Including the process of sensitive information specifically stated in other laws or requesting judicial interpretation

ii) As this paper does not discuss methods, observe i) and clarify the definition of personal medical information, and further develop methods on the safe use.

2.3 Related Works

2.3.1 Methods of Exchanging Medical Data

There are three methods of exchanging previous medical data: Push, Pull and View[5,10,11].

Push: The concept is that the medical information is sent from one provider to another. Transaction between two subjects and other subjects cannot get access to it. For example, hospitals hope that if they push information out onto their local HIE (Health Information Exchange) platform, then everyone else who connects to that platform will be connected. Before using for this, software could be placed in the HIE platform to send push alerts to subscribing physicians when new data related to admission, transfer or discharge are uploaded. If you completed transmission to a certain hospital, a new hospital cannot be accessible with health data delivered to the initial hospital. In other words, it does not guarantee data integration from the data creation up to the use. It presupposes that transmitting system created accurate amounts of information and receiving system accepted equivalent amounts of information without any standard audit trail.

Pull: Request information to other suppliers. For example, since the hospital knows that your cardiologist can receive the requested records to our family doctor whenever they are needed. But on the negative side are no alerts. The pressure on the local physician is to keep track of medical records about any outpatient have been ordered, in order to pull the results a few days later, and to know somehow that their patient was in the Emergency Department or the hospital.

Both Push and Pull, every consent and approval are conducted official and immediately standardized audit trail.

View: A single supplier can observe internal data records of the other supplier. For instance, a doctor in a surgery room can see x-ray pictures you took at the emergency medical center.

Based on the above technological operation, the actual case for Korean medical information system includes Hospital Information System (HIS) as well as EMR (Electronic Medical Record) as its part. EMR includes much data such as demographic statistics, treatment, and genetic information and can be utilized as a storage for biomedical science. In addition, innovative medical solution can be realized when medical researchers and medical service institutes can generally get access to patient data. As EMR data is extremely sensitive, there has been no progress in clinical information exchange. Moreover, patients cannot get access to their own health data and exchange it with researchers or service institutions. It can be operated in terms of technology, yet policy environment are affected by state laws as well as Privacy and Security Policy.

2.3.2 Research Trend on Blockchain Associated with Medical Information

Blockchain technology presented as the above solution is an innovative system for the sake of safe personal information protection management as well as service based on the recent medical information. For IBM, it conducts a joint medical research by using the Blockchain technology with FDA and centers primarily on pharmaceutical information developed for a complete patient data exchange from various sources.

MedRec[12] as a solution is to the needs of patients, the treatment community, and medical researchers. It is decentralized record management system for EMRs that uses blockchain technology to manage authentication, confidentiality, accountability, and data sharing. And as a key feature of this work, it is engaged the medical research community.

South Korea started to conduct this research. Tae-sung Kim et. Al[13] proposed medical treatment information

system for patients suffering from infectious diseases by utilizing a standard FHIR based on a consortium Blockchain network. To do so, his team presents an alternative for a problem of missing reports identified in the previous passive reporting method.

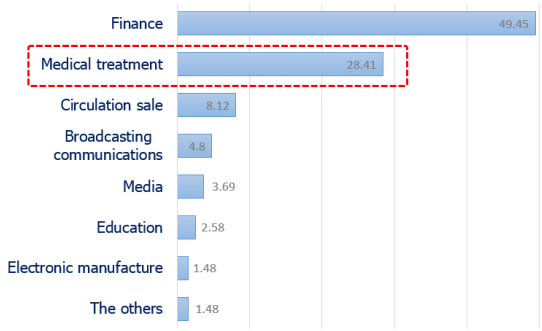
3. Problem Statements

Sharing information among the medical community is main issue in the healthcare industry.

First, university hospitals equipped with actual electronic charts can exchange (part of) patient treatment information through the system and prevent the expansion of diseases without unnecessary examination. However, electronic charts are not properly used in primary medical institutions. In particular, the distribution of information systematization is required for patients' safety as medical suits are more likely to be raised in case of handwritten charts and medical accidents provoke other social costs[14,15].

Second, many problems are posed in terms of the protection of patients' private lives as this information system allows many relevant medical institutions to exchange it due to the collection and preservation of an enormous quantity of personal health information. In other words, the exchange of personal information and the disclosure due to more and more digitization can cause severe interference with privacy as tremendous amounts of patient information is more likely to be leaked in conjunction with the improved accessibility to medical information. According to the survey on the most concerned field in terms of the disclosure of personal information (See Figure 2[16]), finance was ranked the first, and medical industry was ranked the second. In financial industry, all measures were arranged with reinforced security after the massive customer data breach incident happened in 2014. In contrast, medical industry takes little consideration into protective measures despite the far more sensitive and important information than financial information.

Medical information demands special protection compared to other personal information. As digitized information is easily reproduced, private life is more likely to be interfered if medical information is illegally disclosed or inaccurate information is produced.



(Figure 2) Survey on the concerned field in terms of security threat of personal information

Third, the invasion of privacy caused by the disclosure of personal medical information obviously violates Individual's Right to Personal Information Control. Moreover, patients cannot claim full ownership of his medical records. If the patient is given complete control over the information, he can change certain information or even delete parts of it. The disadvantage that patients are incapable of owning their own data is that they do not perceive who uses and exchanges it.

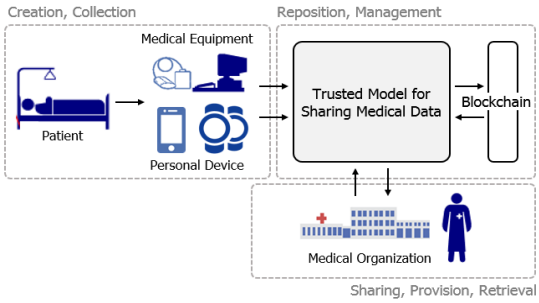
Blockchain technology—independent, in transaction, and under test—is introduced in the medical industry in order to settle these problems[10,17]. In other words, medical organizations can grant preliminary approval on patient information exchange by using the safely encrypted and distributed Blockchain ledger and can be managed independently and completely by individuals. More apparently, medical researchers can gain access to information, thereby contributing to the scientific advance in rare diseases or minor groups in the world.

4. Proposed TMSMD

4.1 Entire Structure Map

Medical information exchange of trust-based Blockchain presented in this Section follows the picture below.The structure adopted in this paper consists of a permissioned Blockchain network. Here a permissioned Blockchain is that the idea of a permissioned Blockchain is one in which transaction processing is performed by a predefined list of subjects with known identities[18]. For example, in medical,

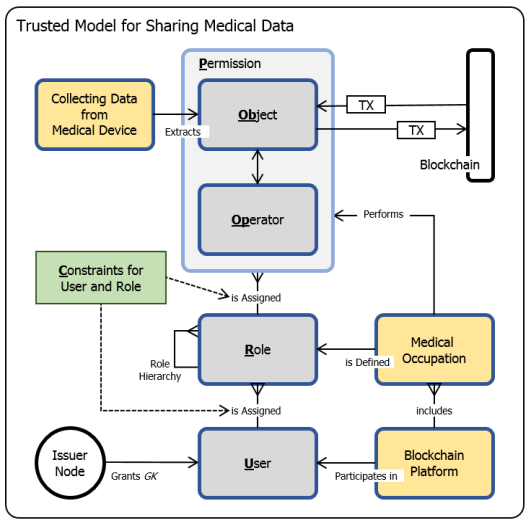
only certain miners might be allowed to create new blocks of transactions and to add them into the Blockchain. The process is performed on condition of participant medical institutions are approved. Thus, this paper is based on exchanging information as patients rely on hospitals as well as among hospitals.



(Figure 3) Entire structure map in medical industry

As Figure 3 shows, it is a network gathered with permissioned participants which are classified into patients and relevant medical institutions such as laboratories, medical institutions, and hospitals. Patients retain the right of personal information. Patient data is created by medical instruments in hospitals and personal medical management instruments (Creation and Collection), and processed data via gathering is placed on the Blockchain (Reposition and Management). Trusted Model enables all relevant medical institutions exchange medical information except for personal information depending on utilization by placing it on the Blockchain, create a block of recorded patient information, or exchange verified block contents in a limited way for access control according to the functions of relevant medical institutions in case of the top secret medical treatment information. And those who share and utilize uploaded information are referred to relevant medical institutions consisting of researchers, medical institutes, and general hospitals(Sharing, Provision and Retrieval). They use medical information for research such as statistics and processing and request information in order to exchange patient information on medical treatment.

As illustrated above, the proposed method presented in this paper provides service for exchanging medical information uploaded on the Blockchain to authorized users



(Figure 4) TMSMD

through role-based access control.

4.2 Trusted Model for Sharing Medical Data

Certified methods consist of a permissioned Blockchain network. Relevant medical institutions such as hospitals, clinics, and researchers could be added to the network after performing a preliminary procedure in which they receive group keys to the top permitted service node (Issuer Node) before joining the network. These institutions are classified according to their roles, endowed with access authorities, verify, confirm all transactions triggered by more than a single notary node in the network, and telecommunicate safely.

As medical institutions ultimately conduct a process on the condition of certification on a permissioned Blockchain network, security is reinforced. Patient information is created in blocks (Ob), it is added to the them after obtaining preliminary or secondary consent from patients. Before obtaining consents, patients can explicitly understand the purpose and what information is used. If they do not agree with sensitive information exchange, they can refuse the addition of blocks.

In case of registering patient information, it is encrypted with open keys of issuer node (group keys) and delivered in Service Node Model of Sharing Medical Data. Since patient

State	Patient Code	Patient Group Key	Patient Hash Length	Patient Hash Data	Encrypted Result Data (binary format)

(Figure 5) Format recorded on the Blockchain

information data is used with hash and saved in encryption, it guarantees integrity. Once created records shall not be revised and participants in a permission Blockchain network are only authorized to gain access to patient information by unlocking passwords with private keys.

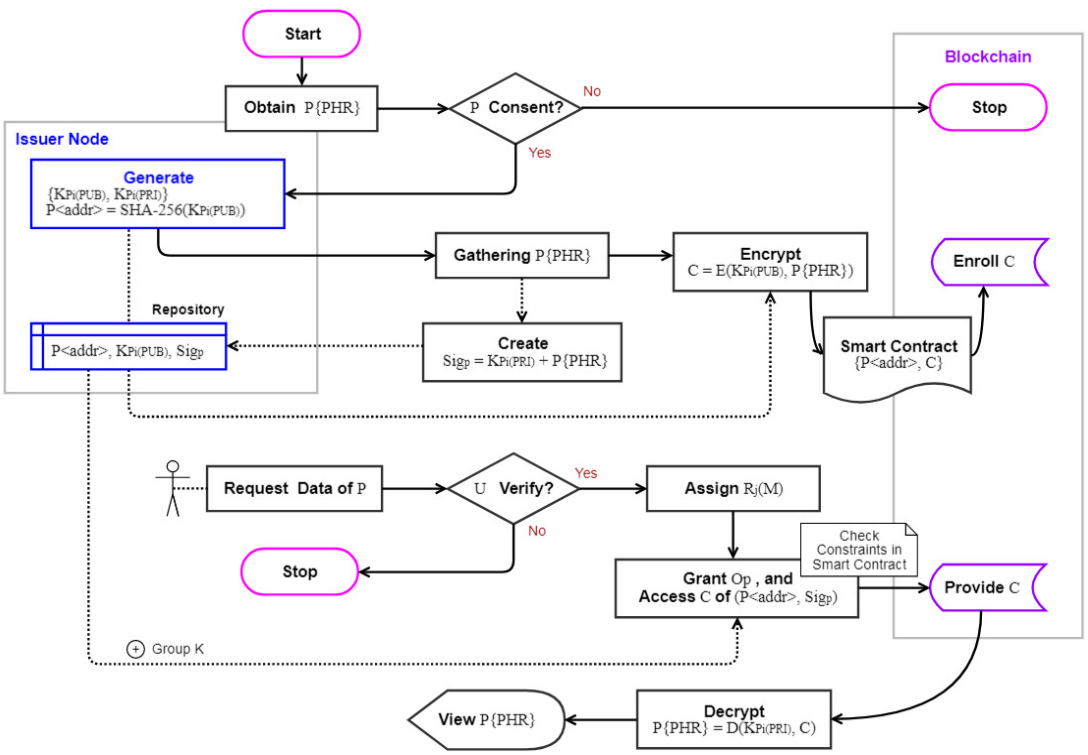
Users(U) are assigned to defined roles(R). The access to patient information is limited depending on their roles. For statistics and research such as researchers in relevant medical institutions, information identifying patients is announced with being eliminated condition. Regarding the other role, general hospitals can transfer patient information to the Blockchain without consents from patients, yet now permitted to open or form blocks. Operators(Op) provide ways to be accessible with patient information including opening, revision, deletion, use, exchange, and offer functions.

5. Result from System Application : Smart Contract

5.1 Design and Operation Plans

This paper presents methods with smart contracts if medical institutions request patient information based on this model. The procedure of proposal methods is comprised of collecting and registering patient information, certification of medical institutions, and sharing patient information.

When medical institutions like hospitals register patient information in patient models, patient information is encrypted with open keys and delivered. Other medical treatment information is delivered with binary values. Information processed for gathering patient information and service checks for available data by obtaining consents from patients under the legal protection. Patient's personal



(Figure 6) Design method based on TMSMD

information among consented data calculates hash value for integrity by performing SHA-256 hashing. Medical treatment information is encrypted with open keys in binary values and recorded on a Blockchain.

Medical institutions can get access to patient information as they undergo authorization process in order to use information recorded by patient models. After going through a preliminary procedure of receiving GK offered by a permissioned Blockchain, they are authorized to participate in the network.

Performing functions of medical institutions verified in terms of effectiveness vary according to the role of patient models. They can search patient information depending on conditions or read it by requesting single needed information.

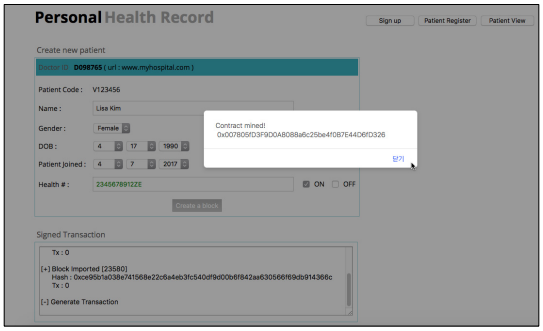
5.2 Realization and Test Environment

A server node and a client node were set to test-net environment in order to realize the movement procedure of the proposed model. A server node as realized environment enabled background to be operated with Ethereum-go language. For database, Ethereum Blockchain applied with Test-net was employed to save patient information. The application of node was realized by using Python language. Smart contract that sets conditions organized web applications with HTML and JavaScript based on Solidity. Moreover, patients' diagnosis information used in the test was produced based on dental information. Diagnosis records are saved as JSON formats.

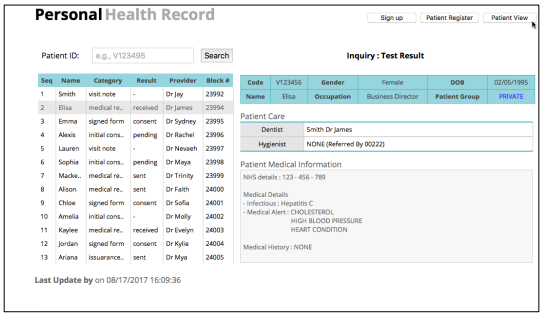
Figure 7 shows a page where patient information is added only authorized to certified medical institutes. If they write and upload medical treatment information and evidence materials, metadata on these contents is written on the Blockchain.

You can see patient information uploaded on the Blockchain in Figure 8 where only patients, doctors, and authorized medical institutions are admitted.

And in Figure 9, you can see this transaction of generation on the permissioned blockchain. The screen can be seen as patient diagnosis information by searching identification number of a certain patient on this page.



(Figure 7) Patient registration page



(Figure 8) Patient diagnosis information page

(Figure 9) Confirm transaction

6. Conclusion

In this paper, we introduced medical treatment exchange system for patients (customers) based on a Blockchain network. This system is a platform that encrypts and records patients' medical information by using this Blockchain and further enhances the security due to its restricted counterfeit.

This provides service to share medical information uploaded on the Blockchain to approved users through role-based access control. In addition, this paper presented results from the designed system complying with domestic laws by using the distributed Blockchain ledger and eventually granting preliminary approval for sharing information. This service will provide an independent information transaction and the Blockchain technology under test will be adopted in the medical industry.

Additional research on this Blockchain technology will continue and more studies will be performed to be safely and completely managed by individuals.

Reference

[1] D. Ivan, “Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records”, HealthIT Final Report, 2016. https://www.healthit.gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf

[2] J.-H. Hwang, “The Improvement and Trend of Personal Information Protection in Medical Organization”, Healthcare policy forum, Vol.14, no.4, 2016.

[3] ″Patient records leak-43 million South Koreans had their medical information leaked″, The Korea Herald, 2015. http://www.koreaherald.com/view.php?ud=20150726000368

[4] C. Zhou, Z. Cui and G.Y. Gao, “Efficient Identity-Based Generalized Ring Signcryption Scheme”, KSII Transactions on Internet and Information Systems, Vol. 10, no. 12, pp. 6116-6134, 2016. https://doi.org/10.3837/tiis.2016.12.022

[5] John D. Halamka, MD, A. Lippman and A. Ekblaw, “The Potential for Blockchain to Transform Electronic Health Records”, HBR WEBINAR, 2017. https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records

[6] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. https://bitcoin.org/bitcoin.pdf

[7] L. S. Sankar, M. Sindhu and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications”, 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 6-7 January, 2017.

[8] J.-S. Park, “On acquaintance, Blockchain is easier than Lego”, Ministry of Science and ICT Webzine, 2017. http://www.msip.go.kr/webzine/posts.do?postIdx=261

[9] Ministry of the Interior and Safety, “Act on the Protection of Personal Information”, 2011.

[10] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao and X. Du, M. Guizani, “MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain”, IEEE Access, vol.5, pp.14757 – 14767, 2017.

[11] Y. Liu, G. Liu, C. Cheng, Z. Xia and J. Shen, “A Privacy-Preserving Health Data Aggregation Scheme”, Transactions on Internet and Information Systems, Vol. 10, no.8, pp. 3852-3864, 2016. https://doi.org/ 10.3837/tiis.2016.08.023

[12] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management”, 2nd International Conference on Open and Big Data (OBD), 22-24 August, 2016.

[13] T.-S. Kim, W.-J. Kim, D.-Y. Lee and I.-K. Kim, “Patient information sharing system for suspected infectious disease based on Block Chain Network in FHIR”, Korea Information Science Society, pp. 2053-2055, 2016.

[14] “Could Blockchain be Good for our Health?”, 2017, https://teleos.wordpress.com/

[15] X. Liu, Y. Li, J. Qu and Y. Ding, “A Lightweight Pseudonym Authentication and Key Agreement Protocol for Multi-medical Server Architecture in TMIS”, KSII Transactions on Internet and Information Systems, Vol. 11, no. 2, pp. 924-944, 2017. https://doi.org/10.3837/tiis.2017.02.016

[16] LG CNS Security Consulting Team, “Is your information safe on medical industry?”, LG CNS Report, 2015, http://blog.lgcns.com/779

[17] A. Petre, “Blockchain Use Cases in Healthcare”, intelligentHQ, 2017, https://www.intelligenthq.com/innovation-management/blockchain-use-cases-in-healthcare/

[18] X. Liu, Y. Li, J. Qu and Y. Ding, ″A Lightweight Pseudonym Authentication and Key Agreement

Protocol for Multi-medical Server Architecture in TMIS", KSII Transactions on Internet and Information Systems, Vol.11, no.2, pp. 924-944, 2017.

◐ 저 자 소 개 ◑

Kyoung-jin Kim

2007 B.S. in Computer Science, Sungshin Women's University, Korea.
2009 M.S. in Computer Science, Sungshin Women's University, Korea.
2013 Ph.D. in Computer Science, Sungshin Women's University, Korea.
2017～present : Professor, Dept. of Convergence Security Engineering, Sungshin Women's University, Korea
Research Interest : Privacy protection, Security framework, Access control, Blockchain
E-mail : kyongjin@sungshin.ac.kr

Seng-phil Hong

1993 B.S. in Computer Science, Indiana State University, USA.
1994 M.S. in Computer Science, Ball State University at Indiana, USA.
1997 Ph.D. Candidate in Computer Science, Illinois Institute of Technology, USA.
2003 Ph.D. in Information Security, KAIST University, Korea.
1997～2005 Research and Development Center in LG-CNS Systems, Inc.
2005～present : Professor, Dept. of Convergence Security Engineering, Sungshin Women's University, Korea
Research Interest : Security Architecture, Privacy protection, E-business security, Blockchain, IoT security
E-mail : philhong@sungshin.ac.kr