Cloud-based Blockchain Technology for Personal Health

Sang-Young Lee

Namseoul University, South Korea sylee@nau.ac.kr

Abstract

The modern paradigm for healthcare has been changing from treatment to management. For the management, it is important to record information not only about diseases and their treatment processes but about routine and periodic health conditions. The environment of medical information is shifting from recording and saving into an EMR system to saving into PHR. Cloud computing means storing and accessing data and programs over the Internet instead of on a local hard drive. A Cloud is an appropriate alternative because it has an easy environment where the integrated PHR is easily built and processed while keeping the system under various EMR systems. The concept of the current medical paradigm has been changing from treatment to management. For the management, it is important to know the current health conditions, as the existing diseases and their treatment processes. The environment of medical information is shifting from recording to saving into PHR which is an integrated record of EMR information and subsidiary patients' health information. PHR is very easy to check patients' health conditions, which is suitable for customized medical services. This study provided how to apply blockchain technology to the medical field and utilize it for PHR applications. For these applications, it suggested architecture for gateway application of healthcare data to control and share PHR data more easily and securely.

Keywords: PHR, Blockchain, Healthcare, Framework

1. Introduction

The benefits of cloud computing are readily apparent when considering what is always required of Information Technology (IT): a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. PHR is for all information relating to personal health. Also, it is a concept that includes personal healthcare services, health information, and healthcare platforms. Its previous systems were Electronic Medical Records (EMR) and Electronic Health Records (EHR) which are medical information systems. While EMR is created and utilized in a single medical institution, HER is utilized in several medical information stored on EMR and HER is an important part of PHR. PHR has evolved from the initial model that checks and shares the integrated personal information scattered across a wide range of institutions and devices. And now, it has been developed as a model to provide useful services such as disease prevention and follow-up management connected with self-care, medical institutions, and insurance companies [3][4][5].

Article history:

Received (September 4, 2020), Review Result (October 9, 2020), Accepted (November 14, 2020)

In general, PHR is a "tool which provides a function to keep and manage entire health information of individuals or families throughout their lifetime. Google Health is a web platform to provide a free service developed by Google. With the platform centrally managed PHR, a patient can retrieve medical information and share it with his/her doctor. Also, the patient can edit and store medical information, insurance-related information, medical records, etc. with the computer at his home. To be specific, it can be used to input the user's PHR, provide health information relating to PHR (symptoms, causes, and treatments), upload PHR information via medical institutes, check drug interactions, search doctors/hospitals, and so on [6][7][8].

The modern paradigm for healthcare has been changing from treatment to management. For the management, it is important to record information not only about diseases and their treatment processes but about routine and periodic health conditions. The environment of medical information is shifting from recording and saving into an EMR system to saving into PHR. PHR is very easy to check patients' health conditions, which is suitable for customized medical services. However, the EMR systems were made of a different type in each medical institute, thereby being difficult to integrate the information into PHR [9][10]. A Cloud is an appropriate alternative because it has an easy environment where the integrated PHR is easily built and processed while keeping the system under various EMR systems. Also, medical information is sensitive information, and its security/safety problems can be resolved by the blockchain. If PHR is built in the Cloud using the blockchain, the medical system can be maintained, and the medical information can be widely applied. Moreover, the algorithm for data distribution processing using blockchain was applied for the high cost of managing data for each individual under the Cloud environment. This method minimizes the cost that is passed on to each person. In doing so, the medical information system is constructed, which will help provide a positive impact on the medical world and suitable medical services.

2. Related works

Blockchain is a data structure, which is composed of blocklists connected with chains. Such blockchain is distributed through peer-to-peer (P2P) networks with the latest version of all nodes. The block is a record of transaction data. Blockchain-based on Bitcoin is one of the distributed ledger technologies, which is a distributed, shared, and encrypted database that serves as an "irreversible and incorruptible repository of information". The block includes a header and body [11][12].

- A version of Block: It represents validation rules that are based on a series of blocks.
- Parent Block Hash: It is a 256-bit hash speed.
- Merkle Tree Root Hash: Hash of all the hashed of all the transactions.
- Timestamp: Currently, it represents the value for every second.
- nBits: it consists of a simple target hash.
- Nonce: It is a 4-byte field, which starts at 0 and is incremented for each hash.

In health-related fields, one of the typical applications of blockchain is the electronic medical record. This area is categorized into three different types: electronic record-centered EMR, interchange-centered HER, and private health record-centered PHR. In these fields, main research have been conducted to manage private medical or health-related data for the generation and storage of electronic documents. In practice, for blockchain in EMR, there have been various case studies carried out mainly on decentralization and immutability of the blockchain, data source, reliability, rigidity, contract, and security and privacy. This study

focused on how to easily share patient-centered data in studies on blockchain applications in diverse medical services to store and manage patients' EMRs. Especially, studies have been conducted to build a medical platform that can control patients' methods and share processes, and utilize the data [13][14].

In particular, in the application to manage healthcare data, blockchain has been introduced to apply the perfect technology to design a medical system. For easy and safe control to share data, this study suggested architecture for gateway applications of healthcare data. In short, it was to suggest blockchain technology using multi-step authentication which may protect and share medical data between different objects. Also, it suggested research scenarios relating to biometric and biomedical systems for the security of medical data. In this study, the Ethereum-based smart contract system was proposed to intelligently protect private medical records.

3. PHR and standards

The PHR-related standards are categorized into three types of exchanges Personal Health Devices (PHD), medical information devices, and Internet of Things (IoT) devices. Firstly, the PHD standard was established in the Institute of Electrical and Electronics Engineers (IEEE) 11073. It has been the ISO international standard by Standard Harmonization between International Organization for Standardization (ISO) and IEEE. ISO/IEEE 11073 PHD Group has continually enacted the device standard for individual health based on ISO/IEEE 11073-20601 which is a standard protocol to measure and transmit personal biometric information.

PHR-based medical information exchange is required to transmit private health information such as medical records, test results, etc. It is classified as shown in the following figure.

This includes standards of terms, code systems, protocols, and medical documents in the health and medical information field. For the term and code system, there are various kinds of standards: SNOMED-CT and UMLS are for the definition of terms, LOINC is for test code, ICD is for diagnostic code, and Rx Norm is for medicine code. For the protocol, there are standards: V2 and V3 of HL7, message standards, are for the exchange of medical information, DICOM for sending medical images, CCD of HL7, and Consolidated CDA for medical documents. For IoT, the standardization that is related to healthcare, including PHR, is on the way. OIC created the Healthcare Task Group and started to develop a standard of healthcare applications and services in the IoT environment. In 2018, oneM2M held an operation showcase by interlocking IoT standard platforms and existing healthcare standards. Recently, with the development of various IoT devices, including wearable devices such as activity trackers, heart rate measurement, etc., sleep monitoring devices, smart home devices, and so on, it is expected that there would be active discussions on the establishment of PHR-related healthcare standard for the future IoT.

Unlike the current system that uses the provider-centered EHR for management, PHR is a patient-centered application program that is managed and used by the patient. The real owner of the information accesses and manages his health information. The ultimate goal of PHR is to help patients securely and conveniently collect, track, and control their perfect health conditions. Also, the information provider manages hospital visit data, vaccination records, prescription records, and physical activity data collected from smartphone devices. From the PHR, patients can use their health information and control how to share the information. They can keep the accuracy of their health record and prevent potential errors in the data. Existing companies, such as Apple and Microsoft, have been trying centralized management through

solutions like Apple Health and Microsoft HealthVault. However, such approaches do not solve the problem to share key data, so they would also face similar obstacles to the heterogeneous EHR system. On the other hand, blockchain is possible to distribute controlled data. This study uses an algorithm agreed upon by various participants. For the participants, it guarantees widespread access and secure data distribution. Additionally, the patients can manage health data with a personal smart device via a service that is connected to the existing health system. Medical professionals have the following advantages:

- they control data access;
- they know the source of data;
- they'll let the patient know when the provider accesses the data;
- its data log is always transparent to the patient; and,
- the patient can search his health information anytime or anywhere.

PHR is defined as an internet-based tool that allows a person access to his health information all his life, for the people who need specific information. PHR will improve the quality of medical care because medical service users can make better decisions, it enables easier access to the required information, and it makes patients and medical teams communicate more effectively.

4. PHR using blockchain

A blockchain is a form of "distributed ledger, which stores a copy of trade in a computer system where different individual or corporate has controlled". In other words, the ledger, storing trade information, is saved in a digitalized unit of 'block'. Block consists of a body and header for storing trade information and cryptic code, respectively. Such blocks are distributed to the computer node of network participants, which is a block system. It functions as a mechanism of chain that if any new trade or changes in an existing trade, a new block is created and connected to the existing block system. An operational structure of the distributed ledger is determined and operated by a pre-established consensus algorithm.

In the blockchain system, blocks with a form of information are connected according to chronological order. The information input is not only saved in the corresponding block but also uploaded in all networks of P2P where the user wants to create a block. Once such information was verified by all users, the block is connected. The information about the created blocks is shared with the corresponding users. All types of information have been shared with all users. So, if someone wants to modify any codes in the blocks with a bad aim, it is not possible to change them without the permission of others. As a result, information gets more perfect structure along with the algorithm.

Blockchain utilized by BitCoin or Ethereum was a form of permissionless type, but currently, permission blockchain has also been proposed. A type of permissionless creates blocks by proof of work and mining process with no limitation of users. On the other hand, the permission form is operated by only authorized users without the mining process. The use of permissionless blockchain not only requires more time to upload blocks but also manages the network users. Regarding the construction of medical information system, permission blockchain is the most optimum configuration with advanced technologies for information integrity.

Blockchain technology has a lot of potential to change the Trust model in various industrial areas and business processes innovatively. However, the technologies of blockchain have been restricted in reality. For instance, the manufacturing industry does not want to share its independent technologies with other companies and the financial industry does not want to

leak out customers' information. On the other hand, the industries in distribution, insurance, and medical areas have expected to introduce blockchain technology into their business. If blockchain technology is introduced to the distribution business, loss or damage of products could be minimized due to the trackable delivery routes. The origin of the product is also identified clearly. In the case of the insurance industry, a new product fitted to the individual is designed based on the accident rate of the individual, the incidence of diseases, and lifestyle, resulting in a decrease in unnecessary loss of cost.

In the field of medical business, accurate treatment has been made by managing detailed information such as medical history, history of the accident, constitution, and medical history, providing better medical care. Moreover, the cost of unnecessary tests could be minimized through this management system, which reduces the patient's financial burden and increases confidence in medical treatment. It is expected that blockchain technology brings innovative changes in diverse areas such as health care, distribution, insurance, and the medical field.



Figure 1. PHR layer

A construction method of the PHR system, based on blockchain, is indicated as follows. A function of PHR should be implemented because security is the most important parameter. This study has been operated by an authorized author in a Cloud-based system exclusively for users (medical institutions and patients). They can be provided a private key for individually secured login. The system enables users to process the data by creating an API (Application Program Interface), resulting in the user's flexible data size. The cloud consists of a few layers, such as 'Layer 1' for patient information, 'Layer 2' for individual medical history with a form of blockchain, and 'Layer 3' for storing database based on standardized HL7 and KOSTOM in the individual patient. Layer 1 has a public key to identify patients who can find the location of the patient within the Cloud.

Layer 2 is composed of several nodes, designated by an individual user, for instance, a patient, medical institution, or pharmacy. When individual users update a block patient's

information, another node will be created and connected in the form of a chain. The complex node configuration enables to the construction of a perfectly secured system. Layer 3 is useful in verifying PHR and utilizing study materials by applying HL7 and KOSTOM for the construction of the standard database.

The users are authorized to update patients' medical information and save the data in both cloud and pre-existing servers simultaneously when they upload the corresponding block (patient information). The user can update the patient's information in the cloud. However, they can't track the patient's PHR since the coded address was recorded in the Header (information of block). Sometimes, a patient's PHR should be confirmed depending on the specific situation. In this case, you should ask for the patient's consent. Patient information in cloud DB can be used for a purpose of research. For this occasion, a new DB should be created by utilizing API and anonymizing the process of DB within the cloud. The researchers registered as authorized users can access the corresponding DB for purpose of the study and the history is recorded in DB.

5. Conclusions

The concept of the current medical paradigm has been changing from treatment to management. For the management, it is important to know the current health condition, as the existing diseases and their treatment processes. The environment of medical information is shifting from recording to saving into PHR which is an integrated record of EMR information and subsidiary patients' health information. PHR is very easy to check patients' health conditions, which is suitable for customized medical services.

Since blockchain technology was introduced, it has been easy to apply to general-purpose technologies in diverse industrial fields, including health-related areas. To apply the technologies to healthcare areas and leverage the latest ones, specific examinations and processes mapping with the relevant fields would be required.

This paper provided how to apply blockchain technology to the medical field and utilize it for PHR applications. For these applications, it suggested an architecture for gateway application of healthcare data to control and share PHR data more easily and securely.

Acknowledgments

Funding for this paper was provided by Nauseous University.

References

- Van Dierendonck, A. J., and B. Arbesser-Rastburg, "Measuring ionospheric scintillation in the equatorial region over Africa, including measurements from sbas geostationary satellite signals," Proc. ION GNSS, Long Beach, CA, Sept., (2004)
- [2] Pelgrum, W., Y. Morton, F. van Graas, P. Vikram, and S. Peng, "Multi-domain analysis of the impact on natural and man-made ionosphere scintillations on GNSS signal propagation," Proc. ION GNSS, Portland, OR, Sept., (2011)
- [3] Gunawardena, S., Z. Zhu, and F. van Graas, "Triple Frequency of front-end for GNSS instrumentation receiver applications," Proc. ION GNSS, Savana, GA, Sept., (2008)
- [4] Peng, S., and Y. Morton, "A USRP2-Based multi-constellation and multi-frequency GNSS software receiver for ionosphere scintillation studies," Proc. ION ITM, San Diego, CA, Jan., (2010)
- [5] Vikram, P., "Event-driven data collection system for studying ionosphere scintillation," MS thesis, Miami University, (2011)

- [6] T. Humphreys, M. Psiaki, P. Kintner, and B. Ledvina, "GPS carrier tracking loop performance in the presence of ionospheric scintillations," ION GNSS Long Beach CA, pp.156-167, Sept., (2005)
- [7] D. Xu, and Y. T. Morton, "A semi-open loop GNSS carrier tracking algorithm for monitoring strong equatorial scintillation," IEEE Transactions on Aerospace and Electronic Systems, vol.54, no.2, pp.722-738, Apr., (2018)
- [8] C. L. Rino, "The theory of scintillation with applications in remote sensing," Hoboken, NJ: IEEE and Wiley, (2011)
- [9] Y. Jiao, C. Rino, Y. Morton, and C. Carrano, "Scintillation simulation on equatorial GPS signals for dynamic platforms," ION GNSS+ Portland OR, pp.1644-1657, Sept., (2017)
- [10] Y. Jiao, D. Xu, Y. Morton, and C. Rino, "Equatorial scintillation amplitude fading characteristics across the GPS frequency bands," Navigation: Journal of The Institute of Navigation, vol.63, no.3, pp.267-281, (2016)
- [11] M. Zhang and J. Zhang, "A fast satellite selection algorithm: Beyond four satellites," IEEE Journal of Selected Topics in Signal Processing, vol.3, no.5, pp.740-747, (2009)
- [12] A. Peng, G. Ou, and G. Li, "Fast satellite selection method for multi-constellation global navigation satellite system under obstacle environments," IET Radar Sonar & Navigation, vol.8, no.9, pp.1051-1058, (2014)
- [13] McGhin T, Choo K, Liu C, and He D., "Blockchain in healthcare applications: Research challenges and opportunities," J Netw Comput App, pp.62-75, (2019)
- [14] Agbo CC, Mahmoud QH, and Eklund JM., "Blockchain technology in healthcare: A systematic review," Healthcare (Basel) vol.4, no.7, pp.123-134, (2019)

This page is empty by intention.