An EMR Sharing and Privacy Protection Mechanism Based on Medical Consortium Blockchain

Zhiyong Li
Information Technology Center
Honghe University
Mengzi, Yunnan, China
lizhiyong@uoh.edu.cn

Lihui Zhang
Academic Affairs Office
Yunnan Normal University
Kunming, Yunnan, China
13888082291@126.com

ABSTRACT
The sharing of Electronic Medical Record(EMR) plays an important role in improving the quality of medical care, reducing costs and enhancing patient experience. But it also raises issues such as privacy leaks and uncontrollable data dissemination. To address these issues, we propose an EMR sharing mechanism based on the medical consortium blockchain. The hospital joins the medical consortium blockchain as a node, storing and maintaining the EMR data it generates. At the same time, the index of EMR is stored on the medical consortium blockchain for query, call and access control. Before accessing the EMR, the patient's authorization needs to be obtained on the medical consortium blockchain. Compared with the traditional mechanism, this mechanism has certain advantages in privacy protection, access control and data security while implementing EMR sharing.

CCS Concepts
• Security and privacy→Human and societal aspects of security and privacy→ Privacy protections.

Keywords
EMR sharing; EHR sharing; blockchain; privacy protection

1. INTRODUCTION
An Electronic Medical Record (EMR), or Electronic Health Record (EHR), is the systematized collection of patient and population electronically-stored health information in a digital format[1]. These records can be shared across different health care settings. EMR may include a range of data, including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal statistics like age and weight, and billing information.

Cloud computing is an on-demand resource usage mode. It configures network, server, storage, application software, and services as a shared pool of computing resources and provides users with on-demand use. Cloud computing has the advantages of dynamic resource expansion, improved resource use efficiency, convenient maintenance and management, and significant reduction in operation and maintenance costs[2]. It has become a mainstream computing resource provision method. EMR data generated by hospital can be stored, managed, and maintained through cloud computing. Considering the security, confidentiality, and availability of EMR data, hospitals often choose to use their own private storage cloud for data storage.

EMR sharing benefits both hospitals and patients. For hospitals, it can help hospitals improve operational efficiency, reduce operating costs, enhance patient experience, avoid medical responsibilities, and increase the popularity of hospitals. For patients, it can help patients manage their own health, use medications precisely, and reduce medical costs[3-5]. However, there are two problems with the sharing of EMR data: First, after EMR are shared, the reproducibility of electronic data will lead to uncontrollable data transmission and even malicious transmission, which is not conducive to the protection of patients' privacy[6]. Second, the ownership issues, EMR Ownership and control should be attributed to the patient who produced the EMR, not to the hospital. Hospitals, as the generating agency of EMR data, have the rights and obligations to store, operate, maintain, and manage these EMR data. Also, hospitals have the responsibility of adopting corresponding security policies to protect the integrity, confidentiality, and availability of the EMR data. However, hospitals are not the actual owners and controllers of these EMR data, and do not have the right to share, disseminate, and disclose these EMR data. The patient who produces the EMR data should be the actual owner and controller of the data. In the traditional way, since the storage and operation of EMR data is the responsibility of the hospital, the data is invisible, unmanageable and uncontrollable to the patient. The patient does not know which EMR data the hospital has stored, does not know whether the EMR data stored in the hospital is used by the hospital, does not know whether the EMR data stored in the hospital is shared by the hospital, and does not know whether the EMR data stored in the hospital has been leaked, even it cannot be traced when EMR data had been leaked.

To solve the above problems, in this paper, combining the laws and regulations of China and the status quo of hospitals, we propose an EMR data sharing mechanism based on consortium blockchain. This mechanism does not change the original network topology, storage mode and security policy of the hospital. It uses of decentralized, distributed, tamperproof and traceable features of the blockchain enable the sharing of EMR data within a medical consortium blockchain. The hospital joins the medical consortium blockchain, stores the EMR data generated by the patient's visit on self-built private storage cloud, and in accordance with relevant national laws and regulations for data

ICCTA 2020, April 14–16, 2020, Antalya, Turkey

ACM ISBN 978-1-4503-7749-2/20/04…$15.00
https://doi.org/10.1145/3397125.3397153

security protection work. At the same time, the index of EMR is stored on the medical consortium blockchain, and smart contract function is used to implement EMR call, share, and authorization. When patients go to other hospitals see a doctor, they can call their own EMR data through private keys; When other hospitals or third-party organizations need access to patient's EMR data, they must be authorized by the patient. To protect privacy, patients should choose to desensitize and anonymize their own EMR data before authorizing third parties to use it.

2. RELATED WORK

In 2015, Guy Zyskind et al.[7] proposed a personal data management system in which decentralized users have ownership and control of their own data. Through introduce blockchain technology, the system implements the automatic access control management protocol without the need of third-party support. Unlike the Bitcoin system, the so-called transaction objects in this system are not financial data, but are instructions and operations such as storing, querying, and sharing data. The system has good effect on data storage and query, but it is not ideal for data operation. In 2015, Guy Zyskind et al.[8] proposed using blockchain, hash tables, and secure multi-party computations to construct the Enigma system, it can implement autonomous control and privacy protection of individual user data without requiring a trusted third party. In 2016, Xiao Yue et al.[9] designed a medical data gateway protection model, patients can achieve shared access control of medical data stored on the blockchain by using a mobile app, enables patients to own, control, and supervise their own EMR data without the need for a third-party authority. In 2016, Asaph Azaria et al.[10] proposed an EMR processing system based on blockchain technology, in which patients can audit, operate, access, and share their own medical data through comprehensive and unchangeable log records. The system also supports scientific research institutes to obtain anonymous EMR through "mining". In 2017, Tsung-Ting Kuo et al.[11] demonstrated the application of blockchains in biomedicine and healthcare, pointed out that blockchains will play a major role in the exchange and sharing of EMR. In 2017, Magyar, Gábor[12] proposed how blockchain technology can help solve the problem of secure data storage while ensuring the availability of data. The three attributes of the blockchain: decentralization, without the need for intermediary and encryption protection, these attributes provide a new method of securely storing patient data while making it publicly available under supervision. In 2017, Rifi et al.[13] proposed that the exchange of key data such as remote access to EHR and body sensor data brings new problems and challenges. Privacy and confidentiality are of great concern, Scalability and interoperability are also important issues that should be considered. In 2018, Guo, Rui et al.[14] presented an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no information other than the evidence that he has attested to it. Furthermore, there are multiple authorities without a trusted single or central one to generate and distribute public/private keys of the patient, which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain.

3. MEDICAL CONSORTIUM BLOCKCHAIN

Blockchain technology originated from Bitcoin[15], but its application is far more than digital currency. It can be used for cross-border payment, smart contracts, electronic notarization, data traceability, privacy protection, etc. It can also be combined with the Internet of Things, big data, cloud computing, etc., resulting in great economic and social benefits. Narrowly speaking, a blockchain is a chained data structure in which data blocks are connected in a sequential manner in a time sequence, and cryptographically ensured an irreversible and unforgeable distributed ledger. Broadly speaking, blockchain technology is a new distributed infrastructure and computing paradigm, which uses blockchain data structures to verify and store data, uses distributed node consensus algorithms to generate and update data, uses cryptographic methods to secure data transmission and access, uses smart contracts compose of automated script code to Program and manipulate data[16]. Blockchain is consider to be a subversive innovation of computing models following mainframes, personal computers, and the Internet, and it is likely to cause a new technological innovation and industrial change globally [17-18].

Blockchain system is generally divided into public blockchain, private blockchain and consortium blockchain according to different application scenarios and design system[17]. Among them, each node of the consortium blockchain usually has an entity organization corresponding to it, and can join and withdraw from the network after authorization. Each organization organizes alliances related to interests to jointly maintain the healthy operation of the blockchain.

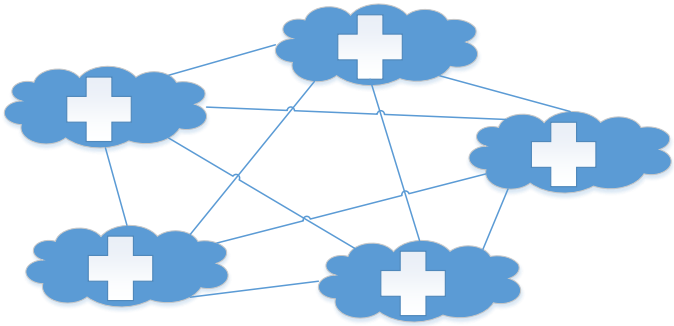

Figure 1. Medical Consortium Blockchain

Considering the existence of bottlenecks in performance, capacity, privacy, isolation, and expansion of public blockchain, and the risk of being controlled by a single agency of private blockchain, we chose to use the consortium blockchain to achieve EMR data sharing. As shown in Figure 1, hospitals form a medical consortium blockchain to share EMR data. The hospitals in the medical consortium blockchain are equal in status, maintain and manage the EMR data generated by its own patient. To ensure the consistency of the data of each hospital node in the medical consortium blockchain, we adopt the POS(Proof of Stake) consensus mechanism—only with the consent of more than half of the nodes in the medical consortium blockchain, and the operations such as access, invocation, and authorization of EMR data can be executed. It should be point out that all nodes will witness the implementation process and record it on the medical consortium blockchain.

4. DESIGN AND IMPLEMENTATION

The EMR usually includes two parts: patient information and medical information. The patient information includes a name, an ID number, a home address, and hospitalization information. The medical information includes a doctor's prescription, medical information, blood analysis results, and a medical examination

report. Because EMR data contains a large amount of patient's privacy information, once it is leaked, it will infringe on the privacy of patients, cause public opinion or social pressure on patients, bring stress and worry to patients. What is more serious is that EMR data may be acquired by foreign research institutions and used to analyze Individual physical conditions and ethnic information, thereby endangering national security.

At the national level, Article 40 of the "The Cybersecurity Law of the People's Republic of China" stipulates that "Network operators shall keep strict confidentiality of user information they collect, establish and improve a user information protection system.", Article 42 "Network operators not be allowed disclose, falsify, or destroy personal information they collect; Network operators also not be allowed provide personal information to others without the consent of the producer of the information. However, after processing, no specific individuals can be identified personal information, and the personal information cannot be restored after processing should be excluded." "Network operators should take technical measures and other necessary measures to ensure the security of the personal information they collect, and prevent the information from being leaked, damaged or lost. In the event of the occurrence or possible occurrence of personal information disclosure, destruction or loss, the network operator shall immediately take remedial measures, inform the user in time according to regulations and report to the relevant competent authority." "The Cybersecurity Law of the People's Republic of China" stipulates that hospitals have the obligation and responsibility to protect patients' EMR data [19].

To meet the national requirements for data management and maintenance, hospitals generally adopt strict security policies to protect EMR data. Figure 2 shows the network topology of a hospital. In the figure, we can see that the entire hospital network is divided into two areas: the hospital Internet area and the hospital business area. And the hospital Internet area is interconnected with the INTERNET, but the hospital business area is not interconnected with the INTERNET. The EMR data generated by the patient visit is stored in the hospital private storage cloud in the lower left corner of the “hospital business network area”. The two areas are separated by a GAP-a technology that enables two or more networks to realize secure data transmission and resource sharing under the condition of disconnected through dedicated hardware, to achieve security isolation between the two areas and provide moderately controllable data exchange, so ensure the security of EMR data stored in the hospital service area. If hackers on the INTERNET want steal EMR data stored in the private storage cloud in the hospital, they must break four firewalls, GAP, IPSs, and virus gateways. This is an almost impossible task.

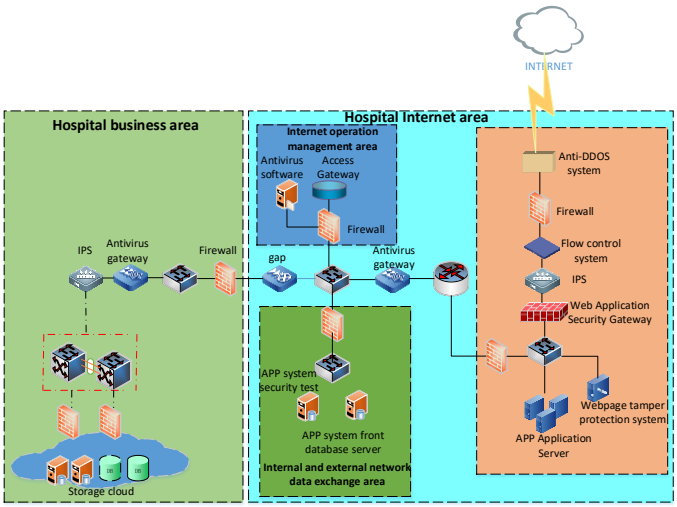

Figure 2. A Hospital Network Topology

Now we analyze the data flow of EMR. As shown in Figure 3, when patient go to the hospital for treatment and check, it generates EMR data, then the hospital stores the EMR data in its private storage cloud. At the same time, the index of EMR is stored on the medical consortium blockchain, and smart contract function is used to implement EMR call, share, and authorization. Here, we assume that when the EMR data is transferred internally in the hospital, the hospital is in accordance with relevant national laws and regulations, such as "The Cybersecurity Law of the People's Republic of China" and “General Data Protection Regulation”(EU, European Union)[20], to ensure the confidentiality, integrity and availability of EMR data during production, storage, transmission and calculation process.

Figure 3. Data flow diagram of EMR

In Fig. 3, since the EMR data of the patient is encrypted using the key of the patient, the patient's right to control the EMR data is guaranteed, and only the patient has the right to check, invoke, and authorize the own EMR data. When a user authorizes a hospital or a third-party organization to access and invoke their own EMR, we can use the traceability of the blockchain to enable patients to monitor and control their own EMR. Patients can decide when, how, and how much of their own EMR data is shared and open. Patients and hospitals can also perform operations such as desensitization, pseudonym, and anonymization on EMR data before sharing, further protecting personal privacy.

In general, the establishment of a medical consortium blockchain to sharing EMR data brings three advantages:

(1) Date security

In the medical consortium blockchain, EMR data is stored in each hospital node to implement distributed storage and improve the system's anti-attack capability. For example, Hospital A retrieves through the index database and knows that Hospital B has this

medical record. After obtaining the patient's authorization on the medical consortium blockchain, it can go to Hospital B to retrieve the medical record. Hospital A can see the medical record, but the data storage structure has not changed. If a hacker breaks through the Hospital A 's database, he can only get the medical record of the Hospital A and cannot threaten all the hospitals.

(2) Protect personal privacy

In terms of privacy protection, it is mainly achieved through the following measures: First, in the medical consortium blockchain, member hospitals maintain the same “ledger”, that is, the index of EMRs, patient access control information, access records, etc. However, no member hospital has the right to manage all the data on the medical consortium blockchain; Second, because the read and write authority is limited, only the hospital in the consortium blockchain can read and write EMR data under the authorization of the patient; Third, before sharing EMR data, patients can perform operation such as desensitization, pseudonymization, and anonymization to ensure personal privacy is not been leaked. Finally, we can introduce homomorphic encryption ideas for privacy protection. Considering such a scenario, hospitals need to share data with each other to perform statistical research on certain types of diseases. The hospital first needs to apply for authorization to the patients on the blockchain. After being authorized by the patient, each hospital conducts statistical operations on the data stored on the local private storage cloud, and only shares the results of statistical calculations, to achieve the purpose of privacy protection.

(3) Data traceability

The shared records and related operations generated in the medical consortium blockchain will be recorded, and these records can only be written and cannot be tampered with. All nodes in the consortium blockchain will witness, which can be used for data traceability. For example, when a user authorizes a hospital or a third-party organization to allow access to its own EMR data, we can use the traceability of the blockchain to enable patients to monitor and control their own EMR. Patients can decide when, how, and how much of their own EMR data is shared and open.

5. CONCLUSION

As a multi-party maintenance, full backup, and information security distributed accounting technology, blockchain brings innovative ideas to medical data sharing. Through the introduction of the medical consortium blockchain, this mechanism has the following advantages: First, distributed storage improves the anti-attack capability; second, only members of the consortium blockchain can read and write data and send transactions, enhancing privacy protection; Third, access control mechanisms can be implemented using smart contracts, reduces costs and solves trust problems. And reading and writing of EMR data must be authorized by the patient to achieve patient ownership and control over their own EMR data; Finally, Patient’s EMR index is stored in a block for sharing, which makes it difficult to tamper with and traceable, enhance the security of data sharing and improve the efficiency of data sharing.

In the future work, the management and authorization of patients' rights will be further studied to provide more fine-grained authority control mechanisms.

6. REFERENCES

[1] HER: electronic health record, URL:https://en.wikipedia.org/wiki/Electronic_health_record.

[2] Baidu Encyclopedia, "cloud computing", URL:https://baike.baidu.com/item/cloud computing/9969353?fr=aladdin

[3] Kemkarl, O. S., and D. P. B. Dahikar. "Can electronic medical record systems transform health care? potential health benefits, savings, and cost using latest advancements in ict for better interactive healthcare learning." International Journal of Computer Science & Communication Networks 2, no. 3/6 (2012): 453-455.

[4] Jothi, Neesha, and Wahidah Husain. "Data mining in healthcare–a review." Procedia Computer Science 72 (2015): 306-313.

[5] Founder Securities,"Medical Reform Releases Medical Big Data Business Value", URL: http://doc.mbalib.com/view/5141abebd44bd5daea9cb5dc5ff39494.html.

[6] Zhou Shuigeng, Li Feng, Tao Yufei, and Xiao Xiaokui. "A Survey of Privacy Protection for Database Application." Chinese Journal of Computers, 2009，32（5）：847-861.

[7] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In Security and Privacy Workshops (SPW), 2015 IEEE, pp. 180-184. IEEE, 2015.

[8] Zyskind, G.; Nathan, O.; Pentland, A. Enigma: Decentralized Computation Platform with Guaranteed Privacy. arXiv 2015.

[9] Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare Data Gateways:Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J. Med. Syst. 2016, 40, 218.

[10] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. International Conference on Open and Big Data (OBD). Vienna, Austria: IEEE; 2016:25–30.

[11] Kuo, Tsung-Ting; Kim, Hyeon-Eui; Ohno-Machado, Lucila.Blockchain distributed ledger technologies for biomedical and health care applications JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION Volume: 24 Issue: 6 Pages: 1211-1220 Published: NOV 2017

[12] Magyar, Gábor. "Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management." In Neumann Colloquium (NC), 2017 IEEE 30th, pp. 000135-000140. IEEE, 2017.

[13] Rifi, Nabil, Elie Rachkidi, Nazim Agoulmine, and Nada Chendeb Taher. "Towards using blockchain technology for eHealth data access management." In Advances in Biomedical Engineering (ICABME), 2017 Fourth International Conference on, pp. 1-4. IEEE, 2017.

[14] Guo, Rui, Huixian Shi, Qinglan Zhao, and Dong Zheng. "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems." IEEE Access 776, no. 99 (2018): 1-12.

[15] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[16] Ministry of Industry and Information Technology, "China Blockchain Technology and Application Development White Paper", URL:http://www.fullrich.com/Home/Index/newsDetail/id/324/newstype/

[17] Swan M. Blockchain: Blueprint for a New Economy. USA:O'Reilly Media Inc., 2015.

[18] Yuan Yong and Wang Feiyue. "Development Status and Prospect of Blockchain Technology" [J]. Journal of Automatica Sinica (JAS),2016,42(4):481-49414.

[19] National People's Congress Standing Committee, Cybersecurity Law of the People's Republic of China.URL: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

[20] The General Data Protection Regulation(GDPR), URL: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation.