Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.039749
Article

Deletion and Recovery Scheme of Electronic Health Records Based on Medical Certificate Blockchain

Baowei Wang[1,2,*], Neng Wang[1], Yuxiao Zhang[1], Zenghui Xu[1] and Junhao Zhang[1]

[1]School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, Jiangsu, China
[2]Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing, 210044, Jiangsu, China
*Corresponding Author: Baowei Wang. Email: wbw.first@163.com
Received: 14 February 2023; Accepted: 17 April 2023; Published: 09 June 2023

Abstract: The trusted sharing of Electronic Health Records (EHRs) can realize the efficient use of medical data resources. Generally speaking, EHRs are widely used in blockchain-based medical data platforms. EHRs are valuable private assets of patients, and the ownership belongs to patients. While recent research has shown that patients can freely and effectively delete the EHRs stored in hospitals, it does not address the challenge of record sharing when patients revisit doctors. In order to solve this problem, this paper proposes a deletion and recovery scheme of EHRs based on Medical Certificate Blockchain. This paper uses cross-chain technology to connect the Medical Certificate Blockchain and the Hospital Blockchain to realize the recovery of deleted EHRs. At the same time, this paper uses the Medical Certificate Blockchain and the InterPlanetary File System (IPFS) to store Personal Health Records, which are generated by patients visiting different medical institutions. In addition, this paper also combines digital watermarking technology to ensure the authenticity of the restored electronic medical records. Under the combined effect of blockchain technology and digital watermarking, our proposal will not be affected by any other rights throughout the process. System analysis and security analysis illustrate the completeness and feasibility of the scheme.

Keywords: Electronic health records; cross-chain; medical certificate blockchain; data deletion and recovery

1 Introduction

An Electronic Health Record (EHR) collects, creates and stores health records electronically. It is an upgraded version of patient paper records. It contains patient identification information, diagnosis information, medical history details, and medication information [1]. EHRs facilitate the patients, doctors, hospitals, and other stakeholders to maintain valuable data and medical records [2]. The sharing of EHRs allows doctors to see the history of previous treatments when patients are seen, so that previous diagnoses and treatment results can be combined to provide a more

comprehensive and accurate analysis of the condition, resulting in a more efficient treatment plan for the patient. Blockchain is a distributed ledger with the technical features of decentralization, immutability, traceability, and unfalsifiability [3], it is a new technology that can be utilized to boost the security. It is a decentralized peer-to-peer network with no central authority [4]. Started initially as a decentralized financial tool, the current iteration of blockchain technology aims to expand the utilities of this technology beyond the financial market, and well into healthcare industries [5]. Thanks to the rise of blockchain, much of the public, including medical professionals, have been able to glimpse a technology that may improve some parts of the healthcare data puzzle [6]. The sharing of EHRs based on blockchain provides a new model for health information exchange and new solutions for privacy protection and data sharing. To a great extent, it improves the security as well as the efficiency of EHRs. In the current state of affairs, however, patients are seen in different hospitals and the patient's EHRs are scattered across different organizational structures. Blockchains of different hospitals may be heterogeneous and data may be difficult to share. In order to meet the communication of heterogeneous blockchains, the cross-chain technology of blockchain is an important technical means to realize the interconnection of blockchains and improve the interoperability and scalability of blockchains [7].

Patient privacy regulation and improper resource sharing risks limit access to EHRs medical data for research and public health purposes [8]. In addition, the General Data Protection Regulation implemented by the European Union gives the data subject the right to request the correction or erasure of data relating to the data subject, or the right to restrict or refuse the processing of the personal data. Therefore, patients have the right to request the deletion of EHRs stored on the hospital's blockchain. After the EHRs is deleted on the hospital blockchain [9], the EHRs will not be able to be shared. At the same time, in most Electronic Health Record systems, only authoritative institutions such as hospitals have EHRs of patients. If there is a dispute between the hospital and the patient, the hospital that owns the data has an advantage, which is unfair to the patient. Therefore, this paper designs a Medical Certificate Blockchain to store the EHRs of patients. Not only can patients have their own personal EHRs but also can share their Personal Health Records with any institution with the patient's permission.

Consolidated-Clinical Document Architecture (C-CDA) has been one of the default export formats for all certified EHRs-that is, US EHRs that comply with the Promoting Interoperability Programs standard-since 2014's Meaningful Use Stage 2 requirements [10]. C-CDA documents are generally represented in XML. They can include structured information like a medication list. They're also good at capturing unstructured information, like images [11]. However, Nowadays, with the rapid development of advanced technologies, an illegal copy of digital documents can be easily generated. If the EHRs are tampered with, it will lead to disputes between doctors and patients. Therefore, it is particularly important to verify the attribution of recovered EHRs. Therefore, our scheme based on XML EHRs system [12] comprehensively utilizes blockchain and digital watermarking technology to realize copyright protection and authentication of EHRs.

We propose an Electronic Health Record deletion and recovery scheme based on the Medical Certificate Blockchain. In this scheme, patients have the right to delete their EHRs stored in the hospital after diagnosis and treatment. When the patient goes back to the hospital for a follow-up visit, there is no EHR of the patient's previous diagnosis for reference. We use prominent cross-blockchain technology to achieve the goal of Electronic Health Record deletion and recovery. Our work can be summarized in the following aspects:

1. We use the Medical Certificate Blockchain to store the Personal Health Records of patients generated in different medical institutions. Personal Health Records are one form of EHRs. The uniqueness of the Personal Health Record is that it records the EHRs generated by patients in different medical institutions. Only the patients themselves can manage and share their health information.

2. We use cross-chain technology to enable EHRs to be shared between the Hospital Blockchain and the Medical Certificate Blockchain to achieve recovery after deletion of EHRs.

3. We incorporate digital watermarking technology to implement EHRs copyright protection to distinguish records from different hospitals and to ensure the authenticated authority of the recovered EHRs.

The rest of the paper is organized as follows: Section 2 summarizes the main related work of sharing of EHRs and copyright of EHRs; Section 3 presents the proposed scheme; Section 4 demonstrates and analyzes the performance of the proposed scheme; Section 5 summarizes the work of the paper.

2 Related Work

2.1 Sharing of EHRs

For the open electronic medical environment, EHRs are shared in different hospitals, and many scholars have successively proposed solutions to different problems. Blockchain technology provides a secure distributed framework for trusted sharing of EHRs with its decentralized and non-tamperable features. Exceline et al. [13] proposed a consortium blockchain-based cloud-stored electronic health record is which provides data integrity, data privacy, storage scalability, and fine-grained access control. Cloud computing has proved its value through the widespread practice these years [14]. Alsayegh et al. [15] propose a secure, blockchain-based EHRs sharing system. After receiving the data owner's authorization, the data requester can use the data provider's keyword search to discover relevant EHRs on the EHRs consortium blockchain.

The above methods are all shared in the consortium chain. It does not consider that hospital blockchains may be heterogeneous, nor that EHRs are private data. If the EHRs stored in different medical institutions are not deleted in time, it is likely to lead to unauthorized data access, resulting in the disclosure of private information [16]. Patients have the right to request the deletion of EHRs stored in hospitals. After the EHR is deleted, it cannot be shared. Cao et al. [9] proposed a cross-blockchain based Electronic Health Record privacy-preserving scheme, which allows patients to delete EHRs data from the hospital blockchain.

Although the existing solution satisfies the requirement of the patient to delete the EHRs stored in the hospital, after the deletion, the patient will come back for a follow-up visit again, and there is no historical diagnosis record, which will add unnecessary trouble to the treatment. Therefore, it is necessary to realize the deletion and recovery of EHRs. We design a Medical Certificate Blockchain so that the stored Personal Health Records can be shared at any time with the patient's permission.

Data recovery has been extensively studied in the past few years, and with the development of Internet technology, Cloud computing has large data centers, which provide certain benefits for data backup as well as data recovery [17]. But sharing data with a cloud provider may result in a loss of full control over the data, and in the event of any failure of the cloud provider, the security of the stored data will not be guaranteed. Therefore, this paper is based on the cross-chain technology of blockchain to realize the recovery of EHRs.

2.2 Copyright Protection for EHRs

Digital copyright protection can be divided into copyright protection methods based on encryption technology and copyright protection methods based on digital watermarking technology. The copyright protection method based on cryptography has the disadvantages of poor security, poor circulation and weak protection. However, the digital watermark always plays a protective role for the original carrier information. When the copyright needs to be verified, it can be extracted from the carrier information and the protection period is permanent.

To sum up: In the digital watermark prevention technology for copyright infringement, watermark technology is considered to be an important technology to overcome data protection problems and verify the relationship between data ownership [18]. The current digital watermarking technology is divided into traditional watermarking technology and digital watermarking technology based on deep learning. Combined with the actual medical background, traditional digital watermarking technology has the advantages of less computational complexity, faster speed, and better watermark robustness than deep digital watermarking technology. Therefore, this paper uses digital watermarking technology to protect the copyright of EHRs.

3 Deletion and Recovery Scheme of EHRs

As shown in Fig. 1. This section aims to present an architecture for deletion and recovery scheme of EHRs based on Medical Certificate Blockchain. Table 1 shows the notations involved in the proposed scheme.

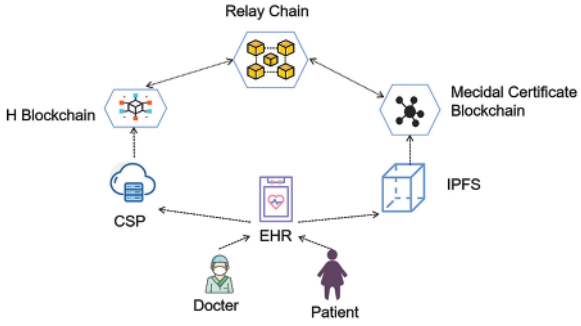

Figure 1: Proposed architecture

Table 1: Some notations used blow

Notations	Description
P	Patient
D	Doctor
E	HER
E’	Encrypted HER
IPFS	Used to store EHR uploaded to the medical certificate blockchain
H Blockchain	Hospital Blockchain. Each hospital has its own hospital blockchain

(Continued)

Table 1: Continued

Notations	Description
CSP	Cloud Service Provider. Store the EHR that need to be uploaded to the hospital blockchain

3.1 Creation of EHRs

Every time patient P goes to hospital H for treatment, he registers his medical treatment number with his ID number, and the password is set by the patient. When visiting a doctor, the patient needs to provide the medical treatment number and enter the password. Only in this way, the doctor D can create or query the patient's Electronic Health Record E in the hospital system. Any behavior of doctor D on Electronic Health Record E will be recorded by the hospital system.

3.2 Storage of EHRs

The entire process of storing EHRs is shown in the Fig. 2.

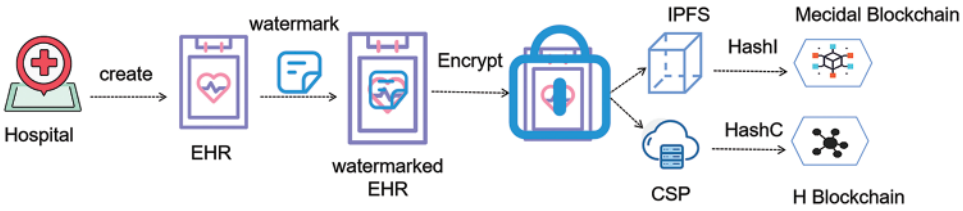

Figure 2: The entire process of storing EHRs

As a valid certificate, the EHR comes from different hospitals, and the generated EHR needs to be protected by copyright, so the generated EHRs E are uploaded to the Electronic Health Record watermark embedding terminal.

In order to reduce the storage burden of the blockchain, the encrypted EHR E' is uploaded to the Cloud Service Provider (CSP), the hash value Hash C is obtained, which is packaged as a block and uploaded to the hospital blockchain.

We have designed a Medical Certificate Blockchain to store the EHRs generated by individual patients in any medical institution. The storage process is: upload the encrypted Electronic Health Record to the IPFS distributed P2P storage network to obtain the unique hash value Hash I. According to the patient's request, the doctor packs the obtained hash value into a block and uploads it to the Medical Certificate Blockchain.

3.3 Patients Demand Deletion of Hospital's Blockchain's EHRs

EHRs involve a large amount of private data of patients. In order to ensure the safety of EHRs and protect the rights of patients, patients will delete the EHRs stored by CSP after the treatment, which can be found according to the index hash value Hash C. In this way, the patient's EHRs cannot be queried in the hospital blockchain, which satisfies the patient's rights.

3.4 The Hospital Requests to Recover Historical EHRs

When a patient goes to the hospital for a follow-up visit, the doctor in the hospital needs to view the historical electronic health to analyze the condition. Since medical information is stored in the Medical Certificate Blockchain, with the permission of the patient, the hospital blockchain initiates a cross-chain transaction. After the cross-chain is initiated successfully, the hash value Hash I shared by the Medical Certificate Blockchain is obtained. According to Hash I, patients' encrypted EHR can be found in IPFS. After relevant decryption operations, the patient's EHR are obtained. Fig. 3 shows the process of restoring EHRs based on cross-chain technology.

1. With the permission of the patient, the H Blockchain sends requests for cross-chain instructions.
2. The Medical Certificate Blockchain receives the transaction information, executes the corresponding cross-chain transaction, and sends the message Hash I to the H Blockchain.
3. The medical certificate block link receives the transaction information and executes the corresponding cross-chain transaction.
4. The H Blockchain obtains the Hash I value of the IPFS address list.
5. The hospital searches the IPFS list for information based on the Hash I value.
6. The hospital obtains the encrypted Electronic Health Record E', decrypts it, the patient's watermarked Electronic Health Records can be obtained finally.

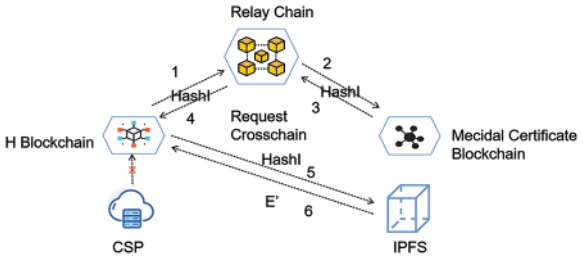

Figure 3: The process of restoring EHRs based on cross-chain technology

According to the entire process of storing EHRS, decrypted EHRs are watermarked. Submit the watermarked EHR to the watermark extraction end of the Electronic Health Record and finally the watermark is obtained.

The hospital compares the extracted watermark with the previously embedded watermark to ensure the security of the EHR, and confirms the copyright of the EHR according to the content of the watermark. Finally, the deletion of the electronic health record can be restored.

4 System Analysis

In order to ensure the feasibility and efficiency of the scheme, we analyze the system.

4.1 Security Analysis

The entire system is based on cross-chain technology. When the Hospital Blockchain and the Medical Certificate Blockchain are cross-chained, different security mechanisms, different consensus algorithms, and different privacy requirements of heterogeneous blockchains need to be considered. Otherwise, the overall security of the blockchain cross-chain will be affected. If any heterogeneous

blockchain has a unilateral security problem, relay chain will detect the abnormality of the application chain and refuse to execute transactions related to this chain. In other words, it's safe.

The system stores the hash value of the patient's EHRs on the blockchain to ensure that the data is not tampered with. Among them, the most critical is to adopt digital watermark-based technology for encryption and copyright authentication to ensure the security of data during transmission.

4.2 System Performance Analysis

We conducted experiments on a virtual machine, which uses Ubuntu version 16.04, CPU1.5 GHz∗4 cores, memory 8 GB, storage 100 G. The system is built using the Bitxhub cross-chain model architecture. In the experiment, a Hyperledger Fabric blockchain is used as the Hospital Blockchain, and an Ethereum blockchain is used as the Medical Certificate Blockchain to simulate the scene of the data recovery process between the two heterogeneous blockchains of the Hospital Blockchain and the Medical Certificate Blockchain, realizing the safe sharing of EHRs. As the number of confirmed patients in hospitals increases, so does the number of EHR uploaded to the Medical Certificate Blockchain. To restore deleted EHRs, there has been an increase in the number of interactions between the Hospital blockchain and the Medical certificate blockchain.

We evaluated the basic performance of the system. The size of each EHRs is not fixed. For files of different sizes, we simulate the time of the entire process of EHR uploading to and downloading from the Medical Certificate Blockchain. For the same computer, the calculation time is not always the same each time. The operation is repeated in 10 rounds, and the average value of the execution time is used as the final result. The results are shown in Fig. 4, which shows that the time required for the system to upload and download files within a certain range meets the actual situation and is feasible.

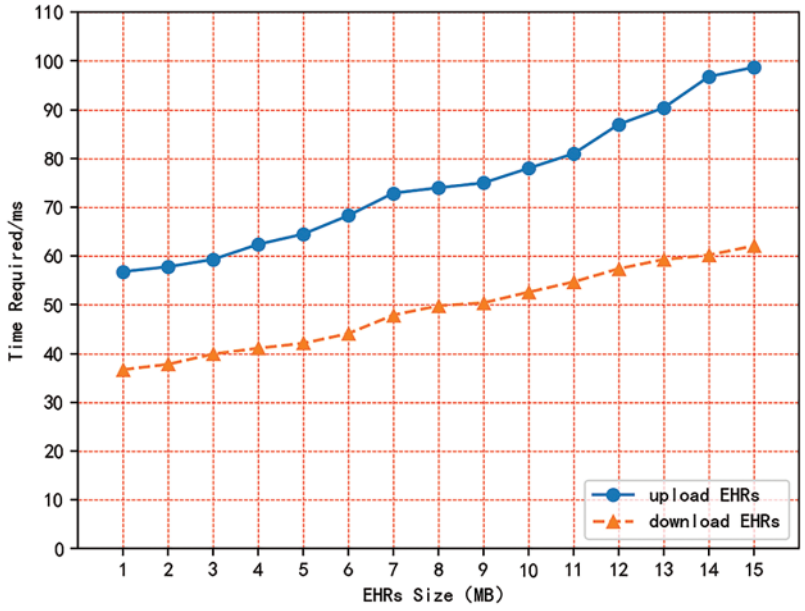

Figure 4: Time required to upload and download EHRs

The main function of this system is the process of deleting and restoring EHRs, that is, the process of EHRs sharing again. For different sizes of EHRs, the time required to restore EHRs is different. As

shown in Fig. 5, We tested that as the number of hospitals increases, the recovery time of three groups of EHRs of different sizes is within 600 ms. In actual situations, this operation is feasible.

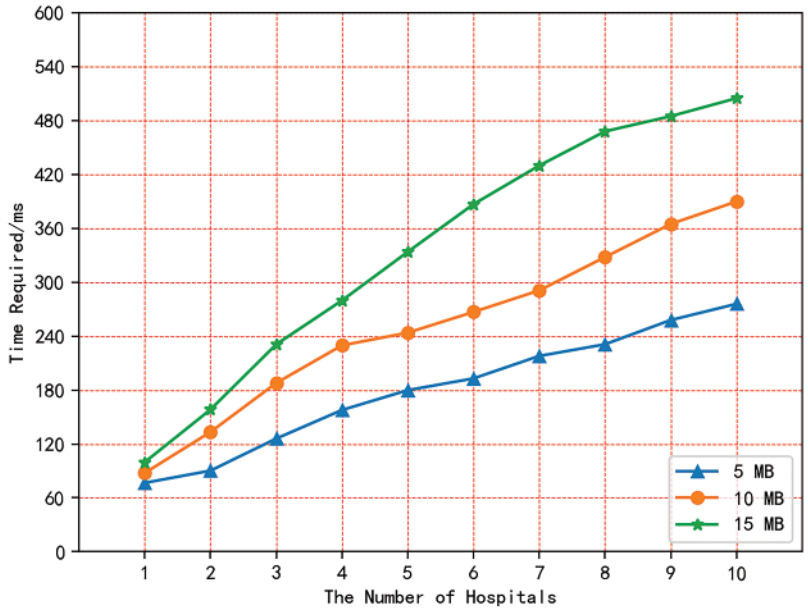

Figure 5: Time required to restore EHRs

In order to evaluate the performance of this system and other shared systems. We compare it with other non-cross-chain EHRs sharing schemes from the perspective of response time, CPU occupancy and throughput. We test the required response time in terms of operation. Fig. 6 show the experimental results. From the results, compared with the previous sharing system based on non-cross-blockchain EHRs sharing systems, the response of this system has certain advantages.

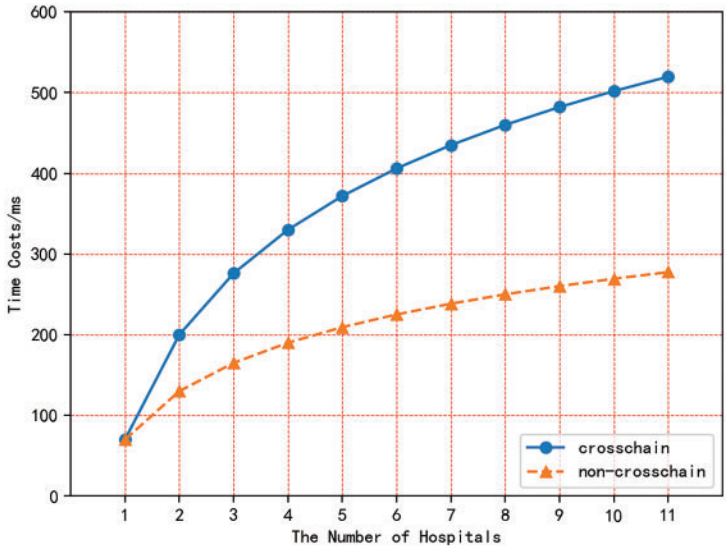

Figure 6: Comparing with different systems of time latency

From the change of CPU occupancy rate over time, the average results obtained from multiple experiments on the same computer are shown in Fig. 7. This cross-chain-based Electronic Health Record sharing system remains at about 50%, while the occupancy rate in other non-cross-chain-based Electronic Health Record sharing solutions is about 60%.

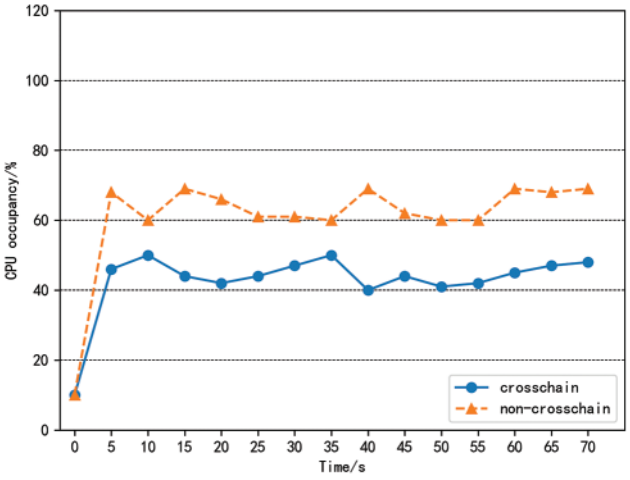

Figure 7: Comparing the CPU occupancy of different systems

Throughput is the number of transactions completed per second, an important technical indicator of the blockchain system, and higher throughput represents high resource utilization and efficiency. As the number of hospitals increases, the number of nodes of each blockchain increases. For a 15 M HER file, the comparison results between the throughput of the cross-chain system and the throughput of the non-cross-chain system are shown in the Fig. 8. In the figure we can see that the TPS of the cross-chain system is higher than that of the non-cross-chain system.

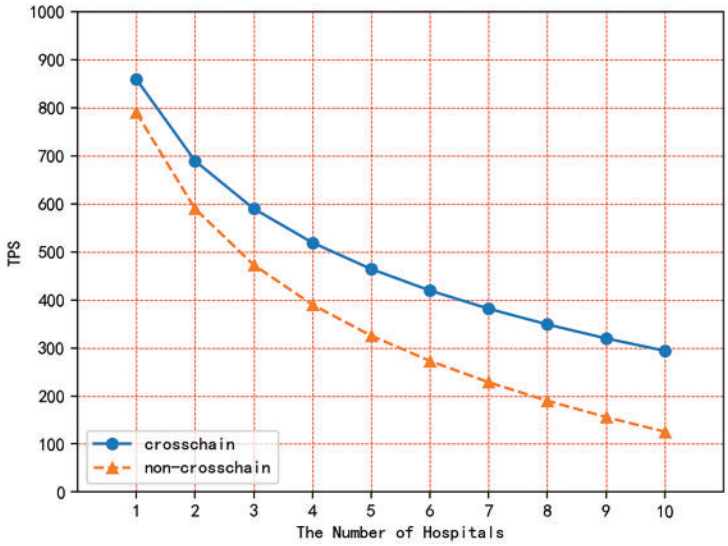

Figure 8: Comparing the throughput of different systems

A comparative analysis of mainstream EHRs sharing systems is conducted in terms of data sharing, scalability, system efficiency, whether to use cross-chain technology, whether to consider data deletion and recovery, etc. The results are shown in Table 2. Compared with other EHRs systems based on blockchain development, when blockchain technology is applied in actual scenarios. There will be problems such as low throughput and difficult expansion with the rapid increase in the number of medical institutions. At the same time, the lack of interconnection and interoperability mechanisms between heterogeneous blockchains of different hospitals largely limits the application space of blockchains. Each chain in the mainstream blockchain platform is still an independent, vertical and closed system, and does not consider the actual scenario where the patient leaves the hospital to delete the electronic health record. Through comparison, it can be seen that the system in this paper realizes the deletion and recovery of electronic medical records through cross-chain technology, with strong data sharing, high system efficiency and scalability.

Table 2: A comparative analysis of mainstream EHRs sharing systems

System	Scalability	Efficiency	Consider the heterogeneity of blockchain	Consider data deletion recoverable
MedRec [19]	Weaker	Lower	No	No
Modelchain [20]	Weaker	Lower	No	No
CEPS [9]	Strong	Higher	Yes	No
This article	Stronger	Higher	Yes	Yes

5 Conclusion

In this paper, we point out the problems that arise after patients have the right to delete the EHRs of the hospital. In order to solve the problem, we design a Medical Certificate Blockchain and use cross-chain technology to realize the sharing between heterogeneous blockchains, and ultimately achieve the deletion and recovery of EHRs. At the same time, the storage of EHRs is stored by the off-chain method of the blockchain. Only the hash value is stored in the blockchain, which saves the storage space of the blockchain. This paper uses cross-chain technology combined with digital watermarking technology, which can not only distinguish the copyright of EHRs, but also verify the authenticity of the restored EHRs. Through the safety analysis and experimental performance test, the proposed program proved to be more considerate of patients' rights, more effectively promotes the process of medical treatment, and saves medical costs.

Funding Statement: This work is supported by the National Natural Science Foundation of China under grant 61972207, U1836208, U1836110, 61672290; the Major Program of the National Social Science Fund of China under Grant No. 17ZDA092, by the National Key R&D Program of China under grant 2018YFB1003205; by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund; by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] X. Yue, H. Wang, D. Jin, M. Li and J. Wei, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, pp. 1–8, 2016.

[2] Faneela, M. A. Khan, S. A. Alsuhibany, W. El-Shafai, M. U. Rehman *et al.,* "An immutable framework for smart healthcare using blockchain technology," *Computer Systems Science and Engineering*, vol. 46, no. 1, pp. 165–179, 2023.

[3] M. Nofer, P. Gomber, O. Hinz and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, pp. 183–187, 2017.

[4] W. N. Al-Sharu, M. K. Qabalin, M. Naser and O. A. Saraerh, "A secure framework for blockchain transactions protection," *Computer Systems Science and Engineering*, vol. 45, no. 2, pp. 1095–1111, 2023.

[5] C. Garg, A. Bansal and R. P. Padappayil, "COVID-19: Prolonged social distancing implementation strategy using blockchain-based movement passes," *Journal of Medical Systems*, vol. 44, pp. 1–3, 2020.

[6] C. Pirtle and J. Ehrenfeld, "Blockchain for healthcare: The next generation of medical records?," *Journal of Medical Systems*, vol. 42, no. 9, pp. 172, 2018.

[7] W. Ou, S. Huang, J. Zheng, Q. Zhang, G. Zeng *et al.,* "An overview on cross-chain: Mechanism, platforms, challenges and advances," *Computer Networks*, pp. 109378, 2022.

[8] O. G. d'Aliberti and M. A. Clark, "Preserving patient privacy during computation over shared electronic health record data," *Journal of Medical Systems*, vol. 46, no. 12, pp. 85, 2022.

[9] S. Cao, J. Wang, X. Du, X. Zhang and X. Qin, "CEPS: A cross-blockchain based electronic health records privacy-preserving scheme," in *ICC 2020–2020 IEEE Int. Conf. on Communications (ICC)*, Dublin, Ireland, pp. 1–6, 2020.

[10] P. A. Ranallo and J. D. Tenenbaum, "Technologies for the computable representation and sharing of data and knowledge in mental health," *Mental Health Informatics: Enabling a Learning Mental Healthcare System*, pp. 155–189, 2021.

[11] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, Maryland, United States, ONC/NIST, pp. 1–11, 2016.

[12] A. Gamal, S. Barakat and A. Rezk, "Standardized electronic health record data modeling and persistence: A comparative review," *Journal of Biomedical Informatics*, vol. 114, pp. 103670, 2021.

[13] C. E. Exceline and S. Nagarajan, "Flexible access control mechanism for cloud stored EHR using consortium blockchain," *International Journal of System Assurance Engineering and Management*, pp. 1–16, 2022.

[14] A. Rudniy, "Data warehouse design for big data in academia," *Computers, Materials & Continua*, vol. 71, no. 1, pp. 979–992, 2022.

[15] M. Alsayegh, T. Moulahi, A. Alabdulatif and P. Lorenz, "Towards secure searchable electronic health records using consortium blockchain," *Network*, vol. 2, no. 2, pp. 239–256, 2022.

[16] J. Liu, X. Li, L. Ye, H. Zhang, X. Du *et al.,* "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records," in *2018 IEEE Global Communications Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, pp. 1–6, 2018.

[17] A. Z. Abualkishik, A. A. Alwan and Y. Gulzar, "Disaster recovery in cloud computing systems: An overview," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 9, pp. 702–710, 2020.

[18] T. Chen, Z. Qiu, G. Xie, L. Yuan, S. Duan *et al.,* "A image copyright protection method using zero-watermark by blockchain and ipfs," *Journal of Information Hiding and Privacy Protection*, vol. 3, no. 3, pp. 131–142, 2021.

[19] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd Int. Conf. on Open and Big Data (OBD)*, Vienna, Austria, pp. 25–30, 2016.

[20] T. T. Kuo and L. Ohno-Machado, "Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," arXiv preprint arXiv:1802.01746, 2018.