Exploiting the Medical Data Storage Implementation and Privacy Protection with Consortium Blockchain and IPFS

Shaojie Liu[1], Bin Wen[1,2,3(✉)], and Zexu Wang[1]

[1] School of Information Science and Technology, Hainan Normal University, Haikou, China
[2] Cloud Computing and Big Data Research Center, Hainan Normal University, Haikou, China
[3] Key Laboratory of Data Science and Intelligence Education of Ministry of Education, Hainan Normal University, Haikou 571158, China
binwen@hainnu.edu.cn

Abstract. Due to the limitations of technologies, the traditional electronic medical record system has the risk of data being tampered with and attacked, which makes personal privacy easy to be leaked. Combined with the consortium blockchain development platform – FISCO BCOS, a new electronic medical record storage model is proposed. The model controls the access of medical records through blockchain and smart contract, strengthens the privacy protection of patients, improves the convenience of medical data sharing, and provides reliable data support for medical research. Finally, the proposed electronic medical record storage model is fully realized, and its effectiveness and practicability are proved.

Keywords: Medical data · Consortium blockchain · Medical service · Privacy protection · Smart contract

1 Introduction

With the continuous development of computer technology, electronic medical record storage has become a popular medical record storage scheme. However, due to the limitations of the technical structure, there is a data barrier between the electronic medical record system of medical units, which hinders the circulation of medical data. This makes it difficult for patients to control and share their own historical medical records, and medical record data are also difficult to be applied to scientific research and analysis. On the other hand, the traditional electronic medical record system contains more patient privacy information. When the database is leaked or attacked, personal privacy information faces a high risk. At the same time, medical record data also have the possibility of tampering and destruction.

H.-N. Dai et al. (Eds.): BlockSys 2021, CCIS 1490, pp. 169–174, 2021.
https://doi.org/10.1007/978-981-16-7993-3_13

The input of scientific research makes the blockchain technology constantly improve and has been widely used in product traceability, financial supply chain and other scenarios. The untamperable and traceable characteristics of blockchain can also meet the technical requirements of application scenarios such as electronic medical record storage and medical data sharing. Using blockchain technology to construct electronic medical system has become an effective solution to improve the privacy of electronic medical records and strengthen the control of permissions.

2 Background

With the continuous development of Internet, cloud computing and network security technologies, the storage, review and transmission of electronic medical records have attracted more and more attention. Thomas F. Stafford [1] discussed the problems of centralized management and privacy disclosure in the existing electronic medical record system through interviews, and analyzed the applicability of blockchain technology in electronic medical record storage and medical information security.

Muhammad Usman et al. [2] firstly discussed how to solve the problems of privacy disclosure and internal tampering in existing medical records storage by blockchain technology. The system ensures the privacy, security and access of medical records through cryptography principle, and solves the problems existing in the existing electronic medical records system to a certain extent.

The characteristics of blockchain technology can provide support for many application scenarios of electronic medical records. Alevtina Dubovitskaya et al. [3] analyzed the shortcomings of the existing electronic medical record system from the perspectives of patient medical record sharing, medical research data collection and multi-agency participation, and introduced blockchain technology to propose an electronic medical record storage scheme to alleviate these problems. The scheme controls the access rights of medical records through smart contracts, encrypts the medical records data and stores them in the cloud database, so as to realize the sharing and privacy protection of patient medical records. The scheme proposed by Yi Chen [4] is similar to the scheme proposed in literature [3]. These strategies have solved some problems faced by the existing electronic medical record storage to a certain extent, but they are lack of thinking about the content storage of medical image medical records.

Medical cases are often accompanied by a large number of image information such as CT images. However, the data structure of blockchain determines that it has a congenital disadvantage in storing large text or image information, which makes it impossible to store these contents in blockchain. Through the thinking of this problem, Sanket Shevkar [5] introduced the InterPlanetary File System (IPFS) into the blockchain electronic medical records management. By storing image data and detailed medical records in IPFS, the occupancy of blockchain resources is reduced, so as to improve the speed of transaction transmission and effectively solve this problem. At the same time, through the way of permission

control to improve the management ability of patients for medical records, not only can ensure the safety of user privacy, but also can achieve the purpose of medical records data sharing. Sihua Wu [6] also proposed a similar model structure, but its research lacks the design of permission control and the use of smart contracts.

This paper aims at study the architecture of medical data storage model with consortium blockchain and IPFS. We will mainly focus on privacy protection and data sharing mechanism in medical data storage process. The rest of the article is arranged as follows. Section 3 gives the related technologies involved in the study. Section 4 includes the system architecture and model optimization. Section 5 gives the implementation and empirical analysis of the model. Conclusions with main contributions of proposed approach are also touched upon in Sect. 6.

3 Related Techniques

3.1 Consortium Blockchain

With the continuous development of block chain technology, according to the different node access mechanisms, a variety of block chain structure systems such as public chain, consortium blockchain and private chain are formed and applied to different needs. FISCO BCOS as a typical open source consortium blockchain underlying platform, by combining with the actual needs, provides a visual middleware tool, can better and faster chain building and management maintenance, transaction delay can be shortened to second level, with high performance.

3.2 Smart Contract

The smart contract is the program code running on the block chain, which is triggered when the external call is detected and meets certain conditions. The execution results are packaged into the block as transactions, and then written into the block chain through consensus. In order to enable blockchain to be applied in a wider range of scenarios, Ethereum developed a fully fledged smart contract development language Solidity. FISCO BCOS also used Solidity as a contract programming language, and added a precompiler contract mechanism to enhance the efficiency of Solidity.

3.3 IPFS

IPFS is a file storage scheme designed by integrating distributed hash tables (DHTs), BitTorrent, version control system, self-certified file systems (SFS) and blockchain. It connects the data block by hash chain to ensure that the data cannot be tampered with. IPFS solves the problem of file loss by backup. At the same time, distributed data transmission effectively eliminates redundancy and saves bandwidth, reduces service cost and waste of idle resources, and alleviates single point failure and DDoS attack.

4 System Architecture and Optimization Design

The research of blockchain, IPFS and FISCO BCOS is of great significance to improve the electronic medical record system, which can strengthen the security and stability of medical record information storage. Based on the actual needs, this paper integrates and improves related technologies, and proposes a new electronic medical record storage model.

Based on the IPFS medical storage consortium chain, this paper takes the FISCO BCOS framework as the service core of the system, and controls the patient's ability to control medical records through smart contracts. The model structure is shown in Fig. 1.

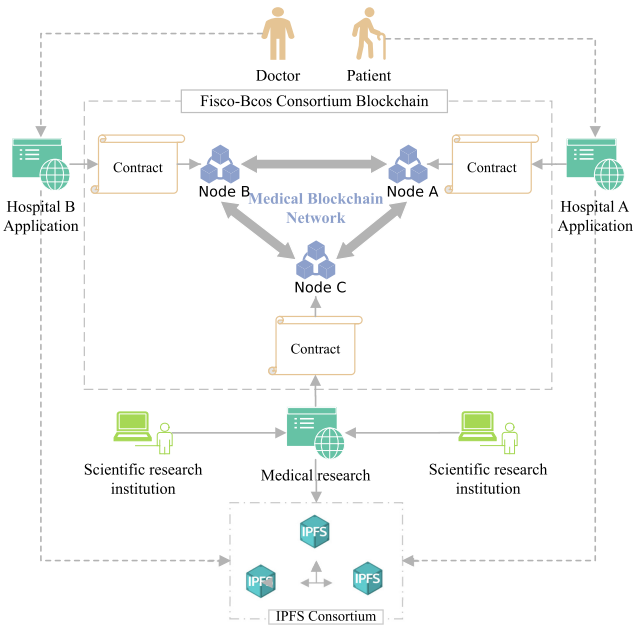

Fig. 1. Improved electronic medical record storage model

Each hospital deploys FISCO BCOS nodes to form the consortium blockchain. Through the deployment of smart contracts, hospitals, departments, doctors and patients accounts are created in the smart contract, and the IPFS address of medical records is stored in it. The smart contract not only stores data information, but also controls the patient's access to medical records.

5 System Implementation

In this paper, the proposed system model is developed and implemented. The front-end interface of the system is based on Vue and ElementUI framework, and the front-end and back-end are asynchronous data interaction through Axios. The back-end of the system uses the popular SpringBoot framework and applies FISCO BCOS's web3j SDK and IPFS's Java SDK to interact with blockchain and IPFS consortium chains, respectively. The smart contract is written in an efficient Solidity language. The main interface of the system is shown in Figs. 2 and 3.

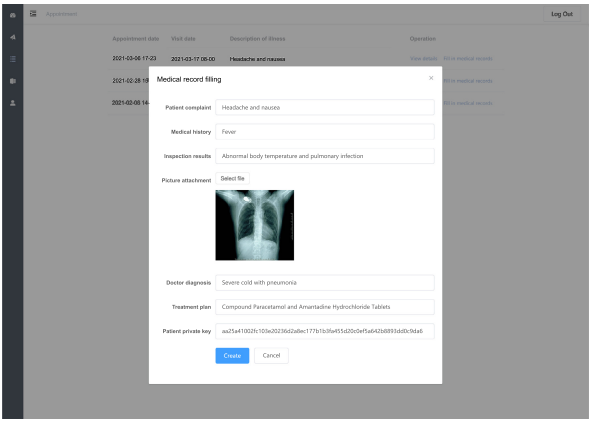

Fig. 2. Add medical records

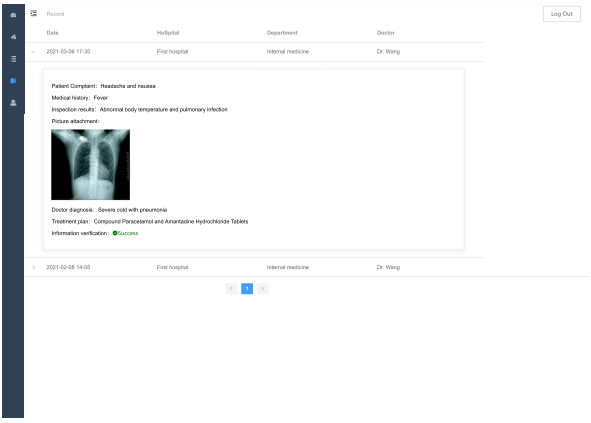

Fig. 3. View medical records

After testing, the developed medical system can well meet the needs of doctors and patients for the storage and sharing of electronic medical records, and can help patients to manage their own historical medical records more conveniently. At the same time, the online reservation function provided by the system also improves the efficiency of medical treatment. Secondly, the system can realize the storage of medical image information and ensure that the data cannot be tampered with through information verification. In summary, the effectiveness and practicability of the proposed model are proved by practice.

6 Conclusions and Future Works

A blockchain electronic medical record storage model based on FISCO-BCOS is proposed, which can break the data barriers between medical units, improve the flow of data, and enhance patient control of medical records by designing smart contracts.

In the future, we will continue to explore an efficient algorithm to improve the efficiency of IPFS medical storage chain, and combine cross-chain technology to expand and develop the comprehensive function of electronic medical system.

Acknowledgements. This research has been supported by the Natural Science Foundation of Hainan Province (No. 620RC605) and Postgraduates' Innovative Research Projects of Hainan Province (No. Hys2020-332).

References

1. Stafford, T.F., Treiblmaier, H.: Characteristics of a blockchain ecosystem for secure and sharable electronic medical records. IEEE Trans. Eng. Manage. **67**(4), 1340–1362 (2020)
2. Usman, M., Qamar, U.: Secure electronic medical records storage and sharing using blockchain technology. Procedia Comput. Sci. **174**(1), 321–327 (2020)
3. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F.: Secure and trustable electronic medical records sharing using blockchain. AMIA Ann. Symp. Proc. **2017**(1), 650–659 (2017)
4. Chen, Y., Ding, S., Xu, Z., Zheng, H., Yang, S.: Blockchain-based medical records secure storage and medical service framework. J. Med. Syst. **43**(1), 1–9 (2018). https://doi.org/10.1007/s10916-018-1121-4
5. Shevkar, S., Patel, P., Majumder, S., Singh, H., Jaglan, K., Shalu, H.: EMRs with blockchain: a distributed democratised electronic medical record sharing platform. arXiv preprint arXiv:2012.05141 (2020)
6. Wu, S., Du, J.: Electronic medical record security sharing model based on blockchain. In: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lumpur, Malaysia, pp. 13–17. Association for Computing Machinery (2019)