Blockchain-based Intelligent Hospital Security and Data Privacy Construction

Qiuzi Huang\textsuperscript{1,3,4}, Shuyu Chen\textsuperscript{1,4}, Hui Zhao\textsuperscript{2,3} and Junhao Wen\textsuperscript{2,4}

\textsuperscript{1}Network Distributed Computing Laboratory, Big Data and Software Institute, Huxi Campus of Chongqing University, Chongqing, China

\textsuperscript{2}Service Computing Laboratory, Big Data and Software Institute, Huxi Campus of Chongqing University, Chongqing, China

\textsuperscript{3}Huxi Campus of Chongqing University, no. 55, Chengnan Road, Shapingba District, Chongqing, China

\textsuperscript{4}Chongqing University, 174 Shazheng Street, Shapingba District, Chongqing, China

sychen@cqu.edu.cn

\textbf{Abstract.} With the rapid development of medical information services, the construction of intelligent hospitals is opening up a new mode of medical treatment in the health care industry. Medical data is gradually becoming more and more important, while it also faces some challenges, among which the most urgent problem to be solved is data security and privacy protection. In the construction of intelligent hospitals, the safety issues among the basic information of patients, the protection of medical information and inter-institutional information sharing have become the focus at this stage. Blockchain technology, with highly secure, reliable architecture and algorithm design have operated stably in the financial industry for more than seven years. The related innovative technologies such as distributed ledgers, smart contracts, symmetric encryptions and consensus mechanisms are used widely in many fields. This paper will take the demonstration construction of Chongqing Intelligent Hospital as an example, which tries to combine the blockchain, homomorphic encryption and zero-knowledge proof technology to carry out the research on the security construction and data privacy protection of intelligent hospitals.

1. Introduction

In the revolution brought by big data technology, information technology has been applied to various fields. In recent years, with the proposal of intelligent hospital construction, we tried to load heterogeneous data such as patients' basic health archives, medical information data and clinical business data into the data mart through a series of data processing operations. The data mart is the data center of the intelligent hospital system. During the construction of intelligent hospital, transparency and readability of data are basic prerequisites\textsuperscript{1}, we assume that all data stored in the data mart is transparent and open and that business data sharing can be achieved. On the one hand it opened up the occlusion between the data, lifting the problem of information silos, while on the other hand it also triggered people to think how to guarantee the security and privacy of data. In the current construction, some parts of medical wisdom systems can connect through the external network that is likely to be the access point for the attacker to access the infrastructure. For example, the attacker violently cracks the
account and password to successfully enters the system. In addition, a large number of servers used by medical institutions, such as NAS servers, have a typical update cycle of several years that accumulate a large number of known vulnerabilities.

The security and privacy of current medical data are mainly facing with two types of threats:

- The middleman uses the sensor channel to attack that the data service between the sensor and the storage sensor;
- Unauthorized persons access data stored locally and remotely.

The integrity and availability of data can be strongly threatened by the above two types of attacks, such as unauthorized accessing, replacement storage data, middleman replacement of data in transit and encrypting or deleting user data, etc[2]. In the construction of an intelligent hospital, the privacy data of the patients or hospitals could be leaked. Data in hospital data marts may be tampered illegally, which could destroy the integrity and correctness of the information. In addition, the stolen data could be used for other illegal purposes. The occurrence of these conditions will seriously threaten the safety and legal rights of patients and hospitals.

Therefore, in the process of building an intelligent hospital, effective protection measures must be taken to ensure the robustness of the data center and the information security of the hospital. How to share all the data under the premise of ensuring the security of the hospital data center has become an urgent problem to be solved.

2. Related works

2.1. Blockchain technology

Blockchain is a new decentralized infrastructure and distributed computing paradigm that has emerged with the increasing popularity of digital cryptocurrencies such as Bitcoin[3]. It is similar to a distributed public account book. In the entire blockchain system, no role can absolutely control the system, and the system does not rely on a centralized, hierarchical structure. Each participating data block has equal rights which jointly maintain the account book updates. The development of blockchain technology solves the trust and security problems of data in the transaction process. It has five characteristics: disintermediation, non-tampering with information, autonomy, openness and anonymity[4].

With the advancement of national systematic projects such as the digitization of medical information and the personal credit information system, more and more authoritative data sources have emerged. In the construction of future intelligent hospitals, we need to collect a large number of sensitive data, such as basic information of patients, into the data mart to optimize hospital data integration and improve disease prediction rate, etc. Blockchain technology may solve the above problems to some extent, so we can introduce the data and store it by using blockchain technology to build a decentralized and trustworthy data system. We can also use blockchain technology to create a person's digital identity, which is real, untampered with, synchronized in real time, and valid for life. In addition, we can use the blockchain system to record the research projects in clinical trials, which ill make the research more objective and perform better to the clinical[5].

2.2. Privacy protection

Each block of data on the blockchain has the same rights, making each data block can obtain a complete data backup. All data traded in the chain is open and transparent, which is a prerequisite of realizing the sharing of medical data in hospitals. However, there is a certain risk that the patient information data will be transparent only in the in-hospital data center by default. Not only do patients want to protect personal information or private data such as their medication records, but hospitals also want their management information to be kept secret from other hospitals or institutions. Once the system of an intelligent hospital is attacked by an irresistible attack, it will have an extremely bad impact on individuals, hospitals, and even the entire intelligent hospital system. Even if some data has desensitized at the beginning, these attacks may affect the privacy protection of the data.
At present, blockchain privacy protection problem can be solved in several ways, such as mixed currency, ring signature, homomorphic encryption, and zero-knowledge proof[6-8]. Combined with the transaction processing characteristics of the intelligent hospital, homomorphic encryption and zero-knowledge proof technology are considered to solve the privacy protection problem of it.

2.2.1 Homomorphic encryption
Homomorphic encryption is a method that can perform calculations accurately on encrypted data. In the construction of intelligent hospital, the basic algorithm operation can be performed without decrypting the encrypted data by using the homomorphic encryption technology on the blockchain. Therefore, homomorphic encryption technology is added to the construction of the intelligent hospital. When accessing sensitive data in the data mart, the characteristics of block chain technology are used to ensure that data are not tampered with, and the privacy of data in the data mart of the intelligent hospitals is guaranteed.

2.2.2 Zero-knowledge proof (ZKPs)
Zero-knowledge proof is a cryptographic technology proposed in the 1980s[9], which can make the verifier believe that a certain statement is correct without providing any useful information to the verifier. It makes possible to make a full judgment without having access to the original information, or to prove the authenticity of a proposal without disclosing the data itself. This is suitable for the scenario of the disease judgment in the intelligent hospital, in which the system gives the diagnosis of the disease while ensuring that the detailed data of the disease in the data mart is sufficiently concealed, thereby giving a diagnosis and treatment reference plan. On the one hand, it fundamentally over-turns a series of data such as public senders, receivers and transaction numbers, and solves the possibility of privacy leakage in this way. And on the other hand, the validity of the public node verification transaction is also guaranteed. It realizes zero-knowledge proof based on blockchain technology, which effectively guarantees the security and privacy of data.

3. Technical application

3.1. Application of blockchain technology in safety construction of intelligent hospitals
Blockchain technology is used to establish data mart. Data mart is composed of data nodes, distributed multiple access and other ways. Just like different types of Shared ledger, it has many backups, which improves the transparency of data in the hospital. Each specific time node recorded in the blockchain is completed in its own authorized scope without other operations. Once the record on the timeline is generated without special "authorization", it cannot be changed[10].

When the patient is in the examination, only the doctor “authorized” by the patient can obtain personal health data, check the medical record so that they can learn about the patient's medical history, analyze the symptoms, make judgments, and give the intelligent analysis opinions with the advice given by the system. In this way, blockchain technology tries to avoid repeating examinations to ensure patient information security and also save times and material resources.

The non-tampering of blockchain makes the data more reliable. We also can ensure the privacy and correctness of electronic medical record combine with using digital signature technology. This not only ensures the information security of electronic medical records, but also fundamentally solves the problem of doubts about the authenticity of it.

3.2. Application of blockchain technology in protecting patient privacy
In the construction of intelligent hospital, it is necessary to the construction of taking patients as the center of information system, using the Internet and big data provide the humanized service for medical staff and patients[11]. It is necessary to consider how to protect the privacy of patients in the process of building an intelligent hospital. It can help patients hide their true identity in the public chain and effectively protect patient privacy information, because of the better anonymity of blockchain
technology[12]. Using encryption technology combined with the blockchain technology decentralized characteristics meets the patients medical privacy and anonymity necessary data which could meet the public health research needs. Drawing on the idea of “DNA wallet” technology, the patient’s basic information, medical records, and past medication records will be stored in a single block by using blockchain technology while the hospital only needs unified identity management. The data block storing the patient's private information just likes the patient's exclusive medical information wallet. It solves the problem that the doctor obtains incomplete information when the patient visits or referrals in different hospitals. Due to the data protection combining with homomorphic encryption technology, the real information of the patients is hidden and the data blocks of all patients are the same, making it difficult to trace the data source. Only the private key can be used for unique identification. Without the authorization of the patients, it is unable to know the true identities of the patients so that the patients do not need to worry about information leakage. This method can solve the patients’ privacy protection problem.

Security is the primary problem that needs to be solved to achieve privacy protection in the process of data exchange. Data encryption makes the data in the data mart present in ciphertext and reduce the probability of information leakage. Using homomorphic encryption technology makes it possible to perform basic algorithm operations without decrypting the encrypted data. In the process of disease prediction, the system only give the results of disease prediction without the real data of the examination results by using zero-knowledge proof technology.

With the support of blockchain technology, patients' personal information can be completely hidden. At the same time, patient-related data can also be applied to research in the field of public health. "authorized" data such as historical treatment records and follow-up treatment effect tracking can be extracted and studied by relevant hospitals or departments, so as to further improve the utilization rate of data.

4. Case model

Based on the strategic action plan of innovation-driven development led by big data intelligence in Chongqing (2018-2020), the Chongqing Municipal Health Planning Commission has carried out the "healthy Chongqing 2030" plan and the construction plan of intelligent hospitals. It has conducted research on the organizational management, strategic planning, capital investment and effectiveness of 50 representative hospitals (including 15 affiliated hospitals, 5 military hospitals in Chongqing, 20 district and county level hospitals, and 10 secondary hospitals). At the same time, we selected the target pilot hospitals by referring to the key construction contents of smart hospitals and the grading value of evaluation index system issued by Chongqing Municipal Health Commission. In the process of building an intelligent hospital, according to the requirements put forward by the project, a staged smart hospital form is formed according to the plan period, as shown in Figure 1.

Figure 1. The staged smart hospital form

In the construction of intelligent hospitals in Chongqing, more attention is paid to security construction and privacy protection issues. Blockchain technology, homomorphic encryption and
zero-knowledge proof technology is applied to data security and privacy construction. As shown below:

- The blockchain technology is applied to establish the private data modules like electronic medical records. Drawing on the idea of “DNA wallet” technology, the patient's basic information, medical records, and past medication records are stored in a single data block. The hospitals only need to perform unified identity management. At the same time, the blockchain technology is used to establish a complete, manageable, readable, and undeniable electronic medical record between the target pilot hospitals. In addition, digital signature technology is used to verify that the “authorized” person adds the correct records according to the related rules. The security of the data is guaranteed as well as its privacy;

- The distributed feature and homomorphic encryption technology of blockchain are applied to data privacy processing. Blockchain adopts distributed data writing and extraction. In this process, we have access control through a visible public address and two encryption keys. In addition, homomorphic encryption technology is used to process desensitized data, so that the system can perform operations, such as retrieval and operation on the encrypted data and obtain correct results. Under the premise of data "fuzziness", data privacy is further guaranteed.

- Zero knowledge proof technology is applied to the diagnosis of diseases and other scenarios. In order to ensure the privacy of data, zero-knowledge proof technology is adopted to carry out the disease pre-diagnosis in the system. Instead of showing the detailed list of relevant data, only the final diagnosis result is displayed. The diagnosis results of the system will provide great support for doctors’ diagnosis. This application scenario in the intelligent hospital system once again guarantees the privacy of data.

In addition, in the demonstration construction of Chongqing Intelligent Hospital, the following security protection measures are planned:

- Prohibit external network access to the intelligent hospital system;
- The online information systems should be independent from the hospitals’ intranet;
- Monitor the intelligent system or services, and ensure them update regularly;
- Modify the default password and delete part of "garbage data" in the database, such as: test account and expired account, etc;
- Create strong passwords for all accounts.

5. Conclusion
This paper discusses the security and privacy protection issues in the process of building an intelligent hospital. Based on the blockchain technology, the data is protected from malicious tampering, thus providing a guarantee for data reliability. In addition, combining blockchain with the technology of homomorphic encryption and zero-knowledge proof, the data is further encapsulated on the basis of not affecting the final result. So that the data is “shielded” and patients’ privacy is protected. This paper takes the construction of Chongqing Intelligent Hospital as an example, and introduces the construction planning especially the safety considerations about it. Under the new situation, the construction of smart hospitals is unstoppable. The related technical mentioned in this paper will guarantee the systematic construction of intelligent hospitals.

Acknowledgements
I would like to express my gratitude to all those who helped me in the process of writing this paper. I do appreciate professor S Y Chen, professor J H Wen, my partners and my boyfriend, who gave me patience, encouragement and professional guidance in the process of writing this thesis. Finally, I would like to acknowledge the Big Data and Software Institute of Chongqing University for its great support.

References
[1] Julián Salas, Josep Domingo-Ferrer. Some Basics on Privacy Techniques, Anonymization and their Big Data Challenges[J]. Mathematics in Computer Science, 2018, 12(3):263-274.
[2] Karim Abouelmehdi, Abderrahim Beni-Hessane, & Hayat Khaloufi. Big healthcare data: preserving security and privacy [J]. Journal of Big Data, 2018, 5(1):1-1.

[3] YUAN Yong, WANG Fei-Yue. Blockchain: The State of the Art and Future Trends [J]. Acta Automatica Sinica, 2016.

[4] Igor Radanović, Robert Likić, View, author's, OrcID, & profile. Opportunities for Use of Blockchain Technology in Medicine [J]. Applied Health Economics and Health Policy, 2018, 16(5):583-590.

[5] Irving Greg, Holden John. How blockchain-timestamped protocols could improve the trustworthiness of medical science [J]. F1000Research, 2016, 5:222.

[6] Li, Jiaxian, Chen, Long, Wu, & Jigang. Block-secure: Blockchain based scheme for secure P2P cloud storage [J]. Information Sciences, 2018, 465:219-231.

[7] Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery [M]. ACM, 2002.

[8] Yao A C. Protocols for secure computations [C] // Symposium on Foundations of Computer Science. IEEE Computer Society, 1982:160-164.

[9] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems [C] // 1985:291-304.

[10] Leslie, Mertz. Hospital CIO Explains Blockchain Potential: An Interview with Beth Israel Deaconess Medical Center's John Halamka [J]. IEEE Pulse, 2018, 9(3):8-9.

[11] Rizwan, Patan, M., Rajasekhar, Babu, K., & Suresh. Design and development of low investment smart hospital using internet of things through innovative approaches [J]. Biomedical Research (0970-938X), 2017, 28(11):4979-4985.

[12] Sushmita, Ruj, Mohammad, Shahriar, Rahman, Anirban, Basu, Shinsaku, & Kiyomoto. BlockStore: A Secure Decentralized Storage Framework on Blockchain [J]. 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), 2018:1096-1103.

[13] Irving Greg, Holden John. How blockchain-timestamped protocols could improve the trustworthiness of medical science [J]. F1000Research, 2016, 5:222.