Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 10, No. 3, 2023

Review on Privacy Protection of Electronic Medical Data in Cross-domain Sharing

Yue Zhang, Mingchuan Zhang

Henan University of Science and Technology, Luoyang 471000, China

Abstract: With the rapid development of information technology, the medical industry is rapidly moving in the direction of smart medical care, and more and more users tend to put their medical data in cloud servers, so as to share them safely among Internet hospitals. Electronic medical data stores all patients' medical information, and its high value is obvious to all, which also leads to the attack of illegal elements, which leads to the leakage of patients' private data. In addition, the cloud server used to store data is semi-trusted, so it is necessary for the intelligent development of the medical industry to ensure that the private data is not leaked when the electronic medical data is shared among internet hospitals. This paper deeply discusses different technical schemes to protect medical data, and then realizes the privacy protection of electronic medical data.

Keywords: Electronic medical data; Cloud storage; Secure sharing.

1. Introduction

Cross-domain sharing of medical big data between hospitals through the Internet enables medical staff to obtain all complete information about the historical diagnosis and treatment of cross-hospital patients, including digital records of various tests and examinations, text introduction of illness, medical graphics, ultrasonic images and other multimedia historical information and analysis results after diagnosis [1-3], and authorized doctors can access and share them online at any time in different hospitals. For example, in the emergency room and inpatient ward of the hospital, all doctors can access the historical medical records with unified format and comprehensive diagnosis and treatment online, so as to ensure that the follow-up diagnosis and treatment plan is well-documented and well-documented, so that different doctors can quickly make reasonable and scientific judgments on the follow-up illness and avoid one-sided medical mistakes [4]. For the existing diagnosis and treatment system, storing the patient's diagnosis and treatment information on the cloud server not only has good reliability, but also ensures that unauthorized users can't access the data stored in the cloud server through the method of data privacy protection, and ensures that the patient's privacy is not leaked [5]. Therefore, if electronic medical data can be integrated with data privacy protection technology, it will certainly promote the safe sharing of medical data and realize the value of medical data.

However, a large number of highly sensitive medical data will be generated and stored in the cloud server during the online treatment of patients in Internet hospitals. The high value of medical data increases the risk of data theft and personal information disclosure of patients. Electronic medical data store patients' personal information and medical records. Once attacked, it will lead to the disclosure of sensitive information such as patients' personal privacy, lead to security risks and conflicts between doctors and patients [6-7], and cause serious losses to them. Whether they can fully trust third-party servers is a subsequent problem. At present, although the relevant laws and regulations are relatively perfect, especially the issue of privacy leakage [8], which has been highly valued by relevant departments in recent years, there are still some illegal users who steal the privacy of the owners of electronic medical data by some illegal means, which may cause great damage to the owners of electronic medical data. Moreover, as a third party, the medical cloud [9-11] brings many benefits, but the problem of data privacy protection is a hidden danger in the medical cloud and hinders its rapid development. In particular, some illegal users may take some illegal measures to steal the privacy of the owner of electronic medical data, causing certain losses to the owner of electronic medical data. Therefore, it is very important to protect data privacy when sharing electronic medical data between hospitals on the Internet [12].

2. Correlation technique

Therefore, while sharing electronic medical data in Internet hospitals, how to protect patients' privacy has become a top priority. The existing main privacy protection technologies are:

2.1. Data desensitization

Data desensitization is a widely used technical means to deal with sensitive information such as patients' personal basic information in medical field [13]. Generally, the sensitivity of medical data is reduced by replacing and distorting sensitive data, so that it cannot be recognized by other data users. Literature [14] desensitizes different types of electronic medical record data, and realizes diversified desensitization strategies through a series of processes such as identification, calculation and desensitization, which meets the needs of patients' privacy protection and also provides a basis for sharing medical big data.

2.2. Identity authentication

Traditional authentication methods of Internet hospitals mainly verify the identity credentials of doctors or patients, and issue different user passwords or signs for users. However, this identification code is often easy to forget, lose, break, be illegally invaded and leaked, and cannot ensure the data security of users. Most of the existing hospitals adopt single sign-on and unified authentication, and the authentication mechanism with high security and reliability can enable users to realize real-time and reliable strong authentication when

accessing hospital information. Literature [15] puts forward a new identity authentication technology through the combination of electronic key and standard protocol, and defines the database according to the authentication result of information, and judges whether the data is legal or not. Literature [16] proposed a multi-server oriented lightweight authentication scheme for telemedicine based on HMAC, which can solve the security threat by using the high security of multiple factors to solve the ambiguity of biometric features.

2.3. Anonymization

Anonymization technology can realize the anonymity of electronic medical data records. Under ideal circumstances, no one can identify them, and it can retain the usability of the data, providing basic support for data mining and research. Literature [17] uses the third-party audit to verify the lightweight integrity of outsourced cloud storage medical data, and at the same time supports multiple data files to be authenticated in batches, and generates anonymous identities and corresponding signature keys for users according to unique identities, so that attackers cannot obtain user identities and protect their identity privacy.

2.4. Encryption

Traditional authentication methods of Internet hospitals mainly verify the identity credentials of doctors or patients, and issue different user passwords or signs for users. However, this identification code is often easy to forget, lose, break, be illegally invaded and leaked, and cannot ensure the data security of users. Most of the existing hospitals adopt single sign-on and unified authentication, and the authentication mechanism with high security and reliability can enable users to realize real-time and reliable strong authentication when accessing hospital information. Literature [15] puts forward a new identity authentication technology through the combination of electronic key and standard protocol, and defines the database according to the authentication result of information, and judges whether the data is legal or not. Literature [16] proposed a multi-server oriented lightweight authentication scheme for telemedicine based on HMAC, which can solve the security threat by using the high security of multiple factors to solve the ambiguity of biometric features.

2.5. Access control

In order to prevent malicious users from invading patients' data privacy, every data access must meet the access policy set by patients. Facing the access requirements of users with different roles, literature [20] combines data encryption with role-based access control (RBAC), and the specific role has special decryption authority, so other users can't access the data. On this basis, Attribute-based Access Control (ABAC) has become a general security access control model, which can realize fine-grained access control of patient electronic data.

2.6. Blockchain

As an open decentralized distributed account book, blockchain has the characteristics of multi-party maintenance, decentralization, data non-tampering, traceability, non-forgery, and programmability [21-23], which can provide platform support for electronic medical records, help solve the privacy problem in the process of medical data sharing, open up data islands, provide a platform for safe sharing and trading of medical data, and generate permanent and irreversible records. Clear data ownership, effectively prevent data leakage. Compared with centralized architecture, blockchain can avoid security risks caused by single point failure or data leakage, thus ensuring data integrity and non-tampering.

2.7. Proxy re-encryption

In the proxy re-encryption scheme, a semi-trusted entity called proxy can convert the ciphertext encrypted for Alice into a new ciphertext, and another user Bob can decrypt it with his own secret information without revealing the underlying plaintext [24]. Because the proxy is not completely trustworthy, it is required that the proxy cannot disclose Alice and Bob's keys and cannot learn plaintext during the conversion process. In the attribute encryption scheme based on ciphertext, the decryption strategy is embedded in the cipher text during encryption. The patient encrypts the electronic medical data and stores it on the cloud server. Users who meet the attribute access policy set by the patient can access the data, so that one-to-many data sharing can achieve fine-grained access control.

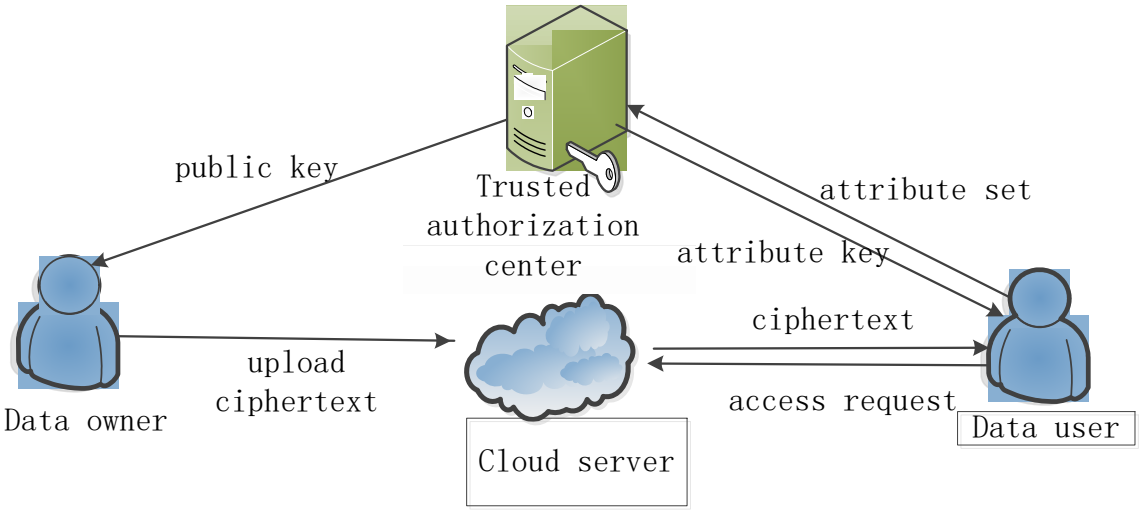

Fig. 1 Proxy re-encryption model diagram

Attribute-based encryption scheme ABE usually includes four participants in cloud computing environment: data

provider, trusted third-party authorization center, cloud storage server and user [25]. The data is stored in the cloud server in encrypted form, and the authorization of access depends on the attributes of the data user. The authorization method is completed by the data user calculating the private key. The system model diagram is shown in Fig. 1. The scheme is described as follows: First, the data owner obtains the system public key from the trusted authorization center and uploads the encrypted ciphertext of the data to the cloud storage server. Then, when a new user joins the system, according to the private key application request of the data user, the trusted authorization center generates the attribute key for the attribute set submitted by the data user. Finally, the data user accesses the data of the data owner, and if his attribute set meets the access structure of the ciphertext data, the ciphertext can be decrypted.

3. Conclusion and prospect

In the smart medical cloud environment, the use of emerging technologies has become a trend in the medical industry. In internet hospitals, medical data has the demand of remote diagnosis, so it is necessary to realize remote sharing of medical data in different internet hospitals. When sharing, people pay more and more attention to whether their privacy data is attacked and their privacy is leaked. In order to protect data privacy, the access control scheme based on attribute encryption has become an important technical means to prevent cloud servers and unauthorized users from accessing data in the cloud. However, when encrypting data to the cloud server, public key encryption has become the first choice for data owners, and how to transform public key encryption into attribute-based encryption with fine-grained access strategy has become the focus of this paper.

Up to now, although there are many safe and efficient feasible schemes, with the rapid development of smart medical industry and the continuous improvement of scientific and technological means, there is still room for development. Although the privacy protection methods of electronic medical data discussed in this paper have achieved certain results, it is still necessary to further study the privacy protection of electronic medical data in the future.

Acknowledgements

National Natural Science Foundation of China (62002102, 62102134).

References

[1] Chen Lanxiang, Lee Wai-Kong, Chang Chin-chen, et al. Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems,2019,95: 420−429.

[2] Hao Wang, Song Yujiao. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. Journal Of Medical Systems, 2018, 18(2): 152−161.

[3] Wang Yong, Zhang Aiqing, Zhang Peiyun, et al. Cloud-Assisted EHR sharing with security and privacy preservation via consortium blockchain. IEEE Access, 2019, 7: 136704−136719.

[4] Jensen Peter B, Jensen Lars J , Brunak Soren . Mining electronic health records: towards better research applications and clinical care[J]. Nature Reviews Genetics, 2012, 13(6):395-405.

[5] Liu Jian, Han Qiujun, Cao Lei. Research on the Construction of Clinical Data Center Based on Electronic Medical Records [J]. China Digital Medicine, 2017,12(3):38-41.

[6] Hoerbst A, Ammenwerth E. Electronic health records a systematic review on quality requirements [J]. Methods of information in medicine, 2010, 49(4):320.

[7] Yong Mingyuan, Lu An. Privacy protection of patients with infectious diseases and public health safety [J]. Medicine and philosophy,2019,40(14):9-11,30.

[8] Wang Tianyi, Liu Aiping. Research on privacy protection of medical data in big data environment [J]. Information technology and network security,2019,38(8):28-32.

[9] Zhou Yousheng, Chen Lvjun. Safe storage and deletion scheme of fine-grained cloud data based on blockchain [J]. Journal of Electronics and Information,2021,43(7):1856-1863.

[10] Zhang Yulei, Liu Xiangzhen, Lang Xiaoli. Multi-server key aggregation searchable encryption scheme in cloud storage environment [J]. Journal of Electronics and Information., 2019, 41(3): 674-679.

[11] XUE Liang, YU Yong, LI Yannan, et al. Efficient attributebased encryption with attribute revocation for assured data deletion[J]. Information Sciences, 2019, 479: 640-650.

[12] hang Jiannan, Li Yingying, Gu Yanju, et al. Discussion on the basic principles of health care data sharing [J]. China Engineering Science, 2020,22(4):93-100.

[13] Zang Hao, Zhao Qiang, Bian Shuirong. Research and design of electronic medical record privacy data desensitization technology based on XML [J]. Information technology and informatization,2017(3):111-114.

[14] Zhang Zhili, Heng Xiuxiu. Study on the method of desensitization of electronic medical record data [J]. China Digital Medicine, 2022,17(10):100-103,120.

[15] Cheng Lei. Access control of medical information database based on identity authentication [J]. Information technology, 2022, 46(9):112-117.

[16] Zhang Min, Xu Chunxiang, Huang Minying. Research on lightweight multi-factor authentication protocol for multi-server in telemedicine environment [J]. Information network security,2019(10):42-49.

[17] Zhang Xiaojun, wangxin, Liao Wencai, et al. Lightweight integrity verification scheme of cloud storage medical data supporting conditional anonymity [J]. Journal of Electronics and Information, 2022,44(12):4348-4356.

[18] Zhu Zongwu, Huang Ruwei. Secure multi-party computing protocol based on efficient homomorphic encryption [J]. Computer science,2022,49(11):345-350.

[19] Lin Qing, Faye Ting, Tian Bo, et al. Storage and retrieval scheme of secret knowledge map based on searchable encryption [J]. Computer Engineering and Science, 2023, 45(1):66-76.

[20] ZHOU, L., VARADHARAJAN, V., HITCHENS, M. Enforcing role-based access control for secure data storage in the cloud[J]. The Computer journal,2011,54(10):1675-1687.

[21] Yuan Yong, Ni Xiao-Chun, Zeng Shuai, WANG Fei-Yue. Blockchain consensus algorithms: the state of the art and future trends.Acta Automatica Sinica, 2018, 44(11): 2011−2022.

[22] Han Xuan, Yuan Yong, Wang Fei-Yue. Security problems on blockchain: the state of the art and future trends. Acta Automatica Sinica, 2019, 45(1): 206−225

[23] Zeng Shuai, Yuan Yong, Ni Xiao-Chun, Wang Fei-Yue. Scaling blockchain towards bitcoin: key technologies, constraints and related issues.Acta Automatica Sinica, 2019, 45(6): 1015−1030.

[24] GUO Lifeng,LU Bo. Efficient proxy re-encryption with keyword search scheme [J]. Journal of Computer Research and Development,2014, 51(6):1221-1228.

[25] Rao Y Sreenivasa. A secure and efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records sharing in cloud computing[J]. Future Generation Computer Systems, 2017, 67(feb.):133-151.