ISBN: 978-981-18-1791-5
2021 the 11th International Workshop on Computer Science and Engineering (WCSE 2021)
doi: 10.18178/wcse.2021.06.001

Research and Progress on Data Security Based on Medical Information System

Cai Zengyu [1 +] , Wang Luqi [2], Feng Yuan [1] and Zhang Jianwei [3]

[1] School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou, 450002, China

[2] School of International Education, Zhengzhou University of Light Industry, Zhengzhou, 450002, China

[3] Software College, Zhengzhou University of Light Industry, Zhengzhou, 450002, China

Abstract. The data security of today's medical information system is one of the important fields of national security encryption technology application, and it is widely used in the development of network information security technology. Based on the introduction of the basic structure and analysis of network hospital data information security technology, it comprehensively analyzes network data control sharing, data encryption, data security service targets and other related medical information system data technologies. This article introduces the application of network information security encryption technology, and studies the development trend of future medical data information security technology system design.

Keywords: network security, encryption technology, hospital data information technology, border security, big data

1. Introduction

With the rapid development of life and the convenience of payment in social development, the network information security of Chinese citizens and even national data has gradually become one of the security vulnerabilities that cannot be ignored in national information security. With the development of hospital data and information technology, illegal intrusion methods have derived a series of intelligent illegal methods to resist the confidentiality, integrity and non-repudiation of information [1]. Due to the diversity and wide spread of data in network information, it is impossible to ensure the safety of data loss and theft in the medical service industry to prevent intruders[2]. In order to realize the security of internal network boundary sharing and prevent external intrusion without affecting the hospital management system, the medical information system urgently needs to encrypt the medical service data [3]. The system that provides hybrid encryption technology can solve the demand problem of tampering with user data through illegal means [4]. In this way, medical data information can be independently verified, and users can be screened. In order to improve medical service data, information encryption security technology, cloud computing, network security, border security, etc. have been applied to the security encryption of medical-related network information. This articles analyzes the data security research of medical information system and the demand trend of realizing technical means, and summarizes the future development of medical information system data security technology.

2. Data Security of Medical Information System

In order to promote the operation of the overall function of data coordination in the medical information system, the system researchers classified the system from the target functions of information sharing, encryption and data security services. As shown in Figure 1. Among them, the main direction of the current popular information system security function is that medical service information needs to be classified

[+] Corresponding author. Tel.: + 8613603452356.
E-mail address:mailczy@163.com.

according to the data security level of availability, confidentiality, integrity, controllability and non-repudiation.

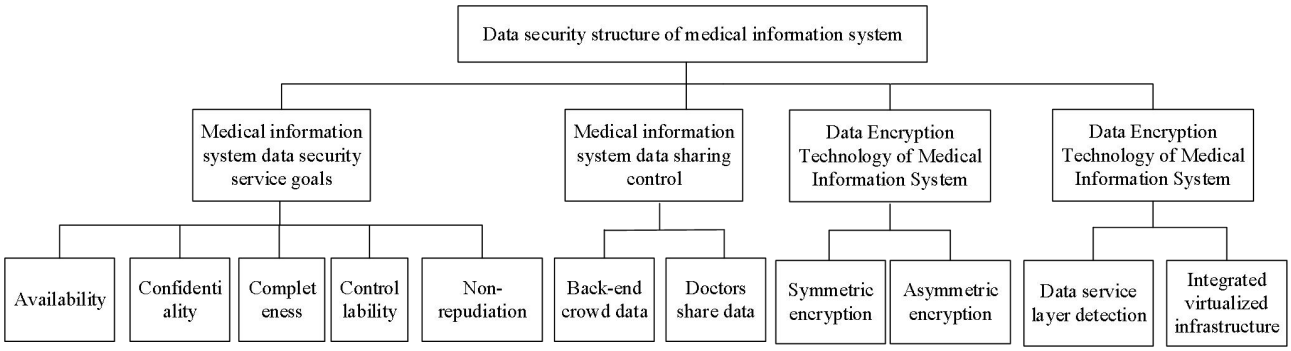

Fig. 1: Classification of data security levels in medical information systems.

3. Research on Data Security Technology of Medical Information System

3.1. Medical Information System Data Sharing Control

Medical information system data information sharing is to connect different computer software through data information so that different computer users can read and use the data created by others. The purpose of information storage and sharing is to ensure data security and realize the control of data information sharing in the medical information system [5]. The basis of data information control is to apply the main body of the control port to the hospital system and reshape the integration of shared data. In the medical information system, the connection of data information sharing and data transmission ports is based on the network information sharing space. There is no unified conclusion about the practicability of the above two port data, but its essence is to control the open access of each open node information and have a certain degree of security [6]. In the Internet environment, users can share the hospital's medical information system data. In this system, users are temporarily granted the right to use data, but the ownership of the data is still controlled by the hospital [7]. Generally, when data information sharing is implemented in a medical information system, the controllability of data availability is separated on the basis of ensuring data sharing through the integrated information sharing data space. By realizing data sharing, it is possible to modify and create the doctor-oriented port and the back-end personnel port [3].

At present, information security technology system researchers and related industry insiders based on medical information system data have achieved extensive results. In most big data servers whose system architecture is based on data centralization, information sharing control and modification are realized through information platforms. Yu Bengong’s research is based on a third-party electronic medical record information integration platform, which proves that the impact of information sharing on computer virus infection is controllable. Through the design of the medical data sharing information system, the use of data information port control improves the control and management viewing rate of the system information by the big data server. This method ensures the safety, effectiveness and controllability of the hospital database [8].

3.2. Data Encryption Technology of Medical Information System

With the rapid development of information encryption security technology system research, the database in the server uses encryption technology to set different security levels for internal information processing. Encryption technology can prevent illegal means from tampering with hospital information system data and improve data security. Symmetric keys are inherently highly confidential and efficient. However, whether users can maintain symmetric keys well and improve the secure path of key transmission has become a major issue. When using medical information system data, the asymmetric key is composed of a public key and a private key. The user inputs the data information that needs to be guided and sent through the public key, and then the receiver uses the personal private key to decrypt and receive the information. Taking into account the advantages and disadvantages of symmetric keys, public keys can well establish the security and confidentiality of information [9]. Data encryption security technology system in medical

information system,Hybrid data encryption technology is used to ensure the security of the system, the confidentiality of information, and the scope of control and management.

At present, the combination of data security encryption in medical information systems and information security used in various industries has achieved certain results. Among them, data encryption technology application secure multi-party computing technology has been greatly optimized in recent years. One of the representative results of the literature is that NETSCAPE provides a secure socket layer [10]. This layer is based on the SSL3.0 electronic certificate connection key used for secure conversations. Encrypting data on this basis can not only ensure the correctness, security and decentralization of the data, but also enable users to use public keys to implement independent node transmission, calculation and extraction processes. In summary, this technology can effectively ensure security, privacy, and can correctly calculate and manage data transmission .

3.3. Data Application Testing Technology of Medical Information System

Data virtualization technology is mainly used to realize the retrieval and data management of network information programs. Regarding the storage of data security in the medical information system, the basis is how to improve the security and sharing of the data in the medical information system, so that the system has the goal of variability. The application of virtual data detection technology can control and manage the data sharing of system data. Considering the security of data, it can be integrated into a virtualized infrastructure [11]. Currently, the data virtual detection technology used for data security on most platforms is gradually being combined with other related levels. The representative example is: HealthNow has established a data service that can quickly and effectively organize data by creating a virtualized data mart, while ensuring the safe integration of display data on various platforms; Huawei launched Hetu Engine within 19 years, Establish a data infrastructure strategy and so on. The use of this technology can effectively avoid the problem of secure storage connection caused by the heterogeneity of data sources, and has a certain effect on the rapid analysis of data in secure computing data.

4. The Prospect of Data Security in Medical Information System

4.1. Problems of Data Security in Medical Information System

With the continuous development of the network, the process of secure data transmission in the medical information system has shown more characteristics, such as uncertainty, complexity, diversity and lack of security. The existing data and information sharing security system technology obviously cannot meet the needs of the future medical service data industry. Although security performance information sharing control technology, data encryption technology and virtualized data detection technology have made certain achievements in various professional fields. However, when it is used in the field of medical data transmission, there is still a long way to go to truly achieve security without leaking information. In recent years, the data security of medical information systems has the following problems:

1) The security of data exchange between medical data and hospitals is insufficient. In recent years, with the popularization of the Internet, Internet application technology has gradually penetrated into the medical industry. The amount of medication information used by doctors in electronic medical records undermines the information security of traditional paper versions. The security and confidentiality of information and data in the medical service industry and users are obviously insufficient.

2) Lack of leadership over personnel control in the hospital system. Although information sharing control has been studied in the planned medical service data information encryption technology, and the application of hybrid key encryption and data virtualization in the field of confidential systems has been studied, but these technologies are always manipulated by human beings. Therefore, there are many problems with hospital system management personnel and open control and observation ports, which may lead to data leakage in the internal medical service industry and lack of learning by operation and maintenance personnel.

3) The information system cannot restrict illegal network access control ports. In the current data security state of the medical industry, the sharing of search ports is also the main risk of information loss and leakage. The existing network firewall technology, the modification of data encryption technology and the

setting of network management access rules can ensure the security of data. However, how to strengthen the prevention of network intrusion is still the main research direction for researchers to strengthen network access control.

4.2. The Future Prospects of Medical Information System Security

As mentioned above, based on the application of various technological achievements, the medical information system still has a long way to go to achieve true information security and confidentiality. In order to ensure the security of the medical information system, it is necessary to promote the integration of the physical layer and the data security encryption technology layer. However, with the popularization of the country and the widespread application of Internet technology, China's existing medical information data sharing security technology is still being gradually developed and improved. In recent years, regarding the possible development directions of data security in medical information systems, this article summarized the following points:

1) Research and enhance the functions of various hybrid encryption technologies. In the data sharing control of different ports in the medical information system, it is particularly important to enhance the hybrid data encryption technology of each port structure in the system. Different hybrid encryption technologies are one of the development trends of medical data security. Although DES symmetric encryption and RSA asymmetric encryption are mixed together to ensure the stability and security of the system. However, because the construction of the Internet involves a wide range of technical levels, It must be further improved in order to enhance the function of hybrid encryption technology in medical information system.

2) Gradually improve the management level. In the future medical information system application planning, users will gradually increase control over data ports. With the construction of information systems, the risk of information leakage will slowly increase. There are many problems in data encryption and data monitoring security services. Among them, further improving the management level has become one of the development directions of medical information systems. While improving the parallelism of medical information systems, it is necessary to improve the application of information network security technology. The medical industry still needs to further improve the data management control system and user access standards.

3) Pay attention to the development of data service security mechanisms. In the process of using data for calculations, it is still necessary to control the privacy of input data, in order to keep network access unimpeded. Reference data virtualization technology can calculate and detect the security of user data, and solve the shared data infrastructure through system management. How to better define the security mechanism of virtualized data services is also an important research goal to improve the security performance of data computing.

4) Enhanced network access control technology. The medical industry realizes data sharing through medical information system, and provides some research directions for computer network security researchers. During the data access period, the sharing of medical data network access ports will lead to a decrease in data security integrity and confidentiality. In order to prevent the network from invading the medical information system, researchers have tried to use technologies such as registration to restrict network access sources and enhance the network access control technology. The focus of enhanced technology is to improve the security and confidentiality of data sharing in the medical information system.

5. Conclusion

This article discusses the data and information encryption security technology system based on the medical information system. It focuses on the basic system structure of network hospital system data and information security technology. Introduced the application of data information technology in medical information systems, such as data control sharing, data encryption technology and virtual detection technology in network information security encryption. Looking forward to the future development of data and information encryption security technology systems. How to improve the data encryption technology used in the medical information system has become the focus of social development. At the same time, all levels of data security in medical information systems require various system connections. We need improve

the detection system for problem-solving approach, in order to achieve security and improve the system of practical.

6. Acknowledgements

This work is supported by the National Natural Science Foundation of China (No. 62072416) , Fourth Batch of Innovative Leading Talents of Zhihui Zhengzhou 1125 Talent Gathering Plan (ZhengZheng [2019] No. 21) and Key Technologies R&D Program of Henan Province (No.202102210176 and No.212102210429) .

7. References

[1] Bo J , Ping S . A Probe into the Information Security of E-Documents in E-Government. *Journal of Shanghai University(Social Sciences Edition)*, 2009,16(3):127-134.

[2] Zhang Y . Construction and Application of Regional Medical Information Sharing System Based on Big Data. *International Journal of Information System Modeling and Design (IJISMD)*, 2020,11(3):40-61.

[3] Langer S . How to encrypt medical data against intrusion. *Diagnostic imaging*, 2000, 22(8):69-71, 79..

[4] Hofheinz D , Kiltz E . Secure Hybrid Encryption from Weakened Key Encapsulation. *International Cryptology Conference on Advances in Cryptology*. Springer-Verlag, 2007, pp. 553-571

[5] Jeong C W , Lee S G , Lee J , et al. Construction of Dynamic Medical Information System for Digital Hospital Environments. *Wireless Personal Communications,* 2016, 91(4):1575-1590.

[6] Chkirbene Z , Mohamed A , Erbad A , et al. Smart Edge Healthcare Data Sharing System. *2020 International Wireless Communications and Mobile Computing (IWCMC).* 2020, pp. 577-582

[7] Karim A . Data security in medical information system. *International Conference on Multimedia Computing and Systems*, IEEE, 2009, pp.391-394

[8] Hua M , De-Jian L , Bing Z . Discussion on Medical Big Data Security Based on the Third-party Medical Cloud. *China Digital Medicine*, 2018,13(03):23-25

[9] Zhang X Z , Zhang Y J . On Data Security and Encryption Algorithms in Cloud Environment. *Applied Mechanics & Materials*, 2015, (3682):1106-1111.

[10] Fang P . Research of Modern Information Encryption Technology Based On Information Security. *Information Security and Technology*, 2011,(10):36-38.

[11] Lans V D , Rick F . *Data Virtualization for Business Intelligence Systems*. Morgan Kaufmann Publishers Inc, 2012.