The Research on the Privacy Protection of Hospital Patient in the Age of Internet Plus

Ying Dang [1, a], Jiangxiao Zhang [2, b], Ruiyu Li [*3, c], Yue Li [4, d], Meng Li [5, e], JunQiao Guo [3, c] and Jingtao Sun [6, f]

[1]Xingtai Medical College, Xingtai, 054000, Hebei, China

[2]Xingtai University, Xingtai, 054000, Hebei, China

[3]Second Affiliated Hospital of Xingtai Medical College, Xingtai, 054000, Hebei, China

[4]Chengde Medical University, Chengde, 054000, China

[5]Health Team, Hotan Detachment of the Xinjiang Armed Police Corps, Hotan, 848011, Xinjiang Uygur Autonomous Region, China

[6]Xingtai Technician College, Xingtai, 054000, Hebei, China

*Corresponding author: Li Ruiyu

[a]email: xtyzdy@126.com, [b]email: wein871@sohu.com, [c]email: Liruiyu651021@163.com

Keywords: Attribute-Based Encryption; Internet Plus; Electronic Medical Records

Abstract. In accordance with the information disclosure problems in hospitals because of the loss of patient medical card or the disclosure of charge data and electronic medical records, we put forward a privacy protection system of the patient in hospital in the age of internet plus. The patient's information can be encrypted based on the patient's attribute. The public key is the patient's ID card information and the private key is kept by the patients themselves. The hospitals can only the use of the patient's public information for encryption. In the internet age, the simple and efficient system is suitable for patient privacy protection in hospital.

Introduction

With the arrival of the era of internet plus, the hospital need to provide more services on the basis of treatment in order to adapt to the era of the internet plus. In the internet plus age, the hospital contains more sub-module such as outpatient and inpatient, laboratories, drug management, equipment and materials management, economic statistics, imaging, medical card and electronic medical records. Many of the sub modules are related to the patient's privacy, such as: outpatient fees, hospital information, medical card, image of personal information and patient's electronic medical records, etc.

Specifically, when the patient pay the fees in the outpatient, the existing hospital system can visit with the patient's personal information casually, which may bring risks to the patient's privacy. If the patient's electronic medical record which contains their basic information, medical history and medication history can be viewed easily, the patient's privacy may be easily disclosed. The existing hospital information system preserves the patient's medical card are generally save the patient's basic information, such as patients telephone number, address, etc. if the information is used illegally, it will bring a lot of trouble to the patients. In summary, in the internet plus the environment, it is a urgent problem that protecting the patient's privacy in the information system during the procedure of outpatient charges, electronic medical records and medical card using.

Basic Knowledge

Treatment System in Hospital in the Age of the Internet Plus. With China's entry into the internet age, there are various industries have begun to apply internet technology gradually including hospitals. However, the hospital is currently used in the form of the "One Card Solution" in the procedure of treatment. In the actual application, there are still some loopholes and defects. In order

to facilitate the preservation patient records, in the internet era plus age, electronic medical records is used which can easily save the patient's basic information, treatment history and used drugs.

Electronic Medical Record. EMR is a systematic and optimized collection of outpatient clinic, emergency treatment and hospitalization information, is a special software for the medical field. Electronic medical records is the specific expression of health records in the hospital, the standardization of electronic medical records is the key to the construction of regional health information and health archives. A new generation of hospital information system construction must be based on electronic medical records, a comprehensive discussion on the various business and management of hospital process, to meet the needs of the hospital internal information resources sharing, but also meet the needs of the regional health business collaboration. Hospital patient medical information can be saved in the form of information, contains the doctor's advice, hospital records, course records, operation information, history of allergies, inspection results, PACS image examination results, nursing, hospital records, such as medical data, both the hierarchical information, also has a hierarchical text information, also contains a graphic image information. Mainly involves the patient data collection, storage, transmission, statistics, analysis and management of use, can be implemented in different medical institutions and medical information in different regions and efficient unified, system integration, connectivity, information sharing, so as to make the patients' medical records more tend to humanization, integration and standardization.

Attribute-Based Encryption. In the age of internet plus, the people of data encryption usually get all the intended recipient's public key and the identity of exactly, but he hoped to add certain decryption requirements for their confidential data to make the of the recipient meeting the requirements is able to share data while others cannot get information.

Attribute-Based Encryption(ABE) meet these requirements in the age of internet Plus. Sahai and Waters[3] proposed encryption attribute-based thinking on the EUROCRYPT firstly in 2005. In 2006, Goyal et al[4] carried out more detailed study on ABE which divided the the ABE into Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute -Based Encryption (CP-ABE).

Construction on ABE Patient Privacy Protection System

System Initialization. Public property information of the patients are needed first such as patient's ID number, name or other public information. The public information which based on ABE encrypted can ensure the safety of patient privacy and limit the access to the information by other people. The patient's privacy can be protected based on Attribute-Based Encryption. Only the patient who keep the private key can visit his information after payment. Only the patient himself can check his electronic medical records in addition to privileged passwords (only a few people know the passwords). The medical cards can used by the patient only. Even if the patient's treatment card loss accidently, the people who pick up the card cannot access to the medical system because his information does not comply with the card owner. And he cannot guess the password of the patient.

Medical Card Information Encryption. After collecting the user's public information, the initialization is based on the public and private keys which the ABE encryption required. When the patient visits his payment information, electronic medical records and medical card information, he should match the public information first. That means if the ABE-based encryption use the patient's ID card information, we need to first check whether the visitor's identity card number match the public information in the system. The password is needed after the matching. If ABE-based encryption uses the patient's name, we should verify the name first and then verify the provided password as described above.

For ease of description, we focus on the description of the patient medical card encryption. After Knowing public and private keys based on encryption based on ABE, the hospital staff require the patients provide his ID card first when he get the medical card. And we ask the patient choose which information as the public key. Suppose the patient choose his ID card number as the public key of encryption, the staff will input the patient's ID card information and ask the patient to input 6

numbers password as the part of the private key for Attribute-Based Encryption. Then we will integration the additional information such as random numbers to generate the private key corresponding to the user ID card information based on ABE encryption. The patient may use the medical card after the initialization of the medical card is complete.

Medical Card Verification. When the patient use the medical card, the ID and public information of ID card may first be read such as ID number. The hospital requires patients to provide their public information such as the patient's ID number. The hospital information system will verify the public key which is the public attribute of patients-whether identity card number is correct. If correct, we will allow the user to provide the corresponding private key; if it is not correct, we will refuse the user to access the medical card directly.

We will also ask the medical card holder whether he is legitimate or not. If he provides a legitimate public key information and then verify his private key-the 6 numbers password which the patient set for the medical card.If the password is correct, the user may visit and use the medical card. If not correct, the used may be refused and warned. After the two steps, the patient's medical card holder should be the corresponding patient. This can avoid the information disclose after the loss of the medical card and protect the patient's privacy.

Conclusion

This paper constructs a system to protect the privacy of patients in hospital in the age of internet plus, considering the procedures of patient's outpatient charging system, electronic medical records and medical card. After using the system, the patient can avoid the information disclose when paying fees. In addition to special high-level visits, only the patient can access their electronic medical records which can also protect his privacy in the record. If the patient's medical card were lost, only the patient could access and use the medical card which can protects the patient card in the patient information. The system use the Attribute-Based Encryption and the public key only use the patient's basic information, which makes the system convenient and efficient, and protect the privacy of patients under the age of internet plus[5].

Acknowledgments

This work was supported by the programs:
Research on information management system of hospital information security (No.2016ZC008), Program for the Top Young Talents of Higher Learning Institutions of Hebei (No.BJ201414), The Program for the Young Talents of Science and technology (No.2016ZZ052) and The Program for educational reform of Xingtai university (JGY15028).

Acknowledgements

This work was financially supported by the Research on information management system of hospital information security (No.2016ZC008), Program for the Top Young Talents of Higher Learning Institutions of Hebei (No.BJ201414), The Program for the Young Talents of Science and technology (No.2016ZZ052) and The Program for educational reform of Xingtai university (JGY15028).

References

[1] Xiong Jinbo, Yao Zhiqiang, Ma Jianfeng, Li Fenghua and Liu Ximeng: ACTA ELECTRONIC SINCA Vol. 42 (2014). p. 366-376
[2] Li Dan and Cao Xiaojia: Software Technology Vol. 32 (2013). p. 223-228
[3] Yu Ping, Ren Guoqin, Wu Jing and Hua Minfeng: Chinese Nursing Research Vol. 29 (2015). p. 881-883
[4] Wang Haibin: JOURNAL OF XIDIAN UNIVERSITY Vol. 42 (2015). p. 97-102.

[5] Guo Zhitao, Yang Tingting, Xu Ruzhi and Wang Zhuxiao: Journal on Communications Vol. 36 (2015). p. 116-126

