Privacy Protection System of EMR Based on Hash Chain

Dang Ying[1,a], Zhang Jiangxiao[2,b], Dang Wei[1,a], Dai Xulei[1,a], Li Ruiyu[3,c,*], Li Yue[4,d] and Li Meng[5,e]

[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
[a] email: xtyzdy@126.com, [b] email: wein871@sohu.com, [c] email: Liruiyu651021@163.com
*Corresponding author: Li Ruiyu

Keywords: EMR, Hash chain, Private key

Abstract: This paper presents a privacy protection system of electronic medical record which deals with the problems of privacy disclosure. Through this system, the patient's latest medical record can be viewed by patient's private key with Hash algorithm. The earlier medical record can be viewed only with the private key which is input by the patient himself, which protect the privacy of the patients. Because of the high computational efficiency of the Hash algorithm, the system has a very high efficiency.

1. Introduction

With the popularization of information technology hardware and software infrastructure, the technology of electronic patient records has been rapidly developed. The high construction of the hospital information system enables the hospital to become "paperless office" and "digital office", which also makes the hospital work efficiency greatly improved. At the same time, it is convenient for patients to see a doctor. The hospital establish a electronic medical record[1] for each patient which can be viewed each time the patient come to the hospital. The system enables the doctors can see the medical history of each patient quickly and accurately, which can save time for patients and improve the accuracy of the doctor.

To be more specific, the hospital offers a medical card for each patient that record the patient's basic information, doctor's visits, detailed medical history, diagnosis and medication. When the patient sees a doctor next time so that patient can enjoy the expert level treatment. Because the medical record of each patient accumulated gradually, the hospital can serve their patients more systematically and more efficiently. This system is convenient for doctors and related medical personnel as well. That means the doctors and related medical personnel can access to the patient's medical history easily. If they leaked the patient's information to traders, the medical history would leak out. People give more importance to privacy[2] in modern society, which means we have to protect our patients' privacy. So it is a urgent problem to protect the patients' medical record.

2. Basic Knowledge

2.1. Electronic Medical Records

Medical records refer to the text, signs, forms, imaging data including the outpatient (emergency) medical records and inpatient medical records. With the continuous development of science and IT technology, the electronic medical record has been gradually entered into medical practice which also called the electronic medical record[3], electronic medical history or electronic health record and so on.

The electronic medical record is the medical record stored in the medical information system which can support the user to obtain complete and accurate data. The system can also give warnings to the medical personnel and serve clinical practice. In addition, it can connect management system, bibliography, basic knowledge of clinical practice and other equipment. It is not a simple electronic information technology substitute for the existing paper medical records. It includes not only the original content of the paper records but also reflects the whole process of medical patients and stores all of the medical information of patients including medical history, various results of examinations and tests and image data. It is the embodiment of a integrated system of personal health information and its related process. Electronic medical records provide timely and accurate information to the medical staff, offer better service to the patients and serve the clinical scientific research, hospital modernization management and remote medical consultation system[4].

Electronic medical record has an absolute advantage. Its promotion and application is a important part in the informatization of hospital and medicine industry which has the following advantages:

2.1.1. Large Storage and Comprehensive Contents

Because of the progress of the computer storage technology, especially the optical disc technology, the storage of the electronic medical record database can be quite large. In addition, the electronic medical record is not simply input written medical records in the system, but collect the information of every department through the hospital information management system (HIS) and auxiliary examination system. It records the detailed information of the patients' doctor visits.

2.1.2. Good Information Sharing and Wide Application

Electronic medical records can be easily transmitted on the network, so the patient can provide a detailed history of the past in any place which offers a convenient condition for the patient's remote consultation.

2.2. Hash Chain

The Hash chain[5], also called hash chain, Hash chain, it is a Singly Linked Lists. First, Hash chain construction is reverse in the initial time of construction and its length is n. Hash chain is proposed by American mathematician Lamport at first as a one-time password mechanism which use cryptography H (x) in a string loop circularly which can quickly and clearly see the back of the information. The single hash function guarantees that the information unable to read reversely. The single nature of the hash chain is suitable for the preservation of multiple medical records[6], which can ensure the safety of the patient's medical history. To achieve the purpose of protecting the privacy of patients, the medical history of the patients can be viewed only in the case of the patient's permission.

2.3. Privacy of Medical Record

The patient's medical records of the patient's records the medical history, family history, previous physical examination results, treatment of heart and other physiological health information

and mental health information[7]. That means it involves all the privacy of patient safety issues. Therefore, how to effectively protect the privacy of patient's medical records is a very important issue.

3. Privacy Protection System of Electronic Medical Records Based on Hash Chain

3.1. System Initialization

First, a hash chain which length is n is initialized and give every node of a hash chain a secret value. Each node stores a certain medical record which contains detailed information. The user records the medical history of the patients in the node of the hash chain from the left to the right according to the time.

When seeing a doctor, the patients needs to provide his private key and the closest node value, using the Hash function H (x) on the user's private key and secret hash value.

The latest medical record can by viewed when the value is correct. The past history of the patients can be found by using the hash function to iterate hash if the patients needs to view the earlier medical history.

3.2. Construction of Hash Chain

In order to construct the electronic medical record privacy protection system based on Hash chain, a Hash chain need to be built. First, a hash chain which length is n is initialized from left to right. The patient view their medical history from right to left due to the patient's medical record is stored from left to right. Each time the patient view their medical history, they need to provide their own private key and the corresponding secret value and the information list from the latest to the earliest which can protect the patients' privacy.

3.3. Storage of the Previous History

When the Hash chain construction is completed, the patient can get their history stored in the Hash chain. The storage order is according to the visiting time distance from left to right which deposited into the Hash chain node. At the same time, the secret value is provided to the users in order to facilitate users to view the past history.

3.4. Viewing Previous History

When the patients need to view the past history, the user's private key and each node of Hash chain need to be provided and hash the two value by using hash function H (x). Then the latest medical history can be viewed with the value. If the earlier medical records are needed, the user private key and the secret value of the corresponding Hash chain node are both needed for viewing the medical history.

4. Security Analysis

The privacy protection system of electronic medical records based on Hash chain is correct, irreversible and high efficiency.

4.1. Correctness

The Hash chain is constructed in advance. After the construction, the user can get the secret value which can be used together with the private key for viewing every patient's medical record.

This access to view electronic medical records access, is obviously correct.

4.2. Irreversibility

The irreversibility of the Hash function ensures that patients, doctors and related medical personnel cannot access to patient records irreversibly. It can also ensure that the doctors and related to medical personnel cannot view more earlier information of the patients by offering the private key once which can ensure the safety of patient's medical records privacy.

4.3. High Efficiency

The Hash function has the advantages of fast execution. in this paper, the system of electronic medical records is accessed through the Hash function when the patient and the doctor viewing the previous medical records which ensures running efficiency of the system is high.

5. Conclusion

This paper aims to introduce a protection system of electronic medical record based on the Hash chain.

The patients can access their past history through the efficient Hash chain. The patient's privacy can be protected due to the unidirectional nature of the Hash chain. And the high efficiency of the implementation of Hash function ensures the efficiency of the system.

Acknowledgements

This work was supported by the programs:

Research on information management system of hospital information security (No.2016ZC008);

Mobile media in the "Internet +" in higher vocational teaching new mode (No. Xtskfz2016037 youth topic);

The Top Young Talents of Higher Learning Institutions of Hebei (No.BJ201414).

References

[1] Qian Danmin. (2010) Analysis on Current Research Stetus of Electronic Health Record in China. Journal of Medical Intelligence, 31(6), 10-12.

[2] Yu Ping, Ren Guoqin, Wu Jing, et al. (2015) Implementation of emergency patient's privacy protection strategy and its effect evaluation. Chinese Nursing Research, 29(3), 881-883.

[3] Zhou Shuanlong. (2014) Discussion on Personal Protection Countermeasures in the Application of Electronic Medical Record in the United States. Journal of Medical Informatics, 35(2), 13-16.

[4] Yang Jinfeng, Yu Qiubin, Jiang Zhipeng. (2014) An Overview of Research on Electronic Medical Record Oriented Named Entity Recognition and Entity Relation Extraction. ACTA AUTOMATICA SINCA 2014, 40(8), 1537-1562.

[5] Zhang, M.Q., Dong, B. and Yang, X.Y. (2009) A New Self-Updating Hash Chain Scheme. International conference on Computational Intelligence and Security, 315-318.

[6] Zhang HaoJun and Zhu Yuefei. (2006) A self-updating Hash chain mechanism. Journal of Wuhan University, 52(5), 596-599.

[7] Dai Ying. (2015) Investigate patient information protected electronic medical record. Electronic Technology & Software Engineering, (8), 221.