Journal of Engineering and Applied Sciences 13 (4): 898-902, 2018
ISSN: 1816-949X

A Study on Information Protection in Hospital Information System

[1]Hee Wan Kim and [2]Yong Gyu Jung
[1]Department of Computer Science and Engineering, Shamyook University,
815 Hwarang-ro, Nowon-gu, 01795 Seoul, Korea
[2]Department of Medical IT, Eulji University, 553 Sanseong-Daero,
Sujeong-gu, Seongnam-si, 13135 Gyeonggi-do, Korea

Abstract: The healthcare system is the core business model for the healthcare ICT industry and allows for identification and access trends in the industry. IT, telecommunications, equipment, medical devices and internet companies provide product development and differentiated services in the healthcare sector for business and convergence. In recent years, there has been a shift in the way healthcare is handled and supporting systems. This change has made a drastic impact on the design of conventional healthcare models. Now, security has been enhanced according to expansion of healthcare market. How to handle limited information such as the Personal Information Protection Act problems of storing and delivering medical information of truthfulness. If the problem is resolved reasonably, medical information must be able to function as security. In the study, we propose the evaluation points in EMR system for hospital information security.

Key words: Health information, security, hospital, EMR, HL7, DB system

INTRODUCTION

It has been the core business model of u-Healthcare-based healthcare system in ICT industries. In the case of healthcare system overseas, it is deemed to be desirable approach to analyze trends in health care around the industry. There are fused with existing business and expanding high-tech product development and differentiated services to the healthcare areas, especially in communications equipment, medical equipment and internet companies. Healthcare ICT is expected one of the fastest growing market. Now, it is the time to need the current advancement of telemedicine technologies. ICT enabled health care and open the ICT industry. In particular it is introducing medical expenses of 7.2% over the age of 65 including remote monitoring of elderly patients (approximately 1.5 trillion) (Baig, 2014). It may generate savings to inform the excellence of telemedicine in Foreign countries through the u-Healthcare demonstration projects. It is also needed to improve domestic legislation. It is allowed between the current medical law and medical telemedicine but remote consultation system and remote patients. It must be cared that human medical services are not allowed. This needs to take advantage of the efficiency of the ICT strategy and technology services but is still insufficient level to perform some of Healthcare-based project. It should provide the basis for strengthening health promotion in relation to national projects to build health care system improving the quality. Healthcare-based industry leads the growth of healthcare ICT market. There is now a need for sophisticated remote medical technology and ICT and open healthcare ICT industries. About 7.2% (about 1.5 trillion) when it causes a lightning effect (Fong *et al*., 2011). The healthcare pilot project needs to receive overseas medical insurance and improve the domestic legal system. The medical treatment under the current medical law is a remote coordination system and the prescription for the patient and outpatient medical services is different. Implement and track healthcare-based projects to leverage ICT technology to increase service strategy effectiveness. It is used as a health promotion program for promoting health for the health promotion of the health care industry. Now security has been enhanced according to expansion of healthcare market. How to handle limited information such as the Personal Information Protection Act problems of storing and delivering medical information of truthfulness. If the problem is resolved reasonably, medical information must be able to function as security.

Information security analysis: It collects various types of malicious code and related information by using honeypot for collecting malicious code or information of the

Corresponding Author: Hee Wan Kim, Department of Computer Science and Engineering, Shamyook University, 815 Hwarang-ro, Nowon-gu, 01795 Seoul, Korea

sinkhole and overseas malicious code collecting site and based on the collected data, basic analysis technology related to artificial intelligence and machine learning. In addition to this, it is necessary to have a linkage analysis methodology such as static and dynamic analysis which is specialized in the field of malicious code security. It is also necessary to develop a storage space efficiency mechanism and a high speed processing algorithm for storing and processing large amount of cumulative data to support this. In this study, we investigate the changes of existing technology to cope with intelligent infringement and malicious code techniques and infer future predictive models such as infringement and malicious code behavior using machine learning analysis processing technology which is emerging recently. Information security analysis technology using machine learning is as follows.

Machine learning (machine learning): An area of artificial intelligence that develops algorithms and techniques that enable computers to learn. It is a way to present predictive values for new data through training data or to learn models that explain given data well.

Inductive learning: A method of learning general concepts from well-known counter examples to examples of concepts that are sought as a method of machine learning and their concepts.

Pattern recognition: It is generally used in a similar way to machine learning and refers to methodologies for finding rules or characteristics from given data. If machine learning is primarily focused on improving predictive performance in artificial intelligence, pattern recognition focuses on finding the best way to describe or visualize the data.

Deep learning: A set of machine learning methodologies that improve the prediction performance of a model by extracting expressions that best describe the characteristics of the data from a large amount of data and learning simple, low-level and high-level concepts.

Malicious code analysis: Even with malicious code with complicated obfuscation algorithms and sophisticated structure, it ultimately has the purpose of system destruction, information deception and so on. If you combine machine learning with a method of collecting malicious code by collecting malicious code after executing malicious code in a sandbox environment, it is not merely to classify and analyze malicious code with or without specific system call calls. The information can be digitized, drawn in a vector space and analyzed using clustering and classification techniques. It is also possible to judge the malicious code type by judging whether the target file which is desired to be judged through clustering is out of the representative malicious code behavior type or by substituting the malicious code classification model created through machine learning with the action information of the target file (Cova *et al*., 2010; Shabtai *et al*., 2010).

Software vulnerability analysis: There have been many studies to combine vulnerability analysis and machine learning. Early studies performed machine learning using information from public databases. However, most studies focused on keyword analysis related to timeliness analysis and vulnerability related to the use and distribution of exploits rather than finding vulnerabilities in real software. Vulnerability extrapolation has also been preceded by the use of syntax trees to identify programming patterns and to perform machine learning based on them to automatically detect new vulnerabilities. A sufficient amount of data must be collected for high accuracy of machine learning. However, in case of software vulnerability there is a limit to the information that can be collected through the public database. In analyzing the compiled binary there are many variables depending on the programming language, coding method and type of compiler. You should use.

MATERIALS AND METHODS

Encryption section will be taken at two aspects. First, it must be built secure system at health measurement devices (glucose meters, heart rate monitors, thermometers, etc.) for encrypted communication between servers and devices for data collection. It could be used the method of public key and symmetric key cryptographic algorithm because unlike the PC system resources are not enough at the same time. It could be 1024 bit or more secret keys and public keys 128 bit to transmit the encryption key to transmit the encryption key for encrypted communication and thereafter transmits the data encrypted and then proceeds through a symmetric key algorithm, AES encryption 128 bit. In addition to one or more of range encryption provides secure encryption 128 bit to do this in a secure encrypted communication between servers and devices (Hardjono and Tsudik, 2000; Date *et al*., 2006).

The system is necessary to store encryption to encrypt the important information such as the customer's personal medical information or confidential information stored in the database to prevent unauthorized

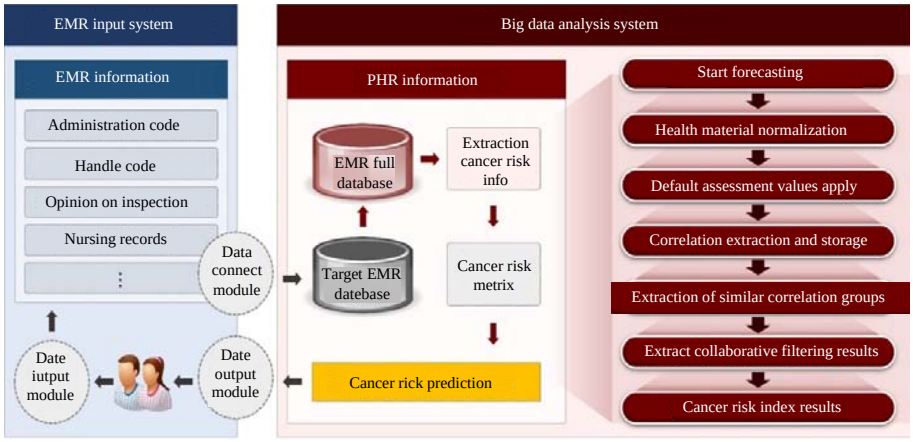

Fig. 1: EMR input system and big data analysis system

modification or destruction to the database. Database encryption is required in order to protect the information stored on devices and media in the appropriate physical security. It must be developed by a column-by-column format with access control encryption. It needs encryption key management and DBMS administrator access control applications. It is developed in conjunction with an existing database management system with encryption method to install the agent program for performing the encryption in the data server. It is centered on the concepts of ubiquitous healthcare services provided to the patients in rural or remote areas from distant hospitals. With this system framework, a physician can securely access and carry the patient information from a mobile device, update the patient information offline on the mobile device and synchronize the data with the server at a later time. The system provides high security to the highly sensitive patient health records. It provides various layers of security and privacy controls to access the patient information (Fig. 1).

RESULTS AND DISCUSSION

According to the definition of the Institute of Medicine (IOM), "Electronic Medical Record (EMR)" is defined as "An expert system using memory and assistive devices based on complete and accurate data and various medical knowledge". An electronic form of medical record established on a computer based patient record system. In 1969 Lindberg D.A.B. Also, claimed to store medical records on a computer. In 1991, the American Medical Association created a report titled "Computer Based Patient Records: An Exervical Technology of Health Care" which began to discuss the computerization of medical records in earnest.

Table 1: Proposed evaluation points

Classification	Proposed evaluation points
Construction of maintenance-free system, server duplication	Network redundancy Disaster recovery system
Equipment interface	Equipment interface needed to increase convenience of work Patient Moniter, anesthesia ECG, TMT, Holter Various function tests (PFT, PWV, etc.)
Need to improve the computing environment	Ensure mobility for location proximity and response Machine room correspondence for obstacle prevention Expansion of EMR response personnel and computer education
Expansion of system performance	Expansion/addition of servers to which all EMRs can be applied Expansion of storage area as EMR capacity increases Complementing network performance due to flow of large capacity EMR information
Improvement of additional equipment environment	Pen Mouse, Tablet PC, Wacom Tablet, etc. Scan form medical record using OCR, Barcode Mobile Point of Care (POC)
Active cooperation of users	Promotion and training for users Personnel composition for EMR improvement in computerized organization Organization of medical records, organization of term management personnel

The development of the domestic hospital information system is difficult to collect information in the hospital and the patients could not share information in the hospitals. The problem should be solved with personal information security. The points are proposed as an evaluation as Table 1.

In recent years, hardware prices and mass storage media (Juke Box) are inexpensive, making rapid

progress. It is possible to reduce the waiting time if the medical records are stored in the clinic without being stored in the warehouse and can be immediately used when the patient visits the hospital. When the waiting time is reduced, parking and waiting space can be solved. This can increase the credibility of the patient which can lead to a patient-centered hospital and a high-value-added hospital. Therefore, it is necessary to introduce EMR as a method for effective management and storage of medical records. EMR is an EMR that keeps records of your personal and medical history as electronic records.

CONCLUSION

It is especially expected that the health care industry is one of the fastest growing ICT markets. However, it is still insufficient level of security issues for the ICT services. It is necessary to solve some of u-Healthcare-based security system. Therefore, the basic user information security, server security, database security, medical equipment such as encrypting communications segment analysis is a security vulnerability on the medical information of various types of security solutions. There are large-scale hospitals in the domestic medical field in the center of the country. It is growing interest in Bigdata and to use predictive techniques for diagnosing disease based on the patient DB (Chawla and Davis, 2013; Bates *et al*., 2014). However, it has not been achieved technologies still to attempt target by the elderly. Therefore, the research and development of bigdata processing and management skills are needed to extract integrated health indicators of elderly diseases and for the diagnosis and prediction of the disease. Also, it is required the development equation life patterns to utilize integrated health information, especially as aging progresses. It has emerged as a major factor causing the change of the high incidence of disease. Dietary patterns to track changes in lifestyle related diseases causing elderly on the change in dietary patterns. It is difficult to browse diagnostics everyday life as the elderly marker. With the changes in lifestyle such as the visual approach of mutual organic component. It is important new direction in the health index diagnosis of the elderly. In order to implement the integrated DB system, it is need to collect health, diet and lifestyle data. It could provide integrated health information as the results of the data analysis.

There is medical information consists of individual information and the sensitive information because of the high risk of abuse in the external outlet. Due to the sensitiveness of medical data, austere privacy and security are inevitable for all parts of healthcare systems. The first consideration is the encryption technology to solve these problems. Encryption technologies such as the current internet banking, cyber securities, credit cards, electronic bidding, electronic money, copyrights or other industry information, privacy, e-Elections, healthcare information systems, confidentiality and integrity of information in various fields user authentication. It has been used in the form of the basic user information security, server security, database security such as encryption analyze the various types of security vulnerabilities in security solutions can have on health information communication section of the medical device to determine its function it should be implemented. It is needed to solve some of u-Healthcare-based security system. Therefore, the basic user information security, server security, database security, medical equipment such as encrypting communications segment analysis are identified a security vulnerability that could have on the medical information of various types of security solutions, should be developed and implemented its features.

ACKNOWLEDGEMENTS

This research is supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT on Development of heterogeneous big data integration and processing technology for cancer care service (2017M3C4A7083412).

REFERENCES

Baig, M.M., 2014. Smart vital signs monitoring and novel falls prediction system for older adults. PhD Thesis, Auckland University of Technology, Auckland, New Zealand.

Bates, D.W., S. Saria, L. Ohno-Machado, A. Shah and G. Escobar, 2014. Big data in health care: using analytics to identify and manage high-risk and high-cost patients. Health Affairs, 33: 1123-1131.

Chawla, N.V. and D.A. Davis, 2013. Bringing big data to personalized healthcare: A patient-centered framework. J. Gen. Internal Med., 28: 660-665.

Cova, M., C. Kruegel and G. Vigna, 2010. Detection and analysis of drive-by-download attacks and malicious JavaScript code. Proceedings of the 19th International Conference on World Wide Web (WWW'10), April 26-30, 2010, ACM, Raleigh, North Carolina, USA., ISBN:978-1-60558-799-8, pp: 281-290.

Date, C.J., A. Kannan and S. Swamynathan, 2006. An Introduction to Database Systems. Pearson Education, Delhi, India, ISBN:978-81-7758-556-8, Pages: 937.

Fong, B., A.C.M. Fong and C.K. Li, 2011. Telemedicine Technologies: Information Technologies in Medicine and Telehealth. John Wiley & Sons, West Sussex, England, ISBN:978-0-470-74569-4.

Hardjono, T. and G. Tsudik, 2000. IP multicast security: Issues and directions. Ann. Des Telecommun., 55: 324-340.

Shabtai, A., Y. Fledel and Y. Elovici, 2010. Automated static code analysis for classifying android applications using machine learning. Proceedings of the 2010 International Conference on Computational Intelligence and Security (CIS'10), December 11-14, 2010, IEEE, Nanning, China, pp: 329-333.