Strategy to Reinforce Security in Telemedicine Services

Mee Ja Chang*, Jun Kwon Jung*, Min Woo Park*, Tai Myoung Chung**

* *Department of Electrical and Computer Engineering, Sungkyunkwan University, Korea*
** *College of Information and Communication Engineering, Sungkyunkwan University, Korea*

mjchang@skku.edu, {jkjung,mwpark}@imtl.skku.ac.kr, tmchung@skku.edu

Abstract— Demand for medical services is increasing rapidly because of worldwide aging and increase in population. Most countries are trying to introduce and disseminate telemedicine service (TMS) to decrease the necessary budget for health services. However, many doctors are concerned about the security of telemedicine services. Security of medical information should be reinforced for widespread use of telemedicine. This study analyzes telemedicine services between patient and doctor, especially medical information security of clinics and medium-size hospitals because these clinics and hospitals typically use PCs, servers, and vendor software. Furthermore, these clinics and hospitals usually do not employ security specialists and are more vulnerable to medical information security threats. This paper considers the security aspects of telemedicine and the Internet of things (IoT) together, because, after all, healthcare-devices perform a function of telecommunication. This paper reviews the necessity and strategy for enhancing security of medical information systems. The risk of data leak in medical information systems is analyzed quantitatively and is used to support the need for reinforcement of security.

Keywords—Telemedicine, IoT telemedicine, Telemedicine security, U-health security, security

I. INTRODUCTION

Information technology is developing consistently with the assistance of wired or wireless communication networks. Telecommunication service providers are trying to renovate themselves to provide a convenient and consumer-oriented service.

Hospital information systems such as order communication systems (OCS), electronic medical records (EMR), picture archiving communication systems (PACS), lab information systems (LIS), and hospital websites have been developed and introduced to university hospitals and private clinics. Doctors in such institutions diagnose and treat their patients much more conveniently with the assistance of these systems.

The concept of telemedicine services was introduced to reduce the cost of medical practice and to provide more convenience for patients during the course of using the hospital information system.

Telemedicine is defined as medical practice, which can happen from a remote location, with the assistance of imaging and diagnostic devices that are installed with wired or wireless communication network technology and hospital information systems.

Internet of things (IoT)-based telemedicine is a kind of medical practice that collects and transfers patients' information using sensors and communication network technology.

Legislation about telemedicine started in the United States in 1997. About 20 states in America promulgated a law for telemedicine in 2011. Even though European countries tried to introduce telemedicine using IT technology, they were not successful in passing unified legislation because of differences in medical law between countries and hence, did not construct a standard telemedicine system [1].

In Japan, where the population is aging as fast as Korea's, telemedicine between doctors began about 40 years ago. However, telemedicine between patients and doctors was not allowed until a large-scale earthquake. After the earthquake, the Japan government allowed telemedicine and even publicized a law about telemedicine in March 2011 because of increased radiation contaminated medically vulnerable areas [2].

The Korean government allowed telemedicine only between doctors until 2014. They started to provide telemedicine services between patients and doctors by way of showing an example in September 2014 [3].

Even though telemedicine offers tremendous advantages, doctors and medical associations in many countries refuse to adopt telemedicine between patients and doctors because of the risk of medical malpractice and their responsibilities, vulnerability of personal data, limited availability of telemedicine technology, problems with standardization and capital costs for IT systems.

Currently, telemedicine is allowed only when patients are in remote areas such as prisons, convalescent hospitals, or doctorless villages in Korea and Japan that are affected by radiation contamination. However, IT experts expect and anticipate that telemedicine will be activated soon between

patients and doctors to resolve the increased medical demand and to reduce the financial impact.

We suggest a possible obstacle in the security aspects of expanding telemedicine and introduce a strategy for reinforcing security in hospital information systems. After researching previous studies of telemedicine security, we analyze several telemedicine system models.

II. PREVIOUS STUDIES OF TELEMEDICINE SECURITY

A. Security in Wired Networks

The Ethernet Passive Optical Network (EPON) system was used to transfer patient and hospital medical records. Yan and Makris et al. reported that the vulnerability in the transfer channel can cause critical damage to the entire telemedicine service. They reported that the Ethernet Passive Optical Network system has security vulnerabilities such as eavesdropping, DoS/DDoS attack, ToS (Theft of Service), and Weak Control protocol (Multi-Point Control Protocol). They suggested several methods such as confidentiality, authentication, access control, summation strategy, and using other network technologies to relieve these problems.

They recommended several solutions such as using data cryptography to prevent access and modification by unauthorized persons, using authentication protocols, using security-enhanced communication device and applying the security technology implemented on the hybrid network [4]-[5].

B. Security in Wireless Networks

Devaraj et al. reviewed safe data transfer methods, patient monitoring, and compression technologies in medical image information using wireless networks in telemedicine systems [6].

C. IoT Security

Jung, Lu, Kim et al. reported that security in the following layers should be interrelated and applied:

. Security in the perception layer is necessary for sensitive patient information.

. Security in the transportation layer is necessary when the sensitive data is transported via WIFI, 3G/LTE and Internet.

. Security in the application layer is necessary when doctors use the sensitive data to care for their patients in the hospital [7-9].

D. Authentication in Telemedicine Systems

Wu et al. reported that a password-based authentication method was suitable for the mobile telemedicine environment. They integrated a concept of pre-calculation in a communication process to improve data integrity, confidentiality, and availability. They suggested that this method would be an alternate way to avoid complex and time-consuming exponential calculation processes. Replay attacks, on-off-line password guessing attacks, stolen-verifier attacks, and impersonation attacks can be prevented by the application of an authentication system [10].

E. The importance of General Telemedicine Security

The standardization of telemedicine security and poor acknowledgment of the system was reviewed in prior studies. Ahn, Noh, and Grag et al. pointed out the problem of poor acknowledgment of security and the lack of solutions to solve the security problem. They also suggested that security in telemedicine systems should be emphasized more than in general information systems. Especially, many authors regarded reliability and availability as an important and primary theme because these two factors are critical and determinant issues in supporting telemedicine systems. A data leak or illegal modification of patient information in telemedicine systems can result in a disaster in patient information management. They also suggested and emphasized that improvement in the quality of study about security will be achieved through the proliferation of telemedicine services and improvement of quality of service [11]-[13].

F. Quantitative Modeling and Method for Reducing the Risk of Sensitive-data leak

Kim et al. suggested the concept of quantitative modeling and the method for reducing the risk of sensitive-data leak by using the analysis of IT systems involved in the case of the data leak by insider or outsider. They tried to represent sensitive information as quantitative variables and added physical and logical paths, which represents data leakage as a formula [14].

A security strategy, which is applied to user-devices and permissioned IDs, is used as a basic variable. They created a formula to measure risk using these variables and suggested a strategy to reduce the risk of sensitive information leakage. Especially, this risk measurement formula is simple to calculate when compared to that of existing quantitative risk analysis methods and is easy to estimate the relative risk of various systems. We used Kim's quantitative modeling and method to analysis our hospital information system security

G. Data Loss Prevention (DLP) System

The main features of Data Loss Prevention (DLP) are as follows:

. Real-time monitoring of information leakage

. Notify staff or special devices automatically when someone violates the policy

. Blocking and preventing information leakage(email, P2P, FTP, messenger)

. Manual or automatic encryption of outbound transmission of information

. Prevention of forced elimination of the DLP solution or bypassing DLP agents

. Controlling devices such as USB, CD, etc.

To prevent personal information and sensitive information leakage, large corporations monitor information leakage with the aid of DLP systems [15]-[19].

III. INTRODUCTION OF STRATEGY TO REINFORCE SECURITY IN TELEMEDICINE SERVICES

A. Telemedicine Model Description

Telemedicine is divided into two parts; "telemedicine between doctors" and "telemedicine between doctors and patients". The study reviews the security of telemedicine services between doctors and patients. The study also reviews the strategy for enhancing security of hospital information systems. The general model of telemedicine is as demonstrated in Figure 1. Temperature, pulsation, and daily activities will be measured and transferred through the gateway and IoT devices. The measured data is stored and analyzed in a server that is located at the monitoring site. Doctors can examine and analyze the stored data. Doctors can also give a prescription to the patient using a video-assisted medical device and request the patient to visit the hospital if necessary.

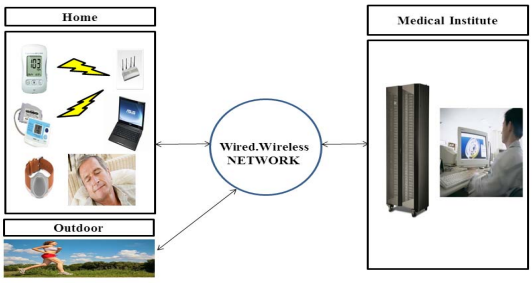

Figure 1. General model of a telemedicine system

When a doctor takes a medical examination by telemedicine, the following aspects should be considered for security.

Materials and methods for securing telemedicine systems using IoT devices

. Patient information sensing:

Authentication at the terminal and encryption of measured information, Use of light-weight encryption algorithm

. Communication between the home gateway and medical devices:

Encryption and integrity when using WIFI, Bluetooth, and Zigbee

. External network including wired or wireless networks:

Use of authentication, encryption, and access control mechanisms to prevent DoS attack, eavesdropping, and forgery

. Servers in the medical institution:

Use of authentication, access control mechanisms, encryption and data loss prevention mechanisms.

An international standard for security of patient information sensing area has not been developed yet. The solution, if developed safely, will be applicable to medical devices. The security of communication between the home gateway and medical devices, which is regarded as the transportation area and the security of external networks were consistently developed and supplemented by existing telecommunication service providers. Therefore, it is necessary to cooperate with telecommunication companies to enhance the level of security. Security of applications is around the hospital information systems that store the medical records that belong to the institution. Leakage of patient information by an unauthorized person may result in critical damage to the entire telemedicine system because patient information is stored abundantly in hospital information systems.

One of the models used in telemedicine is between the patient and medical institute, as shown in Figure 2. The other model is between the patient, central process center and medical institute, as shown in Figure 3. The former model is provided in Korea since September, 2014.

1) Telemedicine between the Patient and Doctor:

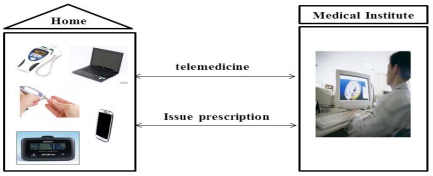

Figure 2. Telemedicine model between patients and doctors

The remote monitoring video communication system was installed in the personal computer of the medical institute. The personal glucometer, sphygmomanometer, and activity meter were prepared at home. The medical data measured from each home, then, would be uploaded using the Internet and transferred safely. Security of information systems at the medical institute should be managed safely.

When the use of telemedicine increases and when the system is established by law, a central process center will become necessary. The role of a central process center is to store data, which is sent and received by patients, pharmacies, and medical institutes.

2) Telemedicine between the patient, Central Process Center and Medical Institute:

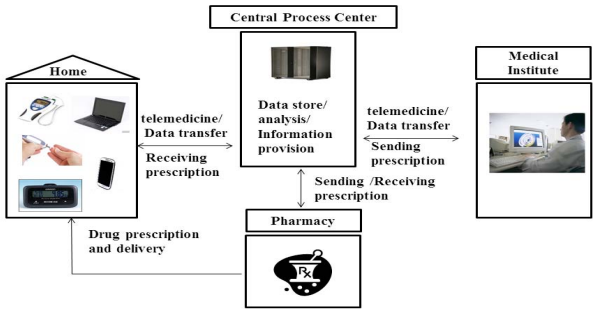

Figure 3. Telemedicine between the patient, central process center, and medical institute

The other important role is to mediate the conflicts related to the telemedicine service by presenting the stored data as supporting evidence. Authentication, access control, confidentiality, integrity, and non–repudiation should be provided by the central process center to store information safely. Authentication, confidentiality, integrity, and non-repudiation can be achieved by encryption. However, access control can only be realized by using access control facilities such as firewalls, IPS and security policies.

Security of the information systems of medical institutes is equally important to the telemedicine models A and B because medical information of the patient is accumulated and stored for an extended period.

A leakage of medical information can occur because of hacking and/or the negligence of medical personnel. An intentional leakage may be caused by an insider or by an outsider who maintains software or data. The distribution of medical institutes in Korea is shown in Table 1. Clinics, pharmacies, and hospitals where IT specialists are not employed, usually use software that is developed by an external software development company. Most private clinics, pharmacies, and hospitals use software developed by software development companies. Typically, maintenance and repair services are provided by the company; therefore patient information leakage can occur by an outsider frequently. The dependency of the medical institutes to software development companies is attributed to a demand for the payment of medical consultation and is shown in Figure 4. The medical insurance billing program should be reviewed because the cost of a drug and the quality of the medical practice varies according to medical insurance policy established by the government[20]-[21].

Table 1. MEDICAL INSTITUTES IN KOREA*

Medical category	Number
Upper-level General Hospital	329
General Hospital	1,468
Care Hospital	1,298
Clinic	28,673
Dental Hospital and Clinic	16,177
Oriental hospital and clinic	13,552
Public health center	3,516
Total	86,010

* Medical institutes in Korea: Hospitals and clinics (by medical law) and pharmacies

Medical institutes prevent access of unauthorized personnel into the hospital information system by using PC-based firewalls or other special firewalls. However, software manufacturers can access the hospital information system if necessary and this makes it difficult to prevent information leakage.

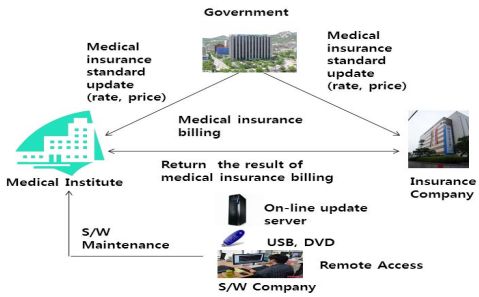

Figure 4. Flow diagram for medical insurance billing

B. How to Strengthen the Security of the Hospital System

For the protection of patient information, Data Loss Prevention (DLP) systems may help to prevent data leakage from the hospital information system. DLP continuously monitors data leaks by insiders and outsiders. A DLP system is the primary security solution in a telemedicine environment.

The model with a DLP system is shown in Figure 5.

The audit trail of illegal access by an unauthorized person, trial of medical information leaks and information of agent deletion will be transferred to the medical institute through a trusted-party server.

The trusted party will report the information leak to doctors or pharmacists immediately for prompt response.

This method is recommended to those without enough reliable hospital information systems manager.

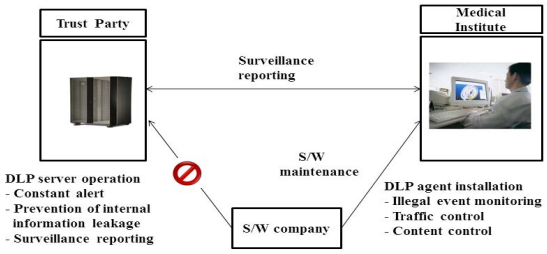

Figure 5. Application of data loss prevention by trusted party

IV. SECURITY ANALYSIS

The risk of personal or sensitive information leaks should be evaluated when DLP is applied to the hospital information system. The information leakage pathway value and risk index were calculated by the quantitative modeling and risk reduction method [14]. The medical institute is regarded as one using a software company for maintenance and as using a desktop PC.

If the medical institute uses servers and an unauthorized person has administrative privileges (illegally), then the risk is similar to the medical institute using a desktop PC.

A. *Method 1. When firewalls are applied for access control:*

. Variables

- UD_1: User Desktop PC
- Physical Path: PP_1 = USB port, PP_2 = communication modem
- Logical Path: LP_1 = leakage program 1, LP_2 = *P2P*, LP_3 = e-mail

. CLP identification

- UD_1(PP) = {PP_1, PP_2}, UD_1 (LP)={LP_1, LP_2, LP_3}
- CLP = {PP_1* LP_1, PP_1*LP_2, PP_1*LP_3, PP_2*LP_1, PP_2*LP_2, PP_2*LP_3}

. The value of maximum leakage risk path (SP = 1)

- PLP_MAX(UD_1) = 1+1+1+1+1+1 = 6

. The value of real leakage risk path

1) *Security Policy: using firewall*

{$SP(PP_2)$= 0.5}(When user can control his S/W)

PLP (UD_1)= 1+1+1+0.5+0.5+0.5 = 4.5

2) *Security Policy: using firewall {$SP(PP_1)$= 1}* (When an outsider gets an administrative account and stops the functioning of the firewall)
PLP(UD_1) = PLP_MAX(UD_1) = 6

. The risk factor of the equipment

1) LRI(UD_1) = PLP(UD_1)/PLP_MAX(UD_1) = 4.5/6 = 0.75
2) LRI(UD_1) = PLP(UD_1)/PLP_MAX(UD_1) = 6/6 =1

B. *Method 2. When DLP is applied*

(Trusted party controls and monitors DLP agents in each medical institute)

. The value of maximum leakage risk path (SP = 1)

- PLP_MAX(UD1) = 1+1+1+1+1+1= 6

. The value of real leakage risk path

- Security Policy: applying DLP {SP(PP_1, PP_2,) = 0.5}
- PLP(UD_1)= 0.5+0.5+0.5+0.5+0.5+0.5 = 3

. The risk factor of the equipment

- LRI(UD_1) = PLP(UD_1)/PLP_MAX(UD_1) = 3/6 = 0.5

As shown in method 1, if an unauthorized outsider possesses an administrative account, the risk of information leakage will be equal to the case of having no security policy despite using a firewall.

As shown in method 2, even if an unauthorized outsider processes an administrative account, the action of the unauthorized person is recognized by the DLP system and is reported to the manager. The risk of information leakage will be reduced because the actions of the unauthorized person are changeable and controllable. Therefore, method 2 is safer than the method 1.

V. CONCLUSION

Telemedicine services will continue to grow in the near future. Many countries, medical device manufacturers, telecommunication service providers, and medical institutes are preparing for telemedicine services and developing telemedicine technology to meet the increased demand for medical services. In this paper, the security of two models of patient–doctor telemedicine and the security requirements while using IoT medical devices are analyzed in this paper. The strategy of reinforcing hospital information system security is also described. The information leakage risk is calculated quantitatively and is used to support the need for reinforcement of security. It will be worthwhile to evaluate the security aspects of the entire telemedicine environment including the networking layer and perception layer of IoT in the near future.

References

[1] Y.H. Yoon, “Enhance issues of the global competitiveness of telemedicine industry in korea”, Retrieved from DBpia database 13(3), Sep 2011

[2] The information committee of KAMS, “The present telemedicine condition of the advanced countries”, Korean Academy of Medical Sciences, Jan 2014, e-Newsletter

[3] H.J. Shon, “The telemedicine pilot project start from September” MINISTRY OF HEALTH & WELFARE press Release in Korea, Sep 2014.

[4] Yan, Y., & Dittmann, L, “Security challenges and solutions for telemedicine over EPON”. ETELEMED, the Sixth International Conference on eHealth, Telemedicine, and Social Medicine, 2014

[5] Makris, L., Argiriou, N., & Strintzis, M. G, “Network and data security design for telemedicine applications”. Inform Health Soc Care, 22(2), 1997

[6] Devaraj, S. J., & Ezra, K, "Current trends and future challenges in wireless telemedicine system". Electronics Computer Technology (ICECT), 2011 3rd International Conference on, 2011
[7] J.W. Jung, "IoT Security : Outlook and challenges.", Embeded World, 2014, *141*(9)
[8] Lu, D., & Liu, T, "The application of IOT in medical system." IT in Medicine and Education (ITME), 2011 International Symposium on, 2011
[9] H. W. Kim, "Security issues in IoT services". Communications of the Korea Information Science Society, 32(6), Retrieved from DBpia database, 2014
[10] Wu, Z., Lee, Y., Lai, F., Lee, H., & Chung, Y. "A secure authentication scheme for telecare medicine information systems". Journal of Medical Systems, 36(3), 2012
[11] Ahn, H., Lee, B., & Jeong, E, "A study of security technique on cloud based healthcare system". *Journal of Security Engineering, 10*(6), Dec.2013
[12] S. C. Noh, "A study on five levels of security risk assessment model design for ensuring the U-healthcare information system", *Journal of Information and Security, 13*(4), 2013
[13] Garg, V., & Brewer, J, "Telemedicine security: A systematic review", *Journal of Diabetes Science and Technology, 5*(3), 2011
[14] Kim S, Kim N, Chung T, Ramage M, Bissell C. "Study on sensitive information leakage vulnerability modeling". Kybernetes, 44(1), 2015
[15] Liu, S., & Kuhn, R, "Data loss prevention". *IT Professional, 12*(2), 2010
[16] Al-Fedaghi, S, "A conceptual foundation for data loss prevention". International Journal of Digital Content Technology and its Applications. 5(3), Mar. 2011
[17] Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V, "A semantics-aware classification approach for data leakage prevention". Information Security and Privacy, 2014
[18] Consortium of CERT(Korea), "CONCERT security consumer report: DLP (data loss prevention)", Nov.2011
[19] Olzak. T, "Improve data protection processes with content discovery, monitoring and filtering", 2007
[20] IST, "Electronic medical record adoption has increased with the proliferation of data that infringes on the accident risk". National IT Industry Promotion Agency, Weekly Technology Trend, Sep. 2011
[21] HIRA, "Health insurance review & assessment service in Korea, in the first half of 2014, cashier statistics indicators". Retrieved 10.30, Oct. 2014