Data Security and Privacy of e-Healthcare in Electronic Medical Environment

Jin Wang[1], Zhongqi Zhang[1], Xiaoqin Yang[1], Liwu Zuo[1], Jeong-Uk Kim[2]

[1] School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China
[3] Department of Energy Grid, Sangmyung University, Seoul 110-743, Korea

Abstract. Electronic healthcare (e-healthcare) is a relatively novel application which is supported by techniques like electronic process, wireless communication, and distributed storage, etc. It is of vital importance to protect the patient-related data from leaking away. In this paper, we proposed a general three-tier medical architecture for e-healthcare applications and discussed its security issues in detail. In addition, we summarized some researches in the domain of e-healthcare for its data security and privacy issues. The security of the distributed data storage in wireless body area networks (WBANs) and the privacy of the patient-related information stored in the database of the medical organization system are discussed respectively. Finally, we concluded some of the achievements from our references.

Keywords: e-healthcare, wireless body area network, security, privacy, medical information system

1 Introduction

Wireless sensor networks consist of many different types of sensors aiming at monitoring a wide variety of ambient conditions [1]. Recently, with the rapid development and implementations of wearable medical sensors and wireless communication, wireless body sensor networks (WBANs) have played a significant role in e-healthcare which allows the vital data or parameters of a human body to be collected by wearable or embedded sensors automatically. Further, the patients' vital data will be transmitted to the database through short-range wireless communication devices. Variety of sensors such as heart rate monitor sensor, blood pressure monitor sensor and pulse Oximeter SpO_2 monitor sensors are already in use. As most sensor devices and their applications are wireless in natural, security and privacy are among major areas of concerns [2].

Fig. 1 is our proposed sensor network in e-healthcare application scenario. The vital data captured by the sensors are transmitted through the wire or wireless network. Obviously, the whole network architecture requires to be protected from the outside malicious invasion. In Tier 1, the WBANs part mainly consists of tiny wireless sensor nodes that are placed in, on, or around the patient's body. These sensors monitor the patient's vital signs, such as electrocardiogram (ECG), pulse, and blood pressure, or important environment parameters like temperature and humidity, consistently. The

patient-related data means the sensor monitor readings, along with the patient profiles of some other information [3]. The sensors collect and transmit the patient-related data to one or more local servers through gateway, which is designed to provide the connection between the information capturing sensor networks to the infrastructure. The servers may provide further data processing, aggregation, or distributed storage. In Tier 2, the patient-related data from all WBANs may ultimately be sent to a centralized healthcare database for permanent records. Thus, the users of patient-related data can either remotely access the data from the database or query information locally from the WBAN, depending on the application scenario.

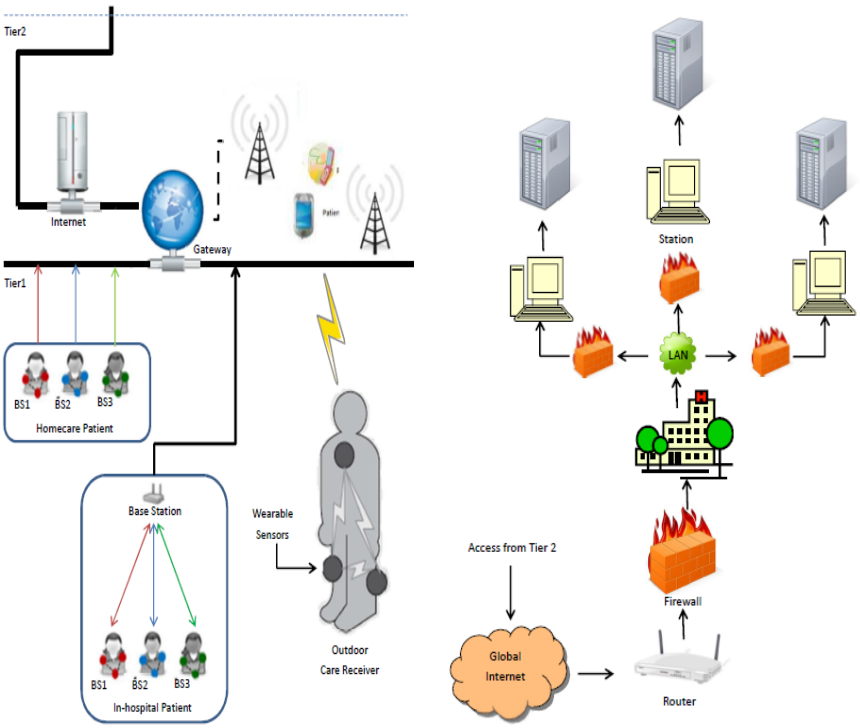

Fig. 1. Our proposed e-healthcare network architecture

Tier 3 is part of a typical architecture of medical organization systems in healthcare application. The initial data captured in Tier 1 is transmitted to the database or distributed storage in Tier 3 and waiting to be read and computerized. Due to all computer hosts are dispersed to different places in network, if we want to share the resources or the data with different host, we must contact through the Internet. There are generally workstations, personal computers, or host systems in the Internet, which can all be connected through the network [4]. As Tier 3 shows, to protect the Internet and the internal data of the medical organization from malicious attacks, Firewalls are generally needed. It is a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts.

2 Importance of e-Healthcare Security and Privacy

There are potential large impacts for sensor network applications in e-healthcare scenario [5]. These can be realized through real-time, continuous vital monitoring to give immediate alerts of changes in patient status. Also, the WBAN operates in environments with open access by various people such as hospital or medical organization, which also accommodates attackers. The open wireless channel makes the data prone to be eavesdropped, modified, and injected. Many kinds of security threats have been existed, such as unauthenticated or unauthorized access, message disclosure, message modification, denial-of-service, node capture and compromised node, and routing attacks, etc. Among which two kinds of threats play the leading role, the threats from device compromise and the threats from network dynamics.

It processes a vast potential for future development. As seen in Fig.2, from 2008 the projected sales of sensors were growing with a high speed [2].

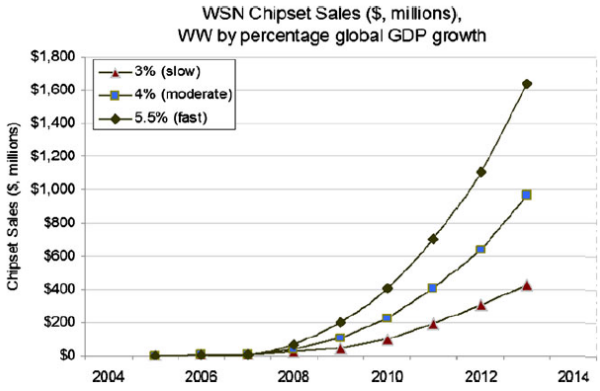

Fig. 2. The projected sales of wireless sensors

A lot of sensitive medical information is being collected, transmitted, stored, and shared among different medical organizations, due to the development of the new e-healthcare networks. Vast majority of such electronic transactions are offered through the Internet, even though the exchange of personal or medical information is clear prerequisite [6]. Therefore, it is clear, specific measures are necessary to ensure that users can access and process personal data. For the purpose, only when they are necessary in accordance with the requirements of the privacy data processing or the purpose of the data processing is reasonable, it will be authorized to perform the task, and the data could be obtained.

The problem of security is rising nowadays. Especially, the privacy of communication through Internet may be at risk of attacking in a number of ways. On-line collecting, transmitting, and processing of personal data cause a severe threat to privacy. Once the utilization of Internet-based services is concerned on-line, the lack of privacy in network communication is the main conversation in the public. This problem is far more significant in modern medical environment, as e-healthcare networks are implemented and developed. According to common standards, the network linked with general practitioners, hospitals, and social centers at a national or international

scale. While suffering the risk of leaking the privacy data, such networks' privacy information is facing great danger. Hence, much attention must be paid to the privacy principle of transparency, so that patients must know who has access to their data and for what purpose.

Generally speaking, intruders include hacker, spies, terrorists, co-intruder, and profession. They use operator commands, macro, and Java Script to break through a computer network with the purpose to retaliate, steal confidential information, and fulfill themselves' senses of accomplishment. For a further conclusion, their success depends on some current problems in the whole computer networks, such as errors in network framework design, management negligence, illegal downloading.

The above motives are the common considerations of our research. As talked previously, we figured that many of the sensor networks applications in the e-healthcare network are heavily relied on technologies that are prone facing security threats.

3 Security Issues

Confidentiality, data integrity, accountability, availability, and access control are the overall system requirements of the fundamental of the security issues. For assuring these security requirements, encryption which raises the challenge of developing efficient key management protocols and Firewalls must be used generally [7].

In [8], M. Farzandipour *et. al.* claimed that requirements of the electronic health records information system security should be ensured that technical and administrative measurers have to be taken in order to achieve the objectives of data protection and security. Their research shows that many countries have begun to move toward electronic health records and a nationwide health information work. They declared that how to protect the whole network for e-healthcare is coming into the major domain of the modern academic circles.

For WBANs, it is vulnerable to threats and risks. An adversary can compromise a sensor node, alter the integrity of the data, eavesdrop on messages, inject fake message, and waste network resource. Unlike wired networks, wireless nodes broadcast their message to the medium [9]. There are a number of challenges one must overcome, including how to make tough balances between security, efficiency, and practicality. There are three major requirements for data storage, confidentiality, dynamical integrity assurance, and dependability. To cope with the three major requirements for data storage in WBAN and enhance the dependability of the data, some solutions have been proposed.

In [10], L. Zhou *et. al.* carried out a novel media-aware traffic security architecture and pointed out for major components to the media-aware traffic security architecture which are key management, batch rekeying, authentication, and watermarking. They classify the key management according to the multimedia traffic that exercise the control and whether the scheme is scalable or not, and changing the key on the basis of synchronization and inefficiency.

In [11], C. H. Liu *et. al.* proposed some medical managerial strategies being applied to the network environment of the medical organization information system so as

to avoid the external or internal information security events. They assumed hackers mainly aim at attacking the information in medical organizations, and classified the hacker attacks into interruption, inception, modification, and fabrication. There are four examples of active and passive intrusions: (1) the intrusion through scanning and identifying vulnerable areas; (2) the intrusion through forging the source address; (3) the intrusion through intercepting data transmitted in the network; (4) the intrusion through password-guessing [4]. The attacks mentioned above are likely to happen in any information systems, as well as in the network system in medical organizations where the attacks appear some changes. To cope with the requirements of the network environment in the medical organization so as to enhance the probability of stopping intrusions and to achieve the internal security of the medical organization, the location of the firewall are carefully considered as shown in Fig. 1. The structure of the firewall is divided into three scenarios as Single-Interfaced Bastion Host, Dual-Interfaced Bastion Host, and Screened Subnet Firewall.

4 Privacy Issues

Within many kinds of privacy right, patient privacy for e-healthcare is calling more and more attentions in the modern medical database world. Authorization of the users in the system should not be overlooked and the users should have autonomy and control over their data of any type [12]. As natural existence, the privacy is part of the social life, the patient's state of illnesses and physical condition is regarded as the private information and secret, hence it achieves the protection of the right of privacy. The medical institutions and their employees have duty to protect the patients' privacy. In the meantime, the scope of the privacy is limited to public advantages. For those who are falling ill, they have the wills to protect their privacy among the connection between human and human, based on their self-recognition.

Privacy in the e-healthcare environment comprises anonymity and unlinkability requirements [13]. Anonymity means the electronic medical records must be hidden from insurance providers, researchers, management staff, and any other related personnel who have no appropriate access privileges. And, unlinkability indicates that multiple electronic medical records cannot be linked to the same owner to prevent the profiling of a patient. In the course of having or being part of a medical practice, doctors may learn information they wish to share with the medical or research community. If this information is shared or published, the privacy of the patients must be respected. Likewise, participants in medical research that are outside the realm of direct patient care have a right to privacy as well.

In [11], B. Malin *et. al.* claimed that one of the major privacy issues has been identifiability, such as the extent to which materials and data stored in electronic healthcare database can be linked to the name of the individuals from which they were derived. A privacy attack is the exploitation of an opportunity of someone to identify a study participant based on public research data. Certainly, such attacks on patients' privacy are plausible, but the ability of malicious attackers to utilize genomic data to compromise privacy is limited [9]. The author suggested that, before the data is sent

for research processing, it should be re-identified, which means that personally identifying data is removed from the dataset. Ideally this means that the dataset alone could not be used to identify a participant.

In [14], H. G. Hwang studied whether Internet users have different privacy concerns regarding the information contained in electronic medical records according to gender, age, occupation, education, and electronic medical records awareness. After research in 213 people, among which 84.5% were non-healthcare staff and 88.8% were college, master, or above educated, they got the data that 48.4% of them were understand the electronic medical records, and 35.7% of them were not fully understand it. The results show that the informants' educational level and electronic medical records awareness are positively correlated with their concerns regarding unauthorized access and secondary use of their electronic medical records. The results of this study indicate that highly educated people have greater information privacy concerns related to electronic medical records, particularly the unauthorized access and secondary use of their personal health information.

5. Conclusions

In this paper, we firstly studied the security issues in e-healthcare environments which include the WBAN as the basic tier of our proposed three-tier medical information architecture. Further, we discussed the security protections for healthcare information system database which is the top tier of network. Finally, we discussed the privacy issues in healthcare information systems, including the different users concerns about the privacy issues and how the identifiability protects the system from privacy attack. However, the researches in e-healthcare privacy issues are not as much as that in security. It is our hope that our research could play a guidance role for the beginner in studying the e-healthcare medical information architecture and draw attention of the e-healthcare privacy researches.

Acknowledgments

This work was supported by the Industrial Strategic Technology Development Program (10041740) funded by the Ministry of Knowledge Economy (MKE）Korea. It was also supported by the Natural Science Foundation of Jiangsu Province (No. BK2012461). Prof. Jeong-Uk Kim is the corresponding author.

References

1. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, A survey on sensor networks. IEEE Communications Magazine, 40, 8 (2002)
2. M. A. Ameen, J. W. Liu and K. Kwak, Security and privacy issues in wireless sensor networks for healthcare applications, Journal of Medical System, 36, 1, (2012)

3. M. Li, W. J. Lou and K. Ren, Data security and privacy in wireless body area networks, IEEE Wireless Communications, 17, 1, (2010)
4. C. H. Liu, Y. F. Chun, T. S. Chen and S. D. Wang, The enhancement of security in healthcare information systems, Journal of Medical System, 36, 3, (2012)
5. M. Welsh, D. Malan, B. Duncan, and T. F. Jones, Wireless sensor networks for emergency medical care. GE Global Research Conference, (2004), Harvard University, Boston, USA
6. Q. Wang, K. Ren, W. J. Lou and Y. C. Zhang, Dependable and secure sensor data storage with dynamic integrity assurance, IEEE International Conference on Computer Communications, (2009) Apr. 19-25, Rio de Janeiro, Brazil
7. H. Alemdar, C. Ersoy, Wireless sensor networks for healthcare: a survey, Journal of Computer Networks, 54, 15 (2010)
8. M. Farzandipour , F. Sadoughi, M. Ahmadi, and I. Karimi, Security requirements and solutions in electronic health records: lessons leraned from a comparative study, Journal of Medical System, 34, 4, (2010)
9. J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Journal of Computer Networks, 52, 12 (2008)
10. L. Zhou and H. C. Chao, Multimedia traffic security architecture for the internet of things, IEEE Network, 25, 3, (2011)
11. B. Malin, G. Loukides, K. Benitez, and E. W. Clayton, Identifiability in biobanks models, measures, and mitigation strategies, Human Genetics, 130, 3, (2011)
12. V. Ikonen, E. Kaasinen, Ethical assessment in the design of ambient assisted living, Architecture and Engineering Approach, (2007), Nov. 14-17, Schloss Dagstuhl, Germany
13. J. Y. Sun, Y. G. Fang, and X. Y. Zhu, Privacy and emergency response in e-healthcare leveraging wireless body sensor networks, IEEE Wireless Communications, 17, 1, (2010)
14. H. G. Hwang, H. E. Han, K. M. Kuo, and C. F. Liu, The differing privacy concerns regarding exchanging electronic medical records of internet users in taiwan, Journal of Medical System, 36, 6, (2012)