A Research on Security and Privacy Issues for Patient related Data in Medical Organization System

Jin Wang[1], Zhongqi Zhang[1], Kaijie Xu[2], Yue Yin[1] and Ping Guo[1]

[1] *School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[2] *School of Environmental Science and Engineering, Nanjing University of Information Science & Technology, Nanjing 210044, China*

Abstract

Recently, with the rapid development and implementation of wireless medical sensors, electronic healthcare (e-healthcare) has gained increasing popularity. Monitor and record some vital parameters of patients are of importance to know the patient's health condition. But malicious attacks happen occasionally, which may cause the patient-related data being leaked or modified. In this paper, we made a survey about some researches in the domain of e-healthcare for its data security and privacy issues, such as the security issues 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 systems. We also proposed a general three-tier medical architecture and discussed its security issues in detail. Finally, we concluded some of the achievements from our references.

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

1. Introduction

Recently, with the rapid development and implementations of wearable medical sensors and wireless communication, 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. Wireless body area sensor networks consist of many different types of sensors aiming at monitoring a wide variety of ambient conditions [1]. Some of the e-healthcare applications for sensor networks are providing interfaces for the patient monitoring. The physiological data collected by the sensor networks can be stored for a long period of time and can be used for medical exploration [1]. Further, the vital data will be transmitted to the database using 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].

A lot of concerns in the e-healthcare domain include breaches in malicious attacks and modification of the patient-resident confidentiality, which great legal and professional consequences are in possess of. While running the wireless e-healthcare system, to make sure there is no risk of endangering the lives of patients is a major concern. The U.S. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule gives federal protection for individual health information possessed by enclosed entities and provides patients with a range of rights with reference to their security and privacy information [3].

Figure 1 is part of our proposed sensor network in e-healthcare application scenario. The vital data captured from the sensors are transmitted through the wire or wireless network.

Many parts of the general architecture are required 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 called patient-related data means the sensor monitor readings, along with the patient profiles of some other information [4]. The sensors collect and transmit the patient-related data to one or more local servers through gateway, which may provide further data processing, aggregation, or distributed storage. Gateway is designed to provide the connection between the information capture sensor networks to the infrastructure base WBANs. 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.

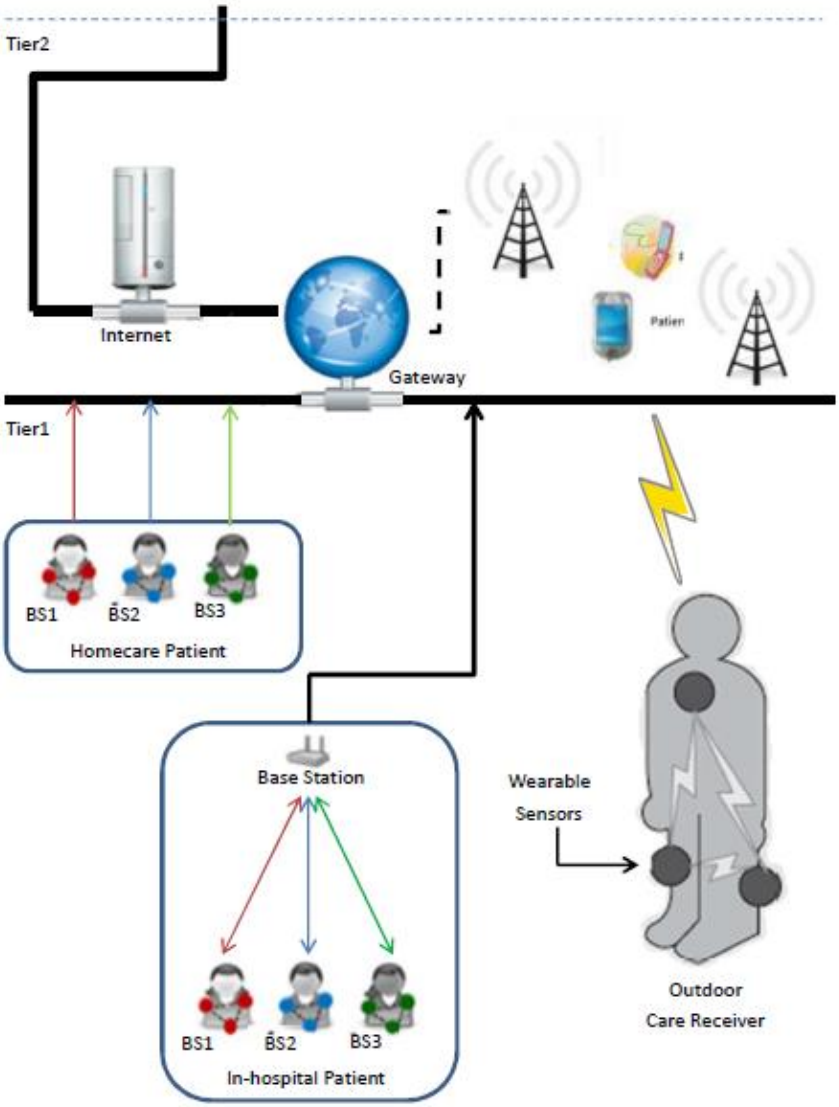

Figure 1. Our Proposed e-healthcare Network Architecture (Tier 1 and Tier 2)

Tier 3 is 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. So if we want to share the resources or the data with different host, we must connect with the Internet. There are generally workstations, personal computers, or host systems in the Internet, which can all be connected through the network [5]. As Tier 3 shows, many systems need protections as medical information contains patients' privacy and the relevant information, such as registration and medication systems. To protect the Internet and the internal data of the medical organization from malicious attacks a Firewall is generally needed. It is a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts.

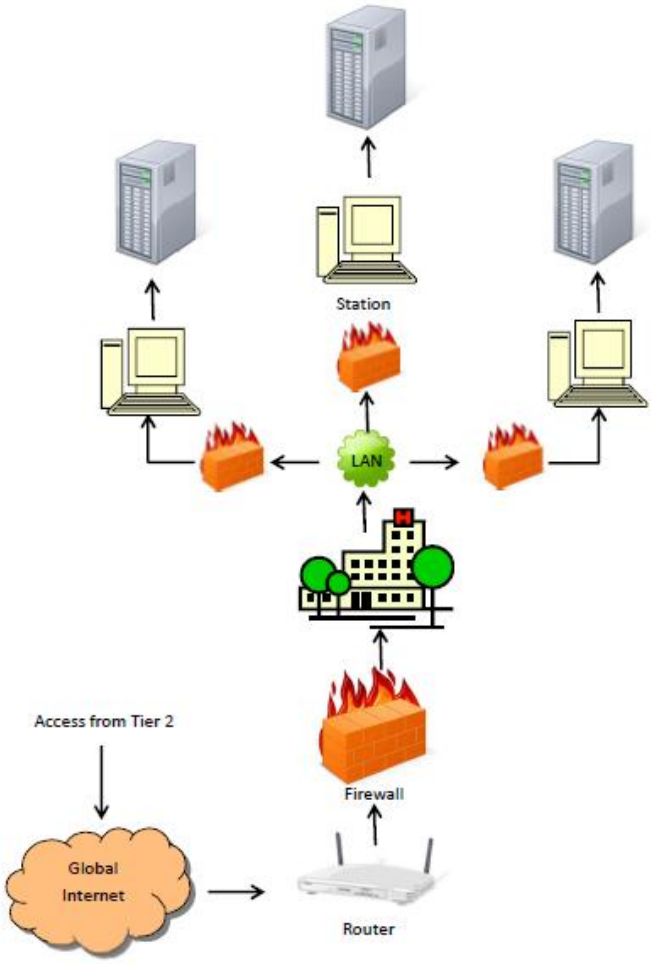

Figure 2. Our Proposed e-healthcare Network Architecture (Tier 3)

The paper is organized as follows. In Section 2 there is a brief overview of the research motivation. Section 3 provides a detailed description of the security issues faced in the e-healthcare environment. We talked about the privacy and access issues in Section 4, and finally, Section 5 provides some discussion and concluding work.

2. Importance of Research in Security and Privacy Issues

There are potential large impacts for sensor networks applications in e-healthcare scenario [6]. 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 being 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 which are analyzed detailed in Table 1 [4]. The patient-related data if not well kept or just stored in one node, could be lost easily due to the device compromise or network dynamics.

Table 1. Two Main Kinds of Threats in WBAN

Device Compromise	Network Dynamics
Sensor nodes in a WBAN are subjected to compromised, as they are usually easy to capture and not temper-proof. If a whole piece of data is directly encrypted and stored in a node along with its encryption key, the compromise of this node will lead to the disclosure of data.	The WBAN is highly dynamic in nature. Due to accidental failure or malicious activities, nodes may join or leave the network frequently. Nodes may die out due to lack of power. Attackers may easily place faked sensors in order to masquerade authentic ones, and could take away legitimate nodes deliberately.

As seen in Figure 3, from 2008 the projected sales of sensors were growing with a high speed. It processes a vast potential for future development [2].

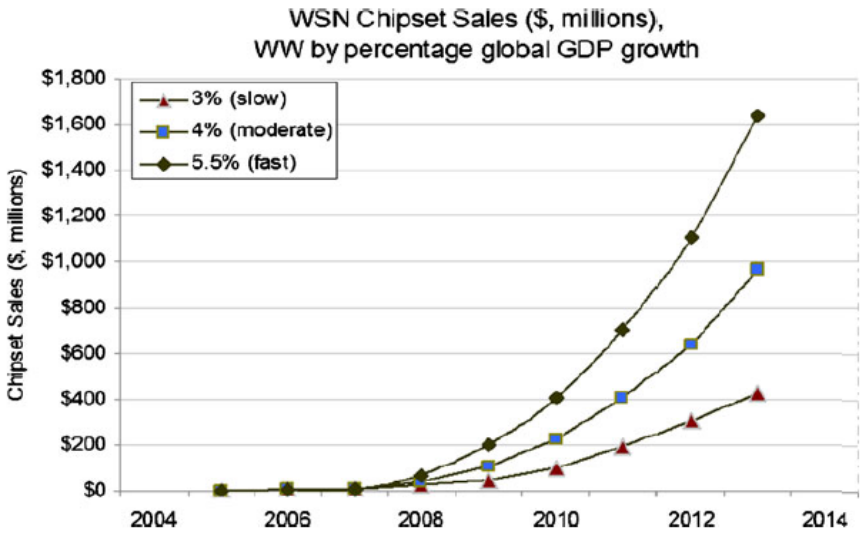

Figure 3. The Projected Sales of Wireless Sensors

Similarly Figure 4 shows the world revenue forecast and growth rate for healthcare, medical and biometrics markets [2]. We can see that sensor networks have a great future ahead with tremendous growth rate.

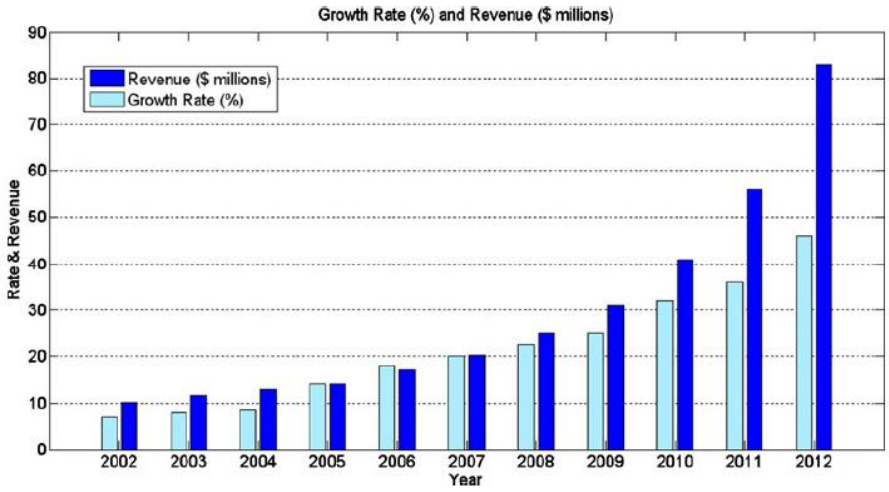

Figure 4. The Growth Rate and Revenue for Healthcare

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 [7]. 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 according to the principle of the protection of privacy, or the purpose of the data processing is a reasonable time, it will be authorized to perform the task, and the data could be obtained.

The problem of security is rising nowadays. However, 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 make up 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 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 can reduce the costs and improve the effectiveness of the healthcare system.

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 healthcare are heavily relied on technologies that are prone to face security threats. 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.

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 [8].

In [9], 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. Their research to requirements and solutions in electronic health records ranges from health information security organization requirements to security requirements of information assets classification and control, from human resources security requirements to physical and environmental security requirements, and even security requirements of communications and operations management of health information.

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 [10]. 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 which are detailed in Table 2. To cope with the three major requirements for data storage in WBAN and enhance the dependability of the data, some solutions have been proposed. The following paragraphs are organized by some existing related works in this domain, and we talked further whether they can satisfy the previously mentioned requirements.

Table 2. Three Major Security Requirements for Data Storage in WBAN

Confidentiality	Patient-related data should be kept confidential during storage periods. Especially, its confidentiality should be robust against node compromise and user collusion.
Dynamical integrity	Patient-related data must not be modified illegally during storage periods, which shall be checked and detected by a node dynamically.
Dependability	Patient-related data must be readily retrievable when node failure or data erasure happens.

In [11], Wang *et al.*, proposed a dependable and secure data storage scheme with dynamic integrity assurance. Based on the principle of secret sharing and erasure coding, they first propose a hybrid share generation and distribution scheme to achieve reliable and fault-tolerant initial data storage by providing redundancy for original data components. To further dynamically ensure the integrity of the distributed data shares, they then propose an efficient data integrity verification scheme exploiting the technique of algebraic signatures. Suppose a

sensor node v has $data$ to be stored, their enhanced scheme can be summarized in the following four steps.

- Step1 v calculates DATA according to the basic scheme and further divides the DATA into two parts, *i.e.*, $\{data, h(data, k_r)\}_{k_r}$ and $\{k_r\}_{K_{UV}}$
- Step2 v then encodes $<\{data, h(data, k_r)\}_{k_r}>$ into n fragments by employing a (m, n) RS code. That is v constructs $M(x) = D_1 + D_2 x + ... + D_m x^{m-1}$, where $\{data, h(data, k_r)\}_{k_r} := \{D_1 \| ... \| D_m\}$. v further obtains n $\overline{S}_j s$ with each $\overline{S}_j$ $\overline{S}_j = M(\alpha^j)$ $(1 \le j \le n)$, where $n \le 2^q - 1$
- Step3 v then employs a (m, n) SS scheme to obtain n shares of $\{k_r\}_{K_{UV}}$ denoted as $\underline{S}_1, ..., \underline{S}_n$
- Step4 v randomly selects n neighbors from NB_v. For each neighbor w_i $(i \in \{1, ..., n\})$, v distributes $\{v, seqno, S_i, S_i\}_{K_{vw_i}}$. The original $data$ is erased.

In [12], S. Chessa *et al.*, used a Redundant Residue Number System (RRNS) to encode data. RRNS encode data as $(h + r)$-tuples of residues using $h + r$ keys, or moduli. Residues are distributed among the mobiles in the network. Recovering the original information requires the knowledge of at least h residues and of the corresponding moduli. Data can be reconstructed in the presence of up to $s \le r$ residue losses, combined with up to $\lfloor \frac{r-s}{2} \rfloor$ corrupted residue. Data security is ensured since mobiles having access to the residues which are able to decode them only if they also know the entire set of moduli. The parameters h and r can be set by the user. However, data integrity is not ensured whenever the number of errors is more than the detecting capability. And to distribute public keys to sensor nodes is not a good choice for interoperability. As to efficiency, the length expansion ratio is $(h + r)/h$ for each file. But to maintain a potentially large set of moduli would overwhelm a sensor node's buffer, which is not efficient for WBANs.

In [13], R. D. Pietro *et al.*, focused on data survival in unattended sensor networks. Some adversaries focus on surgically destroying data which it considers to be of high value. It is the first paper to identify the problem of data survival in Unattended Wireless Sensor Networks (UWSNs). They proposed a straightforward non-cryptographic technique aimed at hiding the data from the adversary. The evaluations show a surprising degree of data survival even when the adversary is relatively long. It also shows that constantly moving data around outperforms keeping data in one place or moving only once, in terms of data survival probability.

However, only making sure the WBANs to be security is far from enough in e-healthcare environment as there are amount of information stored in the database of the medical organization. Hence, some researches have been taken place in the domain of traffic management and healthcare information systems. Traffic management plays a key role in achieving high quality of service (QoS) in a network [14]. Unfortunately, they focused barely in developing mainly to guarantee delay and distortion constraints in conventional traffic management algorithms, which usually neglecting security requirements and not appropriate for security-aware applications. In order to meet the information security requirements for multimedia communication, computation, and services in the environment of an IoT, it is necessary to consider some criteria that refer to the traffic security strategy and performance.

L. Zhou *et al.*, carried out a novel media-aware traffic security architecture in [15] and pointed out for major components to the media-aware traffic security architecture as shown followed in Figure 5. As can be seen in Figure 5, the major components of media-aware traffic security architecture can be divided into four parts, 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.

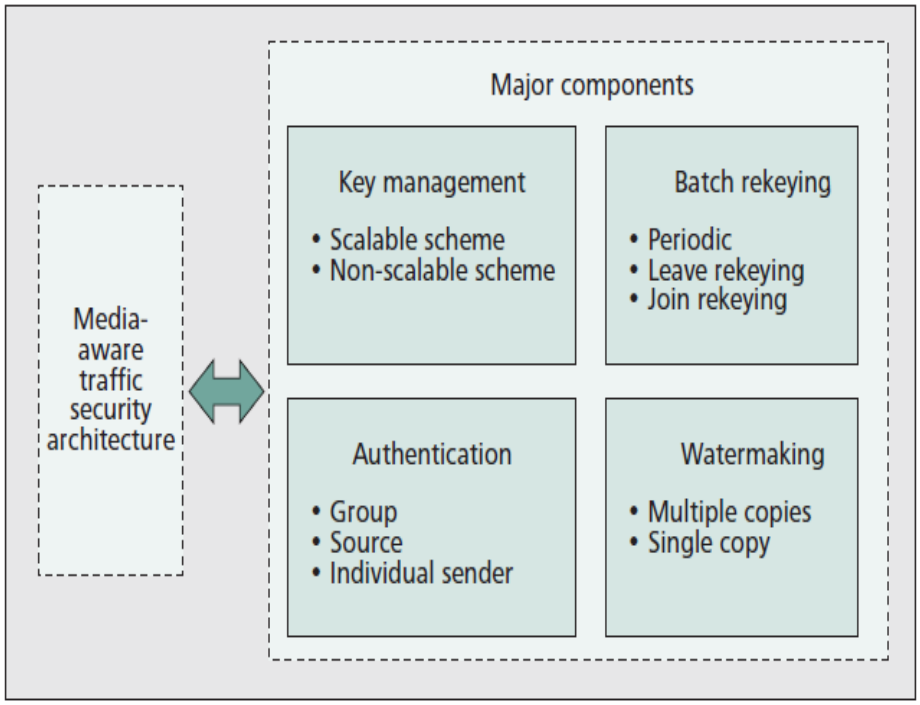

Figure 5. Four Major Components of the Media-Aware Traffic Security Architecture

In [5], 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 [5]. 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 Figure 2. The structure of the firewall is divided into three scenarios as Single-Interfaced Bastion Host, Dual-Interfaced Bastion Host, and Screened Subnet Firewall. The three models of firewall structure are talked in Table 3, detailed.

Table 3. The Three Detailed Models of Firewall Structures

Single-Interfaced Bastion Host	a) Filtering packets: when an external packet enters, it will pass through a packet filtering router which eliminates unqualified packets. And the remaining packets are directed to the bastion host to verify if the packets have any problems. b) Bastion host: it can act as an agent, or a proxy server to perform some security managements. It has functions of verification and it can assist the firewall with verification.
Dual-Interfaced Bastion Host	a) It only use a single host, the entire packet will be delivered over. b) It has two network interface cards, one is connected to the external packet filtering router and the other is connected to the intranet. The purpose of installing two network interface cards is to separate the external network and the intranet, thus avoids direct delivery of packets. This is the advantage of the dual-interfaced bastion host.
Screened Subnet Firewall	a) External packet filtering router. b) Internal packet filtering router. c) Bastion host.

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 [16]. 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 [17]. 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 this way, the application must guarantee a well-defined degree of privacy with precisely formulated and verified rules.

In [18], 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 perpetrators to utilize genomic data to compromise privacy is, for the time being, limited [18]. Before the data is sent for research processing, it is "de-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 [19], 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 people's educational level and electronic medical records awareness are positively correlated with their concerns regarding unauthorized access and secondary use of their electronic medical records. In [17], J. Y. Sun *et al.*, illustrate that an employer may decide not to hire people with physiological disorders, or an insurance company may refuse to provide life insurance knowing a patient's disease history. Their solution to the privacy issues can be concluded as follows: (1) patient use their PDA to send a commitment on the chosen secret and a proof of knowledge for the correct formation; (2) The PDA randomly selects a secret seed η to feed into the PRNG; (3) PDA immediately contacts the primary physician as soon as the body sensors detect abnormal signals.

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. In addition, we studied the importance issues of research in security and privacy in e-healthcare system, including WBANs, finance, and medical organization system. 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.

Acknowledgements

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), and by Jiangsu Province Research and Innovation Project for College Graduates (NO.CXZZ12_05 15). Prof. Jeong-Uk Kim is the corresponding author.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, vol. 40, no. 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, vol. 36, no. 1, **(2012)**.
[3] O. Osunmuyiwa and A. H. Ulusoy, "Wireless security in mobile health", Telemedicine and e-health, vol. 18, no. 10, **(2012)**.
[4] M. Li, W. J. Lou and K. Ren, "Data security and privacy in wireless body area networks", IEEE Wireless Communications, vol. 17, no. 1, **(2010)**.
[5] 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, vol. 36, no. 3, **(2012)**.
[6] M. Welsh, D. Malan, B. Duncan and T. F. Jones, "Wireless sensor networks for emergency medical care", GE Global Research Conference, Harvard University, Boston, USA, **(2004)**.
[7] S. Grizalis, J. Iliadis, D. Gritzalis, D. Spinellis and S. Katsikas, "Developing secure web-based medical applications", Medical Information and Internet Medicine, vol. 24, no. 11, **(1999)**.
[8] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: a survey", Journal of Computer Networks, vol. 54, no. 15, **(2010)**.
[9] 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, vol. 34, no. 4, **(2010)**.
[10] J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey", Journal of Computer Networks, vol. 52, no. 12, **(2008)**.
[11] 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, Rio de Janeiro, Brazil, **(2009)** April 19-25.
[12] S. Chessa and P. Maestrini, "Dependable and secure data storage and retrieval in mobile, wireless networks", International Conference on Dependable System and Networks, San Francisco, California, USA, **(2003)** June 22-25.
[13] R. D. Pietro, L. V. Mancini, C. Soriente, A. Spognardi and G. Tsudik, "Catch me (if you can): data survival in unattended sensor networks", Sixth Annual IEEE Information Conference on Pervasive Computing and communications, Hong Kong, China, **(2008)** March 17-21.
[14] L. Atzori, A. Lera and G. Morabito, "The internet of things: a survey, computer networks", vol. 54, no. 15, **(2010)**.
[15] L. Zhou and H. C. Chao, "Multimedia traffic security architecture for the internet of things", IEEE Network, vol. 25, no. 3, **(2011)**.
[16] V. Ikonen and E. Kaasinen, "Ethical assessment in the design of ambient assisted living", Architecture and Engineering Approach, Schloss Dagstuhl, Germany, **(2007)** November 14-17.
[17] 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, vol. 17, no. 1, **(2010)**.
[18] B. Malin, G. Loukides, K. Benitez and E. W. Clayton, "Identifiability in biobanks models, measures, and mitigation strategies", Human Genetics, vol. 130, no. 3, **(2011)**.
[19] 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, vol. 36, no. 6, **(2012)**.

Authors

Jin Wang Dr. Jin Wang received the B.S. and M.S. degree in the Electronical Engineering from Nanjing University of Posts and Telecommunications, China in 2002 and 2005, respectively. He received Ph.D. degree in the Ubiquitous Computing laboratory from the Computer Engineering Department of Kyung Hee University Korea in 2010. Now, he is a professor in the Computer and Software Institute, Nanjing University of Information Science and technology. His research interests mainly include routing algorithm and protocol design, performance evaluation and optimization for wireless ad hoc and sensor networks. He is a member of the IEEE and ACM.

Zhongqi Zhang he obtained his B.S. degree in the Eletronic and Information Engineering from Nanjing University of Information Science and technology, China in 2012. Now, he is working toward the M.S. degree in the Computer and Software Institute. His current research interests are in performance evaluation for wireless sensor networks, and healthcare with wireless body area networks. He is a student member of IEEE, ACM and CCF.

Kaijie Xu he is a student at the School of Environmental Science and Engineering, Nanjing University of Information Science and Technology. His research interest covers image processing, pattern recognition.

Yue Yin received the Bachelor degree in Applied Computing from Nanjing University of Information and Science Technology in 2011. She is currently pursuing a Master degree in Technology of Computer Application in the former institution. Her research interests include routing algorithms and data replication of wireless sensor networks.

Ping Guo obtained her B.S and M.S degree in the Computer Software and Theory from LanZhou University, China in 1997 and 2005, respectively. She received Ph.D degree in Nanjing University of Science and Technology in 2012. She is a lecturer in the College of Computer & Software, Nanjing University of Information Science & Technology from 2005 till now. Her research interests focus on wireless network security, multiple-hop wireless networks authentication and key management.