Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 10(4): 337-342, Dec. 2012 **Regular Paper**

Analyses of Characteristics of U-Healthcare System Based on Wireless Communication

Jung Tae Kim*, ***Member, KIICE***

Department of Electronic Engineering, Mokwon University, Daejeon 302-802, Korea

Abstract

The medical industries are integrated with information technology with mobile devices and wireless communication. The advent of mobile healthcare systems can benefit patients and hospitals, by not only providing better quality of patient care, but also by reducing administrative and medical costs for both patients and hospitals. Security issues present an interesting research topic in wireless and pervasive healthcare networks. As information technology is developed, many organizations such as government agencies, public institutions, and corporations have employed an information system to enhance the efficiency of their work processes. For the past few years, healthcare organizations throughout the world have been adopting health information systems (HIS) based on the wireless network infrastructure. As a part of the wireless network, a mobile agent has been employed at a large scale in hospitals due to its outstanding mobility. Several vulnerabilities and security requirements related to mobile devices should be considered in implementing mobile services in the hospital environment. Secure authentication and protocols with a mobile agent for applying ubiquitous sensor networks in a healthcare system environment is proposed and analyzed in this paper.

Index Terms: Mobile agent, Privacy and healthcare systems, RFID

I. INTRODUCTION

Today's society is rapidly moving toward an aged society. The rapid changes in modern styles provide ongoing opportunities to build new markets and industries. Radio frequency identification (RFID) systems can be applied to many industries, and include many potential applications such as manufacturing, supply chain management, access control, inventory control, e-passports, pharmacies, and hospital management. RFID has the advantages of low cost and convenience in identifying an object with non-line-of-sight reading.

Ubiquitous technologies based on mobile devices and sensor nodes are able to manage healthcare information with small sensors and devices. As information technologies are rapidly developed, e-healthcare systems are currently being realized. Recently, the trend in healthcare systems has moved toward u-healthcare systems because of smart equipment and devices with low computing power. RFID is an automated data-capture technology that uses low-power radio waves to communicate between readers and tags [1]. RFID technology is also applicable to u-healthcare systems to reduce manual handling errors, monitor patient's medical information accurately, maintain efficient processes, and track patients' location. To utilize this system, new problems should be solved such as security, authentication, and safety [2]. Advanced technologies and existing medical technologies should be combined properly to meet the require-

Received 28 June 2012, **Revised** 10 August 2012, **Accepted** 17 August 2012
***Corresponding Author** E-mail: jtkim3050@mokwon.ac.kr

Open Access **http://dx.doi.org/10.6109/jicce.2012.10.4.337** print ISSN:2234-8255 online ISSN:2234-8883

ments for service efficiency, accuracy, and clinical significance. This kind of fusion technology is called a ubiquitous healthcare system. It should be noted that u-healthcare systems improve and enrich the quality of life. This comes about by the improvement of constraints and medical treatments by connecting a lot of devices with medical treatment. Any security vulnerability may cause a leakage of personal information. Therefore, security protocols should be prepared and taken into consideration prior to the implementation of a u-healthcare system. The owner of personal information can also be threatened by hackers and malicious attackers [3]. For this reason, the Department of Health and Human Services (HHS) in the United States has recently issued "an interim final rule regulating when and how patients must be notified if their healthcare information has been exposed in a security breach by hospitals, physician offices, and other healthcare organizations". Health Insurance Portability and Accountability (HIPAA) is an act introduced in 1996 to protect a patient's rights to medical history. A research group on healthcare is working on developing expertise in several areas and is planning to integrate these in 3G and 4G networking. The hospital information system today integrates individually optimized sections including nurses, other staff, and patients. The remainder of this paper is organized as follows. Section I is the introduction. Section II summarizes related work on the application of RFID related to security issues. Section III presents the analyses of the u-healthcare system, reviews the analysis of the protocol, and discusses various security and privacy issues such as associated attacks. Finally, Section IV provides the conclusions.

II. RELATED WORK

Information related to healthcare services is very confidential and sensitive. Healthcare systems are divided into several part systems in hospitals. Therefore, a divided security mechanism is required to integrate different types of security. In general, we should consider the characteristics of wireless communication between a user's tag and mobile agent, in addition to the wired connection between a mobile device and database. Generally speaking, firewall and traffic analysis can be used for the protection of sensible information from non-authorized attacks over the Internet protocol. Such attacked can be induced by authentication and security problems in this situation [4]. Healthcare staff members increasingly require medical data to be delivered in real time to support their decision making process. The adoption of mobile devices allows this process to occur concurrently. Privacy is an important aspect of pervasive and ubiquitous computing systems, and, in particular, pervasive healthcare. Moncrieff et al. [5] have presented a design framework for implementing privacy measures in ubiquitous computing environments, and have demonstrated its application to pervasive healthcare. Sun et al. [6] have contributed a detailed discussion on the privacy and security issues in e-healthcare systems and viable techniques for these addressing issues. Furthermore, they demonstrated the design challenge in the fulfillment of conflicting goals through an example scenario, where a wireless body sensor network is leveraged, and an optimized solution is proposed to overcome the conflict. Boukerche and Ren [7] introduced the technique of trust evaluation without a centralized trust management authority and proposed a novel trust evaluation model that can efficiently calculate the trustworthiness of mobile healthcare devices and dynamically manage medical nodes. Markovic et al. [8] considered the issues of mobile healthcare security and employ cryptographic techniques to address possible vulnerabilities. They make use of symmetrical cryptographic methods to protect data confidentiality, and asymmetrical cryptographic algorithms such as public key infrastructure (PKI) and digital signature techniques to achieve data integrity.

III. ANALYSES OF U-HEALTHCARE SYSTEM

At the initial model of the u-health system, a m-healthcare system is designed as an enhancement of the e-healthcare system supported by wireless electronic medical record (EMR) access. Fig. 1 depicts the concept of the network topology for the u-healthcare system. It represents a brief network topology for a virtual hospital. This network will be modified and extended based on the security and protocol requirements [9]. To overcome additional vulnerabilities, wireless architecture with embedded security modules should be designed with an essential requirement for wireless EMR access. In particular, a patient's privacy is very important in a hospital information system (HIS) environment. The information should be secured permanently, either when it is transmitted or stored in databases. Security issues could occur with sharing information among interconnected hospitals. Secure access of electronic health record (EHR) with distributed topology units should be also considered. Healthcare networks based on electronic or mobile devices are established by connecting general clinics, hospitals, and national/private medical centers. However, health information which is stored in a healthcare center is usually accessible only to authorized staff of that center in traditional healthcare systems [10]. To improve medical service quality in hospitals and enhance safety control for patients, integration of RFID technologies into medical industries has recently been progressively evolving. Effectively merging RFID techniques with the existing HISs is occurring gradually [11]. Yao et al. [12] has reviewed the

literature on RFID applications in healthcare based on a formal research framework and has identified current opportunities, potential benefits, and adoption barriers. Wang et al. [13] demonstrated the RFID infrastructure of Taipei Medical University Hospital. This architecture shows how data was collected, processed, stored, and transformed into useful information for medical services in the hospital. Yu et al. [14] provided the u-healthcare system with real-time technologies, which a great deal of security precautions. He also described differences between e-healthcare systems and u-healthcare systems, as shown in Table 1.

U-healthcare systems may bring unlimited convenience to the customers and staff of hospitals. However, security vulnerabilities can be found and would be attacked by skilled hackers. Security breaches may result in a loss of data or leakage of personal information unless hospital information systems are designed with security features. However, many organizations commit the mistake of neglecting the security aspect because security features do not generate any visible return on investment for them. As shown in Fig. 1, at the end of the network topology, a mobile device and wireless access point are utilized to implement interaction of transmitted information between the end device and the database servers through the network. An authentication server is located in the middle of the data transmission for access control in the authentication process. To identify security vulnerabilities and threats, security solutions and compact protocol design should be suggested to mitigate all kinds of risks [15]. Table 2 shows the structure of the secure layer and its characteristics.

To mitigate the aforementioned problems, we analyzed a security mechanism that protects EMRs and is suitable for ubiquitous medical service. The mechanism consists of numerous security measures such as authentication and a cryptographic algorithm. According to the structure of the security level, the measures can be categorized into three security layers: authentication based on the network, authentication based on the application, and database protection.

Table 1. Difference between e-healthcare and u-healthcare networks.

e-Healthcare networks	u-Healthcare networks
Any time service	Any time/anywhere service
Mobile/Web interfaces	Mobile/peripheral device interfaces
On line mode	On line/off line mode
Geographically constrained	Geographically distributed
No location tacking	Location-aware solution
Single security agent	Collaborating security agents
Single domain security infrastructure	Multi-domain security infrastructure

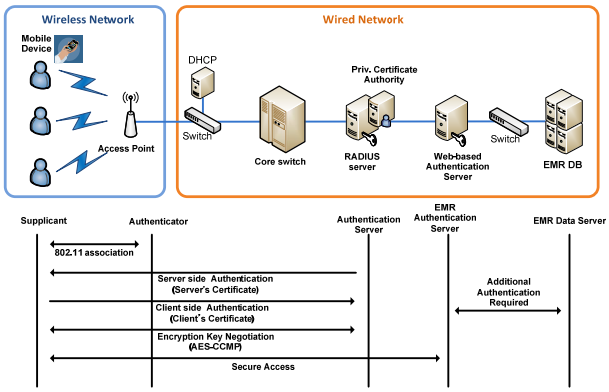

Fig. 1. Example of topology of ubiquitous healthcare system.

The wired equivalent privacy (WEP) protocol was designed to provide the same level of privacy as a wired network. Due to the low complexity of security concerns over the WEP standard, many researchers continue to debate whether WEP alone is sufficient for HIPAA transmission security or not. Consequently, a healthcare delivery organization should use a combination of WEP and other security protocols for wireless networks. In order to avoid potential security breaches such as authentication and privacy protection, the existing healthcare agent architecture should be considered for some special security requirements. The wireless public area network is the connection of servers. The relevant enabling technologies for wireless public area networks are Bluetooth and ZigBee. They are a set of high level communication protocols that use low power resources. The use of RFID is increasing for healthcare systems and patient monitoring systems as well. Deploying RFID technology in the healthcare industry for promoting patient's data and records in the hospital is a complex issue since it involves technological, economic, social, and administrative factors. Table 3 summarizes the major barriers, benefits, and attacks from the collected literature [16].

Table 2. Structure of secure layer for services.

Mobile device	Network	Database
RFID, NFC security issues	Two-way authentication	Private data protection
Privacy, light weight protocol	Digital certification, IPSec, encryption engine	EMR data security
Limited hardware resources and memory	SSL channel	Authentication mechanism
Low memory and power consumption	Challenge response protocol	Encryption engine

RFID: radio frequency identification, NFC: near field communication, IPSec: Internet protocol security, SSL: secure socket layer, EMR: electronic medical record.

Table 3. Benefits of, barriers to, and attacks on RFID applications in healthcare systems.

Benefits	Barriers	Attacks
Increased safety or reduced medical errors	Interference	Denial of service
Real-time data access	Ineffectiveness	Physical attack
Time saving	Standardization	Tag cloning attack
Cost saving	Cost	Replay attacks Spoofing attack
Improved medical process	Privacy and legal issues	Side channel attack
Other benefits: improve resource utilization	Other barriers: lack of organizational support, security	Tag tracking

RFID: radio frequency identification.

Table 4. Comparison of u-healthcare network and IPv6.

Demands of u-Healthcare network	Features of IPv6
A large number of biomedical sensors	Large IP space
Sensor's IP connection automatically	Stateless auto-configuration
Real-time transmission	QoS functions
Sensors hand off and roaming	Mobile IPv6
Biomedical information on internet	IPSec, AH, ESP
IPv6 and IPv4 translation	Dual stack, tunneling, translator

IPSec: Internet protocol security, AH: authentication header, ESP: encapsulating security payload.

A. Authentication Based on Network

As a first step toward security, well-organized authentication processes based on the network should be prepared against various threats, especially for wireless networks. In recent years, hospitals have also introduced wireless communication systems. However, not many hospitals are aware of the security issues because their working process is mainly focused on emergencies rather than security. This may result in a security problem such as information leakage. Fig. 1 describes a topology of ubiquitous healthcare systems. When a mobile agent attempts to connect to Wi-Fi protected access (WPA2)-Enterprise architecture, they must investigate the 802.1X/EAP process. This process has several steps: After the mobile agent establishes an association to the access point (AP), the remote authentication dial in user service (RADIUS) server initiates server-side authentication with the supplicant. In this authentication, the server sends its certificate to the mobile agent and requests that the user reply with the certificate of the mobile agent. Next, the mobile agent starts the client-side authentication by sending its authentication information to the server. After these steps, the mobile agent has proven its credentials in order to be allowed on the network. After authentication is completed, authentication is needed in order to make sure that matching encryption keys are installed on the mobile agent and access point. Negotiation to exchange the advanced encryption standard/counter mode CBC-MAC protocol (AES/CCMP) encryption key is carried out by robust security network (RSN) which is used for communications in a WPA2 network. Once the AES-CCMP encryption keys are successfully installed on both the AP and mobile agent, secure data will be transmitted across the WLAN. There are three methods that offer mutual security levels. To select the proper method, compatibility with the hospital environment should be analyzed. Extensible authentication protocol-message digest5 (EAP-MD5) should not be employed because it has weak security features.

To apply the EAP-transport layer security (TLS) protocol to a wireless network, implementation of the WLAN standard is required. WPA2 is one of the standards in which EAP-TLS can be implemented. Also, WPA2 employs AES-CCMP to overcome the vulnerabilities of other wireless communication standards [17, 18]. Huang et al. [10] presented a healthcare system hierarchical network architecture for wireless sensor networks. When IPv6 over IEEE 802.15.4 is implemented into sensor nodes, furthermore, biomedical sensor positioning is a foundational and crucial subject for detecting the location of elderly or chronic patients at any place, at any time. The global positioning system, multi-dimensional scaling, or radio frequency identification techniques can be also applied to biomedical sensor systems. Table 4 depicts a comparison of u-healthcare network and IPv6 network bases [19].

B. Authentication Based on Application

A user's authorization should be authenticated by a web-based authentication process for accessing the EMR even though the user connects to the network through network authentication.

The security guidance is republished by HIPAA in the US. To understand the prevailing regulations surrounding the protection of healthcare information in the US, it is important to have a basic understanding of the HIPAA Act of 1996. Specifically, HIPAA defines privacy as an individual's interest in limiting who has access to his or her personal healthcare information and specifies that security measures must encompass all the administrative, physical, and technical safeguards in an information system [20]. According to recent studies, two-factor authentication has been reported. These are the usual authentication methods based on a challenge-response handshake and session key agreement during the authentication process. Secure communication with a session key can communicate with confidentiality [21].

Table 5. Key sizes giving equivalent security.

Algorithm		
Integer	**ECC**	**Symmetric key**
512	106	64
1024	163	80
2048	210	112

ECC: elliptic curve cryptography.

Xiao et al. [22] presented distributed architecture of a health agent system and its resource access flow control and agent interaction model with a security policy in health agents. Misik [23] reported on healthcare wireless sensor networks implemented using 802.15.4 beacon-enabled technology, in which security processors are implemented with low power microcontrollers.

In this setting, he proposed using elliptic curve cryptography (ECC) for key distribution in order to decrease energy consumption compared to the better known RSA algorithm. Recently, ECC has been demonstrated as computationally lightweight, yet its security is comparable to that of RSA. For the same security level, ECC has much smaller key sizes compared to RSA, as shown in Table 5 [23].

IV. CONCLUSIONS

The use of the mobile device in the hospital environment provides an opportunity to offer better services for patients and staff. Mobile technology offers many advantages for improving patient information management and reducing the costs of processing time of medical information. We analyzed the issues of security related to privacy and comparison of e-healthcare and u-healthcare system and privacy. Neither a symmetric nor an asymmetric cryptographic deployment is necessary with the lightweight algorithm in a user's device. In future work, we will develop a test bed with an RFID system embedded in a ubiquitous healthcare system to estimate the performance and related problems and improve the security of a pervasive and mobile healthcare system.

ACKNOWLEDGMENTS

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant no. 2012-0007896)

REFERENCES

[1] Y. J. Park and Y. B. Kim, "On the accuracy of RFID tag estimation functions," *Journal of Information and Communication Convergence Engineering*, vol. 10, no. 1, pp. 33-39, 2012.

[2] Y. Xiao, X. Shen, B. Sun, and L. Cai, "Security and privacy in RFID and applications in telemedicine," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 64-72, 2006.

[3] L. Lhotska, P. Aubrecht, A. Valls, and K. Gibert, "Security recommendations for implementation in distributed healthcare systems," in *Proceedings of the 42nd Annual IEEE International Carnahan Conference on Security Technology*, Prague, Czech, pp. 76-83, 2008.

[4] R. K. Pateriya and S. Sharma, "The evolution of RFID security and privacy: a research survey," in *Proceedings of the International Conference on Communication Systems and Network Technology*, Katra, India, pp. 115-119, 2011.

[5] S. Moncrieff, S. Venkatesh, and G. West, "A framework for the design of privacy preserving pervasive healthcare," in *Proceedings of the IEEE International Conference on Multimedia and Expo*, New York: NY, pp. 1696-1699, 2009.

[6] J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 66-73, 2010.

[7] A. Boukerche and Y. Ren, "A secure mobile healthcare system using trust-based multicast scheme," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 387-399, 2009.

[8] M. Markovic, Z. Savic, and B. Kovacevic, "Secure mobile health systems: principles and solutions," in *M-health: Emerging Mobile Health Systems*, New York, NY: Springer, pp. 81-106, 2006.

[9] C. J. Su and B. J. Chen, "Ubiquitous community care using sensor network and mobile agent technology," in *Proceedings of the 7th International Conference on Autonomic & Trusted Computing*, Xian, China, pp. 99-104, 2010.

[10] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 400-411, 2009.

[11] W. Tounsi, J. Garcia-Alfaro, N. Cuppens-Boulahia, and F. Cuppens, "Securing the communications of home health care systems based on RFID sensor networks," in *Proceedings of the 8th Annual Communication Networks and Services Research Conference*, Montreal, Canada, pp. 284-291, 2010.

[12] W. Yao, C. H. Chu, and Z. Li, "The use of RFID in healthcare: Benefits and barriers," in *Proceedings of the IEEE International Conference on RFID-Technology and Applications*, Guangzhou, China, pp. 128-134, 2010.

[13] S. W. Wang, W. H. Chen, C. S. Ong, L. Liu, and Y. W. Chuang, "RFID application in hospitals: a case study on a demonstration RFID project in a Taiwan hospital," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, Kauai: HI, p. 184a, 2006.

[14] W. D. Yu, R. Gummadikayala, and S. Mudumbi, "A web-based wireless mobile system design of security and privacy framework for u-Healthcare," in *Proceedings of the 10th International Conference on e-health Networking, Applications and Services*, Singapore, pp. 96-101, 2008.

[15] D. Acharya, "Security in pervasive health care networks: current R&D and future challenges," in *Proceedings of the 11th International Conference on Mobile Data Management*, Kansas City: MO, pp. 305-306, 2010.

[16] H. Y. Chien, "Varying pseudonyms-based RFID authentication protocols with DOS attacks resistance," in *Proceedings of the IEEE Asia-Pacific Services Computing Conference*, Yilan, Taiwan, pp. 607-614, 2008.

[17] C. C. Hung and S. Y. Huang, "On the study of a ubiquitous healthcare network with security and QoS," in *Proceedings of the IET International Conference on Frontier Computing: Theory, Technologies and Application*, Taichung, Taiwan, pp. 139-144, 2010.

[18] Z. Li, H. Shen, and B. Alsaify, "Integrating RFID with wireless sensor networks for inhabitant, environment and health monitoring," in *Proceedings of the 14th IEEE International Conference on Parallel and Distributed Systems*, Melbourne, Australia, pp. 639-646, 2008.

[19] W. Yao, C. H. Chu, and Z. Li, "The use of RFID in healthcare: benefits and barriers," in *Proceedings of the IEEE International Conference on RFID: Technology and Applications*, Guangzhou, China, pp. 128-134, 2010.

[20] S. Kahn and V. Sheshadri, "Medical record privacy and security in a digital environment," *IT Professional*, vol. 10, no. 2, pp. 46-52, 2008.

[21] R. C. W. Phan, "Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI," *IEEE Transactions on Dependable and Secure Computing*, vol. 6, no. 4, pp. 316-320, 2009.

[22] L. Xiao, P. Lewis, and A. Gibb, "Developing a security protocol for a distributed decision support system in a healthcare environment," in *Proceedings of the 30th ACM/IEEE International Conference on Software Engineering*, Leipzig, Germany, pp. 673-682, 2008.

[23] J. Misic, "Enforcing patient privacy in healthcare WSNs using ECC implemented on 802.15.4 beacon enabled clusters," in *Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications*, Hong Kong, China, pp. 686-691, 2008.

Jung Tae Kim

received an M.S. degree in 1991, and a Ph.D. degree in 2011, both in Electronic Engineering from Yonsei University, Republic of Korea. From 1991 to 1996, he joined Electronic Telecommunication Research Institute (ETRI), where he worked as a senior member of the technical staff. In 2002, he joined the Department of Electronic Engineering, Mokwon University, Korea, where he is presently a professor. His research interest is in the area of information security technology, which includes network security, cryptographic protocols, crypto-processor design, RFID and USN, and wireless security protocols.