Secure Authentication with Mobile Device for Ubiquitous RFID Healthcare System in Wireless Sensor Networks

Jung-Tae Kim, *Member, KIMICS*

***Abstract*—As telecommunication technologies in telemedicine services are developed, the expeditious development of wireless and mobile networks has stimulated wide applications of mobile electronic healthcare systems. However, security is an essential system requirement since many patients have privacy concerns when it comes to releasing their personal information over the open wireless channels. Due to the invisible feature of mobile signals, hackers have easier access to hospital networks than wired network systems. This may result in several security incidents unless security protocols are well prepared. In this paper, we analyzed authentication and authorization procedures for healthcare system architecture to apply secure M-health systems in the hospital environment. From the analyses, we estimate optimal requirements as a countermeasure to its vulnerabilities.**

***Index Terms*—M-health system, U-health System, Mobile device, Wireless network, Security, Authentication**

I.INTRODUCTION

INFORMATION technology is developed, many organizations such as government agencies, public institutions and corporations have employed information and communication systems to improve efficiency of their work process. For the past few years, healthcare organizations over the world have also had a blueprint to adopt the Health Information System (HIS) based on the wireless network infrastructure. As a part of the wireless network, a mobile device has been employed in a large scale of hospitals due to its outstanding mobility. Conventionally physicians, who are in charge, use a paper-based chart when they visit wards or meet regularly for patient check-ups although the hospital has a network-based infrastructure. After the round of visits, medical staffs should bring their chart back to the registration interface of intranet where they can update the medical records. When it comes to the process of working efficiently, it takes time and manpower which repeat unnecessary processes. This problem can be resolved by using the mobile device which provides portability and easy-to-use interface to the hospital staffs. For instance, immediate access to the Electronic Medical Record (EMR) database offered through the mobile device may reduce the processing time to access and update EMR. The owner of personal information will also suffer from hackers due to personal information being used maliciously [1]. 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." [2].Mobile healthcare (m-healthcare) is an important research direction for the application of wireless communication in healthcare systems. Therefore, many wireless technologies, including IEEE 802.11, Bluetooth, and Wi-Fi, are used to form wireless local area networks (WLAN) and connect to the Internet. Mobile networks not only provide mobility to patients, but also allow physicians so they can access patients' data anytime and anywhere. This brings important benefits to both patient and medical service provider. During the process of constructing an m-healthcare system, wireless sensors act as personal digital assistants that monitor the state of a patient, while also working for physicians by sending or receiving instant messages, either to hospitals to query about the patient's information, or to the patient to remind him or her about necessary medication or examinations. In a word, m-healthcare environments can collect, transfer, and exchange medical information in a distributed method. However, security is an essential requirement of the mobile healthcare system, since many patients have privacy concerns when it comes to releasing their information over the open wireless channels [3].On the basis of above issue, we analyzed security mechanism and protocols to prevent any security threats and vulnerabilities under the M-health environment. At the beginning of this paper, related studies with E-health security mechanism will be introduced to compose a secure M-health architecture. Secondly, identity authentication procedures on each network and application layer of the M-health service will be focused as the main point of this paper. Lastly, a security assessment will be conducted to prove the improvements of proposed security mechanism and future works relevant to the healthcare system will also be addressed to reinforce the M-health system.

Manuscript received July 26, 2011; revised August 19, 2011; accepted September 1, 2011.
Jung-Tae Kim is with the Dept. of Electronic Eng., Mokwon University, Korea(Email : jtkim5068@hotmail.com)

II. RELATED WORKS

In the real world, information related with healthcare service is very confidential and sensitive; divided security mechanism is required for mutual security. Telemedicine system often consists of the combination of communication infrastructure, physiology monitoring subsystem and care management subsystem. Mobile healthcare system using RFID was proposed. They present a mobile healthcare service (MHS) platform that uses the RFID technology and mobile devices for identifying and positioning persons and objects both for inside and outside hospital. They also demonstrate how it can be obtained patient's location and bio-information for hospital and government to make real time reaction based on the application for SARS infection control precautions [4]. On top of authentication, the system determines a set of actions performed by the user which is called authorization [5]. Also, healthcare experts increasingly require medical data delivered in real time to support their decision making process. The adoption of mobile devices allows this process to take place concurrently. D.Halperin surveyed that "In the future Mobile Health (M-Health) applications will take advantage of technological advances such as nanotechnology, device miniature, device convergence, high-speed mobile networks, and advanced medical sensors." in his article [6]. When it comes to the performance of processing speed at database query, a concept of bucket index will be implemented to upgrade the DB performance. Gorawski in 2006 proposed the indexing agents running in a distributed mobile agent system, which make up the distributed bucket index. To improve the processing performance and help to control the workload, the idea of bucket index has been implemented in the system based on mobile agents. Consequently, our task in this paper is building a secure and efficient wireless data access architecture using various mechanisms and protocols as a step to the U-health system.

III. PROPOSED SECURITY MECHANISM

The security design of the protocol should not impede normal operations, and should prevent a malicious adversary from getting any information. As mentioned in the background section, M-health may bring unlimited convenience to customers and staffs in hospitals. However, security vulnerabilities can be found and would be used by hackers in terms of Information Technology. Security breaches may result in a loss of data or leakage of personal information unless hospital information systems are designed with security features. However, it is easy to commit a mistake that many organizations neglect security parts as security features do not generate any visual profit for them. According to NewsRx.com about result of security survey conducted with more than 100 global life sciences and health care companies, many organizations including health care companies consider a security part as a lowest priority task, and even the security budget is just a small part of IT budget [7]

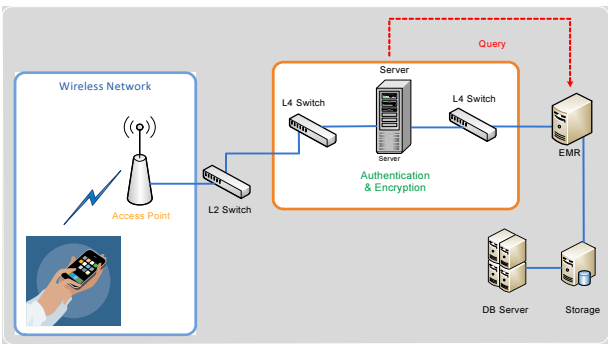

Fig.1. Use of Mobile Phone in M-health

To sum up, it is an obvious fact that well-organized security plan can prevent the expected problems in advance before they happen. It also means they can save money, time and man-power for a recovery after security incidents. Therefore, security parts in organizations should be valued high priority. EHR systems have two main security concerns: transmission and access. Transmission security refers to the healthcare delivery organization's ability to ensure that transmitted data is safe from potential security threats an route, and access security refers to the healthcare delivery organization's ability to ensure that system access is granted only to appropriate individuals. Transmission security concerns typically arise during wireless network implementation. The Wired Equivalent Privacy (WEP) protocol was designed to provide the same level of privacy as a wired network, but due to security concerns over the WEP standard, experts continue to debate whether WEP alone is sufficient for HIPAA transmission security. Consequently, the healthcare delivery organization should use a combination of WEP and other security protocols for wireless networks. Authentication and privacy protection In order to avoid such potential security breaches, the existing Health Agents architecture should tackle some generic security requirements as outlined below [2].

In this section, we will discuss and propose authentication methods based on network and application respectively. Also, database security measures will be proposed in order to establish a secure M-health environment [6].

A. Authentication based on Application

We describe the major security requirements for data security and privacy for ubiquitous networks as follows.

a) Data storage security requirements

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

b) Data access security requirements

1. Access control (privacy)
   A fine-grained data access policy shall be enforced to prevent unauthorized access to patient-related data generated by the WBAN.
2. Accountability
   When a user of the WBAN abuses his/her privilege to carry out unauthorized actions on patient-related data, he/she should be identified and held accountable.
3. Revocability
   The privileges of WBAN users or nodes should be deprived in time if they are identified as compromised or behave maliciously.
4. Non-repudiation
   The origin of a piece of patient-related data cannot be denied by the source that generated it.

c) Other requirements

1. Authentication
   The sender of the patient-related data must be authenticated, and injection of data from outside the WBAN should be prevented.
2. Availability
   The patient-related data should be accessible even under denial-of-service (DoS) attacks.

B. Authentication based on Application

Users must be authenticated by web-based authentication system for accessing to EMR despite the user establishes connection to the network through network authentication. The Security Guidance republished by HIPAA in USA, report advises using two-factor authentication. The usual authentications based on challenge-response handshake, session key agreement during the authentication process and secure communication with a session key enable confidential communication. In the mechanism we proposed, data transmission between mobile device and web-based authentication server is secured by SSL channel. SSL channel automatically generates and exchanges keys. Symmetric cryptography supported by OpenSSL is chosen for cryptographic control because that public key scheme decrypts at speeds more than the maximum 100 times slower than symmetric key scheme. Fig 2 shows authentication between mobile device and secured database [6].

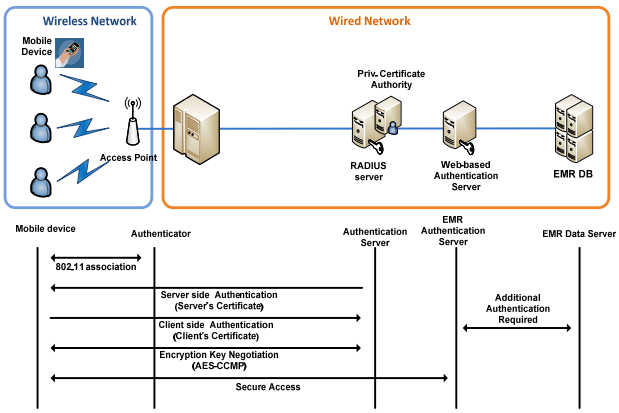

Fig.2. Process of EAP-TLS with WPA2 in a wireless communication network

TABLE 1
TERMS DEFINITION

M	Mobile device
S	Web based authentication server
D	Database
C(x)	Cipher-text
q	Query for response request
r	Response for query
k	Key
n	New key(Random number)
R(x)	Result of request
H(x)	Hash functioned with x
En(x,k)	Encryption of x by key
De(x,k)	Dncryption of x by key

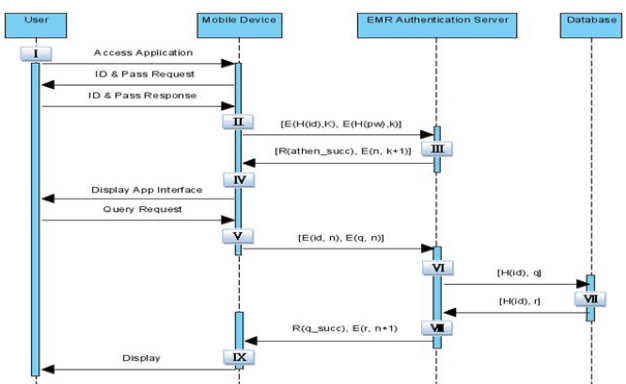

Fig.3. Authentication Process

For help of understanding the scheme in authentication based on application, following user authentication scenario presented in Figure 3. Here, we describe in detail the application based authorization procedure. To prevent unauthorized user access, user verification and identification are required.

I	User verification by pass code
II	$M : C(id) = En(H(id), k)$
	$M : C(pw) = En(H(pw), k)$
	$M \rightarrow S : [C(id), C(pw)]$
III	$S : H(id) = De(C(id), k)$
	$H(id)$is used to check the session for user.
	Session Confirm : Fail
	$S : H(pw) = De(C(pw), k)$
	Authentication Confirm: Success (stat2)
	Generate new key: n
	Create session for 10 minutes
	$S : C(n) = En(n, k+1)$
	$S \rightarrow M : [R(stat2), C(n)]$

IV	$M : n = De(C(n), k+1)$
	Store : n (new key)
V	$M : C(id) = En(H(id), n)$
	$M : C(q) = En(q, n)$
	$M \rightarrow S : [C(id), C(q)]$
VI	$S : H(id) = De(C(id), k)$
	Session confirmation : Created
	$S : q = De(C(q), n)$
	$S \rightarrow D : [H(id), q]$

VII	*Check the requestor's security level by* $H(id)$ *and search response the query*
	$D \rightarrow S : [H(id), r]$
VIII	$S : C(r) = En(r, n+1)$
	The requestor of the respond will be determined by $H(id)$.
	$S \rightarrow M : [R(stat3), C(r)]$
IX	$S : q = De(C(r), n+1)$

As mentioned above, the authorization scheme that based reasonable encryption algorithm and minimum workload oriented design supports the HIS requirement such as a confidentiality and privacy with rapid process. However, more defensive methods should be applied to the HIS against malicious attacks.

IV. SECURITY ANALYSES

As a last step, proposed multi-layer security mechanism is assessed by comparison to fragile security mechanism which can often be used in real industries. The contents are categorized as below. In terms of mutual security, the use of ID and password for access to EMR database can be vulnerable. While, authentication using the digital certificate will prevent illegal access even if hackers obtain the user's ID and password in the proposed mechanism. Also, each individual or group will be assigned different authorization for access to DB based on their role. In addition, the proposed mechanism employs multiple encryption methods to protect data securely. To disclosure data, hackers need to know all different encryption methods and their keys. Next, DB performance in our model satisfies two key factors which include security and speed. Encryption makes data confidential and the bucket index improves the DB speed. On the other hand, the proposed security model has an issue with compatibility. The latest wireless devices may be required because some of old devices cannot support WPA2, but it could be worth to invest in new devices because it may provide mutual security to the wireless hospital system.

TABLE 2
SECURITY ANALYSES

Item	Conventional security mechanism in usual	Proposed multi-layer security Mechanism
Authentication Method	ID & Password authentication	Digital Certificate, ID & Password double authentication,
Authorization	No restriction within hospital intranet	Each individual or group will be assigned different authorisation
Data Encryption	Single encryption prior to transmission	Duplicated encryption prior to transmission (AES-128, CBC, Hash)
DB performance	Secure but slow (B+tree index) [Kim] Or unsecure but fast	Fast and secure (Bucket index, Encrypted)

V. CONCLUSION

The use of the mobile device in the hospital environment offers an opportunity to deliver better services for patients and staffs. In this paper, we proposed the security mechanism focused on the multi-layer authentication with sensible information management in the hospital. It was also implemented with consideration the characteristics of the hospital in the real world, so that optimized security protocols and mechanisms are employed for the high performance and security. Finally, a challenge in the near future will be the integration of Ubiquitous Sensor Network with security protocols to the hospital environment.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology(grant number:2011-0026950)

REFERENCES

[1] Olla, P., Mobile health technology of the future: creation of an M-Health taxonomy based on proximity. International Journal of Healthcare Technology and Management (IJHTM), 2007.
[2] Debargh Acharya, et al, “Security in Pervasive Health Care Networks: Current R&D and Future Challenges”, 11th International Conference on Mobile Data Management”, pp.305-306, 2011.
[3] Azzedine Boukerche, et al, “A Secure Mobile Health System Using Trust-Based Multicast Scheme”, IEEE J. On selected areas in communications, vol.27, no.4, pp.387-399, May 2009.
[4] Cheng-Ju Li et al., “Mobile healthcare service system using WID”. IEEE, International Conference on Networking, Sensing and Control, pp. 1014-1019, Mar. 2004.
[5] I. Vajda and L. Buttyan, “Lightweight authentication protocols for low cost RFID tags,” in Proc, 2nd Workshop on Security in Ubiquitous Computer, pp.76-82, 2003.
[6] Kim, J., and Sahama, T. “A Study on the Encryption Model for Numerical Data”, International Journal of KIMICS, Vol.7, pp. 31-34, 2009.
[7] Stallings, W., Cryptography and Network Security (4th Edition). Prentice Hall., 2006.

Jung-Tae Kim received his Ph.D. degrees in Electronic Engineering from the Yonsei University in 2001. From 1991 to 1996, he joined at ETRI, where he worked as senior member of technical staff. In 2002, he joined the department of electronic engineering, Mokwon University, Korea, where he is presently professor. His research interest is in the area of information security technology that includes network security system design, RFID&USN and wireless security protocol.