Analyses of Enhancement of Authentication Mechanism for Security and Privacy Under Healthcare System With RFID Application

김정태
목원대학교

RFID를 이용한 헬스시스템에서의 정보보안 향상을 인증 메카니즘 분석

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

This paper presents a user authentication scheme for healthcare application using wireless medical sensor networks, where wireless medical sensors are used for patients monitoring. These medical sensors' sense the patient body data and transmit it to the professionals (e.g., doctors, nurses, and surgeons). Since, the data of an individual are highly vulnerable; it must ensures that patients medical vital signs are secure, and are not exposed to an unauthorized person. In this regards, we have proposed a user1 authentication scheme for healthcare application using medical sensor networks. The proposed scheme includes: a novel two-factor professionals authentication (user authentication), where the healthcare professionals are authenticated before access the patient's body data; a secure session key is establish between the patient sensor node and the professional at the end of user authentication. Furthermore, the analysis shows that the proposed scheme is safeguard to various practical attacks and achieves efficiency at low computation cost.

Ⅰ. Introduction

Nowadays u-healthcare which is very sensitive to the character of user's information among other ubiquitous computing field is popular in medical field. u-healthcare deals extremely personal information including personal health/medical information so it is exposed to various weeknees and threat in the part of security and privacy. In this chapter, RFID based patient's information protecting protocol that prevents to damage the information using his or her mobile unit illegally by others is proposed. The protocol separates the authority of hospital doctor, nurse, pharmacy) to access to patient's information by level of access authority of hospital which is registered to management server and makes the hospital do the minimum task. Specially, the management server which plays the role of gateway makes access permission key periodically not to be accessed by others about unauthorized information except authorized information and improves patient's certification and management.

II. Related Work

Despite these kinds of development in technologies for establishing U-healthcare system, U-healthcare system faces another challenge. It is the patient's privacy invasion problem due to unauthorized monitoring and access. In ubiquitous sensor era, it is possible to collect the data from end node and track patient's location without awareness. Even though, concerns about the invasion of personal medical privacy has already appeared in e-health care system and medical industry rules the guideline for usage of personal medical information through HIPPA[1]. The security and privacy challenges in U-healthcare system can be solved by new technologies. This paper proposes the ubiquitous healthcare system which covers patient's physiologic signal sensing, sensed data collection, the data analysis and diagnosis, and patient tracking protecting patient's medical privacy. For access to patient's information and patient' tracking, RFID is adopted, and PKI and smart card are used for the authentication, and permission to access information.

III. Proposed Security Mechanism

Health Insurance Portability and Accountability Act (HIPAA) enacted by the United States Congress in 1996, is the Federal Law that applies to the U.S. healthcare industry [1]. For improving healthcare quality, the HIPAA provides a conceptual guideline that must be strictly observed by all followed organizations. Privacy regulations address the patients' rights to understand and control the use and disclosure of their protected health information (PHI), which is that part of the health information that reveals an individual's identification, such as name, address, telephone number, medical record number, and so on. In this section, we introduce the u-healthcare service network architecture. Particularly we consider u-hospital healthcare network environment in here. The u-hospital network allows the medical steps to use mobile medical devices, to measure and record medical data users, and to get information related to their patient or treatment from HIS. On u-hospital service network environment, we can define four elements: Medical Sensor & Device element, Middleware element, Communication element, and Back-end Information Service element. The medical sensor & device component represents various physical measurement tools which measure biological signals from patients and get information related to treatment or prescription [2,3]. It could be not only wired devices, but also wireless devices which communicate through wireless channel such as WLAN, CDMA, Bluetooth, RF channel. Wei-Bin Lee proposed a cryptographic key management scheme. The proposed process is to facilitate inter-operations of multiple cryptographic mechanisms in order to comply with the HIPAA privacy/security regulations [4]. The proposed scheme can be divided into three phases: registration, encryption, and decryption. The decryption phase is subdivided into two cases because of the consent exceptions [5].

A. Registration Phase

After reading the "Notice of Privacy Practices," each patient has to register at SG. The patient signs and dates the permitting consent to verify acceptance of the PHI access rules, and further sends the signed consent with his/her fundamental data to SG. When receiving the request, SG first checks the validity of the received consent and then creates contract. The contract consists of the signed consent, the data received from the patient, and a summary of the duties of SG as well as its fundamental data, such as identification or name of the organization.

B. Encryption Phase

For simplicity, assume that M is the PHI

part of the health information and R represents the remaining parts. To ensure confidentiality and privacy, M must be encrypted. To encrypt PHI, the patient must enable the health data card by entering his/her PIN or verifying the biometric information. The enabled card will do the following to encrypt M.

C. Decryption Phase

The purpose of the decryption phase is to reveal the encrypted PHI. Without a legal authorization, disclosure of PHI would damage a patient's privacy, and is, therefore, forbidden. Hence, construction of the appropriate operations in the decryption phase is a means to protect privacy and rights of a patient. Due to the consideration of whether the patient is directly involved, two cases have to be discussed in this phase.

IV. Conclusion

Medical contexts are especially interesting because of the legal constraints related to privacy preserving and security. In this paper, we have presented a design framework for implementing privacy measures in ubiquitous computing environments, and demonstrated its application to pervasive healthcare. Given the sensitivity of healthcare environments, and the associated data, addressing privacy issues will play a large part in the adoption of pervasive healthcare applications.

References

[1] "Health Insurance Portability Accountability Act of 1996 (HIPAA)," Centers for Medicare and Medicaid Services (1996) [Online]. Available:http://www.cms.hhs.gov/hipaageninfo. (retrieved: 05/15/2006).

[2] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal of selected areas in communications, V.24, N.2, pp.381-394, February, 2006

[3] H.Y. Chien. "SASI: A New Ultra-weight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing., vol.4, n.4, pp.337-340, Oct. 2007

[4] Wei-Bin Lee and Chien-Ding Lee, "A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations", IEEE Transactions on Information Technology in Biomedicine, V.12, N.1, pp.34-41, 2008

[5] zzedine Boukerche, et al, "A Secure Mobile Health System Using Trust-Based Multicast Scheme", IEEE J. On selected areas in communications, v.27, n.4, may 2009, pp.387-399.

Acknowledgement

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: 2012-0007896)