헬스캐어 시스템에서의 사물 인터넷 통신을 위한 보안 문제 분석

신윤구, 김한규, 김수진, 김정태

목원대학교

Analyses of Security Issues for Internet of Things in Healthcare Application

Yoon-gu Shin, Hankyu Kim, Sujin Kim, Jung Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

ABSTRACT

The use of Radio Frequency Identification technology (RFID) in medical context enables not only drug identification, but also a rapid and precise identification of patients, physicians, nurses or any other healthcare giver. The combination of RFID tag identification with structured and secured Internet of Things (IoT) solutions enables ubiquitous and easy access to medical related records, while providing control and security to all interactions. This paper defines a basic security architecture, easily deployable on mobile platforms, which would allow to establish and manage a medication prescription service in mobility context making use of electronic Personal Health Records. This security architecture is aimed to be used with a mobile e-health application (m-health) through a simple and intuitive interface, supported by RFID technology. This architecture, able to support secured and authenticated interactions, will enable an easy deployment of m-health applications. The special case of drug administration and ubiquitous medication control system, along with the corresponding Internet of Things context, is presented.

Keyword

RFID, Healcare system, IoT, Security, Medical control

Ⅰ. Introduction

Internet of Things (IoT) encompasses a set of technologies that enable a wide range of appliances, devices, and objects (or simply "things") to interact and communicate among themselves using networking technologies. Human beings supply most of the contents and information found on Internet so far, whereas in IoT, small devices are frequently the active element that provides the information. Healthcare systems use a set of interconnected devices to create an IoT network devoted to healthcare assessment, including monitoring patients and automatically detecting situations where medical interventions are required [1].

Ⅱ. Security Issues

The fact that personal private data will be collected through tele-monitoring implies the need for strategies and mechanisms to ensure adequate security and privacy. As highlighted, "having every 'thing' connected, new security and privacy problems arise, e.g., confidentiality, authenticity, and integrity of data sensed and exchanged by 'things'." This author lists the standard security requirements [1, 2].

1) Data authentication: As a principle, retrieved addresses and object information must be authenticated;

2) Access control: Information providers must be able to implement access control on the data

provided;

3) Client privacy: Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system.

Ⅲ. Public Security Techniques of the IoT

In the application system of the Internet of Things, the main security problems are following [3]:

- Skimming: When a terminal device or a RFID (Radio Frequency Identification) card owner is insensible, information has been read.
- Eavesdropping: In the communication period, information is intercepted.
- Spoofing: Forge, copy the data of device, and enter into the system as an impostor.
- Cloning: Cloning the terminal device.
- Killing: Destroy or steal the terminal device.
- Jamming: Jam device by forging data.
- Shielding: Make the terminal device unconnected by taking mechanical measures.

Ⅳ. IoT Architecture and Security Architecture

IoT, as a fusion of heterogeneous networks, not only involves the same security problems with sensor network, mobile communication network and the Internet, but also more particular ones, such as privacy protection problem. The structure of IoT is generally divided into three layers, including perception layer, network layer, and application layer. Some systems take the network support technology (such as network processing, computing technology, middleware technology, etc.) as the processing layer. Literature shows IoT system structure divided by the three layers. It makes a summary of the threats and the requirement analysis about IoT security architecture. It embodies the concept of human central nervous system and social structure. This paper will discuss three layer structures [4]. To resolve the problems of static defense strategies, the proposed approach adopts dynamic and circular defense processes against security threats. Its frame is shown in Fig. 1. It consists of five links. The first link Security Threat Detection collects and analyzes original IoT network packets. The other links perform based on the analysis results provided by the previous link. All links serve IoT security [5].

Fig.1 Frame of IoT security

Ⅴ. Conclusion

In this paper, the public security techniques of the Internet of Things are analyzed. Also, we introduce a deployment model for wireless sensor networks for pervasive healthcare based on the concepts of patient area and medical sensor networks.

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: 2010-0024133)

참고문헌

[1] Y. Zhou, Y. G. Fang, Y. C. Zhang. Securing wireless sensor networks: a survey. IEEE Communications Surveys and Tutorials, pp.6-28. 2008.

[2] Liane Margarida Rockenbach Tarouco, Leandro Márcio Bertholdo, Lisandro Zambenedetti Granville, Lucas Mendes Ribeiro Arbiza, Felipe Carbone, Marcelo Marotta and José Jair Cardoso de Santanna, "Internet of Things in Healthcare : Interoperatibility and Security Issues", International Workshop on Mobile Consumer Health Care Networks, Systems and Services, pp.6121-6125,2011.

[3] Xin Bai and Hongyan Yan, "Study and Design of the Safe HIS on the Internet of Things", 2011 Fourth International Symposium on Computational Intelligence and Design, pp.174-176, 2011

[4]Kai Zhao1 and Lina Ge, "A Survey on the Internet of Things Security", 2013 Ninth International Conference on Computational Intelligence and Security, pp.663-667, 2013

[5] Caiming Liu, Yan Zhang and Huaqiang Zhang, "A Novel Approach to IoT Security Based on Immunology", 2013 Ninth International Conference on Computational Intelligence and Security, pp.771-775, 2013