Advanced Science and Technology Letters
Vol.72 (Healthcare and Nursing 2014), pp.109-112
http://dx.doi.org/10.14257/astl.2014.72.27

# Privacy and Security Issues for Healthcare System with Embedded RFID System on Internet of Things

Jung Tae Kim

[1] Dept. of Electronic Engineering, Mokwon University,
800, Doan-dong, Seo-gu, Daejeon, South Korea
jtkim3050@mokwon.ac.kr

**Abstract.** Today, RFID technologies are being applied in ubiquitous sensor network system to improve the quality of healthcare system. In this paper, we have investigated and surveyed on security and privacy issues in RFID systems and their applications related with IoT (Internet on Things). Wireless sensor networks can be applied for ubiquitous health monitoring, improving users' well-being, making the healthcare system more efficient, and helping to quickly react on emergency situations. To meet the strict security needs of ubiquitous medical applications is a big challenge. We surveyed a deployment model for pervasive healthcare regarding to patient area and medical sensor networks.

**Keywords:** RFID, Healthcare system, Security protocol, Privacy, IoT

## 1 Introduction

Internet of Things (IoT) is a combination and fusion of technologies that capable of interacting and communicating using networking technologies such as RFID, NFC and sensor nodes. It is a general term of all that can enhance the communication of machinery equipment and capability of network technology, which organically combined in communication between devices, device control communications, interactive communication, mobile Internet communications and other types of communication technologies, to share information Internet of Things (IoT) is a global network infrastructure which linking physical and virtual objects by merging with data collection and communication capabilities [1, 2]. It will offer specific object identification and connection capability of sensor as the basis for the development of independent cooperative services and applications. There are many applications for IoT and the representative example is healthcare systems. Healthcare systems use a set of interconnected devices to create an IoT network which devoted to healthcare monitoring system. To apply RFID system in ubiquitous healthcare system with embedded sensor modules based on IoT, enhanced secure mobile health system should be developed using wireless communication to solve security problem. This system includes two-way interactive authentication process, sensor technology, and health informatics. Especially, sensor technologies for identification play an important role in intelligent services using network communications. The personnel private data would be collected through wireless monitoring devices. Due to limited resources of sensor nodes, it is required to needs for strategies and mechanisms to ensure adequate

ISSN: 2287-1233 ASTL

security and privacy. The solution for interoperability and management of homecare network has been studied to use a variety of network management concepts to include Internet of Things such as RFID or WLAN [3, 4].

## 2 Related Works

A variety of IoT applications have a differences industry standards and related specifications. Unified IoT structure has not yet formed. However, to enact the IoT security standards, many organizations have issued standards such as IEEE, ETSI, etc. It gives the development of the IoT security standards [5, 6]. Most of existing IoT solutions is independent small network, there are relatively few exploits which can be attacked. With the sustained development of IoT, the small networks will merge into a large network. By then it would be more difficult to ensure the security. These security problems would be the key factor to decide the development of IoT [7]. Kai Zhao and Lina Ge analyzed a survey on the Internet of Things security. Developing RFID technology in the healthcare industry for promoting patient's The Internet of Things is a new network to realize the connection of any things, anytime and anywhere. Its infrastructure is divided into three layers: perceptive layer, transport layer and processing layer. The perceptive layer is to identify and apperceive things, including label, camera, sensors and GPS etc., the transport layer is to transport and store data, and the processing layer is about information drawing, data mining etc. Xin Bai, et al., analyzed the public security techniques of the Internet of Things, including IOT-MW (Internet of Things-Middleware), encryption, decryption, secret key management, privacy homomorphism, and access control etc. especially the cryptograph query [8]. Biplob R. Ray, et al, analyzed scalable RFID security framework and protocol for supporting Internet of Things. They proposed a novel identification technique based on a hybrid approach (group-based approach and collaborative approach) and security check handoff (SCH) for RFID systems with mobility. The proposed protocol provides customizability and adaptability as well as ensuring the secure and scalable deployment of an RFID system to support a robust distributed structure such as the IoT [9].

## 3 Architecture of e-Healthcare System

To deal with existing security challenges as well as growth in diverse community in an interconnected network, we need a security framework to manage diverse processing requirements and control capabilities. The purpose of the framework design is to meet the needs of new e-health security challenges. To ensure a global system, end-to-end perspective system can uncover unintended threats that may not be available at the individual' element level, we need to have a national level protection standard to meet the emerging e-healthcare needs [10]. As a first step of security, well-organized authentication processes based on network should be prepared against various threats especially for wireless networks which can be more vulnerable due to its invisible feature. In recent years, hospitals also employ wireless

 

communication systems as other enterprises, and the hospitals maintain many personal details for the medical purpose such as patient's medical history. However, only a few hospitals are aware of the security issues because their working process is mainly focused on emergency than security matters. This may result in a security incident such as information leakage. Therefore, we proposed a suitable wireless security mechanism for the hospital. To begin with, the organizational characteristics of the hospital should be analyzed before selecting the wireless mechanism. With mobile devices in HIS, the staff will be able to access EMR systems to view or update patient's medical records. The usual methods to provide security at the network level, in the case of packet networks, are datagram encapsulation. One of the most common technologies used to ensure secure communications in the Internet is the Internet Protocol Security (IPsec) protocol. IPsec is an end-to-end security scheme operating in the IP stack, enabling both authentication and confidentiality [11]. Although IPsec ensures these security services to any protocol in the upper layers, it introduces some overhead that will reduce throughput. The security framework focuses on mechanisms for the distribution and establishment of secret keys that allow bootstrapping secure links, access control to the sensed information, and privacy-aware management of the medical data and user's identities. We combine centralized and distributed security solutions in order to provide an adequate balance between performance and security requirements. Network security and management play an important role in above each level. Then we should analyze the security features in each layer such as perceptual layer, network layer, support layer and application layer. Now, we should take into account to look into the state of research for the security requirements such as encryption mechanism, communication security, protecting sensor data, and cryptographic algorithms in communication channel [12].

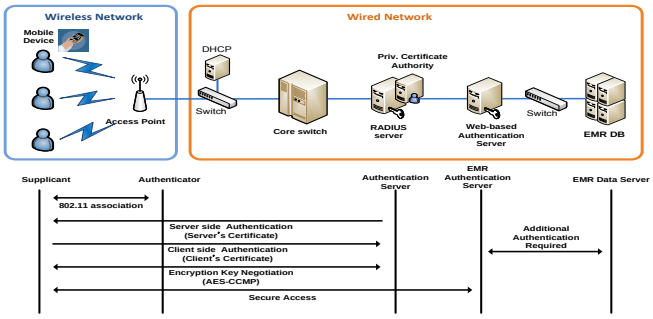


**Fig. 1.** Block diagram of IoT application in healthcare system under wireless communication network

## 4 Conclusion

The development of IoT security is an important part of IoT. This paper respectively explains some problems and solutions from each layer of IoT security structure. Optimized security protocols and mechanisms are employed for the high performance

and security in u-healthcare system. In this paper, security issues on the IoT construction layers is analyzed and appropriate coping strategies are given to build a safe IoT construction so that the IoT can protect revealing healthy and stable development in practical applications. A challenge in the near future will be the integration of IoT with security protocols to the hospital environment. Developing a security protocol in u-healthcare environment is major concern in future.

**Acknowledgments.** 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. Young-Jae Park, et al, “On the Accuracy of RFID Tag Estimation Functions”, Journal of Information and Communication Convergence Engineering, March, pp.33-39 (2012)
2. Yang Xiao, et al, “Security and Privacy in RFID and Applications in Telemedicine”, IEEE Communications Magazine, April, pp.64-72 (2006)
3. Shinyoung Lim,et al, “Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring”, 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing”, pp.327-332 (2010)
4. Wen Yao, Chao-Hsien Chu and Zang Li, “The Use of RFID in Healthcare: Benefits and Barriers”, IEEE International Conference on RFID Technology and Applications, pp.128-134, June (2010)
5. Jeonggil Ko, et al, “Wireless Sensor Networks for Healthcare”, Proceedings of the IEEE, v.98, n.11, pp. 1947-1960 (2010)
6. Lenka Lhotska, et al, “Security Recommendations for Implementation in Distributed Healthcare Systems”, ICCST2008, pp.76-83 (2008)
7. Kai Zhao and Lina Ge, "A Survey on the Internet of Things Security", 2013 Ninth International Conference on Computational Intelligence and Security, pp.663-667, (2013)
8. Xin Bai, Zhengzhou 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)
9. Biplob R. Ray, Jemal Abawajy and Morshed Chowdhury, "Scalable RFID security framework and protocol supporting Internet of Things", Computer Networks 67, pp.89–103, (2014)
10. Azzedine Boukerche and Yonglin Ren, “A Secure Mobile Healthcare System Using Trust-based Multicast Scheme”, IEEE Journal on Selected Areas in Communications, v.27, n.4, pp.387-397, May (2009)
11. Wiem Tounsi, et al, “Securing the Communications of Home Health Care System based on RFID Sensor Networks”, 8th Annual Communication Network and Services Research Conference, pp.284-291 (2010)
12. Yanjun Zuo, Survivable RFID Systems: Issues, Challenges, and Techniques”, IEEE Transactions on Systems, Man, and Cybernetics- part C: Applications and Reviews, v.40, n.4, pp.406-418. July (2010)

 