International Journal of Smart Home
Vol. 8, No. 6 (2014), pp. 131-142
http://dx.doi.org/10.14257/ijsh.2014.8.6.13

Analysis of RFID Application for U-healthcare System in Internet of Things

Jung Tae Kim

Mokwon University, Dept. of Electronic Engineering
Doanbuk-ro 88, Seo-gu, Daejeon, 302-729, Korea
E-mail: jtkim3050@mokwon.ac.kr

Abstract

In the past years, Internet of Things (IoT) has been focused and fused with wireless sensor node such as RFID, NFC tag and small sensor nodes, especially for hospital environment with mobile device. Due to the weakness characteristics of wireless signals, unauthorized person can access easier to hospital networks in wireless part than wired network systems. This may induced in several security problems. Therefore, a lot of threats, attacks and vulnerability are occurred in wireless surroundings because of their limited resources such as small memory and low computation capability in wireless sensor network. RFID is often utilized as a prerequisite for the IoT in healthcare system. We surveyed and analyzed the technologies and characteristics of RFID and its application based on IoT.

Keywords: *Mobile agent, RFID, privacy and healthcare system, security issues*

1. Introduction

As IT (Information Technologies) are rapidly developed and fused with a variety of technology such as nano-technology, sensor, and bio-technology. These technologies give a great breakthrough in many industries. E-healthcare system has been realized in hospitals before. Especially, existing e-healthcare system has been realized in wired communication with specialized area such as database and network protocol in hospital environment. E-healthcare system is moving into U-healthcare system by fusing a variety of sensors and mixed networks. The rapid changes of modern technologies usually provide new requirement, request and give a new opportunity to generate new market and industry. Ubiquitous technologies based on mobile devices and sensor nodes can be applied and managed in healthcare information. Recently the trend of healthcare system has moved to U-healthcare system with wireless and mobility characteristics, many new technologies can be utilized to wireless sensor nodes with smart equipment and devices with low computing power. These kinds of mechanism and devices can be fused with different compact devices module [1]. HIPAA (Health Insurance Portability and Accountability Act) enacted by the United States Congress in 1996, is the Federal Law that applies to the U.S. healthcare industry. To improve healthcare quality, the HIPAA provides a conceptual guideline that must be strictly observed by all dependent organizations. Privacy regulations address the patients' rights to understand and control the use and disclosure of their protected health information (PHI). This part of the health information reveals an individual's identification, such as name, address, telephone number, medical record number, and so on. Advanced technology in wireless communications and computing technologies have great effect on the shift of healthcare systems from paper-based to electronic health record (EHR)-based. It gives rise to increased efficiency in human operations, reduced storage costs and medical errors, improved data

ISSN: 1975-4094 IJSH

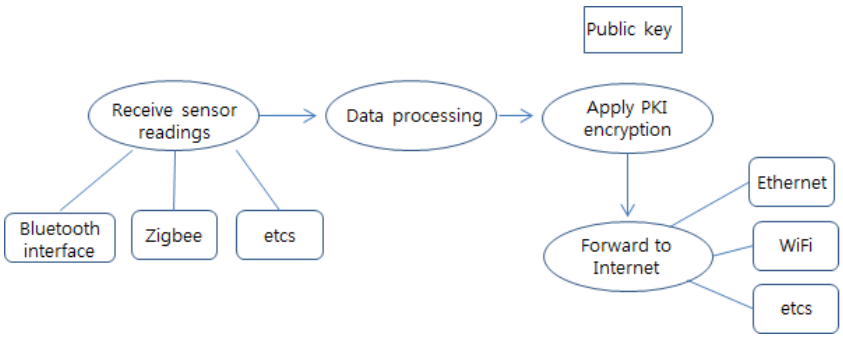
availability and sharing, and so on. Electronic healthcare (e-healthcare) offers a great convenience to patients and healthcare providers, and improves the quality of life. Electronic healthcare is becoming a vital part of our living environment and exhibits many advantages over paper-based legacy systems. Privacy is the essential concern of patients and the biggest obstacle to e-healthcare deployment [2]. The major benefit of RFID technology includes the increasing patient's management and managing documents with its mobility and usability. RFID systems should be considered to resist all kinds of attacks and threats. Until now, many works have done about security issues how they can implement the standard cryptographic. But, a lot of security threats and attacking attempts exist in RFID system. It is not solved yet properly. The application system is moving and converging on IoT (Internet of Things). Hailong Feng, et al, surveyed a recent development about privacy and security of Internet of things [3]. Security and privacy issues of RFID tags can effect both organization and individuals. Unprotected tags may be vulnerable to eavesdropping, traffic analysis, spoofing or denial of service and many unknown problems. Unauthorized readers can affect and infringe the privacy by accessing tags without illegal access control. Even if the content of tag is secure, it also can be tracked by the predictable tag responses: "location privacy" can be affected by a traffic analysis attack. Attackers can also threaten the security of systems. It depends on the original characteristics of RFID. The representative attack is the denial of service attack. Many researcher works to implement security system with low cost and privacy protocol to increase the applicability. A lot of lightweight solutions have been proposed for RFID, but they are still expensive and vulnerable to the security and do not fully resolve the security issues. Therefore, there is a good research scope in the field of designing an efficient ultra-lightweight cryptographic protocol for low-cost RFID system [4]. IoT is considered as one of the advanced major communication in recent years, since it offers the basis for the development of independent cooperative services and applications in wireless communication and network. A variety of research is under study using this concept in different areas, such as building automation, intelligent transport systems, and so on, in particular, healthcare application. For example, IoT's potential application for mobile health applications has been reported in [5]. A ubiquitous and mobile integrated clinical environment platform based on the IoT offers equipment or node for large scale connectivity with different sensors, as well as integration with information systems. This improves accessibility to clinical services, compatibility and ubiquity, enhancing mobility, and guarantees access to medical information, anywhere and anytime. Specifically, the capabilities of technologies for the identification of objects, such as Radio Frequency Identification (RFID), and for communication and ubiquitous access to information, such as wireless personal devices, embedded systems and smart objects should be evaluated further study. The architecture of IoT system is generally divided into three layers: the perception layer, the network layer, and the service layer (or application layer). 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 with extremely private information including personal health/medical information, so it is exposed to various weakness and threat in the part of security and privacy. Particularly we consider U-hospital healthcare network environment in here. The U-hospital network allows the medical step to use mobile medical devices, to measure and record user's medical data, and to have information related to their patient or treatment from health information system. In U-hospital service network environment, we can define four parts: medical sensor and device part, middleware part, communication part, and back-end information service Tier. The

medical sensor and sensor device part represents various physical measurement data which measure biological signals from patients and get information related to treatment or prescription. It consist of not only wired devices, but also wireless devices which communicate through wireless channel such as WLAN, CDMA, Bluetooth, RF channel. Especially, we provide detailed description on the privacy and security issues in U-healthcare systems and IoT application [6]. The term of Internet of Things was first introduced at MIT auto-ID labs in1999. The main concept of IoT is that it investigates to realize object localization and state recognition using wireless sensor networks and radio frequency identification technologies [7]. Internet is referred as the world-wide network of interconnected computer networks based on a standard communication protocol (TCP/IP). Generally, Thing means an object not precisely identifiable. Internet of Things merges internet and things. It is widely used as a meaning of world-wide network of interconnected objects uniquely addressable, based on standard communication protocol. While current Internet is a collection of a variety of devices, namely, a network connecting to physical world objects same as Internet to computers now, for example, everything is addressable with an IPv6 and a pervasive and ubiquitous computing platform. IoT can be expected to contain huge numbers of sensors collecting and passing on data about environmental conditions, physiological measurements, and machine operational data. In addition to the computing devices that consumers use today such as laptops, games consoles and smart phones there will be many devices and appliances with embedded processors running applications (smart things) that people make use of. Many smart things will also be capable of actuation to take physical actions as a result of application control. One of the major problems for the IoT is the new degree of security required to keep all these devices secured. Security concerns expanded to cover personal privacy, financial transaction, and threat of cyber-attacks. It is getting more important security and privacy in IoT. Rapid advancement of ICTs has led to an increasing number of portable devices and sensors, referred as Internet of Things (IoT) that enable various e-Healthcare scenarios such as remote patient monitoring. It is expected that the IoT will induce significant impact on delivery of information in healthcare system. However, high dependability on the IoT technologies in U-Health makes a problem in security and privacy risks. In particular, there are risks with respect to patient identification and reliability from collected information. These days, the modern U-healthcare solutions based on IoT are heading towards open issues.

2. Related Works

As an initial model of U-healthcare system, m-health system is designed as an enhancement of e-health system supported by wireless EMR (Electronic Medical Record) access. The rapid developments in technology and semiconductor process made their cost to reduce sharply and new technologies to emerge. As a result of reduced cost of RFID component, hardware became cheaper with more storage capacity and enhanced processing power. It gives a standard algorithm to be implemented in real world. These developments made it possible for technology to be more adopted among different industries. Advanced technologies and techniques in wireless communications and computing technologies have great effect on the migration of healthcare systems from paper-based to electronic health record (EHR)-based, giving rise to increased efficiency in human operations, reduced storage costs and medical errors, improved data availability and sharing, and so on. Electronic healthcare (e-healthcare) offers great convenience to patients and healthcare providers. Electronic healthcare is becoming a

vital part of our living environment and exhibits advantages over paper-based legacy systems. Privacy is the foremost concern of patients and the biggest impediment to e-healthcare deployment. Although RFID can provide trustworthy benefits in the healthcare industry, it is not widely used due to the lack of security on the RFID tags and limited space for data storage. To solve this kind of concerns, Li-Shiang Tsay, *et al.*, proposed an integrated framework to build a RFID card system by embedding smart tags in insurance cards, medical charts, and medical bracelets to store medical information. Their scheme gives and simplifies the maintenance and transfer of patient data in a secure, feasible and cost effective way [8]. In recent years, hospitals are introduced by wireless communication systems. However, not many hospitals are aware of the security issues because their working process is mainly focused on emergency than security. This may result in a security problem such as information leakage. Therefore, we analyzed a suitable wireless security mechanism for the hospital. The characteristics of the hospital organization should be analyzed before selecting the wireless mechanism. To overcome the additional vulnerabilities and security problem, wireless security architecture should be designed with essential requirement for wireless EMR access. Especially patient' privacy and security issues should be considered more important in hospital information system environment. Biplob R Ray, et al, proposed a novel identification technique based on a hybrid approach with group-based approach and collaborative approach and security check handoff for RFID system 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]. Juhee Kwon, et al, analyzed healthcare security strategies for regulatory compliance and data security and provides policy insight on effective security problems that hardness IT resources, functional capabilities, and managerial capabilities. Their conceptual framework includes two models. The first model examines the effects of security resources, functional capabilities, and managerial capabilities on compliance with a multinomial logic model. The other model identifies the role of compliance as a mediator as well as examines the effects of resources and capabilities on actual data security using a binomial logic model [10]. Hui Suo, et al, analyzed security in Internet of Things and reviewed the research status of key technologies including encryption mechanism, communication security, protecting sensor data and cryptographic algorithms, and briefly outlined the challenges [11]. Generally, to implement conventional cryptographic algorithms with available resources are necessary such as processor speed and memory. So how to apply these cryptographic techniques to the IoT is not clear, many researchers have to make more effort to further research to ensure that algorithms can be successfully implemented using constrained memory and low-speed processor in the IoTs. Antonio F, *et al.*, demonstrated a decentralized approach for security and privacy challenges in the Internet of Things [12]. They provided a concise description of some of the major challenges related to these areas that still need to be overcome in the coming years for a full acceptance of all IoT involved. Also, they proposed a distribution capabilities-based access control mechanism which is built on public key cryptography to meet up with some of these challenges. Architecture of IoT based on security mechanism is shown in Figure 1.



Figue 1. Architecture of IoT based on Security Mechanism

Charalampos Doukas, *et al.*, presented a system based on gateway that aggregate health sensor data and resolve security issues through digital certificates and PKI data encryption [13]. They illustrated the basic functionality of an IoT gateway. An additional feature is the ability to perform some initial data preprocessing before data is encrypted using PKI and forwarded to the Internet using a WiFi or Ethernet network interface. Xin Bai and Hongyan Yan analyzed design of the safe HIS (Hospital Information System) on the Internet of Things. They also studied the public security technologies of the Internet of Things, including IoT-MW (Internet of Things-Middleware), encryption, decryption, secret key management, privacy homomorphism, access control and cryptograph query [14]. Figure 2 depicts a concept of the network topology for the u-health system. It represents a brief network topology for a virtual hospital. This network will be modified and extended based on the requirement of the security issues and protocol requirements. Further network should be designed and take into account in terms of several aspects such as customer friendly, efficiency of working process, cost effective and high performance and enhanced security. This protocol should be identified security vulnerabilities and threats which could occur during the implementation of U-healthcare system. Security solutions and optimized protocol design should be required to mitigate all kinds of risks such as establishment of security policy, analysis of various security technologies applied to hospital, implementation of security primitives in the network, and implementation of security features in the application.

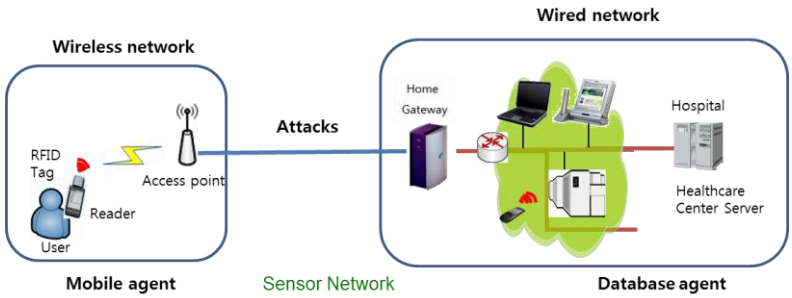


Figure 2. Model of Ubiquitous Healthcare System

IoT includes a set of technologies that enable a wide range of appliances, devices, and objects to interact and communicate among others using networking technologies. Healthcare systems use a set of interconnected devices to create an IoT basis network which dependent to healthcare assessment, including monitoring patients and automatically detecting situation which medical interventions are required. The implementation of protocols in constrained

networks has to deal with some problems related to the particular nature of the physical devices such as the limited computational capacity, the low amount of memory, and the constraints on the energy consumption, make the design of these protocols particularly hard and complicated [15]. Mouza Bana Shemaili, *et al.*, proposed a new lightweight stream cipher for low computational devices such as RFID and wireless sensor network. RFID and wireless sensor network are combined core technologies that can be used for the IoT. Their proposed solution combines both of the LFSR (Linear Feedback Shift Register) and FCSR (Feedback with Carry Shift Register). This has the advantage of having the simplicity of the LFSR and the non-linearity of the FCSR. There is a need to consider common attacks on the available stream cipher design because of weakness of strength in cryptography level [16].

3. Model of Attacks and Threats for RFID Protocol

There are a variety of vulnerable attacks in RFID system and its application due to its limited resources. Security threats to RFID protocols can be classified into weak and strong attacks. Weak attacks are feasible threats just by observing and manipulating communications between a server and tags. Replay attacks and interleaving attacks are examples of weak attacks. Strong attacks are possible threats for an attacker which has compromised a target tag. An RFID tag's memory is vulnerable to compromise by side channel attacks, because the memory of a low cost tag is unlikely to be tamper-proof. Hence, strong as well as weak attacks should be considered in RFID protocol design. Backward traceability, forward traceability and server impersonation attacks are all examples of strong attacks [17]. In this chapter, we introduced 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 easily, and to get information related to their patient or treatment from HIS(Hospital Information System). Under U-hospital service network environment, we can define four layers: medical sensor and device layer, middleware layer, communication layer, and back-end information Service layer. The medical sensor and device layer represents various physical measurement layers which measure biological signals from patients and get information related to treatment or prescription. It could be not only wired devices, but also wireless devices which communicate through wireless channel such as WLAN, CDMA, Bluetooth, RF channel [18]. Kai Zhao and Lina Ge analyzed a survey on security in the Internet of Things. The major issues are key management, algorithm, security routing protocol, data fusion technology, authentications and access control. 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 as the processing layer. The architecture of IoT security is shown in figure 4 [19, 20]. The basic architecture of IoT system is divided into three layers: the application, network and perception layers. Perception layer means that all kinds of information of the physical world used in IoT are perceived and collected in this layer by using sensor, tag and data interface. Network layer take a play role in providing transparent data transmission capability and is also called transport layer. Service layer is called application layer. Its main function includes data management and application service in sub-layer.

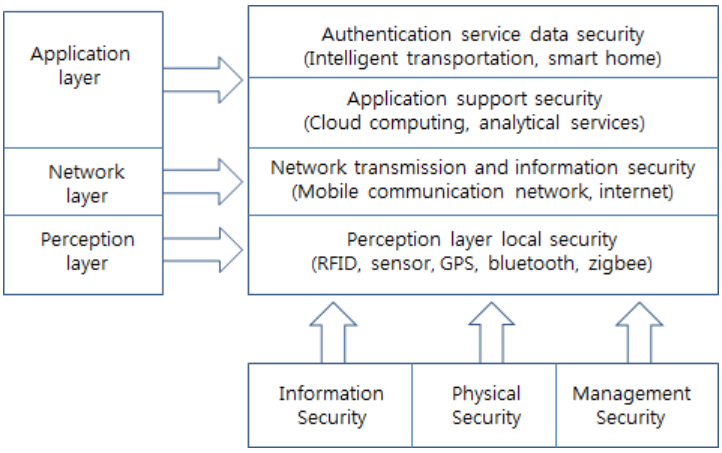


Figure 3. Architecture of IoT based on Security Mechanism

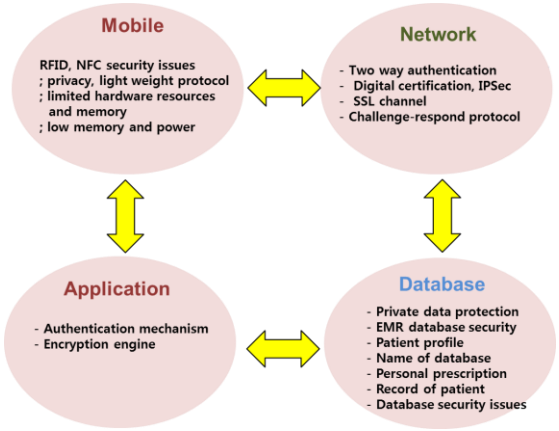


Figure 4. Security Issues in Each Layer

Figure 4 depicts security problem in each layer. The architecture is divided into four layers: user layer, network layer, application layer and database layer. Each layer contains several elements to support their function. To realize U-healthcare system, we should take into consideration factors such as confidentiality by authentication and encryption, data privacy, confidentiality, and availability by authorization, encrypted database and backup of database. The measures can be categorized into four security layers: Authentication based on network, authentication based on application, database protection and user's privacy. To exchange secret information over the Internet, it is necessary to secure the channel. The security may be into the different layers of the TCP/IP model. The usual methods to provide security at the network level are datagram encapsulation. One of the most common technologies used to ensure secure communications in the Internet is the IPsec (Internet Protocol Security). IPsec is an end-to-end security scheme operating in the IP stack, enabling both authentication and confidentiality. Although IPsec ensures these security services to any protocol in the upper layers, it introduces some overhead that will reduce throughput. At the transport layer, the SSL (Secure Socket Layer) protocol is the standard used all over the Internet. The SSL (Secure socket layer) protocol replaces the TCP/IP sockets with SSL sockets, simplifying the implementation of a secure end-to-end secure channel. This approach reduces the implementation time comparing with the time spent designing another

cryptographic system with the same security level. New security protocol for each layer should be developed in mobile healthcare system. To evaluate key exchange protocols for resource-constrained devices, we should consider evaluation criteria such as computation costs and communication costs. To protect users from tracing attack, Kavitha S. M *et al.*, proposed a hardware implementation of RFID with secure mutual authentication protocol [21].

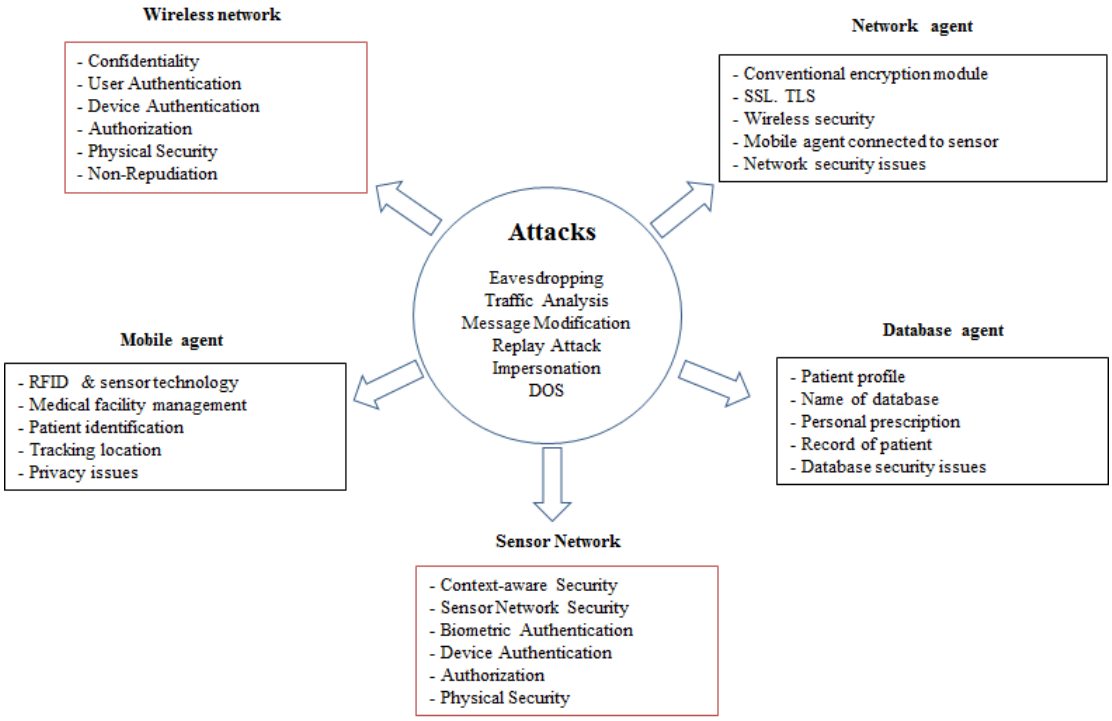


Figure 5. Example of Attacks Model of Ubiquitous Healthcare System [22]

Comparison of benefits, barriers and attacks of RFID applications in healthcare system is shown in table 1 [23]. Table 2 shows structure of secure layer and its characteristics. Wen Yao, *et al.*, surveyed the use of RFID in healthcare system about benefits and barriers by analyzing distributed of literatures, benefits of RFID applications in healthcare and barriers to RFID adoption in healthcare system [24].

Table 1. Benefits, Barriers and Attacks of RFID Applications in Healthcare System [25]

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

Table 2. Structure of Secure Layer and its Characteristics

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

Although the user establishes connection to the network through network authentication, users should be authenticated by web-based authentication system for accessing to EMR. The security guidance republished by HIPAA in USA, report advises two-factor authentication. They consist of the usual authentications based on challenge-response handshake and session key agreement during the authentication process and secure communication with a session key enable confidential communication [25]. Nowadays, RFID application can be applied in many fields for a variety of applications. Although having a great productivity benefits, RFID systems may cause new security and privacy threats to individuals or organizations. Therefore, it is important to protect the security of RFID systems and the privacy of RFID tag owners. Unfortunately, none of the existing solutions provide the contents of tags. Kazuya Sakai, et al., proposed two RFID backward channel protection protocols, namely dynamic bit encoding and optimized dynamic bit encoding and analytical models to estimate simulation results [26]. Security and privacy security should be considered communication security (end-to-end), resilience to attack, data authentication and access control. A number of technologies have been developed to achieve information privacy purposes. Some privacy mechanisms for enhancing technologies are integrating policy-based release of data, virtual private networks, and transport layer security [27, 28]. The security design should fit into these kinds of requirements to solve security problem. The representative policy are concise set of cryptographic and security mechanisms, single security policy framework and configuration parameters policy-dependent. This may require consideration of system perspectives, taking into account the entire system and device lifecycle, ease-of-use and ease-of-deployment. The core challenges of IoTs are universal identity, data and middleware API standards and new business model. IoT will inherit the drawbacks of the current internet, but more invisible scale. To overcome vulnerability of RFID protocol, security design of the protocol should not impede normal operations, and should prevent a malicious adversary from getting any information. We consider the following measures:

A. Secrecy/Authentication

The cryptographic methods used (for example the keyed Hash function H) correspond to the state of the art in industry today, and reasonably guarantee the secrecy of the message. Thus, we assure the recipient that the messages originate from valid sources.

B. Indistinguishableness/Tracking/Passive Replay

Using a freshly generated random nonce with every message in the protocol, it is impossible to track the tag. Assume that an adversary pretends to be a genuine reader. He sends out a query, and receives a message back. Next time he sends a query, along with a fresh nonce, he receives a different message, so he cannot track the tag. Of course, with multiple tags in an area, tracking a specific tag without keys is extremely difficult if not impossible.

C. Forward Security

This means that the current key of a tag has been found, and can be used to extract previous messages (assuming that all its past conversations are recorded). Let's say the adversary somehow finds keys. The tag always communicates using a hash function. The

adversary cannot use the key to decode any of the tag's messages because the one-way hash function H is considered computationally unsolvable. In other words, the adversary needs to have access to the hash digest table for lookups. So, he cannot decipher/recreate any past messages sent with previously used keys.

4. Conclusion

The IoT uses a variety of information sensing identification device and information processing equipment such as RFID, WSN, etc. The health information system based on the wireless network infrastructure is generally adapted nowadays. As a part of the wireless network, a mobile device and agent has been employed in hospitals environmental. Especially, RFID system is widely used to identify objects, sensor module and IoT (Internet on Things) services. Many researcher and scientist try to work to implement low cost security and privacy protocol to increase the applicability in IoT application. A lot of lightweight solutions have been proposed for RFID and IoT Application, but they are still expensive and vulnerable to the security and do not fully resolve the security issues until now because of its limited resources and crypto primitive problem. Until now, open issues are not solved with simple solution with conventional techniques because of wireless characteristics. Several attacks and characteristics of RFID to solve open security issues are analyzed in this paper.

Acknowledgements

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: 2013-052980)

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, **(2012),** pp. 33-39.
[2] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks", IEEE Computer, vol. 36, no. 10, **(2003),** pp.103-105.
[3] H. Feng and W. Fu, "Study of Recent Development about Privacy and Security of the Internets of Things, 2010 International Conference on Web Information Systems and Mining", **(2010),** pp. 91-95.
[4] R. K. Pateriya and S. Sharma, "The Evolution of RFID Security and Privacy: A Review Survey", 2011 International Conference on Communication Systems and Network Technologies, **(2011),** pp. 115-119.
[5] L. Li, "Study on Security Architecture in the Internet of Things, 2012 International Conference on Measurement, Information and Control, **(2012),** pp. 374-377.
[6] J. T. Kim, "Security Issues in RFID Technology and Its Application in IoT, 2014 International Conference on Future Information & Communication Engineering, **(2014),** pp. 419-420.
[7] Q. Zhu, R. Wang, Q. Chen, Y. Liu and W. Qin, "IoT gateway: Bridging Wireless Sensor Networks into Internet of Things", 2010 IEEE International Conference on Embedded and Ubiquitous Computing, **(2010),** pp. 347-352.
[8] L.-S. Tsay, A. Williamson and S. Im, "Framework to Build and Intelligent RFID System for Use in the Healthcare Industry", 2012 Conference on Technologies and Applications of Artificial Intelligence, **(2012),** pp. 109-112.
[9] B. R. Ray, J. Abawajy and M. Chowdhury, "Scalable RFID Security Framework and Protocol Supporting Internet of Things", Computer Networks, vol. 67, **(2014),** pp. 89-103.
[10] J. Kwon and M. E. Johson, "Healthcare Security Strategies for Regulatory Compliance and Data Security", 46th Hawaii International Conference on System Sciences, **(2013),** pp. 3972-3981.
[11] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the Internet of Things: A Review", 2012 International Conference on Computer Science and Electrics Engineering, **(2012),** pp. 648-651.
[12] A. F. Skarmeta, J. L. Hernandez-Ramos and M. V. Moreno, "A Decentralized Approach for Security and Privacy Challenges in the Internet of Things", 2014 IEEE World Forum on Internet of Thins, **(2014),** pp. 67-72.

[13] A. C. Doukas, I. Maglogiannis and V. Koufi, "Enabling Data Protection through PKI Encryption in IoT m-health Devices", Proceedings of the 2012 IEEE 12th International Conference on Bioinformatics and Bioengineering, **(2012),** pp. 25-29.
[14] Xin Bai and H. Yan, "Study and Design of the Safe HIS on the Internet of Things", 2011 Fourth International Symposium on Computational Intelligence and Design, **(2011),** pp. 174-176.
[15] L. Catarinucci, S. Guglielm, L. Mainetti, V. Mighali, L. Patrono, M.L Stefanizzi and L. Tarricone, "An Energy-efficient MAC Scheduler Based on a Switched-beam Antenna for Wireless Sensor Networks", Journal of Communication Software and System, vol. 9, no. 2, **(2013),** pp. 117-127.
[16] M. B. Shemaili, C. Y. Yeun, K. Mubarak and M. J. Zemerly, "A New Lightweight Hybrid Cryptographic Algorithm for the Internet of Things", The 7th International Conference for Internet Technology and Secured Transactions, **(2012),** pp. 87-91.
[17] B. Song, "Server Impersonation Attacks on RFID Protocols, The Second International Conference on Mobile Ubiquitous Computing", Systems, Services and Technologies, **(2009),** pp. 50-55.
[18] 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, **(2009),** pp. 387-397.
[19] K. Zhao and L. Ge, "A Survey on the Internet of Things Security", 2013 9th International Conference on Computational Intelligence and Security, **(2013),** pp. 663-667.
[20] H. Suo, J. Wna, C. Zou and J. Liu, "Security in the Internet of Things: A review", 2012 International Conference on Computer Science and Electronics Engineering, **(2012),** pp. 648-651.
[21] S. M. Kavitha, T. Suresh, and J. M. Rani, "RFID Implementation with Secure Mutual Authentication Protocol", 2012 International Conference on Computing, Electronics and Electrical Technologies, **(2012),** pp. 746-751.
[22] J. T. Kim, "Analyses of Attacks and Vulnerability on the U-healthcare System", 2014 International Conference on Green and Human Information Technology, **(2014),** pp. 110-114.
[23] H.-Y. Chien, "Varying Pseudonyms-based RFID Authentication Protocols with DOS Attacks Resistance", In 2008 IEEE Asia-Pacific Services Computing Conference, **(2008),** pp. 507-615.
[24] W.-B. Lee and C.-D. Lee, "A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations", IEEE Transactions on Information Technology in Biomedicine, vol. 12, no. 1, **(2008),** pp. 34-41.
[25] J. T. Kim, "Enhanced Secure Authentication for Mobile RFID Healthcare System in Wireless Sensor Networks", Future Generation Information Technology (FGIT2012), Springer Communication in Computer and Information Science, 2012, **(2012),** pp. 190-197.
[26] K. Sakai, W.-S. Ku, R. Zimmermann, and M.-T. Sun, "Dynamic Bit Encoding for Privacy Protection against Correlation Attacks in RFID Backward Channel", IEEE Transaction on Computers, vol. 62, no. 1, **(2013),** pp. 112-123.
[27] J. T. Kim, "Attacks and Threats on the U-healthcare Application with Mobile Agent", International Journal of Hybrid Information Technology, vol. 8, no. 4, to be published on July **(2014).**
[28] S.-H. Kwon and D.-W. Park, "Hacking and Security of Encrypted Access Points in Wireless Network", Journal of Information and Communication Convergence Engineering, vol.10, no. 2, **(2012),** pp. 156-161.

Author

Jung Tae Kim, he received his Ph.D. degrees in Electronic Engineering from the Yonsei University in 2001. From 1991 to 1996, he joined at ETRI (Electronic Telecommunication Research Institute), 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 optical security technology that includes network security system design, RFID&USN and wireless security protocol.